RCCE CYBERSECURITY FRAMEWORK

NETWORK SECURITY

- Network Access Control (NAC)
- Authentication, Authorization, and Accounting (AAA) Frameworks
- Pre-Connection Authentication
- Post-Connection Controls
- Role-Based Access Control (RBAC)
- Firewalls
- Packet-Filtering Firewalls
- Stateful Inspection Firewalls
- Next-Generation Firewalls (NGFWs)
- Web Application Firewalls (WAFs)
- Proxy Firewalls
- Intrusion Detection and Prevention Systems (IDPS)
- Network-Based Intrusion Detection Systems (NIDS)
- Host-Based Intrusion Detection Systems (HIDS)
- Intrusion Prevention Systems (IPS)
- Signature-Based, Anomaly-Based, and Behavior-Based Detection
- Virtual Private Network (VPN)
- Site-to-Site VPNs
- Remote Access VPNs
- SSL/TLS VPNs
- Secure Wireless Networks
- WPA2/WPA3 Security Protocols
- Hidden SSIDs and MAC Address Filtering
- Network Segmentation for Wireless Access Points
- Data Loss Prevention (DLP)
- Network DLP
- Endpoint DLP
- Cloud DLP
- Network Segmentation
- Virtual Local Area Networks (VLANs)
- Software-Defined Networking (SDN) for Dynamic Segmentation
- Secure Network Architecture
- Demilitarized Zones (DMZ)
- Zero Trust Network Architecture
- Secure Cloud Networking
- Encryption
- Transport Layer Security (TLS) and Secure Sockets Layer (SSL) for Data in Transit
- IPsec for Protecting Internet Protocol Communications
- End-to-End Encryption Techniques
- Endpoint Security
- Antivirus and Antimalware Software
- Endpoint Detection and Response (EDR) Systems
- Sandboxing
- Detonating Suspicious Files/URLs in a Safe Environment
- Threat Intelligence and Information Sharing
- Cyber Threat Intelligence (CTI) Feeds
- Information Sharing and Analysis Centers (ISACs)
- Network Monitoring and Management
- Security Information and Event Management (SIEM) Systems
- Network Traffic Analysis (NTA)
- Configuration and Patch Management
- Penetration Testing and Vulnerability Assessment
- Network Vulnerability Scanning
- Ethical Hacking to Identify Weaknesses
- Red Team, Blue Team, and Purple Team Exercises
- DNS Security
- DNS Filtering
- DNS Security Extensions (DNSSEC)
- Email Security
- Spam Filters
- Email Encryption
- Phishing Detection and Response
- Secure Protocols

APPLICATION SECURITY

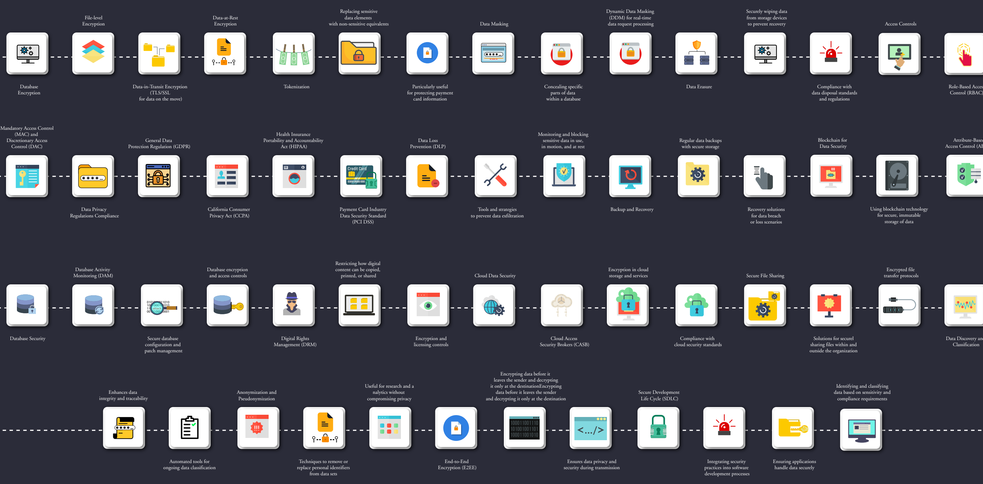
- Secure Coding Practices
- Input Validation to prevent injection attacks
- Output Encoding to prevent data from being executable as executable code
- Authentication and Authorization mechanisms
- Secure Session Management
- Error Handling and Logging without exposing sensitive information
- Application Security Testing
- Static Application Security Testing (SAST) to analyze source code
- Dynamic Application Security Testing (DAST) or runtime testing
- Interactive Application Security Testing (IAST) that combines SAST and DAST
- Software Composition Analysis (SCA) for detecting vulnerable components
- Penetration Testing to simulate real-world attacks
- Threat Modeling
- Identifying security threats and vulnerabilities in application design
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) methodology
- Attack Tree Analysis
- Application Security Frameworks and Standards
- Open Web Application Security Project (OWASP) Top 10 vulnerabilities
- Secure Software Development Lifecycle (SSDLC) guidelines
- NIST Application Security Guidelines
- Encryption and Data Protection
- Implementing SSL/TLS for data in transit
- Data encryption for data at rest
- Proper management of encryption keys
- Identity and Access Management (IAM)
- Implementing Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- OAuth, OpenID Connect, and SAML for secure single sign-on (SSO)
- Application Layer Firewalls and Web Application Firewalls (WAF)
- Filtering, monitoring, and blocking HTTP/HTTPS traffic
- Custom rule sets based on applications' unique requirements
- API Security
- Securing RESTful APIs against common threats
- Rate limiting to prevent abuse
- OAuth for securing APIs with tokens
- Patch Management
- Regularly updating applications and dependencies
- Static Application Security Testing (SAST) to analyze source code
- Automated tools for vulnerability tracking and patching
- Secure Deployment Practices
- Environment hardening
- Using containers for consistent deployment environments
- Automated deployment pipelines that incorporate security checks
- DevSecOps Integration
- Integrating security practices within the CI/CD pipeline
- Automated security scanning and testing in development and deployment processes
- Collaboration between development, security, and operations teams
- Container and Orchestration Security
- Securing Docker and Kubernetes environments
- Managing container vulnerabilities
- Encryption and Data Protection
- Network segmentation and access controls for containerized applications.
- Cloud Security Posture Management (CSPM)
- Securing applications deployed in cloud environments
- Compliance checks against cloud security frameworks
- Automated threat detection and remediation in cloud settings
- Mobile Application Security
- Securing mobile apps against common vulnerabilities
- Implementing secure communication for mobile applications
- Protection against reverse engineering and tampering

ENDPOINT SECURITY

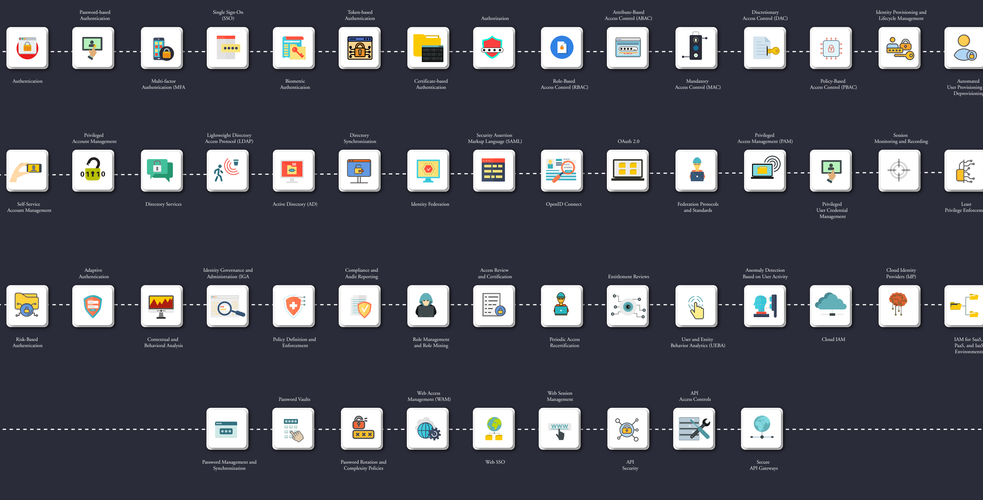
- Antivirus and Antimalware Software
- Real-time malware detection and removal
- Scheduled scans and automatic updates
- Endpoint Detection and Response (EDR)
- Continuous monitoring and response to advanced threats
- Behavioral analysis to detect malicious patterns
- Firewall Protection
- Ingress and egress filtering to control network traffic
- Application-level and packet-filtering firewalls
- Patch Management
- Timely updates of operating systems and applications
- Automated patching tools to ensure up-to-date security
- Encryption
- Full disk encryption (FDE) for data at rest
- File-level encryption for specific sensitive documents
- Mobile Device Management (MDM)
- Remote management of mobile devices
- Device configuration, password enforcement, and wiping capabilities
- Data Loss Prevention (DLP)
- Monitoring, detecting, and blocking sensitive data exfiltration
- Control over transfer and storage of critical data
- Virtual Private Network (VPN)
- Secure remote access via encrypted connections
- Split tunneling and full tunneling options
- Multi-Factor Authentication (MFA)
- Additional authentication layers beyond passwords
- Biometrics, security tokens, and SMS codes
- Security Configuration Management
- Hardens device security settings based on best practices
- Regular audits and adjustments to security configurations
- Email Security
- Filtering spam, phishing, and malicious email contents
- Email encryption for sensitive information
- Zero Trust Security
- Least privilege access controls
- Continuous authentication and verification
- Secure Web Gateways (SWG)
- Filtering unwanted software/malware from web traffic
- Policy enforcement for internet usage
- USB Device Control
- Blocking or restricting the use of unauthorized USB devices
- Monitoring file transfers to and from external devices
- Application Control
- Whitelisting allowed apps
- Blacklisting prohibited applications
- Endpoint Privilege Management
- Limiting administrative privileges on endpoints
- Controlling application execution with elevated rights
- Network Access Control (NAC)
- Enforcing security policies based on device compliance
- Quarantining or restricting access of non-compliant devices
- Threat Intelligence Integration
- Utilizing up-to-date threat information for better protection
- Sharing threat data with security solutions for enhanced detection
- IoT Device Security
- Securing Internet of Things devices integrated into the network
- Managing updates and monitoring for unusual activities

RCCE CYBERSECURITY FRAMEWORK

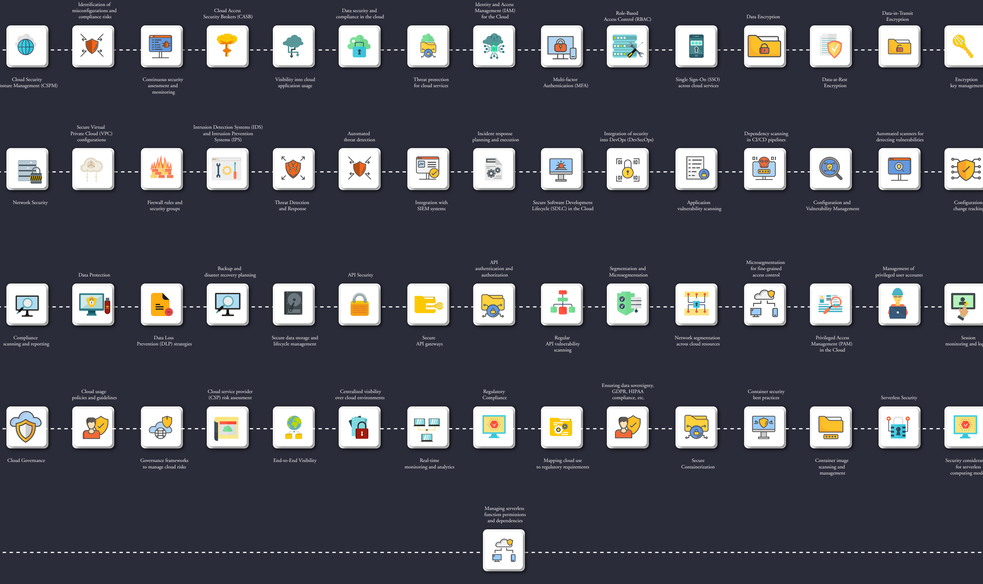
DATA SECURITY



IDENTITY AND ACCESS MANAGEMENT (IAM)



