ROCHESTON CYBERSECURITY UNIVERSITY PARTNERSHIP MODEL

# COMPREHENSIVE CYBERSECURITY ACADEMIC PROGRAMS CATALOG

2026 - 2027 Academic Year

**Bachelor of Science | Master of Science | Graduate Diploma | Professional Certificates**

Powered by the Rocheston Cybernotes

RCCE Certification | ANAB Accredited | US DoD 8140 Approved

This catalog is a comprehensive reference for partner universities adopting the Rocheston Cybersecurity Academic Framework. All programs, course codes, descriptions, credit structures, and lab requirements are designed for direct integration into existing university systems. Partner institutions may customize program names, elective offerings, and scheduling while maintaining the core Rocheston curriculum architecture.

# Table of Contents

# 1. About the Rocheston Academic Partnership

## THE LIVING CURRICULUM ADVANTAGE

Traditional cybersecurity education suffers from a fundamental structural flaw: by the time a textbook is published, the threat landscape has already shifted. Universities spend 18 to 24 months developing curriculum that is obsolete before the first student enrolls. The Rocheston Academic Partnership eliminates this gap entirely.

Through the Rocheston Cybernotes platform, every lecture, lab environment, case study, and assessment is updated continuously. When a zero-day vulnerability like Log4Shell, MOVEit, or the CrowdStrike incident makes global headlines, the curriculum reflects it within 48 hours. Students never learn from yesterday's threats. They learn from today's battlefield.

## WHAT PARTNER UNIVERSITIES RECEIVE

- Complete course syllabi with learning objectives mapped to NICE Framework, NIST CSF 2.0, and MITRE ATT&CK
- Rocheston CyberRange access: hyper-realistic virtual enterprise environments with live threat simulation
- Rocheston Cybernotes: continuously updated digital textbooks, video lectures, and hands-on exercises
- RCCE certification pathway embedded directly into degree programs
- Vulnerability Vines AI: proprietary threat intelligence platform exclusive to RCCE-certified engineers
- AINA OS and Rose X OS lab environments pre-configured for all courses
- Faculty training and certification support
- Annual curriculum review and refresh by Rocheston's threat research team
- Marketing collateral, recruitment support, and employer partnership network

## ACCREDITATION & RECOGNITION

The RCCE (Rocheston Certified Cybersecurity Engineer) credential is ANAB Accredited under ISO/IEC 17024 and approved under the US Department of Defense Directive 8140 (formerly DoD 8570). This means every graduate of an RCCE-aligned program carries a credential recognized by federal agencies, defense contractors, and Fortune 500 enterprises globally.

# 2. Program Overview Matrix

| Program | Type | Credits | Duration | Format | RCCE Level |
|---|---|---|---|---|---|
| **B.S. Cybersecurity Engineering** | Bachelor | 120 | 4 Years | On-Campus / Hybrid | Level 1 & 2 |
| **B.S. Cyber Defense & Intelligence** | Bachelor | 120 | 4 Years | On-Campus / Hybrid | Level 1 & 2 |
| **M.S. Cyber Defense & Strategy** | Master | 36 | 18 Months | 100% Online | Level 3 |
| **M.S. AI Security & Autonomous Systems** | Master | 36 | 18 Months | Online / Hybrid | Level 3 |
| **Grad. Diploma: Offensive Security** | Diploma | 24 | 12 Months | Online / Hybrid | Level 2 |
| **Grad. Diploma: Cyber GRC** | Diploma | 24 | 12 Months | 100% Online | Level 2 |
| **Cert: Cybersecurity Foundations** | Certificate | N/A | 24 Weeks | Bootcamp | Level 1 |
| **Cert: Penetration Testing** | Certificate | N/A | 16 Weeks | Intensive | Level 2 |
| **Cert: Cloud Security Architecture** | Certificate | N/A | 12 Weeks | Online | Level 2 |
| **Cert: AI & ML Security** | Certificate | N/A | 12 Weeks | Online | Level 2 |
| **Cert: ICS/SCADA Security** | Certificate | N/A | 12 Weeks | Online / Hybrid | Level 2 |

# 3. Bachelor of Science in Cybersecurity Engineering (B.S.CE)

**CIP Code:** 11.1003 - Computer and Information Systems Security
**Degree Code:** BSCE-RCU-2025
**Total Credits:** 120 (42 General Education + 78 Major)
**Duration:** 4 Years / 8 Semesters (Full-Time)
**Delivery:** On-Campus with Hybrid Option (up to 40% Online)
**RCCE Path:** RCCE Level 1 (End of Year 2) + RCCE Level 2 (End of Year 4)
**Accreditation:** ABET-Ready Computing Curriculum + ANAB ISO/IEC 17024

## PROGRAM MISSION

The Bachelor of Science in Cybersecurity Engineering prepares students to design, build, and defend the digital infrastructure of modern enterprises. Unlike traditional computer science programs that treat security as an elective afterthought, this program embeds security thinking into every course from day one. Graduates emerge as security-first engineers capable of architecting resilient systems, conducting offensive assessments, and leading incident response operations.

## PROGRAM LEARNING OUTCOMES (PLOS)

Upon completion of this program, graduates will be able to:

- Design and implement secure network architectures using defense-in-depth principles across on-premises, cloud, and hybrid environments
- Conduct penetration testing and vulnerability assessments using industry-standard methodologies (PTES, OWASP, NIST SP 800-115)
- Develop secure applications using secure coding practices in Python, C/C++, Java, and JavaScript
- Perform digital forensics and incident response following chain-of-custody procedures admissible in legal proceedings
- Analyze malware samples using static and dynamic analysis techniques in sandboxed environments
- Implement and manage identity and access management systems including Zero Trust Architecture
- Communicate complex security concepts to technical and non-technical stakeholders through written reports and oral presentations
- Apply ethical reasoning and legal frameworks to cybersecurity decision-making

## CURRICULUM ARCHITECTURE

The program is structured in four phases that progressively build from foundational computing to advanced security specialization. Each phase culminates in a capstone lab exercise conducted in the Rocheston CyberRange.

### Year 1: Foundations of Secure Computing

The first year establishes the mathematical, computational, and networking fundamentals that underpin all cybersecurity operations. Students build their first lab environment using Rose X OS and begin working in the CyberRange within the first month of enrollment.