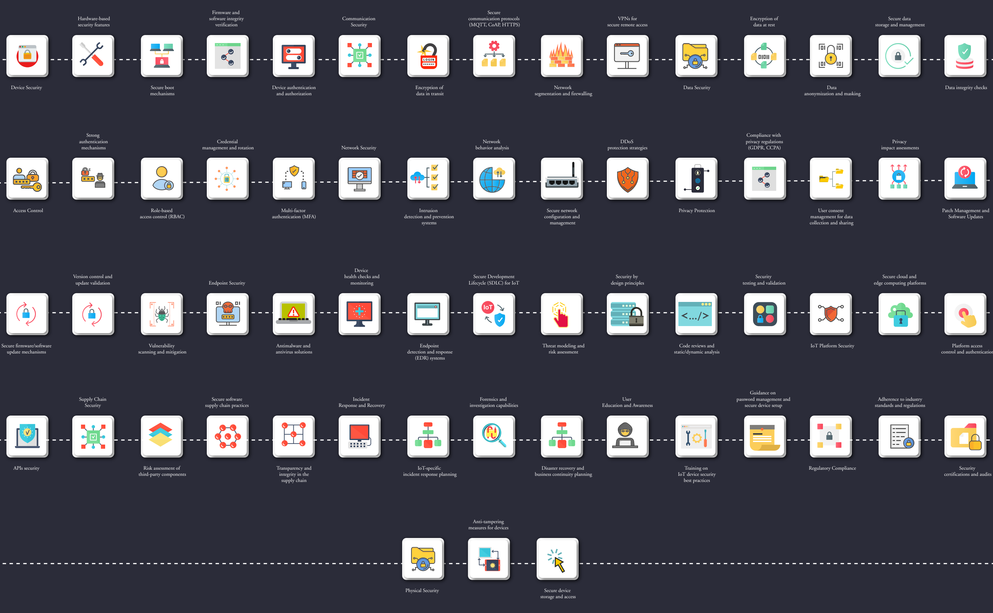
CLOUD SECURITY



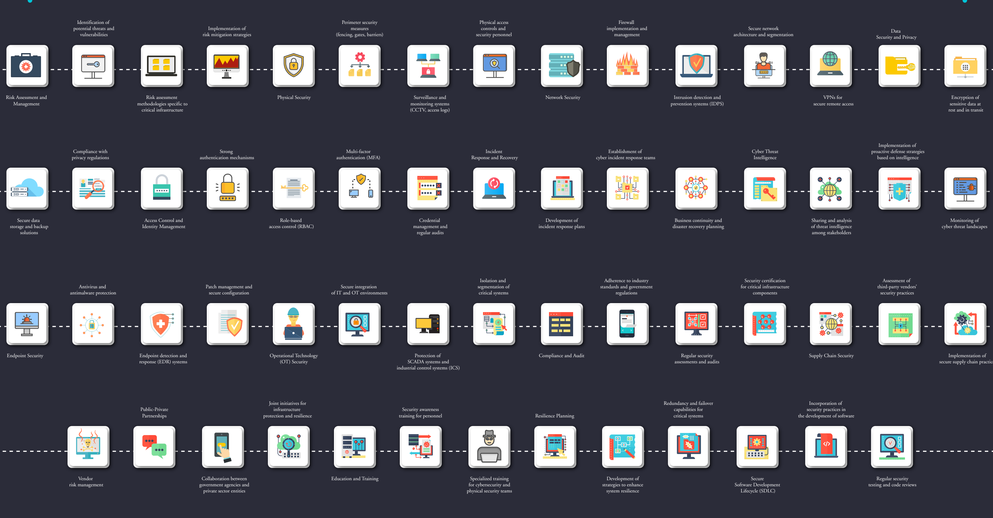
RCCE CYBERSECURITY FRAMEWORK

MOBILE SECURITY

INTERNET OF THINGS (IOT) SECURITY

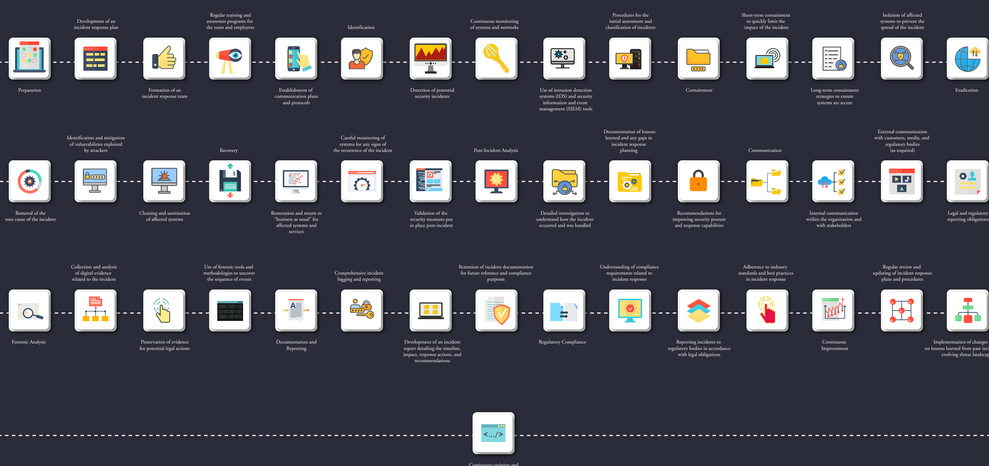


CRITICAL INFRASTRUCTURE SECURITY



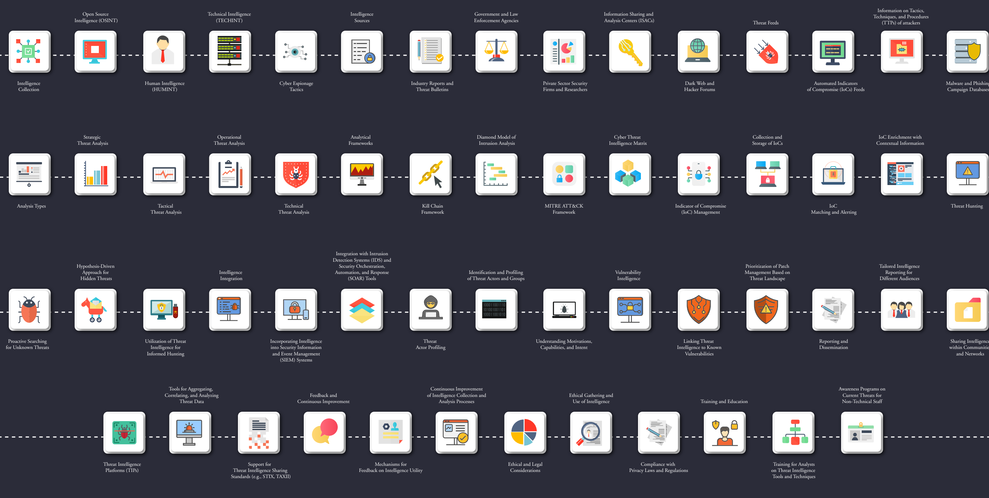
RCCE CYBERSECURITY FRAMEWORK

INCIDENT RESPONSE



DISASTER RECOVERY AND BUSINESS CONTINUITY

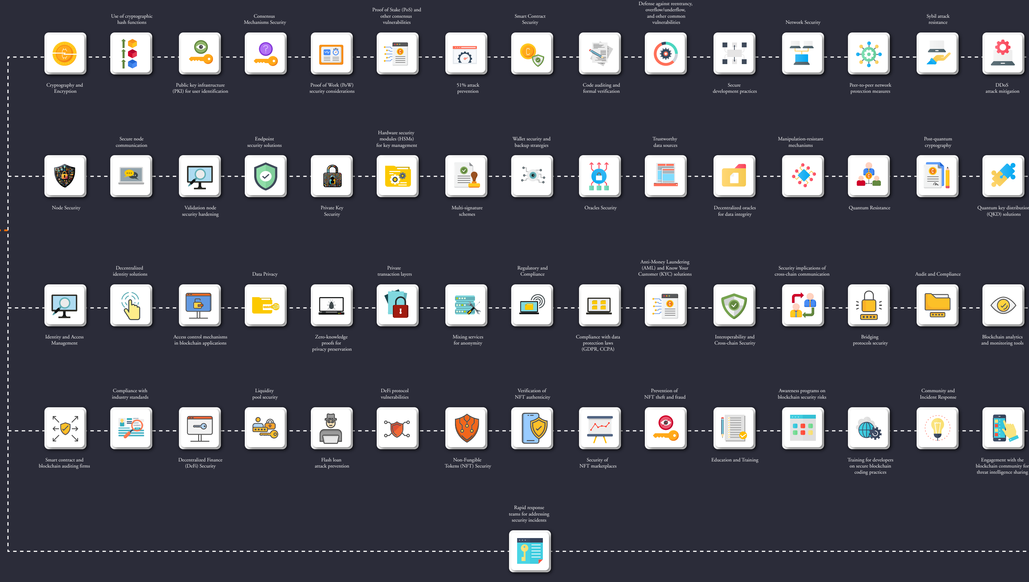
THREAT INTELLIGENCE



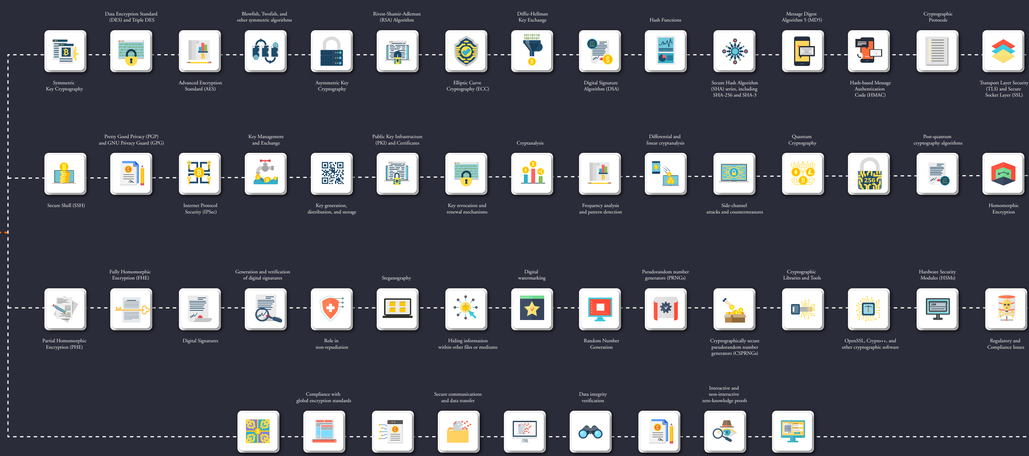
PENETRATION TESTING AND VULNERABILITY ASSESSMENT

RCCE CYBERSECURITY FRAMEWORK

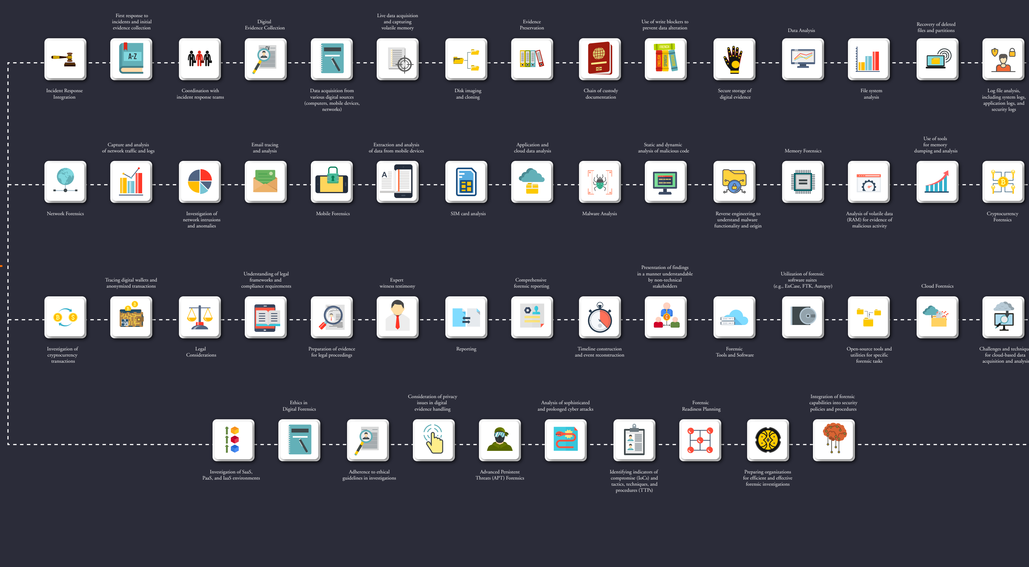
BLOCKCHAIN SECURITY



CRYPTOGRAPHY

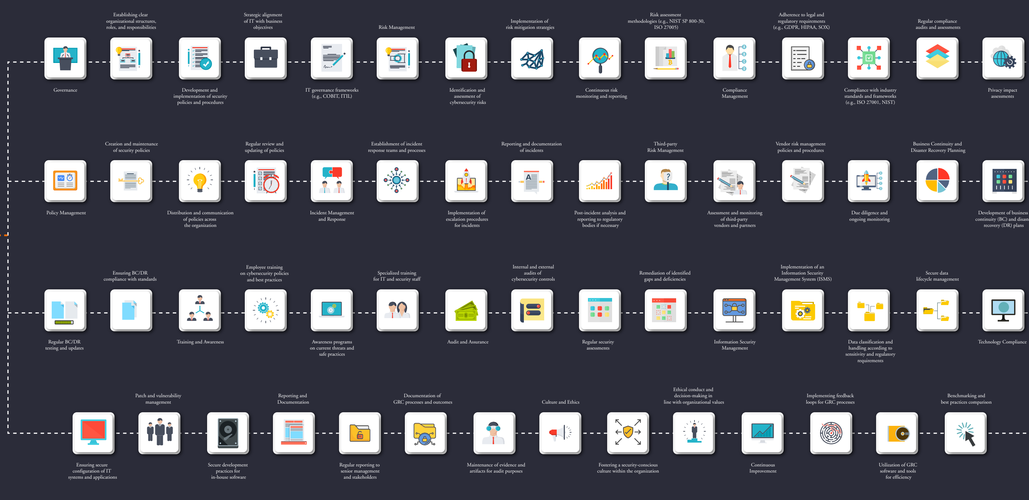


FORENSICS

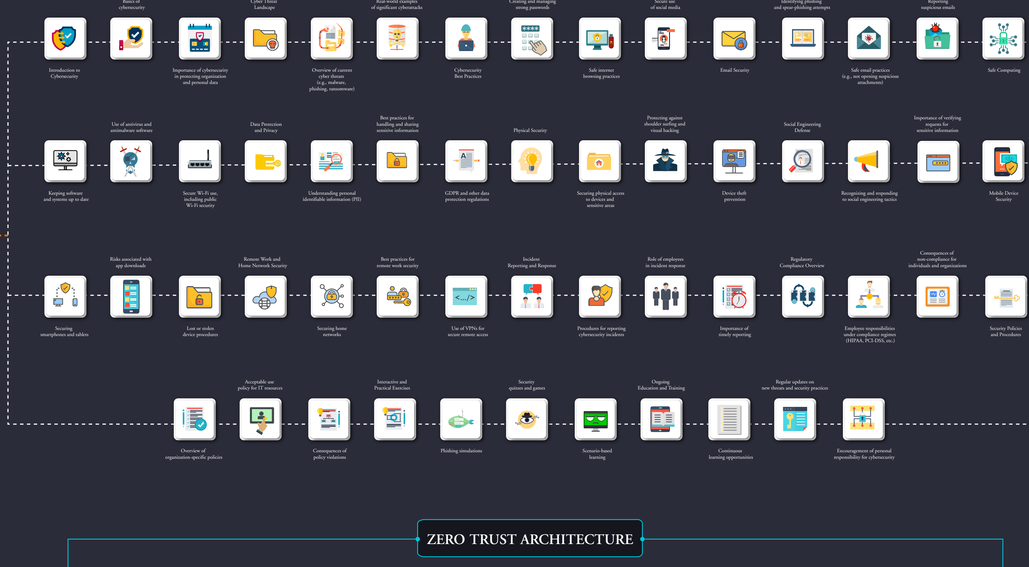


RCCE CYBERSECURITY FRAMEWORK

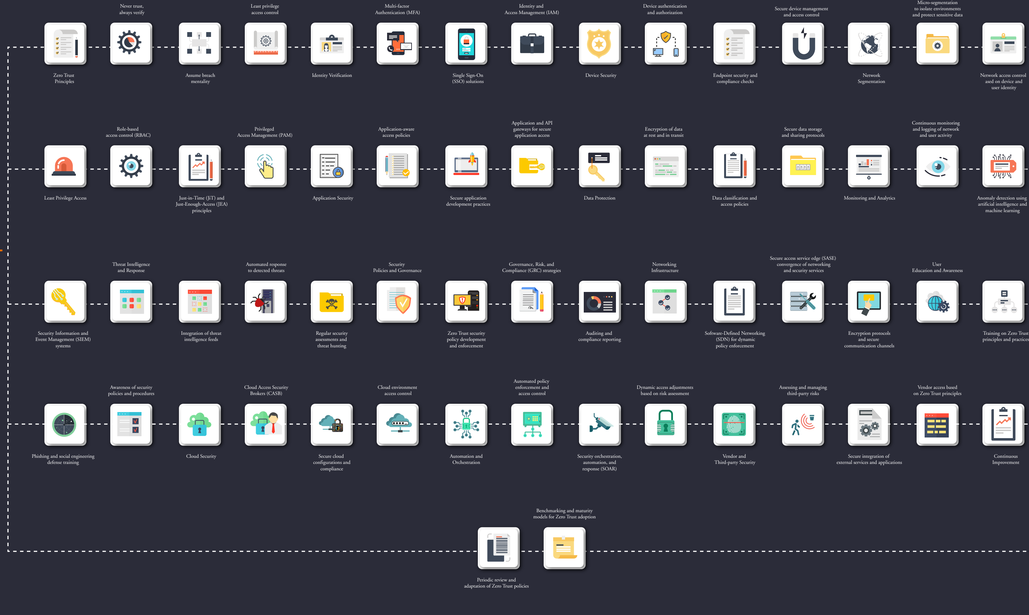
GOVERNANCE, RISK, AND COMPLIANCE (GRC)



SECURITY AWARENESS TRAINING



ZERO TRUST ARCHITECTURE



RCCE CYBERSECURITY FRAMEWORK

CYBER-PHYSICAL SYSTEMS SECURITY

PRIVACY

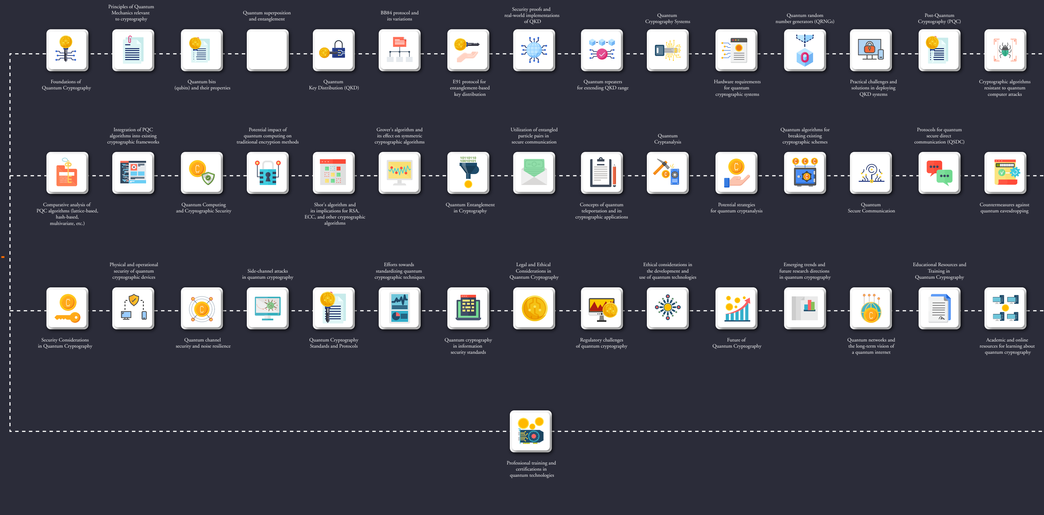
MALWARE ANALYSIS

RCCE CYBERSECURITY FRAMEWORK

CYBER INSURANCE

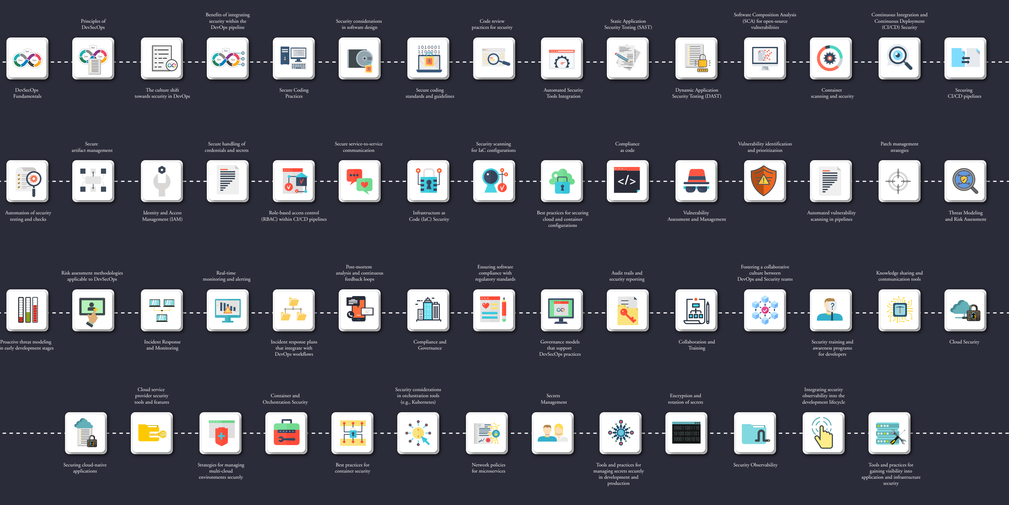
EMBEDDED SYSTEMS SECURITY

QUANTUM CRYPTOGRAPHY

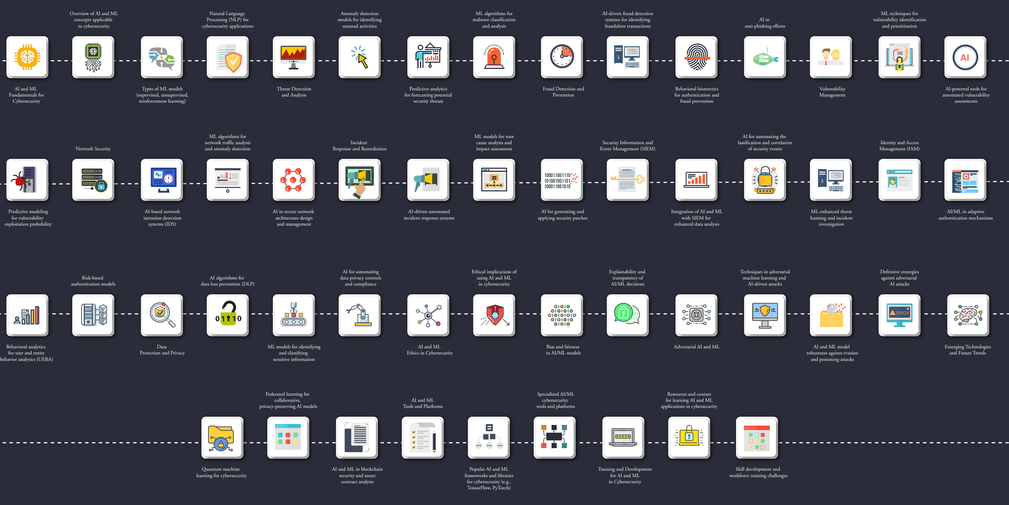


RCCE CYBERSECURITY FRAMEWORK

DEVSECOPS



ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING



RCCE
Cybersecurity Engineer

RCCE
Cybersecurity Engineer

RCCE
Cybersecurity Framework

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

RCCE
DoD 8140

Rocheston Cybersecurity Framework (RCF)

The Rocheston Cybersecurity Framework (RCF) serves as a comprehensive structure designed to outline the necessary competencies and knowledge areas essential for professionals in the field of cybersecurity.

Rooted in the core objective of fostering a deep understanding of the multifaceted landscape of cyber threats and defenses, the RCF is the foundational blueprint for the Rocheston Certified Cybersecurity Engineer (RCCE) certification.

This certification aims to equip professionals with the skills and insights required to navigate and protect the digital infrastructure of modern organizations effectively.

List of Domains:

Network Security
Application Security
Endpoint Security
Data Security
Identity and Access Management (IAM)
Cloud Security
Mobile Security
Internet of Things (IoT) Security
Critical Infrastructure Security
Incident Response
Disaster Recovery and Business Continuity
Threat Intelligence
Penetration Testing and Vulnerability Assessment
Blockchain Security
Cryptography
Forensics
Governance, Risk, and Compliance (GRC)
Security Awareness Training
Zero Trust Architecture
Cyber-Physical Systems Security
Privacy
Malware Analysis
Cyber Insurance
Embedded Systems Security
Quantum Cryptography
DevSecOps
Artificial Intelligence and Machine Learning

RCCE Cybersecurity Framework

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Network Security	Protects network infrastructure and data transmitted over it.	• Network Access Control (NAC) • Authentication, Authorization, and Accounting (AAA) Frameworks • Pre-Connection Authentication • Post-Connection Controls • Role-Based Access Control (RBAC) • Firewalls • Packet-Filtering Firewalls • Stateful Inspection Firewalls • Next-Generation Firewalls (NGFWs) • Web Application Firewalls (WAFs) • Proxy Firewalls • Intrusion Detection and Prevention Systems (IDPS) • Network-Based Intrusion Detection Systems (NIDS) • Host-Based Intrusion Detection Systems (HIDS) • Intrusion Prevention Systems (IPS) • Signature-Based, Anomaly-Based, and Behavior-Based Detection • Virtual Private Network (VPN) • Site-to-Site VPNs • Remote Access VPNs • SSL/TLS VPNs • Secure Wireless Networks • WPA2/WPA3 Security Protocols • Hidden SSIDs and MAC Address Filtering • Network Segmentation for Wireless Access Points • Data Loss Prevention (DLP) • Network DLP • Endpoint DLP • Cloud DLP • Network Segmentation • Subnetting • Virtual Local Area Networks (VLANs) • Software-Defined Networking (SDN) for Dynamic Segmentation • Secure Network Architecture • Demilitarized Zones (DMZ) • Zero Trust Network Architecture • Secure Cloud Networking • Encryption • Transport Layer Security (TLS) and Secure Sockets Layer (SSL) for Data in Transit • IPsec for Protecting Internet Protocol Communications • End-to-End Encryption Techniques • Endpoint Security • Antivirus and Antimalware Software • Endpoint Detection and Response (EDR) Systems • Sandboxing • Detonating Suspicious Files/URLs in a Safe Environment • Threat Intelligence and Information Sharing • Cyber Threat Intelligence (CTI) Feeds • Information Sharing and Analysis Centers (ISACs) • Network Monitoring and Management • Security Information and Event Management (SIEM) Systems • Network Traffic Analysis (NTA) • Configuration and Patch Management • Penetration Testing and Vulnerability Assessment • Network Vulnerability Scanning • Ethical Hacking to Identify Weaknesses • Red Team, Blue Team, and Purple Team Exercises • DNS Security • DNS Filtering • DNS Security Extensions (DNSSEC) • Email Security • Spam Filters • Email Encryption • Phishing Detection and Response • Secure Protocols	• Assess Network Architecture • Evaluate current network architecture for vulnerabilities and security gaps. • Recommend architectural improvements to enhance security. • Implement Security Measures • Deploy firewalls, VPNs, and other security appliances. • Configure network segmentation and isolation strategies to limit attack surfaces. • Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS). • Secure Network Communications • Enforce encryption protocols for data in transit. • Secure wireless access points and technologies. • Conduct Vulnerability Assessments and Penetration Testing • Regularly scan network components for vulnerabilities. • Perform penetration tests to identify weaknesses in network defenses. • Patch Management • Ensure timely application of security patches and updates to network devices. • Monitor for vulnerabilities associated with network hardware and software. • Monitor Network Traffic • Utilize security information and event management (SIEM) systems for real-time analysis. • Analyze network traffic patterns for signs of malicious activity or unauthorized access. • Develop and Enforce Access Controls • Define and implement network access policies. • Manage user permissions and role-based access control. • Incident Response • Participate in incident response activities for network-related security incidents. • Develop and refine incident response plans specifically for network breaches. • Secure Configuration • Harden network devices against attacks by disabling unnecessary services and protocols. • Ensure secure configurations of routers, switches, and other network infrastructure. • Educate and Train Staff • Provide training on network security awareness and best practices. • Advise on secure network design and architecture to IT staff and project teams. • Document Network Security Posture • Maintain comprehensive documentation of network security measures, incidents, and resolutions. • Document security policies and procedures related to network security. • Research Emerging Threats and Technologies • Stay informed about the latest network security threats and countermeasures. • Evaluate and recommend new security tools and technologies to enhance network defenses. • Collaborate with Other Security Professionals • Work with cybersecurity analysts, IT staff, and external consultants to strengthen network security. • Participate in cybersecurity forums and professional groups to share knowledge and best practices. • Compliance and Regulatory Adherence • Ensure network security measures comply with relevant laws, regulations, and standards. • Prepare for and participate in compliance audits.	• Palo Alto Networks Next-Generation Firewall • Fortinet FortiGate • Check Point NGFW • Cisco ASA Firewall • Snort (Open Source) • Cisco Firepower • Sophos XG Firewall • TippingPoint Threat Protection System • NordVPN • Cisco AnyConnect • Pulse Secure VPN • OpenVPN • Cisco Identity Services Engine (ISE) • ForeScout CounterACT • Aruba ClearPass • Symantec Endpoint Protection • McAfee Endpoint Security • Kaspersky Endpoint Security • Sophos Intercept X • Zscaler Internet Access • Symantec Web Security Service • McAfee Web Gateway • Forcepoint Web Security • Symantec Data Loss Prevention • Digital Guardian • Forcepoint DLP • McAfee Total Protection for Data Loss Prevention • Splunk Enterprise Security • IBM QRadar Security Information and Event Management • LogRhythm NextGen SIEM Platform • ArcSight Enterprise Security Manager (ESM) by Micro Focus • Sophos XG Firewall • Fortinet FortiGate UTM • WatchGuard Firebox • Check Point Small Business Security • Tenable Nessus • Qualys Vulnerability Management • Rapid7 Nexpose • CrowdStrike Falcon • SentinelOne • Carbon Black Defense • Microsoft Defender for Endpoint • SolarWinds NetFlow Traffic Analyzer • Plixer Scrutinizer • Wireshark • ManageEngine NetFlow Analyzer • Microsoft Defender Advanced Threat Protection • Symantec Advanced Threat Protection • Fortinet FortiSandbox • Proofpoint Email Protection • Barracuda Email Security Gateway • Cisco Email Security • Mimecast Secure Email Gateway • Cisco Umbrella • Infoblox Secure DNS • Cloudflare DNS Firewall • DigiCert • Let's Encrypt • Sectigo • Netskope Security Cloud • McAfee MVISION Cloud	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Application Security	Focuses on ensuring software and devices are free of threats.	• Secure Coding Practices • Input Validation to prevent injection attacks • Output Encoding to prevent data from being interpretable as executable code • Authentication and Authorization mechanisms • Secure Session Management • Error Handling and Logging without exposing sensitive information • Application Security Testing • Static Application Security Testing (SAST) to analyze source code • Dynamic Application Security Testing (DAST) for runtime testing • Interactive Application Security Testing (IAST) that combines SAST and DAST • Software Composition Analysis (SCA) for detecting vulnerable components • Penetration Testing to simulate real-world attacks • Threat Modeling • Identifying security threats and vulnerabilities in application design • STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) methodology • Attack Tree Analysis • Application Security Frameworks and Standards • Open Web Application Security Project (OWASP) Top 10 vulnerabilities • Secure Software Development Lifecycle (SSDLC) guidelines • NIST Application Security Guidelines • Encryption and Data Protection • Implementing SSL/TLS for data in transit • Data encryption for data at rest • Proper management of encryption keys • Identity and Access Management (IAM) • Implementing Multi-Factor Authentication (MFA) • Role-Based Access Control (RBAC) • OAuth, OpenID Connect, and SAML for secure single sign-on (SSO) • Application Layer Firewalls and Web Application Firewalls (WAF) • Filtering, monitoring, and blocking HTTP/HTTPS traffic • Custom rule sets based on applications' unique requirements • API Security • Securing RESTful APIs against common threats • Rate limiting to prevent abuse • OAuth for securing APIs with tokens • Patch Management • Regularly updating applications and dependencies • Automated tools for vulnerability tracking and patching • Secure Deployment Practices • Environment hardening • Using containers for consistent deployment environments • Automated deployment pipelines that incorporate security checks • DevSecOps Integration • Integrating security practices within the CI/CD pipeline • Automated security scanning and testing in development and deployment processes • Collaboration between development, security, and operations teams • Container and Orchestration Security • Securing Docker and Kubernetes environments • Managing container vulnerabilities • Network segmentation and access controls for containerized applications • Cloud Security Posture Management (CSPM) • Securing applications deployed in cloud environments • Compliance checks against cloud security frameworks • Automated threat detection and remediation in cloud settings • Mobile Application Security • Securing mobile apps against common vulnerabilities • Implementing secure communication for mobile applications • Protection against reverse engineering and tampering	• Secure Software Development Lifecycle (SDLC) Integration • Integrate security practices throughout the SDLC. • Participate in the definition and refinement of secure coding standards. • Threat Modeling • Conduct threat modeling on applications to identify potential security issues. • Collaborate with development teams to understand application architecture and identify security risks. • Static Application Security Testing (SAST) • Implement and manage SAST tools to analyze source code for vulnerabilities. • Review SAST findings and guide developers on remediation. • Dynamic Application Security Testing (DAST) • Perform DAST to identify vulnerabilities in running applications. • Simulate attacks on applications to evaluate their responses. • Software Composition Analysis (SCA) • Conduct SCA to identify vulnerabilities in third-party libraries and dependencies. • Manage the inventory of third-party components and ensure they are up to date and secure. • Secure Code Review • Conduct manual code reviews for critical components. • Provide feedback and guidance to developers on secure coding practices. • Vulnerability Management • Track and prioritize identified vulnerabilities from assessments, penetration tests, and bug bounty programs. • Facilitate the remediation of vulnerabilities by working with development teams. • Penetration Testing • Perform application penetration testing to identify exploitable vulnerabilities. • Develop custom scripts or tools to automate testing procedures. • Security Automation • Integrate security testing tools into CI/CD pipelines. • Automate the security testing and scanning processes wherever possible. • Incident Response for Applications • Participate in incident response activities related to application security incidents. • Conduct post-mortem analysis to prevent future occurrences. • Training and Education • Provide secure coding training to development teams. • Stay updated on the latest application security threats and trends. • Compliance and Regulatory Adherence • Ensure applications meet compliance requirements specific to the industry, such as PCI DSS, GDPR, or HIPAA. • Document application security practices and findings for audit purposes. • Authentication and Authorization • Design and review authentication mechanisms. • Implement and audit authorization controls within applications. • Security Architecture • Design secure application architecture. • Review existing application architectures for security concerns and recommend improvements. • API Security • Secure APIs through proper management, testing, and monitoring. • Apply rate limiting and throttling to protect against abuse. • Mobile Application Security • Assess the security of mobile applications. • Provide guidance on securing mobile application data, both at rest and in transit. • Cloud Application Security • Secure applications deployed in cloud environments. • Implement cloud-specific security controls and configurations.	• OWASP Zed Attack Proxy (ZAP) • Burp Suite • Fortify Software Security Center by Micro Focus • Checkmarx • SonarQube • Veracode • Snyk • GitLab Secure • GitHub Advanced Security • Coverity • Qualys Web Application Scanning • Acunetix • Nessus by Tenable • Rapid7 Nexpose • Rapid7 AppSpider • IBM Security AppScan • Symantec Code Signing • Docker for container security • Kubernetes for container orchestration security • HashiCorp Vault for secrets management • Black Duck by Synopsys • WhiteSource Software • F5 BIG-IP Application Security Manager (ASM) • Cloudflare WAF (Web Application Firewall) • AWS WAF • Azure Application Gateway WAF • ModSecurity (Open Source WAF) • Splunk for security logging and analysis • Elastic Stack for security data analysis and visualization • Metasploit for vulnerability exploitation testing • YARA for malware research and detection • Kiuwan Code Security • Contrast Security • JFrog Xray for artifact analysis • Google Safe Browsing for checking URL reputations • LastPass for secure password management • Duo Security for multi-factor authentication • Okta for identity and access management • Ping Identity for access management and SSO (Single Sign-On) • New Relic for application performance monitoring with security insights • Datadog Security Monitoring • WireShark for network protocol analysis • Postman for API testing and security analysis • OpenSCAP for compliance testing • Let's Encrypt for free SSL/TLS certificates • OpenSSL for SSL/TLS management • CloudSploit by Aqua Security for AWS security scanning • Twistlock by Prisma Cloud (Palo Alto Networks) for container and cloud native security • Tripwire for file integrity monitoring and compliance management	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Endpoint Security	Involves securing endpoints or entry points of end-user devices like desktops, laptops, and mobile devices.	• Antivirus and Antimalware Software • Real-time malware detection and removal • Scheduled scans and automatic updates • Endpoint Detection and Response (EDR) • Continuous monitoring and response to advanced threats • Behavioral analysis to detect malicious patterns • Firewall Protection • Ingress and egress filtering to control network traffic • Application-level and packet-filtering firewalls • Patch Management • Timely updates of operating systems and applications • Automated patching tools to ensure up-to-date security • Encryption • Full disk encryption (FDE) for data at rest • File-level encryption for specific sensitive documents • Mobile Device Management (MDM) • Remote management of mobile devices • Device configuration, password enforcement, and wiping capabilities • Data Loss Prevention (DLP) • Monitoring, detecting, and blocking sensitive data exfiltration • Control over transfer and storage of critical data • Virtual Private Network (VPN) • Secure remote access via encrypted connections • Split tunneling and full tunneling options • Multi-Factor Authentication (MFA) • Additional authentication layers beyond passwords • Biometrics, security tokens, and SMS codes • Security Configuration Management • Harden device security settings based on best practices • Regular audits and adjustments to security configurations • Email Security • Filtering spam, phishing, and malicious email contents • Email encryption for sensitive information • Zero Trust Security • Least privilege access controls • Continuous authentication and verification • Secure Web Gateways (SWG) • Filtering unwanted software/malware from web traffic • Policy enforcement for internet usage • USB Device Control • Blocking or restricting the use of unauthorized USB devices • Monitoring file transfers to and from external devices • Application Control • Whitelisting allowed applications • Blacklisting prohibited applications • Endpoint Privilege Management • Limiting administrative privileges on endpoints • Controlling application execution with elevated rights • Network Access Control (NAC) • Enforcing security policies based on device compliance • Quarantining or restricting access of non-compliant devices • Threat Intelligence Integration • Utilizing up-to-date threat information for better protection • Sharing threat data with security solutions for enhanced detection • IoT Device Security • Securing Internet of Things devices integrated into the network • Managing updates and monitoring for unusual activities	• Endpoint Protection Strategies • Develop and implement comprehensive endpoint security strategies. • Evaluate and select endpoint security solutions (antivirus, antimalware, EDR, etc.). • Vulnerability Assessment and Patch Management • Regularly assess endpoints for vulnerabilities. • Manage and deploy patches and updates to operating systems and software. • Configuration and Hardening • Harden endpoint configurations to minimize vulnerabilities. • Ensure secure baseline configurations for all endpoint types. • Endpoint Detection and Response (EDR) • Configure and maintain EDR solutions. • Monitor EDR tools for real-time threat detection and response. • Application Control and Whitelisting • Implement application control policies and application whitelisting. • Manage and review approved software lists. • Mobile Device Management (MDM) • Deploy and maintain MDM solutions for mobile device security. • Enforce security policies on mobile devices (encryption, remote wipe, etc.). • Endpoint Encryption • Ensure full disk encryption for data-at-rest security on endpoints. • Manage encryption keys securely. • Access Control • Manage user access controls and permissions for endpoint access. • Implement role-based access control (RBAC) for sensitive data and systems. • Network Access Control (NAC) • Employ NAC solutions to control endpoint access to the network. • Configure NAC policies to enforce security compliance on all connecting devices. • Security Awareness and Training • Provide training for users on endpoint security best practices. • Educate users about phishing, social engineering, and safe internet use. • Incident Response and Remediation • Participate in incident response activities for endpoint-related security incidents. • Remediate compromised endpoints and perform root cause analysis. • Secure Remote Access • Implement and secure remote access solutions (VPN, VDI). • Ensure secure connections for remote workers. • Monitoring and Reporting • Continuously monitor endpoints for security incidents and anomalies. • Generate reports for endpoint security posture and incidents. • Compliance and Auditing • Ensure endpoint compliance with relevant regulatory requirements. • Regularly audit endpoint security measures and compliance. • Zero Trust Implementation • Apply principles of Zero Trust architecture to endpoint access and security. • Continuously verify the security posture of endpoints. • Threat Intelligence Integration • Leverage threat intelligence for proactive endpoint security measures. • Update endpoint security measures based on current threat landscape. • Collaboration • Work closely with IT operations, network security, and other teams for holistic security. • Engage with vendors for security tools and updates.	• Symantec Endpoint Protection • McAfee Endpoint Security • Trend Micro Apex One • Kaspersky Endpoint Security • Sophos Intercept X • ESET Endpoint Security • Bitdefender GravityZone • Microsoft Defender for Endpoint • CrowdStrike Falcon • SentinelOne Endpoint Protection Platform • Carbon Black Defense (VMware) • Palo Alto Networks Traps • Malwarebytes Endpoint Protection • Webroot SecureAnywhere Endpoint Protection • CylancePROTECT • NortonLifeLock Endpoint Security • F-Secure Protection Service for Business • Avast Business Antivirus • Cisco AMP for Endpoints • FireEye Endpoint Security • Fortinet FortiClient • Check Point Endpoint Security • Avira Antivirus for Endpoint • Panda Endpoint Protection Plus • Barkly • Ziften Zenith • Ivanti Endpoint Security for Endpoint Manager • Lookout Mobile Endpoint Security • BlackBerry Unified Endpoint Management • MobileIron • VMware Workspace ONE • Absolute Software Endpoint Resilience • Prey Anti-Theft • AirWatch Endpoint Management • Jamf Pro for Apple devices security • Deep Instinct Endpoint Protection • AhnLab V3 Endpoint Security • Comodo Advanced Endpoint Protection • RSA NetWitness Endpoint • Cybereason Total Enterprise Protection	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Data Security	Protects data integrity and privacy through encryption, tokenization, and other methods.	• Data Encryption • Full Disk Encryption (FDE) • Database Encryption • File-level Encryption • Data-in-Transit Encryption (TLS/SSL for data on the move) • Data-at-Rest Encryption • Tokenization • Replacing sensitive data elements with non-sensitive equivalents • Particularly useful for protecting payment card information • Data Masking • Concealing specific parts of data within a database • Dynamic Data Masking (DDM) for real-time data request processing • Data Erasure • Securely wiping data from storage devices to prevent recovery • Compliance with data disposal standards and regulations • Access Controls • Role-Based Access Control (RBAC) • Attribute-Based Access Control (ABAC) • Mandatory Access Control (MAC) and Discretionary Access Control (DAC) • Data Privacy Regulations Compliance • General Data Protection Regulation (GDPR) • California Consumer Privacy Act (CCPA) • Health Insurance Portability and Accountability Act (HIPAA) • Payment Card Industry Data Security Standard (PCI DSS) • Data Loss Prevention (DLP) • Tools and strategies to prevent data exfiltration • Monitoring and blocking sensitive data in use, in motion, and at rest • Backup and Recovery • Regular data backups with secure storage • Recovery solutions for data breach or loss scenarios • Database Security • Database Activity Monitoring (DAM) • Secure database configuration and patch management • Database encryption and access controls • Digital Rights Management (DRM) • Restricting how digital content can be copied, printed, or shared • Encryption and licensing controls • Cloud Data Security • Cloud Access Security Brokers (CASB) • Encryption in cloud storage and services • Compliance with cloud security standards • Secure File Sharing • Solutions for securely sharing files within and outside the organization • Encrypted file transfer protocols • Data Discovery and Classification • Identifying and classifying data based on sensitivity and compliance requirements • Automated tools for ongoing data classification • Anonymization and Pseudonymization • Techniques to remove or replace personal identifiers from data sets • Useful for research and analytics without compromising privacy • End-to-End Encryption (E2EE) • Encrypting data before it leaves the sender and decrypting it only at the destination • Ensures data privacy and security during transmission • Secure Development Life Cycle (SDLC) • Integrating security practices into software development processes • Ensuring applications handle data securely • Blockchain for Data Security • Using blockchain technology for secure, immutable storage of data • Enhances data integrity and traceability	• Data Classification and Discovery • Classify data based on sensitivity and compliance requirements. • Implement data discovery tools to locate sensitive data across systems. • Encryption Management • Deploy encryption solutions for data at rest and in transit. • Manage encryption keys securely, including key rotation and storage. • Tokenization and Data Masking • Implement tokenization and data masking techniques to protect sensitive information. • Apply data obfuscation methods for non-production environments. • Access Control • Design and enforce strict access control policies for data access. • Implement least privilege access principles to minimize data exposure. • Data Loss Prevention (DLP) • Configure and manage DLP solutions to monitor and protect sensitive data. • Develop policies for preventing unauthorized data transfer and storage. • Database Security • Harden database configurations and secure database management systems (DBMS). • Monitor databases for suspicious activities and unauthorized access. • Cloud Data Security • Secure cloud storage and services through encryption and access controls. • Evaluate and apply cloud provider security features and best practices. • Compliance and Regulatory Adherence • Ensure data security measures comply with industry regulations (e.g., GDPR, HIPAA). • Prepare data security documentation and reports for compliance audits. • Vulnerability Management • Conduct regular security assessments of systems storing sensitive data. • Remediate vulnerabilities that could compromise data integrity or privacy. • Incident Response and Data Breach Management • Develop and execute incident response plans for potential data breaches. • Investigate data breaches, perform impact analysis, and lead remediation efforts. • Secure Data Lifecycle Management • Implement procedures for secure data creation, storage, usage, and destruction. • Ensure secure data deletion practices, including secure wiping and disposal. • Backup and Recovery Planning • Establish secure data backup processes to prevent data loss. • Develop and test disaster recovery plans for critical data. • Monitoring and Logging • Implement tools for continuous monitoring of data access and usage. • Analyze logs for indications of data security incidents or breaches. • Endpoint Data Security • Secure endpoint devices to prevent data leakage or unauthorized access. • Encrypt sensitive data stored on portable devices. • Security Awareness Training • Conduct security awareness training focusing on data protection practices. • Educate employees about phishing, social engineering, and safe data handling procedures. • Collaboration with Stakeholders • Work with legal, compliance, and business units to align data security with organizational goals. • Engage with external auditors and regulatory bodies as necessary.	• VeraCrypt for disk encryption • BitLocker for Windows disk encryption • FileVault 2 for macOS disk encryption • McAfee Complete Data Protection • Symantec Endpoint Encryption • Trend Micro Endpoint Encryption • Sophos SafeGuard Encryption • Thales Vormetric Data Security Platform • IBM Guardium Data Protection • Protegrity Data Security • TokenEx Cloud Security Platform • Gemalto SafeNet Data Protection • CipherCloud CASB+ • Voltage SecureData by Micro Focus • Trustwave Data Protection • PKWARE SecureZIP • Comforte SecurDPS Data Protection Suite • nCipher Hardware Security Modules (HSMs) • AWS Key Management Service (KMS) for cloud encryption key management • Microsoft Azure Key Vault for cloud key management • Google Cloud Key Management Service (KMS) • HashiCorp Vault for secrets management • CyberArk Privileged Access Security Solution • RSA Data Protection Manager • Dell EMC CloudLink • Varonis Data Security Platform • Spirion Data Privacy Manager • Digital Guardian Data Protection Platform • Check Point Full Disk Encryption • Tresorit for secure cloud storage • Box with Box Shield for secure collaboration • SpiderOak One Backup for secure cloud backup • Sookasa for Dropbox encryption • Zix Secure File Sharing • WinMagic SecureDoc • AxCrypt for file encryption • SecureDoc by WinMagic for enterprise disk encryption • Egress Secure Workspace for secure collaboration • Druva inSync for endpoint data protection • Symantec VIP for strong authentication • Duo Security for multi-factor authentication • Yubico YubiKey for hardware-based two-factor authentication • PGP (Pretty Good Privacy) for email and file encryption	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Identity and Access Management (IAM)	Ensures that only authorized individuals can access resources in the right context.	• Authentication • Password-based Authentication • Multi-factor Authentication (MFA) • Single Sign-On (SSO) • Biometric Authentication • Token-based Authentication • Certificate-based Authentication • Authorization • Role-Based Access Control (RBAC) • Attribute-Based Access Control (ABAC) • Mandatory Access Control (MAC) • Discretionary Access Control (DAC) • Policy-Based Access Control (PBAC) • Identity Provisioning and Lifecycle Management • Automated User Provisioning and Deprovisioning • Self-Service Account Management • Privileged Account Management • Directory Services • Lightweight Directory Access Protocol (LDAP) • Active Directory (AD) • Directory Synchronization • Identity Federation • Security Assertion Markup Language (SAML) • OpenID Connect • OAuth 2.0 • Federation Protocols and Standards • Privileged Access Management (PAM) • Privileged User Credential Management • Session Monitoring and Recording • Least Privilege Enforcement • Risk-Based Authentication • Adaptive Authentication • Contextual and Behavioral Analysis • Identity Governance and Administration (IGA) • Policy Definition and Enforcement • Compliance and Audit Reporting • Role Management and Role Mining • Access Review and Certification • Periodic Access Recertification • Entitlement Reviews • User and Entity Behavior Analytics (UEBA) • Anomaly Detection Based on User Activity • Cloud IAM • Cloud Identity Providers (IdP) • IAM for SaaS, PaaS, and IaaS Environments • Password Management and Synchronization • Password Vaults • Password Rotation and Complexity Policies • Web Access Management (WAM) • Web SSO • Web Session Management • API Security • API Access Controls • Secure API Gateways	• Develop and implement IAM strategies and policies aligned with organizational security policies and compliance requirements. • Implement robust user authentication mechanisms, including multi-factor authentication and biometrics. • Design and enforce access control policies using RBAC, ABAC, and PBAC models. • Secure and manage privileged accounts through Privileged Access Management (PAM) solutions. • Configure and manage identity federation and Single Sign-On (SSO) across various applications and systems. • Automate user account provisioning and de-provisioning processes for effective user lifecycle management. • Administer directory services technologies such as LDAP and Active Directory. • Implement secure credential storage solutions and manage password policies. • Conduct periodic access reviews and recertifications to ensure appropriateness of access rights. • Monitor IAM systems for irregular activities and generate access and compliance reports. • Respond to IAM-related security incidents, participate in investigations, and implement remediations. • Evaluate, recommend, and implement new IAM tools and technologies. • Ensure IAM practices comply with data protection and privacy regulations like GDPR and HIPAA. • Provide IAM training and awareness programs for employees. • Secure and monitor third-party vendor access to organizational systems. • Stay updated on the latest trends and advancements in IAM solutions. • Participate in internal and external audits related to IAM, preparing necessary documentation and evidence. • Develop secure password practices and educate users on defending against phishing and identity theft. • Implement audit trails and logging for access events to maintain a record of access patterns. • Evaluate third-party IAM practices as part of comprehensive vendor risk management. • Implement solutions for privileged session management and monitoring. • Establish policies for password complexity, expiration, and rotation. • Implement least privilege and need-to-know principles for access management across the organization.	• Okta Identity Cloud • Microsoft Azure Active Directory • OneLogin Unified Access Management • Ping Identity Platform • SailPoint IdentityIQ • CyberArk Privileged Access Security Solution • IBM Security Identity Governance and Intelligence • ForgeRock Identity Platform • Duo Security (Cisco Duo) • RSA SecurID Suite • Centrify Identity Service • LastPass Enterprise • Keeper Business • Thales SafeNet Trusted Access • Google Cloud Identity • Auth0 • JumpCloud Directory-as-a-Service • Oracle Identity Management • AWS Identity and Access Management (IAM) • BeyondTrust Privileged Access Management • Saviynt Security Manager • Keycloak (Open Source) • Axiomatics Policy Server • FIDO Alliance protocols for authentication (U2F, WebAuthn) • HID Global Identity and Access Management • ManageEngine ADManager Plus • Bitium (Acquired by Google) • Avatier Identity Anywhere • Evidian Identity & Access Management • Fischer Identity Suite • NetIQ Identity Manager • EmpowerID • SSOgen Single Sign-On Solution • Vault by HashiCorp for secrets management • Yubico for hardware-based authentication keys (YubiKeys) • OpenIAM Identity Governance • Securden Password Vault • IAM Cloud • Tools4ever IAM • Gluu Server (Open Source Identity and Access Management) • Univention Corporate Server (UCS) with integrated IAM features	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Cloud Security	Pertains to creating secure cloud computing environments.	