## Fall Semester (Year 1)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 1010** | Introduction to Cybersecurity: Threat Landscape & Career Paths | 3 | None | 2 |
| **CYB 1020** | Linux Systems Administration & Kernel Hardening | 4 | None | 4 |
| **CYB 1030** | Python Programming for Security Professionals | 3 | None | 2 |
| **CSC 1100** | Discrete Mathematics for Computing | 3 | None | 0 |
| **ENG 1010** | Technical Writing & Communication | 3 | None | 0 |

## Spring Semester (Year 1)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 1040** | Network Fundamentals: TCP/IP, DNS, DHCP, & Packet Analysis | 4 | CYB 1010 | 4 |
| **CYB 1050** | Windows Server Administration & Active Directory Security | 3 | CYB 1020 | 3 |
| **CYB 1060** | Database Security Fundamentals (SQL, NoSQL, Encryption at Rest) | 3 | CYB 1030 | 2 |
| **CSC 1200** | Calculus for Data Science & Cryptography | 3 | CSC 1100 | 0 |
| **GEN 1020** | Introduction to Ethics & Law in Technology | 3 | None | 0 |

**Year 1 CyberRange Capstone:** Network Reconnaissance Challenge. Students must map a simulated enterprise network of 200+ endpoints, identify 15 planted vulnerabilities, and submit a professional vulnerability assessment report.

## Year 2: Security Operations & Defense

The second year transforms students from IT generalists into security practitioners. Students operate a full Security Operations Center (SOC) in the CyberRange, monitor live threat feeds, and begin their RCCE Level 1 certification preparation.

### Fall Semester (Year 2)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 2010** | Security Operations Center (SOC) Fundamentals & SIEM Deployment | 4 | CYB 1040 | 6 |
| **CYB 2020** | Cryptography: Symmetric, Asymmetric, PKI & Post-Quantum Algorithms | 3 | CSC 1200 | 2 |
| **CYB 2030** | Vulnerability Assessment & Management Lifecycle | 3 | CYB 1040 | 4 |
| **CYB 2040** | Identity & Access Management: Zero Trust Architecture | 3 | CYB 1050 | 2 |
| **CSC 2100** | Data Structures & Algorithms for Security Applications | 3 | CYB 1030 | 0 |

### Spring Semester (Year 2)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 2050** | Threat Hunting & Intelligence Analysis (MITRE ATT&CK Framework) | 4 | CYB 2010 | 6 |
| **CYB 2060** | Secure Software Development Lifecycle (SSDLC) & DevSecOps | 3 | CYB 1030, CYB 1060 | 3 |
| **CYB 2070** | Wireless & Mobile Security: WiFi, Bluetooth, Cellular, IoT | 3 | CYB 1040 | 3 |
| **CYB 2080** | Operating System Internals & Exploit Primitives | 3 | CYB 1020, CSC 2100 | 2 |
| **STA 2100** | Statistics & Probability for Security Analytics | 3 | CSC 1200 | 0 |

**Year 2 CyberRange Capstone:** SOC Operations Marathon. A 48-hour continuous SOC simulation where student teams monitor, detect, triage, and respond to 50+ attack scenarios across a simulated enterprise. Students earn RCCE Level 1 certification eligibility upon successful completion.

## Year 3: Offensive Security & Specialization

Year three is where students become operators. The curriculum shifts from defensive monitoring to offensive operations. Students learn to think like adversaries, conducting full-scope penetration tests, reverse engineering malware, and exploiting web applications. Two elective tracks allow specialization.

### Fall Semester (Year 3)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 3010** | Ethical Hacking & Penetration Testing Methodology (PTES) | 4 | CYB 2030, CYB 2080 | 8 |
| **CYB 3020** | Web Application Security (OWASP Top 10, API Security, WAF Bypass) | 3 | CYB 2060 | 4 |
| **CYB 3030** | Cloud Security Architecture: AWS, Azure, GCP | 3 | CYB 2040 | 3 |
| **CYB 3040** | Digital Forensics & Evidence Handling | 4 | CYB 2050 | 6 |
| **CYB 3E01** | Elective I (See Elective Tracks) | 3 | Varies | Varies |

### Spring Semester (Year 3)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 3050** | Malware Analysis & Reverse Engineering (x86, ARM, .NET) | 4 | CYB 2080 | 6 |
| **CYB 3060** | Network Exploitation & Post-Exploitation Techniques | 3 | CYB 3010 | 4 |
| **CYB 3070** | Incident Response & Crisis Management | 4 | CYB 3040 | 4 |
| **CYB 3080** | Cyber Law, Policy & Regulatory Compliance (GDPR, CCPA, HIPAA) | 3 | GEN 1020 | 0 |
| **CYB 3E02** | Elective II (See Elective Tracks) | 3 | Varies | Varies |

**Year 3 CyberRange Capstone:** Full Penetration Test Engagement. Students receive a black-box scope targeting a simulated financial institution. They must conduct reconnaissance, exploitation, privilege escalation, data exfiltration, and deliver a 50+ page professional penetration testing report with executive summary, technical findings, and remediation roadmap.

## Elective Tracks (Choose One)

### Track A: Red Team Operations

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **CYB 3E10** | Advanced Exploitation: Buffer Overflows, ROP Chains, Heap Spraying | 3 | CYB 3010 | 6 |
| **CYB 3E11** | Social Engineering & Physical Security Assessment | 3 | CYB 3010 | 2 |
| **CYB 3E12** | Red Team Infrastructure: C2 Frameworks, Evasion & Persistence | 3 | CYB 3060 | 4 |
| **CYB 3E13** | Purple Teaming & Adversary Emulation (MITRE CALDERA) | 3 | CYB 3E12 | 4 |

## Track B: Cyber Defense & Intelligence

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 3E20** | Advanced Threat Intelligence: OSINT, HUMINT & Dark Web Analysis | 3 | CYB 2050 | 3 |
| **CYB 3E21** | Security Architecture & Zero Trust Network Design | 3 | CYB 3030 | 2 |
| **CYB 3E22** | Endpoint Detection & Response (EDR) Engineering | 3 | CYB 2010 | 4 |
| **CYB 3E23** | Deception Technology: Honeypots, Honeynets & Canary Tokens | 3 | CYB 3E22 | 3 |