• Cloud Security Posture Management (CSPM) • Identification of misconfigurations and compliance risks • Continuous security assessment and monitoring • Cloud Access Security Brokers (CASB) • Visibility into cloud application usage • Data security and compliance in the cloud • Threat protection for cloud services • Identity and Access Management (IAM) for the Cloud • Multi-factor Authentication (MFA) • Role-Based Access Control (RBAC) • Single Sign-On (SSO) across cloud services • Data Encryption • Data-at-Rest Encryption • Data-in-Transit Encryption • Encryption key management • Network Security • Secure Virtual Private Cloud (VPC) configurations • Firewall rules and security groups • Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) • Threat Detection and Response • Automated threat detection • Integration with SIEM systems • Incident response planning and execution • Secure Software Development Lifecycle (SDLC) in the Cloud • Integration of security into DevOps (DevSecOps) • Application vulnerability scanning • Dependency scanning in CI/CD pipelines • Configuration and Vulnerability Management • Automated scanners for detecting vulnerabilities • Configuration change tracking • Compliance scanning and reporting • Data Protection • Data Loss Prevention (DLP) strategies • Backup and disaster recovery planning • Secure data storage and lifecycle management • API Security • Secure API gateways • API authentication and authorization • Regular API vulnerability scanning • Segmentation and Microsegmentation • Network segmentation across cloud resources • Microsegmentation for fine-grained access control • Privileged Access Management (PAM) in the Cloud • Management of privileged user accounts • Session monitoring and logging • Cloud Governance • Cloud usage policies and guidelines • Governance frameworks to manage cloud risks • Cloud service provider (CSP) risk assessment • End-to-End Visibility • Centralized visibility over cloud environments • Real-time monitoring and analytics • Regulatory Compliance • Mapping cloud use to regulatory requirements • Ensuring data sovereignty, GDPR, HIPAA compliance, etc. • Secure Containerization • Container security best practices • Container image scanning and management • Serverless Security • Security considerations for serverless computing models • Managing serverless function permissions and dependencies	• Assess and improve security posture of cloud environments (IaaS, PaaS, SaaS). • Implement and manage identity and access control measures in cloud platforms. • Configure and maintain cloud security services such as firewalls, VPNs, and encryption. • Perform vulnerability assessments and penetration testing of cloud applications and services. • Develop and enforce policies for cloud data protection, including encryption in transit and at rest. • Monitor cloud environments for security incidents and anomalies using cloud-native and third-party tools. • Respond to and remediate security incidents within cloud environments. • Ensure compliance with regulatory standards applicable to cloud data and services (e.g., GDPR, HIPAA). • Implement secure DevOps practices in cloud deployments, including CI/CD security. • Design and enforce network segmentation and microsegmentation strategies in cloud environments. • Manage secure configurations for cloud resources and services. • Collaborate with cloud service providers to stay updated on new security features and best practices. • Conduct regular security reviews and audits of cloud architectures and deployments. • Educate and train staff on cloud security best practices and awareness. • Implement robust data backup and disaster recovery processes in the cloud. • Work closely with IT and development teams to integrate security into cloud-based projects. • Architect and manage secure API integrations and gateways in cloud environments. • Manage and secure containers and Kubernetes environments hosted in the cloud. • Utilize cloud access security brokers (CASBs) to enforce security policies across cloud services. • Perform threat modeling and risk assessment for cloud deployments and services. • Secure management of secrets and credentials in cloud environments. • Optimize cloud service costs related to security services and resources. • Stay informed on emerging cloud security threats and technologies. • Implement and maintain compliance and governance frameworks for cloud environments. • Develop and test cloud incident response plans and procedures.	• AWS Security Hub • Microsoft Azure Security Center • Google Cloud Security Command Center • Palo Alto Networks Prisma Cloud • Check Point CloudGuard • Symantec Cloud Workload Protection • Cisco CloudLock • McAfee MVISION Cloud • Trend Micro Cloud One • Netskope Security Cloud • Qualys Cloud Platform • Zscaler Internet Access and Zscaler Private Access • Fortinet FortiGate Cloud • Cloudflare Cloud Security Solutions • Sophos Cloud Optix • Dome9 (acquired by Check Point) • Tenable.io • CrowdStrike Falcon Cloud Workload Protection • Bitglass CASB • IBM Cloud Security and Compliance Center • Armor Anywhere • Barracuda CloudGen Firewall • Aqua Security • Lacework • CloudPassage Halo • DivvyCloud by Rapid7 • F5 BIG-IP Cloud Edition • Aporeto (acquired by Palo Alto Networks) • Kaspersky Hybrid Cloud Security • A10 Networks Thunder Cloud • Forcepoint CASB • Alert Logic SIEMless Threat Management • Aviatrix Secure Cloud Network Platform • Darktrace Cloud • Orca Security • Wiz • Sysdig Secure • Saviynt Security Manager for Cloud • VMware Secure State • Fugue Cloud Security • Varonis Data Security Platform for Cloud • HashiCorp Vault for Secrets Management • CipherCloud • Imperva Cloud WAF • Radware Cloud WAF Service • Valtix Cloud Security Platform • Arctic Wolf Managed Detection and Response (MDR) for Cloud	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Mobile Security	Addresses security for personal and corporate information stored on mobile devices.	• Device Security • Screen locks (PINs, patterns, biometrics) • Secure boot mechanisms • Full device encryption • Jailbreaking and rooting detection • Application Security • App sandboxing • Secure app development practices • App permission management • Regular updates and patching • Application vetting and blacklisting • Network Security • Secure Wi-Fi connections (VPN usage for public networks) • Firewall protection for mobile devices • Protection against network-based attacks (Man-in-the-Middle attacks) • Data Protection • Data encryption for stored data and data in transit • Use of secure containers for corporate data • Data loss prevention (DLP) strategies • Mobile Device Management (MDM) • Remote wipe capabilities • Remote device locking • Device tracking and location services • Inventory and asset management • Enforcement of security policies • Mobile Identity and Access Management • Multi-factor authentication (MFA) • Single sign-on (SSO) for mobile applications • Certificate-based authentication • Threat Detection and Response • Malware protection and antivirus solutions • Phishing protection (SMS, email) • Anomaly detection for unusual device behavior • Secure Mobile Communications • End-to-end encrypted messaging and calling • Secure email communication • Protection against eavesdropping • Privacy Protection • Tools for managing and limiting data shared with apps and advertisers • Awareness and training on privacy settings • Secure Mobile Payments and Transactions • Tokenization of payment information • Secure element hardware for payment apps • Biometric authentication for transactions • Operating System and Firmware Security • Timely OS updates and patches • Secure boot to protect against unauthorized OS modifications • User Education and Awareness • Training on secure usage of mobile devices • Awareness of social engineering attacks • Compliance and Legal Requirements • Compliance with regulations like GDPR, HIPAA for mobile data • Legal considerations for Bring Your Own Device (BYOD) policies • Physical Security • Theft and loss prevention measures • Secure disposal and recycling of devices	• Implement and manage Mobile Device Management (MDM) or Mobile Application Management (MAM) solutions. • Develop and enforce mobile security policies and guidelines. • Perform regular security assessments of mobile applications and devices. • Configure and enforce device encryption and secure data storage on mobile devices. • Manage secure mobile access to corporate networks and data. • Design and implement secure authentication mechanisms for mobile access. • Monitor and respond to mobile security incidents and threats. • Ensure compliance with relevant regulations and standards for mobile security, such as GDPR for data privacy. • Conduct mobile application security testing, including static and dynamic analysis. • Secure integration of mobile devices with enterprise systems and applications. • Implement network security measures for mobile devices, including VPNs and secure Wi-Fi connections. • Educate employees on mobile security best practices and awareness. • Manage updates and patches for mobile operating systems and applications. • Assess and mitigate risks associated with mobile device loss or theft, including remote wipe capabilities. • Monitor mobile app stores for unauthorized or malicious versions of corporate apps. • Implement application whitelisting and blacklisting on corporate mobile devices. • Perform threat modeling for mobile applications and ecosystems. • Develop and implement API security strategies for mobile applications. • Secure mobile payment and financial transaction capabilities. • Collaborate with mobile application developers to embed security in the development lifecycle. • Evaluate and implement mobile security technologies and products. • Secure the use of BYOD (Bring Your Own Device) in the corporate environment. • Manage credentials and access control for mobile devices. • Investigate and remediate vulnerabilities disclosed through bug bounty programs or other sources. • Secure mobile messaging and communications within the corporate environment. • Address security concerns related to mobile cloud services and storage. • Implement security measures for wearables and other connected devices integrated with mobile platforms.	• Lookout Mobile Endpoint Security • Zimperium zIPS • Wandera Mobile Threat Defense • Symantec Endpoint Protection Mobile • McAfee MVISION Mobile • Microsoft Intune • IBM MaaS360 with Watson • MobileIron Unified Endpoint Management (UEM) • VMware Workspace ONE UEM • BlackBerry Unified Endpoint Manager (UEM) • Cisco Meraki Systems Manager • Sophos Mobile Security • Trend Micro Mobile Security & Antivirus • Norton Mobile Security • Kaspersky Mobile Antivirus • Avast Mobile Security • Bitdefender Mobile Security & Antivirus • ESET Mobile Security & Antivirus • F-Secure SAFE • AirWatch by VMware • Jamf Pro (for Apple devices) • SOTI MobiControl • ManageEngine Mobile Device Manager Plus • Google Android Enterprise • Samsung Knox • Apple iOS and iPadOS device management • Prey Anti Theft • Malwarebytes for Android • Cerberus anti theft • Comodo Mobile Security • Check Point SandBlast Mobile • Amtel Mobile Device Management (MDM) • 360 Security - Antivirus • Fortinet FortiClient VPN • Pulse Secure VPN	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Internet of Things (IoT) Security	Deals with safeguarding connected devices and networks in the IoT ecosystem.	• Device Security • Hardware-based security features • Secure boot mechanisms • Firmware and software integrity verification • Device authentication and authorization • Communication Security • Encryption of data in transit • Secure communication protocols (MQTT, CoAP, HTTPS) • Network segmentation and firewalling • VPNs for secure remote access • Data Security • Encryption of data at rest • Data anonymization and masking • Secure data storage and management • Data integrity checks • Access Control • Strong authentication mechanisms • Role-based access control (RBAC) • Credential management and rotation • Multi-factor authentication (MFA) • Network Security • Intrusion detection and prevention systems • Network behavior analysis • Secure network configuration and management • DDoS protection strategies • Privacy Protection • Compliance with privacy regulations (GDPR, CCPA) • User consent management for data collection and sharing • Privacy impact assessments • Patch Management and Software Updates • Secure firmware/software update mechanisms • Version control and update validation • Vulnerability scanning and mitigation • Endpoint Security • Antimalware and antivirus solutions • Device health checks and monitoring • Endpoint detection and response (EDR) systems • Secure Development Lifecycle (SDLC) for IoT • Threat modeling and risk assessment • Security by design principles • Code reviews and static/dynamic analysis • Security testing and validation • IoT Platform Security • Secure cloud and edge computing platforms • Platform access control and authentication • APIs security • Supply Chain Security • Risk assessment of third-party components • Secure software supply chain practices • Transparency and integrity in the supply chain • Incident Response and Recovery • IoT-specific incident response planning • Forensics and investigation capabilities • Disaster recovery and business continuity planning • User Education and Awareness • Training on IoT device security best practices • Guidance on password management and secure device setup • Regulatory Compliance • Adherence to industry standards and regulations • Security certifications and audits • Physical Security • Anti-tampering measures for devices • Secure device storage and access	• Assess and improve the security posture of IoT devices and ecosystems. • Implement secure communication protocols for IoT devices. • Perform vulnerability assessments and penetration testing on IoT systems. • Design and apply encryption solutions for data at rest and in transit within IoT ecosystems. • Manage device identity and ensure robust authentication mechanisms for IoT devices. • Develop and enforce IoT security policies and guidelines. • Monitor IoT devices and networks for security incidents and anomalies. • Respond to and remediate IoT security incidents. • Ensure compliance with relevant IoT security standards and regulations. • Implement and maintain secure firmware/software update processes for IoT devices. • Assess and mitigate risks associated with third-party components and services in IoT solutions. • Collaborate with IoT device manufacturers and vendors on security requirements and best practices. • Conduct regular security audits of IoT environments. • Educate and train staff on IoT security best practices and awareness. • Design and implement network segmentation strategies to isolate IoT devices. • Optimize the use of IoT security tools and technologies, such as intrusion detection systems specifically designed for IoT. • Secure integration of IoT devices with existing enterprise systems and networks. • Develop and test IoT incident response plans and procedures. • Utilize threat intelligence to stay informed about emerging IoT threats and vulnerabilities. • Manage access controls and permissions for IoT device management interfaces. • Implement data privacy measures for personally identifiable information collected by IoT devices. • Secure IoT cloud and data storage components. • Develop security architectures for IoT deployments, addressing both hardware and software aspects. • Leverage machine learning and AI for advanced threat detection in IoT ecosystems. • Address specific security challenges of IoT verticals such as industrial IoT (IIoT), smart homes, healthcare, and automotive. • Participate in IoT security standards development and industry forums. • Research and evaluate new IoT security technologies and innovations.	• Armis Security • Cisco IoT Security • Palo Alto Networks IoT Security • Symantec IoT Security • McAfee IoT Security • Check Point IoT Protect • Fortinet FortiNAC • Trend Micro IoT Security • Zingbox IoT Guardian • Kaspersky IoT Secure Gateway • Microsoft Azure Sphere • AWS IoT Device Defender • Siemens Industrial Edge • IBM Watson IoT Platform Security • Mocana Security Platform • Forescout Platform • Sophos XG Firewall with IoT Security • Avast Omni • Bitdefender BOX IoT Security Solution • Norton Core Secure WiFi Router • BullGuard IoT Scanner • Snort (for network traffic analysis applicable to IoT) • OpenVAS (for vulnerability scanning within IoT networks) • WireShark (for network protocol analysis in IoT systems) • Raspberry Pi for building and testing IoT environments securely • Docker for containerizing IoT applications securely • Eclipse IoT for developing secure IoT applications • Thales Cinterion IoT Security Module • Sectigo IoT Identity Management • Infineon OPTIGA Trust Platform for IoT device identity and data protection • DigiCert IoT Device Manager • Particle Secure IoT Platform • Losant Enterprise IoT Platform • Telit deviceWISE IoT Platform • Nozomi Networks Guardian for IoT and industrial control systems security • Dragos Platform for industrial IoT security • Black Duck Software (for identifying and securing open source risks in IoT software) • Cloudflare for IoT (provides secure and performant networking for IoT devices) • Rubicon Labs Identity Service for IoT security and access management	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Critical Infrastructure Security	Involves the protection of systems, networks, and assets essential to the functioning of a society and economy.	• Risk Assessment and Management • Identification of potential threats and vulnerabilities • Risk assessment methodologies specific to critical infrastructure • Implementation of risk mitigation strategies • Physical Security • Perimeter security measures (fencing, gates, barriers) • Surveillance and monitoring systems (CCTV, access logs) • Physical access controls and security personnel • Network Security • Firewall implementation and management • Intrusion detection and prevention systems (IDPS) • Secure network architecture and segmentation • VPNs for secure remote access • Data Security and Privacy • Encryption of sensitive data at rest and in transit • Secure data storage and backup solutions • Compliance with privacy regulations • Access Control and Identity Management • Strong authentication mechanisms • Role-based access control (RBAC) • Multi-factor authentication (MFA) • Credential management and regular audits • Incident Response and Recovery • Development of incident response plans • Establishment of cyber incident response teams • Business continuity and disaster recovery planning • Cyber Threat Intelligence • Sharing and analysis of threat intelligence among stakeholders • Implementation of proactive defense strategies based on intelligence • Monitoring of cyber threat landscapes • Endpoint Security • Antivirus and antimalware protection • Endpoint detection and response (EDR) systems • Patch management and secure configuration • Operational Technology (OT) Security • Secure integration of IT and OT environments • Protection of SCADA systems and industrial control systems (ICS) • Isolation and segmentation of critical systems • Compliance and Audit • Adherence to industry standards and government regulations • Regular security assessments and audits • Security certification for critical infrastructure components • Supply Chain Security • Assessment of third-party vendors' security practices • Implementation of secure supply chain practices • Vendor risk management • Public-Private Partnerships • Collaboration between government agencies and private sector entities • Joint initiatives for infrastructure protection and resilience • Education and Training • Security awareness training for personnel • Specialized training for cybersecurity and physical security teams • Resilience Planning • Development of strategies to enhance system resilience • Redundancy and failover capabilities for critical systems • Secure Software Development Lifecycle (SDLC) • Incorporation of security practices in the development of software • Regular security testing and code reviews	• Assess and enhance the security posture of critical infrastructure systems and networks. • Implement robust access control measures to safeguard critical systems. • Develop and enforce security policies and procedures specific to critical infrastructure protection. • Conduct vulnerability assessments and penetration testing of critical infrastructure components. • Manage and secure network communications for critical systems, including the implementation of secure communication protocols. • Monitor critical infrastructure systems for cybersecurity threats and vulnerabilities. • Design and execute incident response plans tailored to the critical infrastructure sector. • Ensure compliance with national and international regulations and standards related to critical infrastructure security. • Implement physical security measures to protect critical infrastructure components. • Provide cybersecurity training and awareness programs for personnel involved in critical infrastructure operations. • Coordinate with government agencies and other entities on matters related to critical infrastructure protection. • Develop redundancy and disaster recovery plans to ensure the resilience of critical infrastructure services. • Secure remote access to critical infrastructure systems to prevent unauthorized access. • Leverage threat intelligence to anticipate and mitigate potential threats to critical infrastructure. • Implement and maintain security measures for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. • Manage encryption and VPNs for protecting data related to critical infrastructure. • Apply data analytics and machine learning techniques for advanced threat detection in critical infrastructure environments. • Regularly update and patch critical systems and software to defend against known vulnerabilities. • Perform security risk assessments to identify and mitigate risks to critical infrastructure assets. • Collaborate with vendors and third-party service providers to ensure the security of outsourced services and components. • Participate in sector-specific information sharing and analysis centers (ISACs) to exchange security-related information and best practices. • Develop and maintain an inventory of critical infrastructure assets and their associated vulnerabilities. • Implement secure configurations for devices and systems within the critical infrastructure network. • Establish and maintain secure backup systems and procedures for critical data and configurations. • Audit and review security practices and controls regularly to ensure their effectiveness.	• Fortinet FortiGate (Firewalls) • Palo Alto Networks NGFW (Next-Generation Firewalls) • Symantec Industrial Control System Protection • McAfee Network Security Platform • Cisco Industrial Network Director • Check Point Quantum Security Gateways • Honeywell Forge Cybersecurity Suite • Dragos Platform for Industrial Cybersecurity • Nozomi Networks Guardian • Siemens Ruggedcom (Network Infrastructure) • Tenable Nessus (Vulnerability Management) • Tripwire Industrial Visibility (Asset Identification and Threat Detection) • Kaspersky Industrial CyberSecurity • Claroty Continuous Threat Detection • CrowdStrike Falcon (Endpoint Protection) • CyberArk Privileged Access Security • Darktrace Industrial Immune System • Rapid7 InsightVM (Vulnerability Management) • IBM QRadar (Security Information and Event Management) • Belden Hirschmann (Network Infrastructure for Industrial Environments) • Waterfall Security Solutions Unidirectional Gateways • ABB Ability Cybersecurity for Electrical Systems • Rockwell Automation Threat Detection Services • Schneider Electric EcoStruxure Security Expert • LogRhythm SIEM (Security Information and Event Management) • RSA NetWitness Platform • Sophos Intercept X for Endpoint • F5 BIG-IP Access Policy Manager • VMware NSX (Network and Security Virtualization) • Zscaler Internet Access (Cloud-based Web Security) • Cisco Identity Services Engine (ISE) • Axonius Cybersecurity Asset Management • FireEye Network Security and Forensics • Microsoft Azure Sentinel (Cloud-native SIEM) • SANS Institute ICS Security Training • Industrial Defender ASM (Automation Systems Manager) • Owl Cyber Defense Cross Domain Solutions • Varonis Data Security Platform (Data Protection) • AirWatch by VMware (Mobile Device Management) • Splunk Enterprise Security (Data Analytics and SIEM) • OPSWAT Critical Infrastructure Protection • Wallix Bastion (Privileged Access Management) • CyberX (part of Microsoft) for IoT/OT Security • Keysight (formerly Ixia) Threat Simulator (Security Testing and Validation)	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Incident Response	The approach to managing and addressing security breaches or attacks.	• Preparation • Development of an incident response plan • Formation of an incident response team • Regular training and awareness programs for the team and employees • Establishment of communication plans and protocols • Identification • Detection of potential security incidents • Continuous monitoring of systems and networks • Use of intrusion detection systems (IDS) and security information and event management (SIEM) tools • Procedures for the initial assessment and classification of incidents • Containment • Short-term containment to quickly limit the impact of the incident • Long-term containment strategies to ensure systems are secure • Isolation of affected systems to prevent the spread of the incident • Eradication • Removal of the root cause of the incident • Identification and mitigation of vulnerabilities exploited by attackers • Cleaning and sanitization of affected systems • Recovery • Restoration and return to “business as usual” for affected systems and services • Careful monitoring of systems for any signs of the recurrence of the incident • Validation of the security measures put in place post-incident • Post-Incident Analysis • Detailed investigation to understand how the incident occurred and was handled • Documentation of lessons learned and any gaps in incident response planning • Recommendations for improving security posture and response capabilities • Communication • Internal communication within the organization and with stakeholders • External communication with customers, media, and regulatory bodies (as required) • Legal and regulatory reporting obligations • Forensic Analysis • Collection and analysis of digital evidence related to the incident • Preservation of evidence for potential legal actions • Use of forensic tools and methodologies to uncover the sequence of events • Documentation and Reporting • Comprehensive incident logging and reporting • Development of an incident report detailing the timeline, impact, response actions, and recommendations • Retention of incident documentation for future reference and compliance purposes • Regulatory Compliance • Understanding of compliance requirements related to incident response • Reporting incidents to regulatory bodies in accordance with legal obligations • Adherence to industry standards and best practices in incident response • Continuous Improvement • Regular review and updating of incident response plans and procedures • Implementation of changes based on lessons learned from past incidents and evolving threat landscape • Continuous training and skills development for the incident response team	• Develop and maintain an incident response plan tailored to organizational needs. • Conduct regular incident response drills and exercises to ensure team preparedness. • Monitor security systems and tools for indicators of compromise. • Perform initial incident triage to classify and prioritize incidents based on severity. • Gather and preserve digital evidence following forensic best practices. • Analyze security incidents to determine the scope, impact, and root cause. • Coordinate the containment of incidents to prevent further unauthorized activity. • Lead the eradication of threats from the environment, including the removal of malware and unauthorized access. • Manage the recovery process to restore affected systems and services to operational status securely. • Communicate incident status and details to stakeholders, including management, IT teams, and potentially affected parties. • Document incident details, investigative findings, and lessons learned in detailed reports. • Perform post-incident reviews to identify improvements to security posture and incident response processes. • Stay updated on the latest cybersecurity threats, vulnerabilities, and incident response techniques. • Collaborate with external entities such as law enforcement, legal counsel, and cybersecurity organizations during and after incidents. • Advise on the implementation of security measures to prevent the recurrence of similar incidents. • Manage the use of incident response tools and software for efficient response to incidents. • Provide guidance and support for the development and implementation of incident response automation and orchestration capabilities. • Collaborate with IT and network teams to ensure the secure configuration of systems and networks to aid in rapid incident response. • Contribute to security awareness training programs by sharing insights and lessons learned from real incidents. • Support the continuous improvement of the incident response plan based on evolving threats, organizational changes, and lessons learned from incidents. • Coordinate with cybersecurity insurance providers during the incident response process, when applicable. • Manage and secure remote access for incident response team members to ensure timely response actions. • Implement strategies for detecting and responding to insider threats. • Coordinate vulnerability management efforts in response to incidents to address identified weaknesses in systems and applications.	• Splunk Enterprise Security • IBM QRadar Security Information and Event Management (SIEM) • Rapid7 InsightIDR • LogRhythm NextGen SIEM Platform • TheHive Project (Open Source, Incident Response Platform) • CrowdStrike Falcon Insight (Endpoint Detection and Response) • Tanium (Endpoint Management and Security) • Malwarebytes Endpoint Detection and Response • SentinelOne (Endpoint Protection Platform) • Carbon Black Response (now VMware Carbon Black EDR) • Palo Alto Networks Cortex XDR • FireEye Endpoint Security • AlienVault USM (Unified Security Management) • Cybereason Malop Detection Engine • ArcSight ESM (Enterprise Security Manager) by Micro Focus • Microsoft Defender for Endpoint • Cisco SecureX • Check Point SandBlast Agent • FortiEDR by Fortinet • Proofpoint Threat Response • Swimlane (Security Orchestration, Automation, and Response SOAR) • Phantom Cyber (now part of Splunk for SOAR) • D3 Security Incident Response Platform • Resilient Incident Response Platform (IBM Security) • Siemplify (Security Orchestration, Automation and Response) • Cynet 360 AutoXDR • Exabeam Security Management Platform • Kaspersky Endpoint Detection and Response • Digital Guardian Endpoint DLP and Threat Awareness • OpenText EnCase Endpoint Security • Secureworks Red Cloak Threat Detection and Response • Sophos Intercept X Advanced with EDR • NETRESEC NetworkMiner (Network Forensic Analysis Tool) • WireShark (Network Protocol Analyzer) • FTK Imager (Forensic Imaging Tool) • Autopsy (Open Source Digital Forensics Platform) • GRR Rapid Response (Open Source Incident Response Framework) • MISP (Malware Information Sharing Platform & Threat Sharing) • Volatility (Open Source Memory Forensics Framework) • Sysinternals Suite by Microsoft (Utilities for Windows diagnostics including Process Explorer) • SANS SIFT (The SIFT Workstation, Incident Forensics & Investigation) • Cuckoo Sandbox (Automated Dynamic Malware Analysis) • YARA (Tool aimed at helping malware researchers identify and classify malware samples) • Redline (Tool for forensic investigators)	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Disaster Recovery and Business Continuity	Planning for recovery and continuation of operations in the event of a cyber incident.	• Risk Assessment and Business Impact Analysis (BIA) • Identification of potential threats and vulnerabilities • Assessment of the impact of different disaster scenarios on business operations • Business Continuity Planning • Development of strategies to maintain essential functions during and after a disaster • Identification of critical business functions and processes • Determination of acceptable downtime for critical functions • Disaster Recovery Planning • Specific plans for IT infrastructure recovery • Focus on restoring data and IT systems critical to business operations post-disaster • Emergency Response and Management • Procedures for immediate response to a disaster situation • Assignment of roles and responsibilities for disaster response • Communication Plan • Internal communication strategy for stakeholders and employees • External communication protocol with customers, suppliers, and regulators • Data Backup Solutions • Regular, secure backup of all critical data • Use of off-site backups and cloud storage for redundancy • Disaster Recovery Sites • Use of hot, warm, and cold sites for IT infrastructure recovery • Consideration of geographical diversity to mitigate localized disasters • Recovery Point Objective (RPO) and Recovery Time Objective (RTO) • Defining acceptable loss of data and downtime in disaster scenarios • Incident Response Integration • Coordinating disaster recovery efforts with incident response teams • Procedures for transitioning from incident response to disaster recovery • Vendor and Supplier Coordination • Management of third-party services and dependencies essential for recovery • Ensuring vendors have their own BC and DR plans that align with organizational needs • Testing and Exercise Programs • Regular testing of the DR and BC plans to ensure effectiveness • Simulation exercises to train staff and identify plan improvements • Training and Awareness • Education programs for employees on their roles in DR and BC plans • Ensuring all staff are aware of emergency procedures • Plan Maintenance and Review • Regular review and updates to DR and BC plans to reflect changes in the business operations, technology, and threat landscape • Documentation of lessons learned from tests and actual incidents • Regulatory Compliance and Documentation • Ensuring plans meet industry regulatory requirements • Proper documentation of all DR and BC procedures and policies • Insurance Considerations • Evaluating insurance coverage for different types of disasters • Understanding the claims process and documentation required	• Develop and maintain disaster recovery (DR) plans focused on restoring IT operations after a cyber incident. • Collaborate with business continuity (BC) planning teams to ensure IT DR plans are aligned with overall business recovery objectives. • Conduct regular risk assessments to identify critical IT assets and systems required for business operations. • Design and implement redundancy, backup solutions, and data replication strategies to minimize data loss. • Establish and maintain off-site data backup locations ensuring data is secure and recoverable. • Implement failover mechanisms for critical systems to ensure high availability. • Perform regular DR and BC drills and exercises to test the effectiveness of the plans. • Update DR and BC plans based on changes in the business environment, IT infrastructure, or lessons learned from drills and actual incidents. • Ensure secure and efficient restoration procedures for servers, networks, applications, and data. • Develop emergency communication plans to notify stakeholders, including employees, management, and external partners, during a disaster. • Coordinate with external vendors and service providers to ensure they can support recovery objectives. • Monitor for emerging threats and vulnerabilities that could impact DR and BC capabilities. • Document and maintain clear recovery procedures and responsibilities for IT staff and other involved parties. • Train IT staff and relevant personnel on their roles and responsibilities within the DR and BC plans. • Evaluate and incorporate cloud-based solutions and services as part of the DR strategy. • Ensure compliance with legal, regulatory, and industry standards related to data recovery and business continuity. • Manage cybersecurity insurance policies to cover the costs associated with data breaches and system recoveries. • Implement cybersecurity measures to protect backup data and DR systems from cyber attacks. • Assess the impact of cybersecurity incidents on business operations to prioritize recovery efforts. • Maintain an inventory of hardware, software, and support resources required for recovery operations. • Monitor the performance and health of systems in recovery environments to ensure they meet the required recovery objectives. • Coordinate post-recovery activities to return operations to normal business environments. • Analyze and document the cause of incidents, recovery performance, and any identified gaps in DR and BC plans. • Develop strategies to improve resilience against future disruptions, incorporating new technologies and practices.	