## Track C: Application Security & DevSecOps

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 3E30** | Advanced Secure Coding: C/C++ Memory Safety & Rust | 3 | CYB 2060 | 3 |
| **CYB 3E31** | Container & Kubernetes Security | 3 | CYB 3030 | 3 |
| **CYB 3E32** | API Security & Microservices Hardening | 3 | CYB 3020 | 2 |
| **CYB 3E33** | Automated Security Testing: SAST, DAST, IAST & CI/CD Pipelines | 3 | CYB 3E31 | 3 |

## Year 4: Advanced Topics & Capstone

The final year addresses emerging frontiers in cybersecurity and culminates in a two-semester capstone project. Students also complete their RCCE Level 2 certification preparation and participate in the national Rocheston Cyber War Games competition.

### Fall Semester (Year 4)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 4010** | AI Security: Adversarial ML, Model Poisoning & LLM Exploitation | 4 | STA 2100, CYB 3050 | 4 |
| **CYB 4020** | Blockchain Security & Smart Contract Auditing | 3 | CYB 2020 | 3 |
| **CYB 4030** | Industrial Control Systems & SCADA Security | 3 | CYB 1040, CYB 3070 | 4 |
| **CYB 4040** | Advanced Cryptographic Systems & Post-Quantum Readiness | 3 | CYB 2020 | 2 |
| **CYB 4900** | Capstone I: Project Proposal, Research & Design | 3 | Senior Standing | 2 |

### Spring Semester (Year 4)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CYB 4050** | Autonomous Vehicle & Drone Security | 3 | CYB 4010, CYB 4030 | 4 |
| **CYB 4060** | Quantum Computing & Cryptographic Implications | 3 | CYB 4040 | 2 |
| **CYB 4070** | Cyber Warfare, Nation-State Threats & Attribution | 3 | CYB 3080 | 0 |
| **CYB 4080** | Professional Practicum: Industry Internship (400 hrs minimum) | 3 | Advisor Approval | 20 |
| **CYB 4910** | Capstone II: Implementation, Testing & Defense | 4 | CYB 4900 | 8 |

**Year 4 Capstone:** Red vs. Blue War Game. The graduating class is divided into Red Team (attackers) and Blue Team (defenders) for a 72-hour continuous cyber operation. Red Team must compromise a simulated Fortune 500 enterprise while Blue Team defends it. External industry judges score both teams. Top performers receive Rocheston Cyber Warrior distinction on their RCCE Level 2 certification.

# SELECTED COURSE DESCRIPTIONS

## CYB 1010 - Introduction to Cybersecurity

A comprehensive survey of the cybersecurity landscape including threat actors (nation-states, APT groups, hacktivists, insiders), attack vectors, defense frameworks, and career pathways. Students explore the CIA triad, risk management fundamentals, and the cybersecurity kill chain. Weekly guest lectures from industry practitioners provide real-world context. Lab exercises use the Rocheston CyberRange to simulate basic network attacks and defenses.

## CYB 1020 - Linux Systems Administration & Kernel Hardening

Deep immersion into Linux operating systems with emphasis on security-critical administration. Students master command-line operations, shell scripting (Bash, Zsh), file system permissions, SELinux/AppArmor mandatory access controls, kernel parameter tuning via sysctl, and service hardening. Labs use Rose X OS as the primary platform. Students configure, harden, and audit Linux servers to CIS Benchmark Level 2 standards.

## CYB 2010 - SOC Fundamentals & SIEM Deployment

Students build and operate a complete Security Operations Center in the CyberRange. Course covers SIEM architecture (Splunk, Elastic SIEM), log aggregation from 50+ sources, correlation rule development, alert triage workflows, and Tier 1/2/3 analyst responsibilities. Students process 10,000+ security events per lab session, developing the pattern recognition skills essential for threat detection.

## CYB 3010 - Ethical Hacking & Penetration Testing

The flagship offensive security course. Students learn the complete penetration testing methodology (PTES): pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. Tools include Kali Linux, Burp Suite, Metasploit, Cobalt Strike (educational license), Nmap, and custom Python exploit scripts. Eight hours of weekly lab time simulate real engagement conditions.

## CYB 4010 - AI Security: Adversarial ML & LLM Exploitation

An advanced course addressing the security implications of artificial intelligence. Topics include adversarial example generation (FGSM, PGD, C&W attacks), model inversion and extraction, data poisoning, backdoor attacks on neural networks, prompt injection and jailbreaking of large language models, and defensive techniques including adversarial training, input sanitization, and model monitoring. Students audit a live AI system as their final project.

## CYB 4910 - Capstone II: Implementation, Testing & Defense

The culminating academic experience. Students implement the system designed in Capstone I, conduct rigorous security testing, and present their work to a panel of faculty, industry professionals, and Rocheston engineers. Projects must demonstrate mastery of at least three security domains and include a comprehensive written report, working prototype, and 30-minute oral defense. Past projects have included custom SIEM platforms, zero-trust network architectures, and AI-powered threat detection systems.

# 4. Bachelor of Science in Cyber Defense & Intelligence (B.S.CDI)

**CIP Code:** 43.0116 - Cyber/Computer Forensics and Counterterrorism
**Degree Code:** BSCDI-RCU-2025
**Total Credits:** 120 (42 General Education + 78 Major)
**Duration:** 4 Years / 8 Semesters (Full-Time)
**Delivery:** On-Campus with Hybrid Option
**RCCE Path:** RCCE Level 1 (End of Year 2) + RCCE Level 2 (End of Year 4)
**Focus:** Intelligence Analysis, Digital Forensics, Homeland Security

## PROGRAM MISSION

While the B.S.CE program focuses on engineering and offensive operations, the B.S.CDI program is designed for students pursuing careers in intelligence analysis, law enforcement cybercrime units, homeland security, and federal agencies. The curriculum emphasizes analytical tradecraft, forensic methodology, counterintelligence, and the intersection of cyber operations with national security.

## PROGRAM LEARNING OUTCOMES

- Conduct comprehensive digital forensic examinations of computers, mobile devices, cloud accounts, and IoT devices following legally defensible procedures
- Analyze cyber threat intelligence using structured analytic techniques (SATs) and produce intelligence products in standard formats (STIX/TAXII)
- Apply counterintelligence principles to identify and mitigate insider threats in enterprise environments
- Evaluate national cybersecurity policies, international cyber norms, and the legal frameworks governing cyber operations
- Perform open-source intelligence (OSINT) collection and dark web investigations while maintaining operational security
- Design and implement security monitoring architectures for critical infrastructure protection

## CURRICULUM ARCHITECTURE

### Year 1-2: Shared Foundation

Years 1 and 2 share the same foundational curriculum as the B.S.CE program (see Section 3), ensuring all students have identical core competencies in networking, Linux administration, Python, SOC operations, and cryptography. The programs diverge in Year 3.

### Year 3: Intelligence & Forensics Specialization

### Fall Semester (Year 3)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CDI 3010** | Advanced Digital Forensics: Disk, Memory & Network Analysis | 4 | CYB 3040 | 8 |
| **CDI 3020** | Cyber Threat Intelligence Production & Analysis | 3 | CYB 2050 | 3 |
| **CDI 3030** | Open Source Intelligence (OSINT) & Dark Web Investigations | 3 | CYB 2050 | 4 |
| **CDI 3040** | Counterintelligence & Insider Threat Detection | 3 | CYB 2040 | 2 |
| **CDI 3E01** | Elective I (See Intelligence Electives) | 3 | Varies | Varies |

### Spring Semester (Year 3)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CDI 3050** | Mobile & IoT Forensics (iOS, Android, Embedded Systems) | 4 | CDI 3010 | 6 |
| **CDI 3060** | Cybercrime Investigation & Law Enforcement Coordination | 3 | CYB 3080 | 2 |
| **CDI 3070** | Cloud Forensics: AWS, Azure, M365 & SaaS Evidence Collection | 3 | CYB 3030 | 4 |
| **CDI 3080** | Geopolitical Cyber Conflict & Attribution Methodology | 3 | CDI 3020 | 0 |
| **CDI 3E02** | Elective II (See Intelligence Electives) | 3 | Varies | Varies |

## Year 4: Advanced Intelligence & Capstone

### Fall Semester (Year 4)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CDI 4010** | Advanced Malware Forensics & Threat Actor Profiling | 4 | CYB 3050, CDI 3020 | 6 |
| **CDI 4020** | Critical Infrastructure Protection & Resilience Planning | 3 | CYB 4030 | 2 |
| **CDI 4030** | AI-Powered Threat Detection & Behavioral Analytics | 3 | STA 2100, CYB 4010 | 3 |
| **CDI 4040** | National Security Policy & Cyber Warfare Doctrine | 3 | CDI 3080 | 0 |
| **CDI 4900** | Capstone I: Intelligence Research Project Design | 3 | Senior Standing | 2 |

### Spring Semester (Year 4)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **CDI 4050** | Election Security & Disinformation Defense | 3 | CDI 3020 | 2 |
| **CDI 4060** | Privacy Engineering & Surveillance Technology Ethics | 3 | CYB 3080 | 0 |
| **CDI 4070** | Professional Practicum: Federal Agency or Defense Contractor (400 hrs) | 3 | Advisor Approval | 20 |
| **CDI 4080** | Expert Witness Testimony & Forensic Report Writing | 3 | CDI 3060 | 0 |
| **CDI 4910** | Capstone II: Intelligence Product Delivery & Defense | 4 | CDI 4900 | 8 |

# 5. Master of Science in Cyber Defense & Strategy (M.S.CDS)

**CIP Code:** 11.1003 - Computer and Information Systems Security
**Degree Code:** MSCDS-RCU-2025
**Total Credits:** 36 (12 Courses)
**Duration:** 18 Months (Full-Time) / 24 Months (Part-Time)
**Delivery:** 100% Online (Executive Format: Asynchronous + Monthly Intensives)
**Prerequisites:** B.S. in STEM or 3+ Years Industry Experience
**RCCE Path:** RCCE Level 3 (upon completion)
**Thesis Option:** Yes (6 credits replace 2 electives)

## PROGRAM MISSION

The Master of Science in Cyber Defense & Strategy is designed for mid-career professionals seeking to transition from technical practitioner to strategic leader. The program bridges the gap between hands-on security operations and C-suite decision-making, producing graduates who can architect enterprise security programs, brief boards of directors on cyber risk, lead incident response during crises, and shape organizational security culture.

## PROGRAM LEARNING OUTCOMES

- Design and implement enterprise security architectures that align with business objectives and risk tolerance
- Develop and execute cyber risk management frameworks using quantitative and qualitative methodologies
- Lead cross-functional incident response teams during active cyber crises with clear communication to stakeholders
- Evaluate and implement emerging security technologies including AI-driven defense, zero trust, and extended detection and response (XDR)
- Conduct advanced offensive operations including APT simulation and red team campaign planning
- Author security policies, compliance documentation, and board-level risk reports

## CURRICULUM STRUCTURE

Students complete 8 core courses, 2 track-specific courses, and either 2 electives or a thesis. Three specialized tracks allow professionals to focus their expertise.

### Core Curriculum (24 Credits)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **MCS 6010** | Enterprise Security Architecture & Design Patterns | 3 | Admission | 3 |

| | | | | |
|---|---|---|---|---|
| **MCS 6020** | Advanced Threat Analysis & Intelligence-Driven Defense | 3 | Admission | 3 |
| **MCS 6030** | Cyber Risk Quantification & Business Impact Analysis | 3 | Admission | 0 |
| **MCS 6040** | Incident Command & Crisis Leadership | 3 | MCS 6020 | 4 |
| **MCS 6050** | Offensive Security Operations: Red Team Campaign Planning | 3 | MCS 6020 | 6 |
| **MCS 6060** | Security Program Development & Maturity Assessment | 3 | MCS 6030 | 0 |
| **MCS 6070** | Applied Cryptographic Engineering & PKI Management | 3 | Admission | 2 |
| **MCS 6080** | Research Methods in Cybersecurity | 3 | Admission | 0 |