• Veeam Backup & Replication • Zerto Virtual Replication • VMware Site Recovery Manager (SRM) • Datto Business Continuity and Disaster Recovery (BCDR) • Acronis Cyber Protect • Commvault Complete Backup & Recovery • Rubrik Cloud Data Management • Cohesity DataProtect • Arcserve Unified Data Protection • IBM Spectrum Protect • Azure Site Recovery • AWS Backup • Google Cloud Backup and DR • NetApp SnapMirror for Data Replication • Veritas NetBackup • Carbonite Backup and Recovery Solutions • Unitrends Recovery Series Backup Appliances • SolarWinds Backup • Nakivo Backup & Replication • AOMEI Backupper • EaseUS Todo Backup • Altaro VM Backup • Barracuda Backup • StorageCraft ShadowProtect • Asigra Cloud Backup • R1Soft Server Backup Manager • NovaStor DataCenter Backup • Quest Rapid Recovery • Oracle Data Guard for Database Replication • DRaaS (Disaster Recovery as a Service) providers like IBM Resiliency Services, Microsoft Azure DRaaS, Sungard AS, and iland Secure DRaaS • Business Continuity Management (BCM) software like Fusion Risk Management, SAI Global, and Everbridge • Incident Management Systems like ServiceNow, BMC Helix, and Cherwell • Risk Assessment and Management tools like RSA Archer, LogicManager, and Riskonnect • Data Replication tools like Dell EMC RecoverPoint and Hitachi Universal Replicator	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Threat Intelligence	Analyzing and comprehending information about existing or emerging threats.	• Intelligence Collection • Open Source Intelligence (OSINT) • Human Intelligence (HUMINT) • Technical Intelligence (TECHINT) • Cyber Espionage Tactics • Intelligence Sources • Industry Reports and Threat Bulletins • Government and Law Enforcement Agencies • Private Sector Security Firms and Researchers • Information Sharing and Analysis Centers (ISACs) • Dark Web and Hacker Forums • Threat Feeds • Automated Indicators of Compromise (IoCs) Feeds • Information on Tactics, Techniques, and Procedures (TTPs) of attackers • Malware and Phishing Campaign Databases • Analysis Types • Strategic Threat Analysis • Tactical Threat Analysis • Operational Threat Analysis • Technical Threat Analysis • Analytical Frameworks • Kill Chain Framework • Diamond Model of Intrusion Analysis • MITRE ATT&CK Framework • Cyber Threat Intelligence Matrix • Indicator of Compromise (IoC) Management • Collection and Storage of IoCs • IoC Matching and Alerting • IoC Enrichment with Contextual Information • Threat Hunting • Proactive Searching for Unknown Threats • Hypothesis-Driven Approach for Hidden Threats • Utilization of Threat Intelligence for Informed Hunting • Intelligence Integration • Incorporating Intelligence into Security Information and Event Management (SIEM) Systems • Integration with Intrusion Detection Systems (IDS) and Security Orchestration, Automation, and Response (SOAR) Tools • Threat Actor Profiling • Identification and Profiling of Threat Actors and Groups • Understanding Motivations, Capabilities, and Intent • Vulnerability Intelligence • Linking Threat Intelligence to Known Vulnerabilities • Prioritization of Patch Management Based on Threat Landscape • Reporting and Dissemination • Tailored Intelligence Reporting for Different Audiences • Sharing Intelligence within Communities and Networks • Threat Intelligence Platforms (TIPs) • Tools for Aggregating, Correlating, and Analyzing Threat Data • Support for Threat Intelligence Sharing Standards (e.g., STIX, TAXII) • Feedback and Continuous Improvement • Mechanisms for Feedback on Intelligence Utility • Continuous Improvement of Intelligence Collection and Analysis Processes • Ethical and Legal Considerations • Ethical Gathering and Use of Intelligence • Compliance with Privacy Laws and Regulations • Training and Education • Training for Analysts on Threat Intelligence Tools and Techniques • Awareness Programs on Current Threats for Non-Technical Staff	• Collect threat intelligence from a variety of sources, including open-source intelligence (OSINT), industry reports, and threat intelligence platforms. • Analyze and assess the credibility, reliability, and relevance of threat data. • Process and aggregate threat data to identify trends, tactics, techniques, and procedures (TTPs) of adversaries. • Produce actionable intelligence to inform and improve cybersecurity defenses. • Disseminate threat intelligence findings to relevant stakeholders within the organization. • Integrate threat intelligence into security tools and systems for automated defense and alerting. • Develop and maintain a threat intelligence database or library for historical analysis and reference. • Collaborate with external organizations, such as industry forums, ISACs (Information Sharing and Analysis Centers), and law enforcement for information sharing. • Monitor dark web and hacker forums for potential threats and leaked organizational data. • Use threat intelligence to proactively hunt for threats within the organization's networks and systems. • Provide recommendations for threat mitigation and preventive measures based on intelligence findings. • Conduct regular briefings and reports on the threat landscape to management and security teams. • Tailor threat intelligence feeds and alerts to match the organization's specific environment and risk profile. • Continuously update and refine threat intelligence collection and analysis methodologies to adapt to the evolving threat landscape. • Evaluate the effectiveness of implemented security measures and suggest improvements based on threat intelligence insights. • Participate in cyber incident response activities, leveraging threat intelligence for context and guidance. • Train cybersecurity and IT teams on using threat intelligence tools and interpreting intelligence reports. • Track and analyze threat actors' campaigns, motivations, and infrastructure. • Work with security architecture and engineering teams to design defenses based on the latest threat intelligence. • Perform attribution analysis to identify potential threat actors behind observed attacks or security incidents. • Stay informed about the latest cybersecurity technologies and threat intelligence analysis techniques. • Ensure compliance with legal and regulatory requirements related to threat intelligence collection and dissemination. • Assess the potential impact of emerging threats on the organization and prioritize response efforts accordingly. • Automate the collection and analysis of threat intelligence for efficiency and scale. • Support the development of cybersecurity policies and strategies by providing expert insights into the threat landscape.	• Recorded Future • CrowdStrike Falcon X • FireEye Threat Intelligence • IBM X-Force Exchange • Anomali ThreatStream • Palo Alto Networks AutoFocus • Cisco Talos • AlienVault OTX (Open Threat Exchange) • ThreatConnect • Maltego • MISP (Malware Information Sharing Platform) • STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated Exchange of Indicator Information) • Blueliv Threat Compass • McAfee Global Threat Intelligence • Symantec DeepSight Intelligence • Proofpoint Emerging Threats Intelligence • IntSights Threat Intelligence Platform • Flashpoint Intelligence Platform • EclecticIQ Platform • Digital Shadows SearchLight • ZeroFOX • LookingGlass ScoutPrime • Cybersixgill Investigative Portal • TruSTAR • DomainTools Iris • Kaspersky Threat Intelligence Portal • Farsight Security DNSDB • Infoblox Threat Intelligence Data Exchange • Censys • Shodan • VirusTotal • OpenPhish • PhishTank • Spamhaus • GreyNoise Intelligence • AlientVault USM Anywhere (Unified Security Management) • Chronicle (now part of Google Cloud) • Cybereason Malop Hunting Engine • SentinelOne Singularity • FortiGuard Labs • ThreatQuotient • RiskIQ External Threats	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Penetration Testing and Vulnerability Assessment	Identifying and testing vulnerabilities in systems and networks.	• Planning and Scoping • Defining the goals and scope of the assessment • Identifying the systems, applications, and networks to be tested • Establishing rules of engagement and legal considerations • Vulnerability Assessment • Automated scanning of systems and applications to identify known vulnerabilities • Utilization of vulnerability scanning tools and software • Assessment of patch levels and compliance with security policies • Penetration Testing Techniques • Black Box Testing: Testing without prior knowledge of the target system • White Box Testing: Testing with comprehensive details about the infrastructure • Grey Box Testing: Testing with limited knowledge about the target system • Testing Types • External Penetration Testing: Targeting externally visible servers and devices • Internal Penetration Testing: Mimicking an insider attack or a breach that has bypassed external defenses • Web Application Testing: Focused on applications accessible via the internet or an intranet • Wireless Security Testing: Examining Wi-Fi networks for vulnerabilities • Social Engineering: Testing the human element of security • Automated and Manual Testing • Use of automated tools for broad vulnerability identification • Manual testing for complex attack simulations and business logic vulnerabilities • Exploitation • Attempting to exploit identified vulnerabilities to understand the potential impact • Use of exploit frameworks like Metasploit • Documentation of exploitation attempts and outcomes • Post-Exploitation • Determining the value of the compromised system • Understanding how the system can be used as a pivot point for further exploitation • Reporting and Analysis • Comprehensive reporting of identified vulnerabilities, exploitation results, and sensitivity of the data accessed • Risk analysis and prioritization based on potential impact and exploitability • Recommendations for remediation • Remediation and Reassessment • Working with stakeholders to address identified vulnerabilities • Verifying that vulnerabilities have been adequately mitigated or remedied • Re-testing to ensure remediation efforts were successful • Ethical and Legal Considerations • Ensuring all testing is authorized and within ethical boundaries • Adherence to legal requirements and best practices • Continual Improvement • Integrating findings into the organization's security posture • Adjusting policies, procedures, and controls based on lessons learned • Tools and Resources • Utilization of various open-source and commercial tools for scanning and exploitation • Keeping tools updated with the latest vulnerability databases and exploit modules • Education and Skills Development • Ongoing training and certification for penetration testers and security analysts • Awareness training for IT staff and developers on common vulnerabilities and secure coding practices	• Conduct vulnerability assessments to identify weaknesses in systems and networks. • Perform penetration testing to exploit vulnerabilities and assess the impact of potential breaches. • Develop and execute test plans for various types of penetration tests (e.g., black-box, white-box, grey-box). • Utilize a range of penetration testing tools and methodologies to simulate cyber attacks. • Analyze and interpret penetration testing results to identify security flaws. • Create detailed reports documenting vulnerabilities, exploitation techniques, and recommendations for mitigation. • Collaborate with IT and development teams to prioritize and remediate identified vulnerabilities. • Stay updated on the latest security vulnerabilities, exploits, and testing tools. • Customize penetration testing tools and scripts to suit specific organizational needs or targets. • Perform retests on systems post-remediation to ensure vulnerabilities have been effectively resolved. • Engage in social engineering assessments to evaluate human-related vulnerabilities. • Conduct wireless network assessments to identify and exploit security weaknesses. • Perform web application penetration testing to discover vulnerabilities like SQL injection, cross-site scripting, and others. • Evaluate and test physical security measures as part of comprehensive penetration testing. • Participate in the development and refinement of penetration testing policies and procedures. • Conduct secure code reviews to identify vulnerabilities in application source code. • Perform configuration audits on systems and network devices to identify security misconfigurations. • Collaborate with external auditors or testers as needed for independent security assessments. • Educate and train IT staff and developers on common vulnerabilities and secure coding practices. • Maintain detailed records of testing methodologies and tools used for each assessment. • Ensure all penetration testing activities are authorized and comply with legal and ethical standards. • Participate in incident response activities by providing expertise on potential breach methods and vulnerabilities exploited. • Advise on the implementation of security controls and measures to mitigate the risk of future attacks. • Monitor public and private vulnerability databases and feeds for new threats and vulnerabilities relevant to the organization. • Use threat modeling to identify potential attack vectors and prioritize testing efforts. • Continuously improve technical skills and knowledge in areas relevant to penetration testing and vulnerability assessment.	• Metasploit Framework • Nessus • Burp Suite • OWASP Zed Attack Proxy (ZAP) • Qualys Vulnerability Management • Rapid7 Nexpose • Acunetix Web Vulnerability Scanner • Nmap • Wireshark • Nikto • Kali Linux • OpenVAS • sqlmap • Aircrack-ng • John the Ripper • Hashcat • Cobalt Strike • Core Impact • Immunity Canvas • Social-Engineer Toolkit (SET) • Network Mapper (Nmap) • Sqlninja • w3af (Web Application Attack and Audit Framework) • Arachni • Gobuster • Hydra • Paros Proxy • Fiddler • AppSpider • BeEF (Browser Exploitation Framework) • L0phtCrack • Maltego • Shodan • Censys • Security Onion • Tcpdump • Hping • Snort • OSSEC • YARA • IDA Pro • Ghidra • Binary Ninja • Radare2 • Nessus Agent • Tenable.io • Tenable.sc (SecurityCenter) • Postman for API testing • OWASP Dependency-Check • Retina Network Security Scanner • Veracode • Checkmarx • Fortify Software Security Center • IBM Security AppScan • GitGuardian • Snyk • Detectify • Intruder • Acunetix by Invicti • Nuclei	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Blockchain Security	Security measures tailored for blockchain technology.	• Cryptography and Encryption • Use of cryptographic hash functions • Public key infrastructure (PKI) for user identification • Consensus Mechanisms Security • Proof of Work (PoW) security considerations • Proof of Stake (PoS) and other consensus vulnerabilities • 51% attack prevention • Smart Contract Security • Code auditing and formal verification • Defense against reentrancy, overflow/underflow, and other common vulnerabilities • Secure development practices • Network Security • Peer-to-peer network protection measures • Sybil attack resistance • DDoS attack mitigation • Node Security • Secure node communication • Validation node security hardening • Endpoint security solutions • Private Key Security • Hardware security modules (HSMs) for key management • Multi-signature schemes • Wallet security and backup strategies • Oracles Security • Trustworthy data sources • Decentralized oracles for data integrity • Manipulation-resistant mechanisms • Quantum Resistance • Post-quantum cryptography • Quantum key distribution (QKD) solutions • Identity and Access Management • Decentralized identity solutions • Access control mechanisms in blockchain applications • Data Privacy • Zero-knowledge proofs for privacy preservation • Private transaction layers • Mixing services for anonymity • Regulatory and Compliance • Compliance with data protection laws (GDPR, CCPA) • Anti-Money Laundering (AML) and Know Your Customer (KYC) solutions • Interoperability and Cross-chain Security • Security implications of cross-chain communication • Bridging protocols security • Audit and Compliance • Blockchain analytics and monitoring tools • Smart contract and blockchain auditing firms • Compliance with industry standards • Decentralized Finance (DeFi) Security • Liquidity pool security • Flash loan attack prevention • DeFi protocol vulnerabilities • Non-Fungible Tokens (NFT) Security • Verification of NFT authenticity • Security of NFT marketplaces • Prevention of NFT theft and fraud • Education and Training • Awareness programs on blockchain security risks • Training for developers on secure blockchain coding practices • Community and Incident Response • Engagement with the blockchain community for threat intelligence sharing • Rapid response teams for addressing security incidents	• Assess and enhance the security posture of blockchain applications and platforms. • Implement and manage cryptographic practices, including key management and encryption standards specific to blockchain. • Conduct vulnerability assessments and penetration testing on blockchain systems and smart contracts. • Develop and enforce security policies and procedures for blockchain development and deployment. • Monitor blockchain networks for malicious activities such as double spending, 51% attacks, and other consensus attacks. • Secure blockchain wallets and private keys against unauthorized access and theft. • Design and implement access control mechanisms for blockchain transactions and data access. • Investigate and respond to security incidents and breaches within blockchain ecosystems. • Collaborate with developers to embed security best practices in the design and development of blockchain applications. • Perform code audits and security reviews of smart contracts to identify and remediate vulnerabilities. • Educate and train staff on blockchain security risks, best practices, and preventive measures. • Stay updated on emerging blockchain technologies, threats, and security solutions. • Collaborate with regulatory bodies and adhere to compliance standards related to blockchain technology. • Implement network security measures to protect the blockchain network infrastructure. • Monitor and secure blockchain nodes and endpoints against unauthorized access and attacks. • Analyze blockchain protocols for potential security weaknesses and propose enhancements. • Develop secure architectures for decentralized applications (DApps) and platforms. • Participate in the blockchain community to share knowledge and stay informed on security developments. • Conduct risk assessments to identify and prioritize security risks within blockchain projects. • Implement and manage identity and authentication systems within blockchain ecosystems. • Develop disaster recovery and contingency plans for blockchain systems. • Collaborate with external security experts and auditors for independent security assessments of blockchain systems. • Implement security measures to protect against Sybil attacks and node compromise. • Manage and secure API integrations within blockchain applications. • Develop strategies to secure cross-chain transactions and interoperability among different blockchain platforms. • Implement measures to secure off-chain data and oracles interfacing with blockchain systems. • Ensure secure data storage and privacy measures for blockchain-based systems, considering data immutability. • Address scalability and performance implications from a security perspective within blockchain solutions.	• MyEtherWallet (MEW) • MetaMask • Ledger Nano S and X (Hardware Wallets) • Trezor (Hardware Wallet) • KeepKey (Hardware Wallet) • Electrum Bitcoin Wallet • Trust Wallet • BitGo Cryptocurrency Wallet • Blockchain.info Wallet • CipherTrace • Chainalysis KYT (Know Your Transaction) • Elliptic • Coinfirm AML Platform • Crystal Blockchain Analytics • BlockSeer • Scorechain • Quantstamp (Smart Contract Security) • ConsenSys Diligence (Smart Contract Audit) • CertiK (Blockchain and Smart Contract Verification) • Trail of Bits (Security Assessments and Smart Contract Audits) • OpenZeppelin (Security audits and secure development framework) • Guardtime (Data integrity solutions using blockchain) • Symantec Blockchain Security Monitoring Service • Kaspersky Blockchain Security • Hosho (Smart Contract Audits and Penetration Testing) • Solidified (Smart Contract Audit Platform) • PeckShield (Blockchain Security and Data Analytics) • Fortanix Runtime Encryption (Protects cryptographic keys) • nShield HSMs by Thales (Hardware Security Modules for key management) • IBM Blockchain Platform (With integrated security features) • Gemalto SafeNet KeySecure (Cryptographic key management) • Sentinel Protocol (Collective security intelligence platform for blockchain) • CipherTrace Armada (Designed for banks and financial institutions to monitor blockchain transactions) • AnChain.AI (AI-powered blockchain security) • Blockchain Security by Palo Alto Networks • SecureKey (Identity and authentication using blockchain) • BlockArmor (Blockchain-enabled cybersecurity solution) • BitFury Crystal (Blockchain analytics for AML compliance) • Zero Trust Architecture solutions for blockchain platforms	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Cryptography	Protecting information through the use of codes, so that only those for whom the information is intended can read and process it.	• Symmetric Key Cryptography • Data Encryption Standard (DES) and Triple DES • Advanced Encryption Standard (AES) • Blowfish, Twofish, and other symmetric algorithms • Asymmetric Key Cryptography • Rivest-Shamir-Adleman (RSA) Algorithm • Elliptic Curve Cryptography (ECC) • Diffie-Hellman Key Exchange • Digital Signature Algorithm (DSA) • Hash Functions • Secure Hash Algorithm (SHA) series, including SHA-256 and SHA-3 • Message Digest Algorithm 5 (MD5) • Hash-based Message Authentication Code (HMAC) • Cryptographic Protocols • Transport Layer Security (TLS) and Secure Socket Layer (SSL) • Secure Shell (SSH) • Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG) • Internet Protocol Security (IPSec) • Key Management and Exchange • Key generation, distribution, and storage • Public Key Infrastructure (PKI) and Certificates • Key revocation and renewal mechanisms • Cryptanalysis • Frequency analysis and pattern detection • Differential and linear cryptanalysis • Side-channel attacks and countermeasures • Quantum Cryptography • Quantum key distribution (QKD) • Post-quantum cryptography algorithms • Homomorphic Encryption • Partial Homomorphic Encryption (PHE) • Fully Homomorphic Encryption (FHE) • Digital Signatures • Generation and verification of digital signatures • Role in non-repudiation • Steganography • Hiding information within other files or mediums • Digital watermarking • Random Number Generation • Pseudorandom number generators (PRNGs) • Cryptographically secure pseudorandom number generators (CSPRNGs) • Cryptographic Libraries and Tools • OpenSSL, Crypto++, and other cryptographic software • Hardware Security Modules (HSMs) • Regulatory and Compliance Issues • Encryption export controls • Compliance with global encryption standards • Applications of Cryptography • Secure communications and data transfer • Blockchain and cryptocurrencies • Data integrity verification • Zero-Knowledge Proofs • Interactive and non-interactive zero-knowledge proofs • Applications in privacy-preserving protocols	• Develop and implement cryptographic policies and procedures. • Design and manage secure key management systems. • Conduct regular cryptographic audits and assessments. • Implement encryption solutions for data at rest and in transit. • Ensure compliance with regulatory and legal requirements related to cryptography. • Perform vulnerability assessments of cryptographic implementations. • Stay updated with the latest cryptographic algorithms and best practices. • Securely configure and maintain cryptographic tools and libraries. • Develop and review cryptographic architecture for information systems. • Provide expert advice on cryptographic solutions and strategies. • Collaborate with IT and development teams to integrate encryption into applications and systems. • Manage Public Key Infrastructure (PKI) for digital certificates and signatures. • Train staff on the correct use and understanding of cryptographic technologies. • Respond to and remediate cryptographic security incidents. • Analyze and select appropriate cryptographic algorithms based on security requirements. • Implement and manage hardware security modules (HSMs) and other cryptographic hardware. • Conduct cryptographic research to support organizational security needs. • Evaluate and advise on the use of cryptographic controls in cloud environments. • Develop scripts or tools to automate cryptographic operations and tasks. • Collaborate with vendors and third parties to ensure cryptographic standards are met. • Implement secure hashing for integrity verification and non-repudiation. • Design and enforce policies for cryptographic key lifecycle management. • Monitor the performance and effectiveness of cryptographic systems. • Participate in the design and development of new encryption technologies and products. • Ensure secure deletion and destruction of cryptographic keys as per policy. • Advise on cryptographic aspects of blockchain technology and applications. • Protect against cryptographic attacks such as side-channel attacks, cryptanalysis, etc. • Document cryptographic procedures and key management practices. • Participate in cryptography standards bodies and forums. • Implement measures to secure encrypted data against emerging threats like quantum computing.	• OpenSSL • GnuPG (GPG) • VeraCrypt • BitLocker • FileVault • PGP (Pretty Good Privacy) • RSA Security (RSA SecurID) • AES Crypt • KeePass • LastPass • TrueCrypt (Discontinued, but was widely used) • CipherCloud • HashiCorp Vault • Keybase • Microsoft Azure Key Vault • AWS Key Management Service (KMS) • Google Cloud Key Management Service • Thales eSecurity (formerly Vormetric) • Secure Sockets Layer (SSL) Certificates from authorities like: • DigiCert • Let's Encrypt • Comodo • Symantec • GeoTrust • Thawte • Crypto++ (C++ cryptographic library) • libsodium (Modern, easy-to-use software library for encryption, decryption, signatures, password hashing and more) • Bouncy Castle (Java and C# cryptographic APIs) • PyCryptodome (Python Cryptography Toolkit) • NaCl (Networking and Cryptography library) • Keycloak (Open Source Identity and Access Management) • YubiKey (Hardware security keys by Yubico) • Authy (Two-factor Authentication) • Duo Security (Two-factor Authentication) • Nitrokey (Secure Hardware for encryption, key storage, and two-factor authentication) • AxCrypt (File Encryption Software) • Symantec Encryption Desktop • Entrust Datacard (Digital Security Solutions) • ProtonMail (Encrypted Email Service) • Tutanota (Secure Email Service) • Signal Protocol (End-to-end encryption protocol used by Signal Messenger) • WireGuard (Simple and fast VPN with modern cryptography) • OpenVPN (Open Source VPN) • IPsec (Internet Protocol Security) • Secure Multipurpose Internet Mail Extensions (S/MIME) • CryptoAPI (Microsoft Cryptographic API)	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Forensics	Investigating and analyzing digital attacks to preserve evidence and understand the attack path.	• Incident Response Integration • First response to incidents and initial evidence collection • Coordination with incident response teams • Digital Evidence Collection • Data acquisition from various digital sources (computers, mobile devices, networks) • Live data acquisition and capturing volatile memory • Disk imaging and cloning • Evidence Preservation • Chain of custody documentation • Use of write blockers to prevent data alteration • Secure storage of digital evidence • Data Analysis • File system analysis • Recovery of deleted files and partitions • Log file analysis, including system logs, application logs, and security logs • Network Forensics • Capture and analysis of network traffic and logs • Investigation of network intrusions and anomalies • Email tracing and analysis • Mobile Forensics • Extraction and analysis of data from mobile devices • SIM card analysis • Application and cloud data analysis • Malware Analysis • Static and dynamic analysis of malicious code • Reverse engineering to understand malware functionality and origin • Memory Forensics • Analysis of volatile data (RAM) for evidence of malicious activity • Use of tools for memory dumping and analysis • Cryptocurrency Forensics • Investigation of cryptocurrency transactions • Tracing digital wallets and anonymized transactions • Legal Considerations • Understanding of legal frameworks and compliance requirements • Preparation of evidence for legal proceedings • Expert witness testimony • Reporting • Comprehensive forensic reporting • Timeline construction and event reconstruction • Presentation of findings in a manner understandable by non-technical stakeholders • Forensic Tools and Software • Utilization of forensic software suites (e.g., EnCase, FTK, Autopsy) • Open-source tools and utilities for specific forensic tasks • Cloud Forensics • Challenges and techniques for cloud-based data acquisition and analysis • Investigation of SaaS, PaaS, and IaaS environments • Ethics in Digital Forensics • Adherence to ethical guidelines in investigations • Consideration of privacy issues in digital evidence handling • Advanced Persistent Threats (APT) Forensics • Analysis of sophisticated and prolonged cyber attacks • Identifying indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) • Forensic Readiness Planning • Preparing organizations for efficient and effective forensic investigations • Integration of forensic capabilities into security policies and procedures	• Conduct digital forensic investigations on various types of systems (e.g., computers, mobile devices, networks). • Preserve and analyze data from electronic sources to identify potential evidence. • Ensure the integrity and security of evidence through proper chain of custody procedures. • Utilize forensic tools and software for data recovery, analysis, and documentation. • Identify attack vectors and tactics, techniques, and procedures (TTPs) used by attackers. • Collaborate with incident response teams to contain and mitigate breaches. • Prepare detailed forensic reports documenting the evidence found, analysis methods used, and conclusions. • Testify as an expert witness in legal proceedings regarding forensic findings. • Stay updated with the latest advancements in digital forensic technologies and methodologies. • Develop and maintain forensic analysis capabilities, including setting up forensic laboratories and toolkits. • Provide recommendations to improve security posture based on forensic findings. • Train law enforcement, cybersecurity teams, and other relevant personnel in digital forensics. • Reverse engineer malware and analyze malicious code to understand behavior and impact. • Conduct post-breach analysis to determine the scope and impact of incidents. • Perform memory forensics to analyze system memory for evidence of compromise. • Establish and follow standard operating procedures (SOPs) for forensic processes. • Work with external forensic experts and law enforcement agencies as needed. • Conduct network forensics to examine network traffic and logs for signs of unauthorized access or malicious activity. • Implement and manage forensic monitoring tools to detect and investigate suspicious activities. • Develop scripts and tools to automate forensic analysis tasks. • Secure and manage forensic evidence storage to preserve the integrity of data. • Collaborate with cybersecurity engineers to close security gaps revealed during forensic investigations. • Participate in cybersecurity incident simulations and exercises to improve forensic readiness. • Advise on legal and regulatory compliance issues related to digital evidence and forensics. • Analyze file systems, including NTFS, FAT32, exFAT, HFS+, and ext4, for forensic evidence. • Collaborate with stakeholders to understand and fulfill forensic analysis requirements. • Continuously update forensic analysis techniques to cope with evolving digital environments and devices. • Ensure forensic activities are conducted in an ethical and legally compliant manner.	• EnCase Forensic • FTK (Forensic Toolkit) • Autopsy + The Sleuth Kit • Magnet AXIOM • X-Ways Forensics • Cellebrite UFED • Oxygen Forensic Detective • Paraben Corporation tools (E3 Forensic Platform) • AccessData Mobile Phone Examiner Plus (MPE+) • Volatility Framework • Wireshark • SANS SIFT (SANS Investigative Forensic Toolkit) • ProDiscover Forensic • BlackBag BlackLight • Belkasoft Evidence Center • Nuix Workstation • MOBILedit Forensic Express • Recon ITR (In-theater Review) • Paladin by Sumuri • Forensic Explorer • Passware Kit Forensic • ElcomSoft tools (e.g., Elcomsoft Phone Breaker, Elcomsoft Forensic Disk Decryptor) • Internet Evidence Finder (IEF) by Magnet Forensics • Kroll Artifact Parser and Extractor (KAPE) • Redline by FireEye • Bulk Extractor • Cyber Triage • Ghiro - Digital Image Forensics Tool • NetworkMiner • RAM Capturer by Belkasoft • DEFT (Digital Evidence & Forensics Toolkit) • Browser History Viewer • SQLite Forensic Reporter • Sysinternals Suite by Microsoft • Harlan Carvey's RegRipper • ExifTool - For metadata extraction • Hashdeep - For file hashing and integrity • F-Response - For remote forensics and analysis • Binwalk - Firmware Analysis Tool • gdb - The GNU Project Debugger • IDA Pro - Disassembler and debugger • HxD - Hex Editor and Disk Editor • Axiom Cyber by Magnet Forensics - For remote collection • NFAT (Network Forensic Analysis Tool) • Cuckoo Sandbox - Automated malware analysis • HELIX3 – Incident response live CD • MacQuisition by BlackBag - Forensics data acquisition and imaging tool for Mac • Aircrack-ng – For WiFi network security auditing	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Governance, Risk, and Compliance (GRC)	Ensuring that organizational processes adhere to established regulations and standards.	