## Track A: CISO & Security Leadership (6 Credits)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **MCS 7110** | Cyber Governance, Board Communication & Fiduciary Responsibility | 3 | MCS 6030 | 0 |
| **MCS 7120** | Regulatory Compliance Engineering (SOX, PCI-DSS, NIST, FedRAMP) | 3 | MCS 6060 | 0 |

## Track B: Cyber Warfare & Advanced Operations (6 Credits)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **MCS 7210** | Advanced Persistent Threat Simulation & Adversary Emulation | 3 | MCS 6050 | 8 |
| **MCS 7220** | Malware Engineering: Implant Development & Evasion Techniques | 3 | MCS 6050 | 6 |

## Track C: Future Technologies & AI Defense (6 Credits)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **MCS 7310** | Securing AI/ML Pipelines: From Training Data to Deployment | 3 | MCS 6020 | 4 |
| **MCS 7320** | Post-Quantum Cryptography & Zero-Knowledge Proof Systems | 3 | MCS 6070 | 2 |

## Elective Options (6 Credits) or Thesis

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **MCS 7E01** | Supply Chain Security & Third-Party Risk Management | 3 | MCS 6060 | 0 |

| | | | | |
|---|---|---|---|---|
| **MCS 7E02** | Cloud-Native Security: Serverless, Containers & Service Mesh | 3 | MCS 6010 | 3 |
| **MCS 7E03** | Cyber Insurance, Liability & Legal Strategy | 3 | MCS 6030 | 0 |
| **MCS 7E04** | Privacy Engineering & Data Protection by Design | 3 | MCS 6060 | 0 |
| **MCS 7E05** | Security Automation & Orchestration (SOAR) | 3 | MCS 6040 | 3 |
| **MCS 7E06** | Threat Modeling: STRIDE, PASTA & Attack Trees | 3 | MCS 6010 | 2 |
| **MCS 9900** | Master's Thesis (replaces 2 electives) | 6 | MCS 6080 | 0 |

# 6. Master of Science in AI Security & Autonomous Systems (M.S.AISAS)

**CIP Code:** 11.0104 - Informatics (AI Security Specialization)
**Degree Code:** MSAISAS-RCU-2025
**Total Credits:** 36 (12 Courses)
**Duration:** 18 Months (Full-Time) / 24 Months (Part-Time)
**Delivery:** Online with Monthly In-Person Lab Intensives
**Prerequisites:** B.S. in CS/Engineering/Math or Equivalent + Programming Proficiency
**RCCE Path:** RCCE Level 3 with AI Security Specialization

## PROGRAM MISSION

This program addresses the most critical emerging gap in cybersecurity: the security of artificial intelligence systems. As organizations deploy AI for everything from autonomous vehicles to medical diagnosis to financial trading, the attack surface expands exponentially. Graduates of this program will be among the first specialists capable of auditing, defending, and red-teaming AI systems at enterprise scale.

## CORE CURRICULUM (24 CREDITS)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **AIS 6010** | Foundations of Machine Learning for Security Professionals | 3 | Admission | 3 |
| **AIS 6020** | Adversarial Machine Learning: Attack & Defense | 3 | AIS 6010 | 4 |
| **AIS 6030** | Large Language Model Security: Prompt Injection, Jailbreaking & Guardrails | 3 | AIS 6010 | 4 |
| **AIS 6040** | AI Supply Chain Security: Data Poisoning, Model Theft & Provenance | 3 | AIS 6020 | 3 |
| **AIS 6050** | Autonomous Systems Security: Vehicles, Drones & Robotics | 3 | AIS 6010 | 4 |
| **AIS 6060** | Privacy-Preserving AI: Federated Learning, Differential Privacy & MPC | 3 | AIS 6010 | 2 |
| **AIS 6070** | AI Governance, Ethics & Regulatory Frameworks (EU AI Act, NIST AI RMF) | 3 | Admission | 0 |
| **AIS 6080** | Research Seminar in AI Security | 3 | Admission | 0 |

## ADVANCED ELECTIVES (12 CREDITS - CHOOSE 4)

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **AIS 7010** | Deep Reinforcement Learning Security & Reward Hacking | 3 | AIS 6020 | 3 |
| **AIS 7020** | Computer Vision Security: Adversarial Patches & Deepfake Detection | 3 | AIS 6020 | 4 |
| **AIS 7030** | AI Red Teaming Methodology & Automated Vulnerability Discovery | 3 | AIS 6030 | 6 |
| **AIS 7040** | Securing AI in Healthcare: FDA Compliance & Patient Safety | 3 | AIS 6070 | 2 |
| **AIS 7050** | Financial AI Security: Algorithmic Trading & Fraud Detection Systems | 3 | AIS 6040 | 2 |
| **AIS 7060** | Neuromorphic & Edge AI Security | 3 | AIS 6050 | 3 |
| **AIS 9900** | Master's Thesis in AI Security (replaces 2 electives) | 6 | AIS 6080 | 0 |

# 7. Graduate Diploma in Offensive Security Operations

**Credential Code:** GDOSO-RCU-2025
**Total Credits:** 24 (8 Courses)
**Duration:** 12 Months
**Delivery:** Online with Bi-Monthly Virtual Lab Intensives
**Prerequisites:** B.S. Degree or 2+ Years in IT/Security
**RCCE Path:** RCCE Level 2
**Stackable:** Credits transfer into M.S.CDS (Track B)

## PROGRAM OVERVIEW

The Graduate Diploma in Offensive Security Operations is a focused, accelerated credential for professionals who want deep technical expertise in penetration testing, red teaming, and adversary simulation without committing to a full master's degree. All 24 credits are transferable into the M.S.CDS program for students who later wish to pursue the full master's degree.

## CURRICULUM

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **OSO 5010** | Penetration Testing Mastery: Methodology, Tools & Reporting | 3 | Admission | 8 |
| **OSO 5020** | Web Application Exploitation: Beyond OWASP Top 10 | 3 | OSO 5010 | 6 |
| **OSO 5030** | Network & Infrastructure Exploitation: AD Attacks, Pivoting & Tunneling | 3 | OSO 5010 | 6 |
| **OSO 5040** | Wireless, Bluetooth & RF Exploitation | 3 | OSO 5030 | 4 |
| **OSO 5050** | Cloud Penetration Testing: AWS, Azure & GCP Attack Paths | 3 | OSO 5030 | 6 |
| **OSO 5060** | Malware Development for Red Teamers: Custom Implants & C2 | 3 | OSO 5030 | 6 |
| **OSO 5070** | Evasion Engineering: AV/EDR Bypass, AMSI Unhooking & Living-Off-The-Land | 3 | OSO 5060 | 6 |
| **OSO 5080** | Red Team Operations Capstone: Full-Scope Adversary Simulation | 3 | All Above | 12 |

## CAPSTONE DETAILS

The OSO 5080 capstone is a 4-week, full-time simulated red team engagement conducted entirely in the Rocheston CyberRange. Students operate in teams of 3-4, given a realistic scope and rules of engagement against a simulated enterprise with 500+ endpoints, Active Directory forests, cloud infrastructure, and defensive security teams. Deliverables include a complete red team report, attack narrative, and remediation advisory.

# 8. Graduate Diploma in Cyber Governance, Risk & Compliance

**Credential Code:** GDGRC-RCU-2025
**Total Credits:** 24 (8 Courses)
**Duration:** 12 Months
**Delivery:** 100% Online (Asynchronous with Weekly Live Sessions)
**Prerequisites:** B.S. Degree or 3+ Years Professional Experience
**RCCE Path:** RCCE Level 2 with GRC Specialization
**Stackable:** Credits transfer into M.S.CDS (Track A)

## PROGRAM OVERVIEW

Designed for professionals transitioning into security leadership, compliance, or risk management roles, this diploma provides the strategic and regulatory knowledge required for CISO-track careers. The program covers every major compliance framework, risk quantification methodology, and governance structure used in Fortune 500 enterprises, federal agencies, and regulated industries.

## CURRICULUM

| Code | Course Title | Cr. | Prerequisites | Lab Hrs/Wk |
|---|---|---|---|---|
| **GRC 5010** | Cybersecurity Governance Frameworks: NIST CSF 2.0, ISO 27001, COBIT | 3 | Admission | 0 |
| **GRC 5020** | Cyber Risk Quantification: FAIR, Monte Carlo Simulation & Risk Registers | 3 | GRC 5010 | 2 |
| **GRC 5030** | Regulatory Compliance Deep Dive: HIPAA, PCI-DSS, SOX, GLBA | 3 | GRC 5010 | 0 |
| **GRC 5040** | Data Privacy Law & Engineering: GDPR, CCPA, LGPD & Global Frameworks | 3 | GRC 5030 | 0 |
| **GRC 5050** | Federal Cybersecurity Compliance: FedRAMP, CMMC, FISMA & NIST 800-171 | 3 | GRC 5010 | 0 |
| **GRC 5060** | Third-Party Risk Management & Supply Chain Security | 3 | GRC 5020 | 0 |
| **GRC 5070** | Security Program Metrics, Reporting & Board Communication | 3 | GRC 5020 | 0 |
| **GRC 5080** | GRC Capstone: Enterprise Security Program Design & Assessment | 3 | All Above | 4 |

# 9. Professional Certificate in Cybersecurity Foundations

**Certificate Code:** PCCF-RCU-2025
**Duration:** 24 Weeks (480 Contact Hours)
**Format:** Intensive Bootcamp (Evening/Weekend or Full-Time Immersive)
**Prerequisites:** None (Designed for Career Changers)
**RCCE Path:** RCCE Level 1 Exam Preparation
**Outcome:** Job-Ready Portfolio + RCCE Level 1 Certification Eligibility

## PROGRAM OVERVIEW

The zero-to-hero accelerator. This program takes individuals with no prior cybersecurity experience and transforms them into employable security analysts in 24 weeks. Students spend 480+ hours in the Rocheston CyberRange, building skills through progressive scenario-based training that simulates real-world security operations from day one. No theoretical lectures without corresponding hands-on labs.

## MODULE BREAKDOWN

| Module Code | Module Title | Hours |
|---|---|---|
| **PCCF-M01** | Computing Foundations: OS Concepts, Command Line & File Systems | 40 |
| **PCCF-M02** | Linux Administration for Security (Rose X OS) | 40 |
| **PCCF-M03** | Network Fundamentals: TCP/IP Stack, Routing & Switching | 40 |
| **PCCF-M04** | Network Security: Firewalls, IDS/IPS, VPNs & Segmentation | 40 |
| **PCCF-M05** | Python Programming for Security Automation | 40 |
| **PCCF-M06** | Windows Security & Active Directory Fundamentals | 30 |
| **PCCF-M07** | Vulnerability Assessment & Scanning Tools | 30 |
| **PCCF-M08** | Security Operations: SIEM, Log Analysis & Alert Triage | 40 |
| **PCCF-M09** | Introduction to Penetration Testing | 40 |
| **PCCF-M10** | Incident Response Fundamentals & Playbook Development | 30 |
| **PCCF-M11** | Cloud Security Essentials (AWS/Azure) | 30 |
| **PCCF-M12** | Career Preparation: Resume, Portfolio, Mock Interviews & RCCE Exam Prep | 40 |

## HANDS-ON LAB HOURS BY DOMAIN

Minimum 320 of the 480 contact hours are spent in live lab environments:

- Network defense and monitoring: 80 hours
- Vulnerability scanning and assessment: 60 hours
- SOC operations and SIEM: 60 hours
- Penetration testing: 50 hours
- Python scripting and automation: 40 hours
- Incident response simulations: 30 hours

# 10. Professional Certificate in Penetration Testing & Red Teaming

**Certificate Code:** PCPT-RCU-2025
**Duration:** 16 Weeks (320 Contact Hours)
**Format:** Intensive Online with Weekend Lab Sprints
**Prerequisites:** RCCE Level 1 or Equivalent Experience (2+ Years in Security)
**RCCE Path:** RCCE Level 2 Exam Preparation (Offensive Track)