• Governance • Establishing clear organizational structures, roles, and responsibilities • Development and implementation of security policies and procedures • Strategic alignment of IT with business objectives • IT governance frameworks (e.g., COBIT, ITIL) • Risk Management • Identification and assessment of cybersecurity risks • Implementation of risk mitigation strategies • Continuous risk monitoring and reporting • Risk assessment methodologies (e.g., NIST SP 800-30, ISO 27005) • Compliance Management • Adherence to legal and regulatory requirements (e.g., GDPR, HIPAA, SOX) • Compliance with industry standards and frameworks (e.g., ISO 27001, NIST) • Regular compliance audits and assessments • Privacy impact assessments • Policy Management • Creation and maintenance of security policies • Distribution and communication of policies across the organization • Regular review and updating of policies • Incident Management and Response • Establishment of incident response teams and processes • Implementation of escalation procedures for incidents • Reporting and documentation of incidents • Post-incident analysis and reporting to regulatory bodies if necessary • Third-party Risk Management • Assessment and monitoring of third-party vendors and partners • Vendor risk management policies and procedures • Due diligence and ongoing monitoring • Business Continuity and Disaster Recovery Planning • Development of business continuity (BC) and disaster recovery (DR) plans • Regular BC/DR testing and updates • Ensuring BC/DR compliance with standards • Training and Awareness • Employee training on cybersecurity policies and best practices • Awareness programs on current threats and safe practices • Specialized training for IT and security staff • Audit and Assurance • Internal and external audits of cybersecurity controls • Regular security assessments • Remediation of identified gaps and deficiencies • Information Security Management • Implementation of an Information Security Management System (ISMS) • Data classification and handling according to sensitivity and regulatory requirements • Secure data lifecycle management • Technology Compliance • Ensuring secure configuration of IT systems and applications • Patch and vulnerability management • Secure development practices for in-house software • Reporting and Documentation • Regular reporting to senior management and stakeholders • Documentation of GRC processes and outcomes • Maintenance of evidence and artifacts for audit purposes • Culture and Ethics • Fostering a security-conscious culture within the organization • Ethical conduct and decision-making in line with organizational values • Continuous Improvement • Implementing feedback loops for GRC processes • Utilization of GRC software and tools for efficiency • Benchmarking and best practices comparison	• Develop and implement GRC policies and procedures. • Conduct risk assessments to identify security vulnerabilities and compliance gaps. • Implement risk management strategies and controls to mitigate identified risks. • Ensure compliance with relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, PCI-DSS). • Monitor and report on compliance status and risk levels to management and stakeholders. • Manage documentation and evidence required for compliance audits and certifications. • Develop and oversee security awareness training programs to ensure staff understand GRC requirements. • Collaborate with IT and business units to integrate GRC practices into organizational processes. • Coordinate with external auditors and assessors during compliance audits and assessments. • Implement and manage tools and technologies for GRC management (e.g., GRC platforms). • Advise on security and compliance implications of new projects, technologies, and business initiatives. • Create and maintain a risk register to track and prioritize risks across the organization. • Develop incident response plans and procedures to address risks and compliance violations. • Monitor changes in laws, regulations, and standards that affect the organization's GRC posture. • Facilitate risk analysis and business impact analysis for critical systems and processes. • Establish metrics and key performance indicators (KPIs) to measure GRC effectiveness. • Perform vendor and third-party risk assessments to ensure compliance with organizational standards. • Coordinate remediation efforts for identified risks and compliance issues. • Provide guidance on data protection and privacy practices to uphold compliance requirements. • Manage contracts and agreements to include necessary security and compliance clauses. • Conduct periodic reviews and updates of GRC policies to reflect changes in the threat landscape or regulatory environment. • Foster a culture of security and compliance within the organization. • Liaise with legal counsel to understand regulatory requirements and implications for security policies. • Coordinate GRC initiatives across multiple locations and jurisdictions for organizations with international operations. • Participate in industry forums and groups to stay informed on GRC trends and best practices. • Implement a GRC framework (e.g., COBIT, NIST) tailored to the organization's needs and objectives. • Establish a governance structure to oversee GRC activities, including committees or working groups. • Manage and resolve conflicts between security practices and business operations to align with GRC goals.	• RSA Archer • MetricStream • IBM OpenPages with Watson • SAP GRC • ServiceNow Governance Risk and Compliance • LogicManager • SAI Global Compliance 360 • Galvanize (formerly ACL and Rsam) • Lockpath Keylight Platform • Diligent Compliance • OneTrust • ZenGRC by Reciprocity • Qualys Compliance Suite • NAVEX Global RiskRate • Thomson Reuters Connected Risk • Modulo Risk Manager • Seclore • ProcessGene GRC Software Suite • Nasdaq BWise • Enablon Governance Risk and Compliance Software • Resolver • Continuity Logic • Symfact • ComplianceQuest • VComply • Isolocity • StandardFusion • Riskonnect • Alyne • Ideagen Pentana • 6clicks Risk and Compliance • Predict360 by 360factors • Hyperproof • SureCloud Compliance Management • Workiva Wdesk • LogicGate Risk Cloud • Convercent by OneTrust • Netwrix Auditor	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Security Awareness Training	Educating employees and users about the importance of cybersecurity measures and practices.	• Introduction to Cybersecurity • Basics of cybersecurity • Importance of cybersecurity in protecting organization and personal data • Cyber Threat Landscape • Overview of current cyber threats (e.g., malware, phishing, ransomware) • Real-world examples of significant cyberattacks • Cybersecurity Best Practices • Creating and managing strong passwords • Safe internet browsing practices • Secure use of social media • Email Security • Identifying phishing and spear-phishing attempts • Safe email practices (e.g., not opening suspicious attachments) • Reporting suspicious emails • Safe Computing • Keeping software and systems up to date • Use of antivirus and antimalware software • Secure Wi-Fi use, including public Wi-Fi security • Data Protection and Privacy • Understanding personal identifiable information (PII) • Best practices for handling and sharing sensitive information • GDPR and other data protection regulations • Physical Security • Securing physical access to devices and sensitive areas • Protecting against shoulder surfing and visual hacking • Device theft prevention • Social Engineering Defense • Recognizing and responding to social engineering tactics • Importance of verifying requests for sensitive information • Mobile Device Security • Securing smartphones and tablets • Risks associated with app downloads • Lost or stolen device procedures • Remote Work and Home Network Security • Securing home networks • Best practices for remote work security • Use of VPNs for secure remote access • Incident Reporting and Response • Procedures for reporting cybersecurity incidents • Role of employees in incident response • Importance of timely reporting • Regulatory Compliance Overview • Employee responsibilities under compliance regimes (HIPAA, PCI-DSS, etc.) • Consequences of non-compliance for individuals and organizations • Security Policies and Procedures • Overview of organization-specific policies • Acceptable use policy for IT resources • Consequences of policy violations • Interactive and Practical Exercises • Phishing simulations • Security quizzes and games • Scenario-based learning • Ongoing Education and Training • Continuous learning opportunities • Regular updates on new threats and security practices • Encouragement of personal responsibility for cybersecurity	• Develop and implement a comprehensive security awareness training program. • Identify target audiences within the organization and tailor training content to their roles. • Create engaging training materials, including presentations, videos, and handouts. • Deliver regular training sessions, workshops, and webinars on various cybersecurity topics. • Educate employees on recognizing and responding to phishing attacks and other social engineering tactics. • Teach best practices for password management and data protection. • Inform about the dangers of public Wi-Fi and secure methods for remote work. • Cover secure browsing practices and the risks associated with downloading and installing unauthorized software. • Explain the legal and business consequences of non-compliance with cybersecurity policies. • Incorporate training on mobile device security and the secure use of personal devices in the workplace. • Update and revise training materials regularly to address new and emerging cyber threats. • Develop and administer quizzes and assessments to measure training effectiveness. • Provide specific training on compliance requirements relevant to the organization (e.g., GDPR, HIPAA). • Organize cybersecurity awareness events and campaigns to keep security top of mind. • Use simulated phishing exercises to educate employees on the threats and test their awareness. • Offer advanced training modules for IT staff and employees with access to sensitive information. • Track employee training completion and compliance with mandatory training requirements. • Gather feedback from employees on training sessions to identify areas for improvement. • Collaborate with HR to integrate cybersecurity training into onboarding processes for new hires. • Stay updated with the latest cybersecurity risks and trends to ensure training content is current. • Liaise with external cybersecurity experts and organizations to source or co-develop training materials. • Communicate regularly with management and stakeholders about the status and effectiveness of the training program. • Develop a reporting mechanism to highlight the impact of training on reducing security incidents. • Foster a culture of security within the organization through ongoing education and engagement. • Provide resources and support for employees who wish to learn more about cybersecurity best practices. • Advocate for and secure budget and resources needed to maintain and expand the security awareness training program.	• KnowBe4 Security Awareness Training • Proofpoint Security Awareness Training • Mimecast Awareness Training • Cofense PhishMe • Terranova Security Awareness Training • Kaspersky Automated Security Awareness Platform • Webroot Security Awareness Training • Sophos Phish Threat • Security Mentor Security Awareness Training • MediaPRO Security Awareness Training • ESET Cybersecurity Awareness Training • Wombat Security Technologies (acquired by Proofpoint) • Curricula Security Awareness Training • Inspired eLearning Security Awareness Training • CyberRiskAware • Phriendly Phishing • SafeStack Academy • NortonLifeLock Cyber Safety • NINJIO Security Awareness Training • Barracuda PhishLine • CybSafe • Popcorn Training – Security Awareness Training • Living Security • Hoxhunt • Ataata (acquired by Mimecast) • Habitu8 • Click Armor • CyberSmartCultureAI Security Culture Platform	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Zero Trust Architecture	A security model that does not automatically trust entities within the security perimeter.	• Zero Trust Principles • Never trust, always verify • Assume breach mentality • Least privilege access control • Identity Verification • Multi-factor Authentication (MFA) • Single Sign-On (SSO) solutions • Identity and Access Management (IAM) • Device Security • Device authentication and authorization • Endpoint security and compliance checks • Secure device management and access control • Network Segmentation • Micro-segmentation to isolate environments and protect sensitive data • Network access control based on device and user identity • Least Privilege Access • Role-based access control (RBAC) • Just-in-Time (JiT) and Just-Enough-Access (JEA) principles • Privileged Access Management (PAM) • Application Security • Application-aware access policies • Secure application development practices • Application and API gateways for secure application access • Data Protection • Encryption of data at rest and in transit • Data classification and access policies • Secure data storage and sharing protocols • Monitoring and Analytics • Continuous monitoring and logging of network and user activity • Anomaly detection using artificial intelligence and machine learning • Security Information and Event Management (SIEM) systems • Threat Intelligence and Response • Integration of threat intelligence feeds • Automated response to detected threats • Regular security assessments and threat hunting • Security Policies and Governance • Zero Trust security policy development and enforcement • Governance, Risk, and Compliance (GRC) strategies • Auditing and compliance reporting • Networking Infrastructure • Software-Defined Networking (SDN) for dynamic policy enforcement • Secure access service edge (SASE) convergence of networking and security services • Encryption protocols and secure communication channels • User Education and Awareness • Training on Zero Trust principles and practices • Phishing and social engineering defense training • Awareness of security policies and procedures • Cloud Security • Cloud Access Security Brokers (CASB) • Secure cloud configurations and compliance • Cloud environment access control • Automation and Orchestration • Automated policy enforcement and access control • Security orchestration, automation, and response (SOAR) • Dynamic access adjustments based on risk assessment • Vendor and Third-party Security • Assessing and managing third-party risks • Secure integration of external services and applications • Vendor access based on Zero Trust principles • Continuous Improvement • Periodic review and adaptation of Zero Trust policies • Benchmarking and maturity models for Zero Trust adoption	• Conduct a thorough assessment of the current security architecture and identify areas for implementing Zero Trust principles. • Develop and implement a Zero Trust security strategy aligned with organizational goals and risk tolerance. • Design network segmentation to limit lateral movement within the network. • Implement strong user identity verification mechanisms, including multi-factor authentication (MFA). • Ensure strict access control policies and enforce least privilege access for all users, devices, and applications. • Develop and apply micro-segmentation strategies to secure sensitive data and critical assets. • Configure and maintain security enforcement points (e.g., firewalls, access gateways) to monitor and control traffic based on Zero Trust policies. • Integrate security solutions for comprehensive visibility and enforcement across all layers of the architecture (network, endpoint, application, data, identity). • Automate security policy enforcement to dynamically adapt access controls and permissions based on real-time context and risk assessment. • Utilize behavior analytics and machine learning to detect abnormal behavior indicative of potential security threats. • Perform continuous monitoring and logging of all network and user activities for anomaly detection and forensic analysis. • Regularly review and adjust Zero Trust policies and controls based on evolving threats and changing organizational needs. • Collaborate with IT operations, development, and business units to embed Zero Trust principles into the organization's culture and processes. • Provide training and awareness to employees on the importance of Zero Trust security and best practices for compliance. • Conduct penetration testing and vulnerability assessments to validate the effectiveness of Zero Trust controls and identify areas for improvement. • Engage with vendors and industry experts to stay informed on the latest Zero Trust technologies, standards, and practices. • Create detailed documentation on Zero Trust architecture implementations, policies, procedures, and incident response plans. • Respond to security incidents within a Zero Trust environment, leveraging detailed access and activity logs to support investigation and remediation efforts. • Advise on regulatory compliance implications of Zero Trust architecture and ensure that implementations meet applicable legal and industry standards. • Manage projects to upgrade legacy systems and applications to be compatible with Zero Trust requirements. • Develop metrics and indicators to measure the effectiveness and maturity of the Zero Trust architecture. • Collaborate with external stakeholders, including regulatory bodies, industry groups, and cybersecurity communities, to share knowledge and best practices related to Zero Trust security.	• Cisco Duo Security • Zscaler Zero Trust Exchange • Palo Alto Networks Prisma Access • Akamai Enterprise Application Access • Okta Identity Cloud • Illumio Adaptive Security Platform • Google Cloud BeyondCorp Enterprise • Microsoft Azure Active Directory (Conditional Access) • Check Point Software Technologies Infinity • Symantec (Broadcom) Secure Access Cloud • Fortinet Zero Trust Access • VMware Workspace ONE • CrowdStrike Falcon Zero Trust • CyberArk Privileged Access Security • Centrify Zero Trust Privilege Services • Appgate SDP • Forcepoint Dynamic Edge Protection • Trend Micro Zero Trust Secure Access • Cloudflare Access • Idaptive by CyberArk • F5 BIG-IP Access Policy Manager (APM) • Airlock Digital Application Allowlisting • Trustwave Zero Trust Security Services • Proofpoint Meta • Cato Networks SASE Cloud • Menlo Security Isolation Platform • Wandera Zero Trust Network Access • Guardicore Centra Security Platform • ColorTokens Xtended ZeroTrust™ Platform • Bitglass Total Cloud Security • Silverfort Unified Identity Protection Platform • Preempt Security (now part of CrowdStrike) • Thycotic Secret Server • Saviynt Enterprise Identity Cloud • SecureAuth Identity Platform • Versa Networks Secure Access Service Edge (SASE) • Netskope Security Cloud • Untangle NG Firewall • Lookout Secure Access Service Edge (SASE) • Twingate • Aruba ClearPass Policy Manager • Juniper Networks Zero Trust Security	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Cyber-Physical Systems Security	Protecting the cyber aspects of physical systems like infrastructure and industrial control systems.	• Risk Assessment and Management • Identifying and evaluating risks to CPS • Developing and implementing risk mitigation strategies • Network Security • Secure communication protocols for CPS networks • Firewall and intrusion detection systems tailored for CPS • Network segmentation and access control • System Resilience and Redundancy • Designing resilient CPS architectures • Implementing redundancy for critical components and systems • Data Security and Privacy • Encryption of data at rest and in transit • Secure data storage and access controls • Anonymization and privacy-preserving technologies • Device and Endpoint Security • Secure boot and hardware roots of trust • Firmware integrity verification • Device authentication and authorization mechanisms • Identity and Access Management • Role-based access control (RBAC) for system users • Multi-factor authentication (MFA) for critical access points • Management of digital identities and credentials • Incident Detection and Response • Real-time monitoring and anomaly detection • Forensic analysis tools and techniques for CPS • Incident response planning and execution • Software Security • Secure software development lifecycle (SDLC) for CPS • Vulnerability assessment and patch management • Application whitelisting and software restriction policies • Physical Security Integration • Protection of physical access to CPS components and facilities • Surveillance and monitoring of physical threats • Environmental controls and disaster recovery planning • Supply Chain Security • Assessing the security of third-party components and vendors • Managing the risks associated with outsourced CPS elements • Secure software and hardware update mechanisms • Regulatory Compliance and Standards Adherence • Adhering to industry-specific security standards and regulations • Documentation and auditing for compliance verification • Engagement with regulatory and standardization bodies • Operational Technology (OT) Security • Distinct security measures for OT environments • Separation and secure integration of OT and IT networks • Specialized security training for OT personnel • Human Factors and Training • Security awareness and training programs for system operators and users • Addressing social engineering and insider threats • Human-machine interface (HMI) security considerations • Interoperability and Compatibility • Ensuring secure integration of CPS components and systems • Standards for cross-domain communication and data exchange • Backward compatibility and legacy system security • Emerging Technologies • Security implications of incorporating AI and ML into CPS • Blockchain for secure and transparent CPS operations • Security for CPS in cloud and edge computing environments • Continuous Monitoring and Improvement • Ongoing assessment of security posture • Adaptation to emerging threats and technologies • Security metrics and benchmarking for continuous improvement	• Conduct risk assessments for cyber-physical systems (CPS) to identify vulnerabilities and potential threats. • Implement security measures tailored to the unique requirements of CPS, including industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. • Design and enforce access control policies for physical devices and network interfaces. • Secure communications between CPS components, employing encryption and secure protocols. • Monitor CPS environments for unusual activities or signs of cyberattacks using specialized tools and techniques. • Respond to and investigate security incidents within cyber-physical environments, including forensic analysis of ICS/SCADA systems. • Develop and maintain security policies and procedures specific to CPS environments. • Collaborate with engineering and operational teams to incorporate security best practices into the design, deployment, and maintenance of CPS. • Conduct regular vulnerability scans and penetration testing on CPS components to evaluate their resilience against attacks. • Implement network segmentation and isolation strategies to limit the spread of potential cyberattacks within CPS networks. • Develop disaster recovery and business continuity plans that address the unique aspects of CPS and related critical infrastructure. • Provide training and awareness programs to educate staff on the cybersecurity risks associated with CPS and promote secure operational practices. • Work with vendors and third-party service providers to ensure that components and services used in CPS meet security requirements. • Stay informed about the latest threats, vulnerabilities, and technological advances related to CPS security. • Participate in industry forums, working groups, and information sharing and analysis centers (ISACs) focused on CPS security. • Advise on regulatory compliance matters related to the security of CPS, including requirements specific to critical infrastructure sectors. • Implement measures to secure CPS against emerging threats, such as ransomware attacks targeting ICS/SCADA systems. • Develop and utilize simulation and modeling tools to assess the security posture of CPS and predict the impact of potential cyberattacks. • Integrate artificial intelligence and machine learning techniques to enhance the detection of anomalies and threats in CPS environments. • Collaborate with physical security teams to ensure a comprehensive approach to securing cyber-physical systems. • Develop custom security solutions to address unique challenges in protecting CPS, given their operational constraints and requirements. • Coordinate with national and international cybersecurity initiatives and standards bodies to contribute to and align with broader CPS security efforts.	• Nozomi Networks Guardian • Dragos Platform • Claroty Continuous Threat Detection • Schneider Electric EcoStruxure Security Expert • Siemens Industrial Security Services • Cisco Industrial Network Director • Honeywell Forge Cybersecurity Suite • Palo Alto Networks IoT Security • Fortinet FortiGate Next-Generation Firewall • Tenable.ot (formerly Indegy) • Rockwell Automation Threat Detection Services • Belden Tripwire Industrial Visibility • Forescout SilentDefense • CyberX (acquired by Microsoft) • Kaspersky Industrial CyberSecurity • Check Point Quantum Security Gateways for Industrial Control Systems • Trend Micro TXOne Networks • Sophos XG Firewall with Xstream • ABB Ability Cyber Security for Control Systems • McAfee Application Control for Industrial Systems • Radiflow iSID Industrial Threat Detection System • IBM Security QRadar SIEM • Yokogawa Industrial Cyber Security • Wallix Bastion for Critical Infrastructure Protection • Keysight (formerly Ixia) Threat Simulator • Armis Asset Visibility and Security • Sentryo (acquired by Cisco) Industrial IoT/OT Solutions • Owl Cyber Defense Solutions (Data Diode Solutions) • Waterfall Security Solutions Unidirectional Gateways • Darktrace Industrial Immune System • Bayshore Networks Industrial Cyber Protection • Inductive Automation Ignition (for SCADA with security modules) • Raz-Lee Security iSecurity Anti-Ransomware • OPSWAT Critical Infrastructure Protection • SecurityMatters (acquired by Forescout) SilentDefense • Mocana TrustPoint (Embedded Security for IoT) • Sasa Software GateScanner Critical Infrastructure Protection • L7 Defense Ammune™ for Industrial and IoT Security	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Privacy	Addresses protecting personal information and ensuring compliance with privacy laws.	• Data Identification and Classification • Identification of personal and sensitive data • Classification based on sensitivity and regulatory requirements • Privacy Laws and Regulations Compliance • General Data Protection Regulation (GDPR) • California Consumer Privacy Act (CCPA) • Health Insurance Portability and Accountability Act (HIPAA) • Other national and international privacy laws and frameworks • Privacy Policies and Procedures • Development and implementation of privacy policies • Regular reviews and updates to policies • Procedures for privacy policy enforcement • Data Protection Techniques • Data encryption for data at rest and in transit • Anonymization and pseudonymization of personal data • Secure data storage and destruction practices • Consent Management • Mechanisms for obtaining, managing, and documenting user consent • Options for individuals to manage their consent and preferences • Access Control and Identity Management • Role-based access controls (RBAC) for data access • Secure authentication methods • Logging and monitoring of access to personal data • Data Subject Rights • Procedures for data subjects to exercise their rights (e.g., access, rectification, erasure, and data portability) • Response mechanisms for data subject requests • Data Breach Response and Notification • Incident response plans that include provisions for data breaches • Mechanisms for notifying affected individuals and regulators • Privacy Impact Assessments (PIAs) • Regular assessments to identify and mitigate privacy risks in projects and processes • Documentation of PIAs and risk mitigation measures • Data Minimization and Purpose Limitation • Practices to limit data collection to what is strictly necessary • Ensuring data is used only for its original intended and consented purpose • Vendor and Third-Party Data Processor Management • Assessments and agreements to ensure vendors comply with privacy requirements • Monitoring and auditing of third-party data processors • Privacy by Design and Default • Integration of privacy considerations into the early stages of project and product development • Ensuring that default settings favor privacy protection • Employee Training and Awareness • Regular training on privacy policies, legal requirements, and best practices • Promotion of a privacy-aware culture within the organization • International Data Transfers • Compliance with regulations governing cross-border data transfers • Use of legal mechanisms like Standard Contractual Clauses (SCCs) and Privacy Shield • Monitoring and Audit • Regular auditing of privacy practices and controls • Continuous monitoring for compliance with privacy laws and policies • Emerging Privacy Challenges • Addressing privacy concerns related to new technologies (e.g., IoT, AI, and blockchain) • Adapting to changes in privacy law and technology	• Conduct privacy impact assessments to identify how personal data is collected, used, stored, and shared. • Implement data protection measures, including encryption, anonymization, and pseudonymization of personal data. • Develop and maintain privacy policies and procedures in compliance with relevant privacy laws (e.g., GDPR, CCPA). • Design and enforce data access controls to ensure only authorized personnel can access personal information. • Monitor systems and networks for privacy breaches or violations of personal data. • Respond to privacy incidents, including breach detection, investigation, and notification in accordance with legal requirements. • Conduct regular audits to ensure compliance with privacy laws and regulations. • Provide privacy training and awareness programs to educate employees about handling personal data and privacy best practices. • Manage data subject requests, such as access, rectification, erasure, and data portability requests. • Advise on privacy by design and default principles during the development and deployment of new technologies and systems. • Coordinate with legal and compliance teams to keep abreast of new privacy legislation and regulatory requirements. • Implement and manage tools for data discovery and classification to identify and protect personal information. • Develop and maintain documentation of data processing activities and privacy compliance measures. • Participate in vendor and third-party assessments to ensure their compliance with privacy standards and requirements. • Advocate for and embed privacy considerations into the organizational culture and decision-making processes. • Collaborate with IT and security teams to ensure privacy controls are integrated within cybersecurity frameworks. • Develop and test privacy incident response plans and procedures. • Manage and secure customer consent and preference settings in line with privacy regulations. • Monitor privacy trends, advisories, and best practices to continuously improve the organization's privacy posture. • Address privacy aspects within contracts, agreements, and third-party engagements. • Implement measures for secure collection, transmission, and deletion of personal data. • Collaborate with data protection officers (DPOs) or privacy officers, where applicable, to align cybersecurity and privacy strategies. • Establish metrics and reporting mechanisms to measure privacy program effectiveness and compliance. • Ensure secure development practices are followed to protect personal data in applications and systems from the outset.	• OneTrust Privacy Management Software • TrustArc Privacy Platform • BigID Data Intelligence Platform • WireWheel Privacy Management Platform • Securiti PrivacyOps • Datagrail Privacy Platform • Integris Software (now part of OneTrust) • Spirion Data Privacy Manager • AvePoint Compliance Guardian • Exterro Privacy Management • Varonis Data Security Platform • Symantec Data Loss Prevention (DLP) • IBM Guardium Data Protection • Cisco Data Privacy and Compliance Solutions • RSA Data Privacy and Security • Talend Data Fabric for Data Governance • Informatica Data Privacy and Protection • Microsoft Compliance Manager • Privacy Analytics Eclipse • Nymity Privacy Management Software (now part of TrustArc) • IDology for Identity Verification and Compliance • Jumio for Online Identity Verification • DPOrganizer Privacy Management Software • Ethyca Data Privacy and Compliance • IAPP (International Association of Privacy Professionals) Resources and Tools • Collibra Data Governance • Tresorit for Secure Cloud Storage • ProtonMail for Encrypted Email • Signal Private Messenger for Encrypted Messaging • Threema for Secure Messaging and Calls • NordVPN for Secure Internet Connection and Privacy • Tor Browser for Anonymous Web Browsing • DuckDuckGo for Private Web Search • Brave Browser with Built-in Privacy Features • LastPass for Secure Password Management • Dashlane for Password Management and Online Privacy • Apple App Privacy Report for iOS Apps Monitoring • Mozilla Firefox Privacy Protections • 1Password for Secure Password and Information Storage • Cookiebot for Cookie Consent and Compliance • Quantcast Choice for GDPR and CCPA Consent Solution • Osano for Data Privacy and Compliance • Wire for Secure and Private Communications • Startpage Private Search Engine • ExpressVPN for Encrypted Internet Access	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Malware Analysis	The practice of dissecting malware to understand its functionality, origin, and potential impact.	