## MODULE BREAKDOWN

| Module Code | Module Title | Hours |
|---|---|---|
| **PCPT-M01** | Advanced Reconnaissance: OSINT, Subdomain Enumeration & Asset Discovery | 30 |
| **PCPT-M02** | Network Penetration Testing: Scanning, Exploitation & Pivoting | 40 |
| **PCPT-M03** | Web Application Penetration Testing: Injection, Auth Bypass & Logic Flaws | 40 |
| **PCPT-M04** | Active Directory Attacks: Kerberoasting, DCSync, Golden Tickets & Delegation | 40 |
| **PCPT-M05** | Cloud Penetration Testing: AWS IAM Abuse, Azure AD Attacks, GCP Pivoting | 30 |
| **PCPT-M06** | Wireless & Physical Penetration Testing | 20 |
| **PCPT-M07** | Post-Exploitation: Persistence, Exfiltration & Reporting | 30 |
| **PCPT-M08** | Custom Exploit Development: Python, PowerShell & C | 30 |
| **PCPT-M09** | AV/EDR Evasion: Obfuscation, Process Injection & AMSI Bypass | 30 |
| **PCPT-M10** | Capstone: Black-Box Penetration Test Against Simulated Enterprise | 30 |

# 11. Professional Certificate in Cloud Security Architecture

**Certificate Code:** PCCS-RCU-2025
**Duration:** 12 Weeks (240 Contact Hours)
**Format:** Online with Hands-On Cloud Labs
**Prerequisites:** IT Experience (1+ Year) or PCCF Certificate
**RCCE Path:** RCCE Level 2 Exam Preparation (Cloud Track)

## MODULE BREAKDOWN

| Module Code | Module Title | Hours |
|---|---|---|
| **PCCS-M01** | Cloud Computing Fundamentals: IaaS, PaaS, SaaS & Shared Responsibility | 20 |
| **PCCS-M02** | AWS Security: IAM, VPC, GuardDuty, Security Hub & CloudTrail | 30 |
| **PCCS-M03** | Azure Security: Entra ID, NSGs, Sentinel, Defender for Cloud | 30 |
| **PCCS-M04** | GCP Security: IAM, VPC Service Controls, Chronicle & SCC | 20 |
| **PCCS-M05** | Container Security: Docker Hardening, Kubernetes RBAC & Pod Security | 30 |
| **PCCS-M06** | Serverless Security: Lambda/Functions Threats & Mitigation | 20 |
| **PCCS-M07** | Cloud Infrastructure as Code Security: Terraform, CloudFormation & Policy-as-Code | 20 |
| **PCCS-M08** | Cloud Incident Response & Forensics | 20 |
| **PCCS-M09** | Multi-Cloud Security Architecture & Zero Trust in the Cloud | 20 |
| **PCCS-M10** | Capstone: Secure Cloud Architecture Design & Penetration Test | 30 |

# 12. Professional Certificate in AI & Machine Learning Security

**Certificate Code:** PCAI-RCU-2025
**Duration:** 12 Weeks (240 Contact Hours)
**Format:** Online with GPU-Powered Lab Environments
**Prerequisites:** Python Proficiency + Basic ML Knowledge or PCCF Certificate
**RCCE Path:** RCCE Level 2 with AI Security Specialization

## MODULE BREAKDOWN

| Module Code | Module Title | Hours |
|---|---|---|
| **PCAI-M01** | Machine Learning Fundamentals for Security Professionals | 20 |
| **PCAI-M02** | Adversarial Attacks on Classification & Detection Models | 30 |
| **PCAI-M03** | Large Language Model Security: Prompt Injection & Output Manipulation | 30 |
| **PCAI-M04** | Data Poisoning, Backdoor Attacks & Training Pipeline Security | 30 |
| **PCAI-M05** | Model Extraction, Inversion & Membership Inference Attacks | 20 |
| **PCAI-M06** | AI Red Teaming: Methodology, Tools & Frameworks | 30 |
| **PCAI-M07** | Defensive AI: Adversarial Training, Input Validation & Monitoring | 20 |
| **PCAI-M08** | AI Governance: NIST AI RMF, EU AI Act & Responsible AI | 20 |
| **PCAI-M09** | Deepfake Detection & Synthetic Media Analysis | 20 |
| **PCAI-M10** | Capstone: AI System Security Audit & Red Team Report | 20 |

# 13. Professional Certificate in Industrial Control Systems Security

**Certificate Code:** PCIC-RCU-2025
**Duration:** 12 Weeks (240 Contact Hours)
**Format:** Online with Virtual ICS/SCADA Lab Environment
**Prerequisites:** IT/OT Experience (1+ Year) or PCCF Certificate
**RCCE Path:** RCCE Level 2 with ICS Security Specialization
**Industry Alignment:** IEC 62443, NERC CIP, NIST SP 800-82

## MODULE BREAKDOWN

| Module Code | Module Title | Hours |
|---|---|---|
| **PCIC-M01** | Industrial Control Systems Architecture: PLCs, RTUs, HMIs & SCADA | 20 |
| **PCIC-M02** | OT Network Protocols: Modbus, DNP3, OPC-UA, EtherNet/IP & BACnet | 30 |
| **PCIC-M03** | IT/OT Convergence: Network Segmentation & Purdue Model Implementation | 30 |
| **PCIC-M04** | ICS Threat Landscape: TRITON, Industroyer, Stuxnet & Emerging Threats | 20 |
| **PCIC-M05** | ICS Vulnerability Assessment & Penetration Testing (Safe Methods) | 30 |
| **PCIC-M06** | ICS Network Monitoring & Anomaly Detection | 20 |
| **PCIC-M07** | Incident Response for Industrial Environments | 20 |
| **PCIC-M08** | ICS Regulatory Compliance: IEC 62443, NERC CIP & NIST 800-82 | 20 |
| **PCIC-M09** | Securing Smart Grid, Water Treatment & Manufacturing Systems | 20 |
| **PCIC-M10** | Capstone: ICS Security Assessment of Simulated Power Grid | 30 |

# 14. Rocheston CyberRange Lab Environments

## OVERVIEW

The Rocheston CyberRange is the engine that powers every program in this catalog. Unlike static virtual machines or pre-recorded demonstrations, the CyberRange provides a hyper-realistic, continuously evolving simulation of enterprise, government, and industrial networks. Every student, from first-semester freshmen to master's candidates, trains in the same platform used by Fortune 500 security teams and government agencies.