• Basic Analysis • Static Properties Analysis: Examining basic properties without executing malware (hashes, strings, file format) • Signature Recognition: Identifying known malware through signatures • Static Code Analysis • Disassembly: Converting binary code into assembly language for analysis • Decompilation: Attempting to convert compiled code back into source code • Code Review: Analyzing the source or decompiled code for malicious functionality • Dynamic Analysis • Behavioral Analysis: Running malware in a controlled environment to observe its behavior • Sandboxing: Isolating the malware in a virtual environment to prevent it from causing harm • Network Traffic Analysis: Monitoring network activity generated by the malware • Advanced Dynamic Analysis • Debugging: Stepping through malware execution to understand its process • Hooking and API Monitoring: Intercepting and monitoring function calls and system events • Memory Dump Analysis: Examining the memory contents for malicious patterns or artifacts • Automated Analysis Tools • Malware Analysis Platforms (e.g., Cuckoo Sandbox, FireEye) • Online Scanning Services (e.g., VirusTotal, Malwr) • Reverse Engineering Tools (e.g., IDA Pro, Ghidra) • Threat Intelligence Gathering • Extracting Indicators of Compromise (IoCs) • Correlating analysis findings with threat intelligence databases • Attribution: Attempting to trace malware back to its source • Malware Typology • Identifying types of malware (virus, worm, trojan, ransomware, etc.) • Understanding malware tactics, techniques, and procedures (TTPs) • Forensic Analysis • Analyzing artifacts left by malware on infected systems • Timeline Reconstruction: Establishing the sequence of events during the infection • Countermeasures • Developing signatures or rules to detect and block malware • Suggesting mitigation strategies to prevent infection or limit damage • Cryptographic Analysis • Analyzing the use of cryptographic routines in malware • Identifying command and control (C2) server communication encryption • Root Cause Analysis • Identifying vulnerabilities or configuration issues that allowed the malware infection • Suggesting patches or configuration changes to prevent similar incidents • Report Writing • Documenting findings, analysis techniques, and recommendations • Communicating the risk and impact to stakeholders • Ethics and Legal Considerations • Ethical guidelines for malware analysis • Legal considerations, especially related to privacy and unauthorized access • Malware Evolution and Trends • Researching emerging malware threats and trends • Adapting analysis techniques to evolving malware complexity • Collaboration and Sharing • Sharing findings with the cybersecurity community • Contributing to malware analysis repositories and forums	• Collect and catalog malware samples for analysis. • Perform static analysis to examine malware without executing it, analyzing the code structure and potential payloads. • Conduct dynamic analysis by running malware in a controlled, isolated environment to observe its behavior. • Use reverse engineering tools and techniques to understand malware's inner workings and objectives. • Identify malware communication channels, including command and control (C2) servers. • Analyze malware delivery mechanisms, such as phishing emails or compromised websites. • Decode and analyze obfuscated code used in malware to hide its true purpose. • Develop signatures or indicators of compromise (IoCs) that can be used to detect malware presence. • Collaborate with threat intelligence teams to share findings and correlate malware with known threat actors or campaigns. • Document analysis findings, including technical details, impact assessment, and mitigation recommendations. • Update malware threat intelligence databases with new information. • Contribute to the development or enhancement of automated malware analysis tools and systems. • Provide guidance to incident response teams for malware removal and system remediation based on analysis results. • Educate IT and security teams on new malware threats and defense strategies. • Stay current with the latest malware trends and analysis techniques. • Participate in cybersecurity community forums and platforms to exchange malware information and defense tactics. • Assess the risk and potential impact of malware on the organization's environment. • Research and utilize sandboxing technologies for safer malware execution and analysis. • Develop scripts or tools to automate aspects of malware analysis. • Collaborate with law enforcement or cybersecurity organizations for sharing malware information and combating cyber threats. • Test security controls and defenses against specific malware to evaluate their effectiveness. • Analyze malware encryption techniques, including ransomware encryption mechanisms. • Participate in peer reviews of malware analysis findings to validate conclusions and share knowledge. • Collaborate with software developers to advise on secure coding practices that can mitigate malware risks. • Lead or participate in training sessions or workshops on malware analysis for cybersecurity staff. • Assess the vulnerability of organizational systems and networks to specific malware threats. • Work with external security vendors and researchers to obtain malware samples and share analysis outcomes.	• IDA Pro (Interactive DisAssembler) • Ghidra • OllyDbg • WinDbg • Radare2 • Binary Ninja • x64dbg • GDB (GNU Debugger) • PEiD • VirusTotal • Hybrid Analysis • Joxean Koret's DiE (Detect It Easy) • Cuckoo Sandbox • Maltego • Wireshark • Fiddler • Tcpdump • Burp Suite • Apktool (for Android APK analysis) • JADX (Java Decompiler) • dnSpy (.NET Decompiler) • Volatility (for memory forensics) • Rekall (another memory forensic framework) • Process Hacker • Process Monitor (Sysinternals) • RegShot (for registry comparison) • HxD Hex Editor • YARA (pattern matching tool) • Strings (for binary data scanning) • The Sleuth Kit (for disk analysis) • Autopsy (graphical interface for The Sleuth Kit) • Sysinternals Suite (for Windows analysis) • REMnux (Linux distribution for malware analysis) • FireEye FLARE VM (Windows-based malware analysis distribution) • Kaspersky GReAT's KAPE (Kroll Artifact Parser and Extractor) • Joe Sandbox • Any.run • Immunity Debugger • Shellter (for PE infector and dynamic malware analysis) • PDFiD and PDF-Parser (for PDF malware analysis) • VirusBlokAda Vba32 AntiRootkit • VMRay Analyzer • Sophos Sandstorm • FortiGuard Sandbox • Comodo Valkyrie • CrowdStrike Falcon Sandbox • RSA NetWitness Investigator • ThreatGrid • Intezer Analyze • Cerbero Suite • CAPEv2 (Malware Configuration And Payload Extraction) • SANS Investigative Forensics Toolkit (SIFT) • Triage (by Hatching) • PackerDetect (for identifying packed executables) • Capa (for detecting capabilities in executable files)	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Cyber Insurance	Financial product that businesses and individuals can purchase to help mitigate potential financial impacts following a cybersecurity incident.	• Understanding Cyber Insurance • Definitions and key concepts in cyber insurance • The importance of cyber insurance in risk management strategies • Types of Cyber Insurance Coverage • First-party coverage: Direct losses to the policyholder • Third-party coverage: Liability to others caused by a cybersecurity incident • Coverage for data breaches, ransomware attacks, and business interruption • Legal costs and regulatory fines coverage • Costs related to crisis management and public relations • Assessment of Cyber Risks • Identifying and evaluating potential cyber risks faced by an organization • Risk assessment methodologies specific to cyber insurance • Policy Terms and Conditions • Understanding exclusions, deductibles, and coverage limits • Key clauses, such as retroactive and extended reporting periods • Underwriting Process • Criteria and processes used by insurers to assess risk and determine premiums • The role of cybersecurity audits and assessments in underwriting • Claims Process • Procedures for filing a claim following a cybersecurity incident • Documentation and proof requirements • Timelines and steps involved in claims validation and settlement • Cyber Insurance Market Trends • Evolving cyber threat landscape and its impact on cyber insurance • Trends in cyber insurance policy offerings and premiums • Cybersecurity Best Practices and Insurance • The impact of implementing cybersecurity best practices on insurance premiums and coverage • Insurer recommendations for cybersecurity controls and measures • Incident Response Planning and Cyber Insurance • Integration of cyber insurance into incident response planning • How cyber insurance can support and facilitate effective incident response • Regulatory and Legal Considerations • Compliance with regulations and laws affecting cyber insurance • Legal precedents and cases relevant to cyber insurance claims • Selecting a Cyber Insurance Policy • Factors to consider when choosing a cyber insurance provider and policy • The role of insurance brokers and advisors in the selection process • Renewal and Review of Cyber Insurance Policies • Regular review and adjustment of cyber insurance coverage based on changing risk profiles • Renewal processes and considerations • Challenges and Controversies in Cyber Insurance • Issues related to attribution and act of war exclusions • Challenges in quantifying cyber risks and potential losses • Emerging Issues in Cyber Insurance • Coverage for emerging threats like deepfakes, AI-driven attacks, and cryptojacking • The future of cyber insurance in the context of rapidly evolving technology and threats	• Assess the organization's cybersecurity risks to determine the appropriate level of cyber insurance coverage needed. • Review and understand the terms and conditions of cyber insurance policies. • Collaborate with legal, finance, and insurance professionals to select the best cyber insurance policy. • Ensure compliance with cyber insurance policy requirements, such as implementing specific security controls. • Prepare and maintain documentation required for obtaining and maintaining cyber insurance coverage. • Conduct regular cybersecurity risk assessments to update insurance providers on the risk profile. • Facilitate communication between cybersecurity teams and insurance providers during the policy acquisition and renewal processes. • Develop incident response plans that align with cyber insurance policy requirements. • Report cybersecurity incidents to insurance providers in accordance with policy terms. • Gather and prepare evidence of damages and losses for cyber insurance claims. • Assist in the cyber insurance claims process by providing technical insights and analysis on cybersecurity incidents. • Monitor changes in the cybersecurity landscape to adjust cyber insurance coverage as necessary. • Advise on improvements to cybersecurity practices to potentially reduce cyber insurance premiums. • Coordinate cybersecurity audits or assessments required by cyber insurance providers. • Work with insurance brokers to understand the nuances of different cyber insurance products. • Stay informed about trends and changes in the cyber insurance market. • Liaise with other departments (e.g., HR, IT, legal) to ensure organization-wide understanding and compliance with cyber insurance policy requirements. • Train IT and cybersecurity teams on the importance of cyber insurance and their roles in maintaining coverage. • Evaluate the effectiveness of current cyber insurance coverage in mitigating financial impacts of cybersecurity incidents. • Maintain records of cybersecurity incidents, responses, and recoveries to support future insurance claims and policy renewals. • Collaborate with external cybersecurity experts as needed for insurance assessments or claims. • Monitor the organization's adherence to cybersecurity best practices as required by cyber insurance policies. • Participate in cybersecurity awareness initiatives to reduce the risk of incidents that could impact insurance claims. • Manage the retention and destruction of sensitive information in accordance with cyber insurance policy terms. • Assess third-party vendors and partners for risks that could affect cyber insurance coverage and liabilities.	• Risk Management Information Systems (RMIS): • Ventiv Technology • Origami Risk • Marsh ClearSight • Cyber Risk Assessment and Management Platforms: • BitSight Security Ratings • RiskRecon • SecurityScorecard • Prevalent Third-Party Risk Management • FICO Cyber Risk Score • Compliance Management Tools: • OneTrust • TrustArc • LogicManager • NAVEX Global RiskRate • Incident Response Planning Tools: • RSA Archer • D3 Security Incident Response • Business Continuity Planning (BCP) Software: • Fusion Risk Management • Everbridge • Assurance Software • Data Breach Cost Calculators: • IBM & Ponemon Institute's Cost of Data Breach Calculator • NetDiligence Cyber Calculator • Cybersecurity Frameworks (for aligning organizational security postures, potentially impacting cyber insurance premiums or eligibility): • NIST Cybersecurity Framework • ISO/IEC 27001 • CIS Controls • Vulnerability Scanning and Management Tools: • Tenable Nessus • Qualys Cloud Platform • Rapid7 InsightVM • Legal and Regulatory Compliance Tools: • ComplyAssistant • VeraSafe • Cybersecurity Training Platforms (to potentially reduce cyber insurance premiums by demonstrating proactive risk mitigation): • KnowBe4 • Proofpoint Security Awareness Training • Mimecast Awareness Training •	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Embedded Systems Security	Secures embedded systems, which are computer systems with a dedicated function within a larger electrical or mechanical system.	• Introduction to Embedded Systems Security • Understanding embedded systems and their importance • Overview of security challenges specific to embedded systems • Threat Modeling for Embedded Systems • Identifying potential threats and vulnerabilities in embedded systems • Assessing risk levels and potential impact • Secure Boot and Trusted Execution • Implementing secure boot processes to ensure integrity of bootloaders and firmware • Utilizing Trusted Platform Modules (TPM) or Hardware Security Modules (HSM) for secure operations • Firmware Security • Techniques for secure firmware development and deployment • Firmware update mechanisms and secure firmware over-the-air (FOTA) updates • Hardware Security • Designing hardware with security in mind (e.g., secure hardware elements, tamper-resistant packaging) • Hardware-based cryptographic features and accelerators • Software Security • Applying secure coding practices for embedded software development • Static and dynamic analysis of embedded software • Access Control and Authentication • Implementing strong access control mechanisms • Authentication techniques tailored to embedded systems (e.g., device authentication) • Network Security for Embedded Systems • Securing communication protocols commonly used in embedded systems • Protection against network-based attacks targeting embedded devices • Encryption and Data Protection • Utilizing encryption to protect data stored on and transmitted by embedded systems • Key management best practices in an embedded context • Operating System Security • Security features and considerations for embedded operating systems • Choosing and hardening an operating system for embedded use • IoT and Embedded Systems Security • Security considerations for IoT devices and environments • IoT-specific security protocols and standards • Supply Chain Security • Mitigating risks associated with the hardware and software supply chain • Conducting security assessments of third-party components • Regulatory and Compliance Issues • Understanding regulatory requirements impacting embedded systems security • Compliance with industry-specific security standards • Incident Response and Recovery • Planning and executing incident response specific to embedded systems • Recovery procedures for compromised embedded systems • Security Testing for Embedded Systems • Penetration testing and vulnerability assessments for embedded devices • Simulation and testing tools specifically for embedded environments • Emerging Threats and Future Challenges • Keeping up with emerging security threats targeting embedded systems • Designing embedded systems with future security challenges in mind	• Conduct security assessments and vulnerability analyses on embedded systems. • Develop security strategies tailored to protect embedded systems against cyber threats. • Design and implement secure boot mechanisms to ensure the integrity of firmware and software at startup. • Implement encryption and cryptographic solutions to protect data at rest and in transit within embedded systems. • Develop and enforce access control and authentication mechanisms for embedded devices. • Harden embedded operating systems and software applications against attacks. • Configure and manage firewalls and intrusion detection systems (IDS) specific to embedded environments. • Regularly patch and update firmware and software on embedded devices to address security vulnerabilities. • Monitor embedded systems for unauthorized access and suspicious activities. • Respond to and investigate security incidents involving embedded systems. • Implement data protection and privacy measures in compliance with relevant regulations. • Advocate for and apply secure coding practices during the development of embedded software. • Collaborate with product design and development teams to integrate security into the lifecycle of embedded products. • Educate engineering and development teams on potential security risks associated with embedded systems. • Utilize threat modeling to identify and mitigate potential attack vectors specific to embedded systems. • Develop secure communication protocols for interconnected embedded devices. • Manage the secure configuration and decommissioning of embedded devices. • Conduct pen-testing exercises on embedded systems to identify exploitable vulnerabilities. • Participate in the development and maintenance of security policies and standards for embedded system security. • Advise on the selection and implementation of security hardware modules like Trusted Platform Modules (TPM) in embedded systems. • Stay abreast of trends and advancements in embedded systems security and cyber threats targeting such systems. • Collaborate with external security researchers and the cybersecurity community to address vulnerabilities in embedded systems. • Document security designs, assessments, and incidents specific to embedded systems. • Ensure business continuity and disaster recovery plans include strategies for embedded system security. • Implement secure update mechanisms for remote firmware and software updates. • Coordinate with vendors and suppliers to ensure the security of third-party components used in embedded systems. • Develop automated tools and scripts to streamline security processes related to embedded systems. • Leverage machine learning and AI techniques to enhance security monitoring and anomaly detection in embedded systems.	• IAR Embedded Workbench • Arm Keil MDK (Microcontroller Development Kit) • Segger Embedded Studio • Microchip MPLAB X IDE • Atmel Studio (now part of Microchip Technology) • NXP MCUXpresso IDE • STMicroelectronics STM32CubeIDE • Wind River VxWorks • Green Hills Software Integrity RTOS • QNX Neutrino RTOS • FreeRTOS • µC/OS-II and µC/OS-III • Embedded Linux (various distributions such as Yocto Project, Buildroot) • wolfSSL for embedded SSL/TLS • mbedTLS (formerly PolarSSL) • OpenSSL (with considerations for footprint on embedded systems) • TinyCrypt for lightweight crypto operations • Secure Elements like Atmel CryptoAuthentication or Infineon OPTIGA Trust • Hardware Security Modules (HSMs) for key storage and cryptographic operations • JTAG Debuggers (Segger J-Link, ST-LINK, Xilinx Platform Cable) • Lauterbach TRACE32 for debugging and trace • Black Duck Software for identifying and securing open source components • Checkmarx for static code analysis • Klocwork by Perforce for static code analysis and security • Synopsys Coverity for static analysis and security testing • LDRA tool suite for software analysis and testing • Codenomicon Defensics for fuzz testing • BeagleBone or Raspberry Pi for prototyping security solutions • Tenable Nessus for vulnerability scanning (with considerations for embedded environments) • Metasploit Framework for penetration testing (with considerations for embedded environments) • Wireshark for network protocol analysis, including communication with embedded devices • Binwalk for firmware analysis • Ghidra for reverse engineering and binary analysis • Radare2 for reverse engineering and binary analysis • ChipWhisperer for side-channel attack analysis • JTAGulator for identifying JTAG pinouts on hardware • OWASP Embedded Application Security Project for guidelines and best practices	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Quantum Cryptography	Utilizes principles of quantum mechanics to secure data and communications in a way that is theoretically immune to hacking.	• Foundations of Quantum Cryptography • Principles of Quantum Mechanics relevant to cryptography • Quantum bits (qubits) and their properties • Quantum superposition and entanglement • Quantum Key Distribution (QKD) • BB84 protocol and its variations • E91 protocol for entanglement-based key distribution • Security proofs and real-world implementations of QKD • Quantum repeaters for extending QKD range • Quantum Cryptography Systems • Hardware requirements for quantum cryptographic systems • Quantum random number generators (QRNGs) • Practical challenges and solutions in deploying QKD systems • Post-Quantum Cryptography (PQC) • Cryptographic algorithms resistant to quantum computer attacks • Comparative analysis of PQC algorithms (lattice-based, hash-based, multivariate, etc.) • Integration of PQC algorithms into existing cryptographic frameworks • Quantum Computing and Cryptographic Security • Potential impact of quantum computing on traditional encryption methods • Shor's algorithm and its implications for RSA, ECC, and other cryptographic algorithms • Grover's algorithm and its effect on symmetric cryptographic algorithms • Quantum Entanglement in Cryptography • Utilization of entangled particle pairs in secure communication • Concepts of quantum teleportation and its cryptographic applications • Quantum Cryptanalysis • Potential strategies for quantum cryptanalysis • Quantum algorithms for breaking existing cryptographic schemes • Quantum Secure Communication • Protocols for quantum secure direct communication (QSDC) • Countermeasures against quantum eavesdropping • Security Considerations in Quantum Cryptography • Physical and operational security of quantum cryptographic devices • Quantum channel security and noise resilience • Side-channel attacks in quantum cryptography • Quantum Cryptography Standards and Protocols • Efforts towards standardizing quantum cryptographic techniques • Quantum cryptography in information security standards • Legal and Ethical Considerations in Quantum Cryptography • Regulatory challenges of quantum cryptography • Ethical considerations in the development and use of quantum technologies • Future of Quantum Cryptography • Emerging trends and future research directions in quantum cryptography • Quantum networks and the long-term vision of a quantum internet • Educational Resources and Training in Quantum Cryptography • Academic and online resources for learning about quantum cryptography • Professional training and certifications in quantum technologies	• Study and apply quantum cryptographic principles such as quantum key distribution (QKD) to secure communications. • Develop and implement quantum-resistant algorithms to safeguard data against future quantum computer threats. • Collaborate with research teams to stay abreast of advancements in quantum computing and quantum cryptography. • Design and conduct experiments to test the security and feasibility of quantum cryptographic systems. • Assess the organization's current cryptographic practices for vulnerabilities to quantum computing threats. • Integrate quantum cryptographic solutions into existing security architectures to enhance data protection. • Develop secure communication protocols based on quantum cryptography for sensitive information exchange. • Educate IT and cybersecurity teams on the potential impact of quantum computing on cybersecurity. • Establish partnerships with quantum technology providers and participate in quantum cryptography pilots and projects. • Conduct risk assessments to identify areas where quantum cryptography can provide the most significant security benefits. • Participate in standardization efforts for quantum cryptography and quantum-resistant algorithms. • Provide expertise on transitioning from traditional cryptographic methods to quantum-secure alternatives. • Design and implement secure key management practices for quantum cryptographic systems. • Monitor the performance and security of quantum cryptographic implementations. • Prepare documentation and reports on quantum cryptography projects, including design specifications, testing results, and deployment plans. • Advise on the procurement of quantum cryptographic devices and technologies. • Develop contingency and disaster recovery plans that account for quantum cryptographic systems. • Facilitate the secure integration of quantum cryptographic technologies with cloud services and infrastructure. • Evaluate the long-term viability and scalability of quantum cryptographic solutions for organizational needs. • Lead training sessions and workshops on quantum cryptography for technical and non-technical audiences. • Engage with academic and industrial research communities to explore innovative applications of quantum cryptography. • Ensure compliance with legal and regulatory requirements relevant to quantum cryptography. • Address challenges related to interoperability between quantum and non-quantum cryptographic systems. • Contribute to the development of policies and guidelines for the ethical use of quantum cryptography. • Participate in cybersecurity forums and conferences to share knowledge and insights on quantum cryptography.	• ID Quantique Quantum Key Distribution (QKD) Systems • QuintessenceLabs qStream Quantum Random Number Generator • Qubitekk Quantum Key Distribution • Toshiba Quantum Key Distribution System • MagiQ Technologies Quantum Cryptography Solutions • Quantum Xchange Phio TX • SeQureNet Quantum Cryptography Solutions • PQShield Post-Quantum Cryptography (PQC) Solutions • ISARA Radiate Quantum-safe Toolkit • Crypto Quantique QuarkLink IoT Security Platform • Cambridge Quantum Computing t|ket⟩ Quantum Software Stack • IBM Qiskit for Quantum Computing • Microsoft Quantum Development Kit • Google Cirq for Quantum Computing • Rigetti Forest Quantum Computing Platform • AIT Austrian Institute of Technology QKD Systems • NuCrypt Photonic Quantum Communication Devices • QuantumCTek Quantum Communication Devices • Qunnect Quantum Networking Devices • SK Telecom IDQ QKD Systems (In partnership with ID Quantique) • EvolutionQ Security Consulting and Software for Quantum Risk Management • Quantum Delta NL Quantum Network Products and Services • BT Quantum Secure Communications Solutions • QRate Quantum Random Number Generators • SpeQtral Quantum Secure Communication Solutions • Quantum Communication Victoria (QCV) QKD Systems • Crypta Labs Quantum Random Number Generator • KETS Quantum Security Quantum Cryptography Solutions • Toshiba Quantum Random Number Generator • Artos Quantum Cryptography Solutions	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
DevSecOps	DevSecOps integrates security practices within the DevOps process, aiming to ensure the development, deployment, and maintenance of secure software.	• DevSecOps Fundamentals • Principles of DevSecOps • The culture shift towards security in DevOps • Benefits of integrating security within the DevOps pipeline • Secure Coding Practices • Security considerations in software design • Secure coding standards and guidelines • Code review practices for security • Automated Security Tools Integration • Static Application Security Testing (SAST) • Dynamic Application Security Testing (DAST) • Software Composition Analysis (SCA) for open-source vulnerabilities • Container scanning and security • Continuous Integration and Continuous Deployment (CI/CD) Security • Securing CI/CD pipelines • Automation of security testing and checks • Secure artifact management • Identity and Access Management (IAM) • Secure handling of credentials and secrets • Role-based access control (RBAC) within CI/CD pipelines • Secure service-to-service communication • Infrastructure as Code (IaC) Security • Security scanning for IaC configurations • Best practices for securing cloud and container configurations • Compliance as code • Vulnerability Assessment and Management • Vulnerability identification and prioritization • Automated vulnerability scanning in pipelines • Patch management strategies • Threat Modeling and Risk Assessment • Proactive threat modeling in early development stages • Risk assessment methodologies applicable to DevSecOps • Incident Response and Monitoring • Real-time monitoring and alerting • Incident response plans that integrate with DevOps workflows • Post-mortem analysis and continuous feedback loops • Compliance and Governance • Ensuring software compliance with regulatory standards • Governance models that support DevSecOps practices • Audit trails and security reporting • Collaboration and Training • Fostering a collaborative culture between DevOps and Security teams • Security training and awareness programs for developers • Knowledge sharing and communication tools • Cloud Security • Securing cloud-native applications • Cloud service provider security tools and features • Strategies for managing multi-cloud environments securely • Container and Orchestration Security • Best practices for container security • Security considerations in orchestration tools (e.g., Kubernetes) • Network policies for microservices • Secrets Management • Tools and practices for managing secrets securely in development and production • Encryption and rotation of secrets • Security Observability • Integrating security observability into the development lifecycle • Tools and practices for gaining visibility into application and infrastructure security	• Integrate security tools and processes into the Continuous Integration/Continuous Deployment (CI/CD) pipeline. • Perform automated security scanning and testing in development and production environments. • Develop and enforce security policies and guidelines for software development practices. • Collaborate with development teams to ensure secure coding practices are followed. • Conduct threat modeling and risk assessments for applications and infrastructure. • Manage and configure security monitoring tools to detect and respond to vulnerabilities and attacks. • Implement and manage identity and access control mechanisms in DevOps environments. • Facilitate the integration of security into agile development processes. • Monitor and analyze code repositories for security issues introduced in code commits. • Automate the patching process for software and infrastructure vulnerabilities. • Lead security awareness and training initiatives for development and operations teams. • Collaborate with IT and operations teams to ensure secure configuration management. • Conduct regular security reviews and audits of applications and infrastructure. • Respond to and remediate security incidents in collaboration with incident response teams. • Develop and maintain documentation for security processes and procedures within the DevSecOps framework. • Leverage container security tools and practices to secure containerized applications. • Manage secrets and credentials securely in DevOps workflows. • Advocate for a security-first culture within the development and operations teams. • Stay updated with the latest cybersecurity threats, vulnerabilities, and best practices. • Evaluate and recommend new security tools and technologies for the DevSecOps pipeline. • Participate in code reviews with a focus on identifying security issues. • Collaborate with external security auditors and consultants for third-party security assessments. • Ensure compliance with regulatory and legal requirements related to information security. • Facilitate the creation of automated security dashboards to report on security metrics and KPIs. • Collaborate on the development of disaster recovery and business continuity plans for DevOps environments. • Engage with the broader cybersecurity and DevOps communities to share knowledge and best practices. • Guide the development and implementation of microservices security strategies. • Implement network segmentation and Zero Trust security models in DevOps practices. • Analyze application dependencies for known vulnerabilities using software composition analysis tools. • Coordinate with cloud service providers to ensure cloud-based DevOps environments meet security standards.	• Jenkins for Continuous Integration/ Continuous Deployment (CI/CD) • GitLab CI/CD for source code management and CI/CD • GitHub Actions for CI/CD and automation • Docker for containerization • Kubernetes for container orchestration • Ansible for configuration management and deployment • Terraform for infrastructure as code • Chef for configuration management • Puppet for configuration management • SonarQube for static code analysis • Fortify Software Security Center for application security • Checkmarx for static and dynamic code analysis • Veracode for application security testing • Aqua Security for container security • Twistlock (now part of Prisma Cloud by Palo Alto Networks) for container and cloud security • Snyk for dependency scanning and vulnerability management • Black Duck by Synopsys for open-source security and license compliance • JFrog Xray for artifact analysis and security • HashiCorp Vault for secrets management • CyberArk Conjur for secrets management in DevOps environments • OWASP ZAP for dynamic application security testing (DAST) • Nessus by Tenable for vulnerability scanning • Qualys Cloud Platform for vulnerability management • Rapid7 InsightVM for vulnerability management • Splunk for log management and SIEM • Elastic Stack (Elasticsearch, Logstash, Kibana) for log management and analysis • Prometheus and Grafana for monitoring and visualization • Datadog for cloud-scale monitoring • New Relic for performance monitoring • WhiteSource for software composition analysis • Clair by CoreOS for static analysis of vulnerabilities in containers • Trivy by Aqua Security for container vulnerability scanning • GitSecured by Checkmarx for Git repository scanning • CircleCI for CI/CD • Brigade for scripting CI/CD pipelines in Kubernetes • Argo CD for Kubernetes-based GitOps continuous delivery • CloudSploit by Aqua Security for cloud security posture management • Bridgecrew by Prisma Cloud for infrastructure as code security	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE

Domains	Description	Sections	Cybersecurity Engineer Tasks, Duties and Responsibilities	Tools and Software Recommended	Training Required	Certification Required
Artificial Intelligence and Machine Learning	Artificial Intelligence (AI) and Machine Learning (ML) in the context of cybersecurity encompass a wide array of applications and methodologies designed to enhance the protection of digital assets and infrastructure.	• AI and ML Fundamentals for Cybersecurity • Overview of AI and ML concepts applicable to cybersecurity • Types of ML models (supervised, unsupervised, reinforcement learning) • Natural Language Processing (NLP) for cybersecurity applications • Threat Detection and Analysis • Anomaly detection models for identifying unusual activities • Predictive analytics for forecasting potential security threats • ML algorithms for malware classification and analysis • Fraud Detection and Prevention • AI-driven fraud detection systems for identifying fraudulent transactions • Behavioral biometrics for authentication and fraud prevention • AI in anti-phishing efforts • Vulnerability Management • ML techniques for vulnerability identification and prioritization • AI-powered tools for automated vulnerability assessments • Predictive modeling for vulnerability exploitation probability • Network Security • AI-based network intrusion detection systems (IDS) • ML algorithms for network traffic analysis and anomaly detection • AI in secure network architecture design and management • Incident Response and Remediation • AI-driven automated incident response systems • ML models for root cause analysis and impact assessment • AI for generating and applying security patches • Security Information and Event Management (SIEM) • Integration of AI and ML with SIEM for enhanced data analysis • AI for automating the classification and correlation of security events • ML-enhanced threat hunting and incident investigation • Identity and Access Management (IAM) • AI/ML in adaptive authentication mechanisms • Behavioral analytics for user and entity behavior analytics (UEBA) • Risk-based authentication models • Data Protection and Privacy • AI algorithms for data loss prevention (DLP) • ML models for identifying and classifying sensitive information • AI for automating data privacy controls and compliance • AI and ML Ethics in Cybersecurity • Ethical implications of using AI and ML in cybersecurity • Bias and fairness in AI/ML models • Explainability and transparency of AI/ML decisions • Adversarial AI and ML • Techniques in adversarial machine learning and AI-driven attacks • AI and ML model robustness against evasion and poisoning attacks • Defensive strategies against adversarial AI attacks • Emerging Technologies and Future Trends • Quantum machine learning for cybersecurity • Federated learning for collaborative, privacy-preserving AI models • AI and ML in blockchain security and smart contract analysis • AI and ML Tools and Platforms • Popular AI and ML frameworks and libraries for cybersecurity (e.g., TensorFlow, PyTorch) • Specialized AI/ML cybersecurity tools and platforms • Training and Development for AI and ML in Cybersecurity • Resources and courses for learning AI and ML applications in cybersecurity • Skill development and workforce training challenges	• Design and implement AI/ML-based security solutions to identify and mitigate threats. • Develop machine learning models for anomaly detection and predictive analytics in cybersecurity. • Integrate AI algorithms into existing security systems for enhanced threat detection. • Conduct research on emerging AI/ML threats and develop defensive strategies. • Utilize natural language processing (NLP) for analyzing and filtering malicious content. • Create and manage datasets for training and testing machine learning models. • Monitor and evaluate the performance of AI/ML models to ensure their accuracy and effectiveness. • Stay updated with the latest advancements in AI/ML technologies and security applications. • Collaborate with data scientists and security analysts to refine AI/ML security solutions. • Implement AI-driven automation for routine cybersecurity tasks to improve efficiency. • Design AI/ML models to detect and respond to zero-day vulnerabilities and advanced persistent threats (APTs). • Develop security measures to protect AI/ML systems from adversarial attacks and data poisoning. • Educate and train cybersecurity teams on incorporating AI/ML into their workflows. • Conduct AI/ML vulnerability assessments to identify potential risks in deploying AI/ML models. • Collaborate with IT teams to ensure the secure deployment of AI/ML models and applications. • Utilize AI/ML techniques for improving security incident response and forensic analysis. • Apply AI/ML algorithms for secure user authentication and access control. • Develop ethical guidelines for the responsible use of AI/ML in cybersecurity. • Use AI/ML for enhancing network security through traffic analysis and intrusion detection. • Engage in academic and industry collaborations to advance AI/ML security research. • Participate in conferences and workshops to share knowledge and learn about AI/ML in cybersecurity. • Document AI/ML model development processes, including data sourcing, model training, and deployment strategies. • Ensure compliance with legal and regulatory requirements related to AI/ML and data privacy. • Develop backup and recovery procedures for AI/ML models to prevent data loss. • Integrate AI/ML-driven insights into cybersecurity reporting and decision-making processes.	• TensorFlow • PyTorch • Keras • Scikit-learn • H2O.ai • RapidMiner • IBM Watson • Amazon SageMaker • Microsoft Azure Machine Learning • Google Cloud AI Platform • Darktrace • Cylance • CrowdStrike Falcon • Vectra AI • Sift Science • Endgame • Deep Instinct • Malwarebytes Nebula • SentinelOne • FortiAI by Fortinet • Cisco Cognitive Threat Analytics • Splunk Machine Learning Toolkit • Exabeam Advanced Analytics • LogRhythm AI Engine • Recorded Future • FireEye Helix • Palo Alto Networks Cortex • Check Point Infinity • Sophos Intercept X with Deep Learning • Carbon Black Predictive Security Cloud • Symantec Targeted Attack Analytics • ArcSight Intelligence (formerly Interset) • D3 Security SOAR Platform with AI • SecBI Autonomous Investigation • Fidelis Elevate with Machine Learning • Awake Security NDR Platform • Niara by HPE (Behavioral Analytics) • Uptycs Threat Detection with osquery • Elastic Security (Elasticsearch with Machine Learning) • IBM Qradar with Watson • Anomali with AI and ML for Threat Intelligence • AlienVault USM Anywhere (Threat Detection and Response) • WireX Systems NDR (Network Detection and Response) • Cybereason MalOp Detection Engine • Vectra Cognito Detect • Aqua Security Trivy (Container Security) • Tenable.ai for Vulnerability Management	RCCE Level 1, RCCE Level 2, RCCI, CCO	RCCE