## LAB ENVIRONMENT CATEGORIES

### 1. Enterprise Simulation Environments

Full-scale replicas of corporate IT infrastructure with 500+ endpoints:

- Multi-forest Active Directory with 10,000+ user accounts, group policies, and trust relationships
- Email servers (Exchange/M365), file shares, SharePoint, and collaboration platforms
- Web application portfolio: E-commerce, CRM, internal tools (15+ applications with intentional vulnerabilities)
- Cloud infrastructure: AWS VPCs, Azure subscriptions, and GCP projects with misconfigurations
- Network infrastructure: Cisco, Palo Alto, and Fortinet firewalls, VPN gateways, and load balancers
- Endpoint diversity: Windows 10/11, macOS, Linux workstations, mobile devices, and IoT sensors

### 2. Critical Infrastructure Simulation

- Power grid SCADA system with PLCs, RTUs, and HMI interfaces
- Water treatment facility with Modbus and DNP3 protocol traffic
- Manufacturing floor with OPC-UA industrial automation
- Smart building management system (BACnet/IP)
- Healthcare network with DICOM imaging, HL7 messaging, and EHR systems

### 3. Attack Simulation Ranges

- Ransomware deployment and containment scenarios (LockBit, BlackCat, Royal simulations)
- Advanced Persistent Threat campaigns (APT28, APT41, Lazarus Group TTPs)
- Supply chain attack simulations (SolarWinds, Kaseya, MOVEit recreation)
- DDoS attack generation and mitigation (Layer 3/4/7)
- Insider threat scenarios with behavioral indicators

### 4. Specialized Technology Labs

- AI/ML Security Lab: GPU-powered environment for adversarial ML experiments
- Blockchain & Smart Contract Lab: Ethereum testnet with vulnerable contracts
- Quantum Computing Simulator: Post-quantum cryptography testing
- IoT Exploitation Lab: Firmware analysis, JTAG/UART debugging, RF interception

- Automotive Security Lab: CAN bus simulation for vehicle security research

## PLATFORM FEATURES

- 48-Hour Zero-Day Integration: When major vulnerabilities hit the news, corresponding lab scenarios appear within 48 hours
- Difficulty Scaling: Labs automatically adjust difficulty based on student performance and progression
- Rocheston Raven Gamification: Coin rewards, leaderboards, achievement badges, and spinning wheel bonuses
- Real-Time Scoring: Automated assessment of student actions with detailed feedback
- Collaboration Mode: Team-based exercises with role assignments (Red/Blue/Purple/White teams)
- Recording & Replay: All lab sessions are recorded for review, grading, and portfolio building

# 15. RCCE Certification Alignment & DoD 8140 Approved Job Roles

## RCCE CERTIFICATION LEVELS

### RCCE Level 1: Security Practitioner

Validates foundational cybersecurity knowledge and hands-on skills. Aligned with NICE Framework Work Roles: Cyber Defense Analyst (PR-CDA-001), Vulnerability Assessment Analyst (PR-VAM-001).

- Achieved through: B.S. Year 2 completion, Professional Certificate in Cybersecurity Foundations
- Exam format: 120 multiple choice questions + 4-hour practical lab examination
- Domains: Network Security, Operating Systems, Cryptography Fundamentals, Threat Analysis, Vulnerability Assessment, Incident Response Basics

### RCCE Level 2: Security Engineer

Validates advanced technical skills in offensive and defensive operations. Aligned with NICE Framework Work Roles: Exploitation Analyst (AN-EXP-001), Cyber Defense Infrastructure Support (PR-INF-001).

- Achieved through: B.S. Year 4 completion, Graduate Diplomas, Advanced Professional Certificates
- Exam format: 80 advanced questions + 8-hour practical penetration test
- Domains: Advanced Penetration Testing, Malware Analysis, Cloud Security, Forensics, Secure Architecture, Threat Intelligence

### RCCE Level 3: Security Architect

Validates strategic leadership and enterprise security architecture capabilities. Aligned with NICE Framework Work Roles: Information Systems Security Manager (OV-MGT-001), Cyber Workforce Developer (OV-SPP-001).

- Achieved through: M.S. degree completion
- Exam format: 60 scenario-based questions + 24-hour enterprise security challenge + written defense
- Domains: Enterprise Architecture, Risk Management, Security Program Development, Advanced Cryptography, AI Security, Strategic Leadership

## DOD 8140 WORK ROLE MAPPING

The RCCE credential is approved under US Department of Defense Directive 8140 for the following work role categories. This means graduates holding the RCCE can apply directly for these DoD civilian and contractor positions without needing additional baseline certifications:

| DoD 8140 Work Role | Category | RCCE Level Required |
|---|---|---|
| Cyber Defense Analyst | Protect and Defend (PR) | **Level 1** |
| Vulnerability Assessment Analyst | Protect and Defend (PR) | **Level 1** |
| Cyber Defense Incident Responder | Protect and Defend (PR) | **Level 2** |

| | | |
|---|---|---|
| Exploitation Analyst | Analyze (AN) | **Level 2** |
| Threat/Warning Analyst | Analyze (AN) | **Level 2** |
| Cyber Defense Infrastructure Support | Protect and Defend (PR) | **Level 2** |
| Information Systems Security Manager | Oversee and Govern (OV) | **Level 3** |
| Security Architect | Securely Provision (SP) | **Level 3** |
| Cyber Workforce Developer | Oversee and Govern (OV) | **Level 3** |
| Authorizing Official | Oversee and Govern (OV) | **Level 3** |

# WHAT CAN I DO AFTER GRADUATING? DOD 8140 APPROVED JOB ROLES FOR RCCE HOLDERS

One of the most common questions students ask is: what job can I actually apply for after I graduate? Because the RCCE is approved under DoD Directive 8140, graduates are immediately eligible to apply for the following roles across the Department of Defense, military branches, intelligence community, and defense contractor organizations. No additional baseline certification is required.

## RCCE Level 1 Graduates (B.S. Year 2 / Professional Certificate Completers)

With RCCE Level 1, you qualify for entry-level and mid-level positions in the Protect and Defend (PR) category. These are the front-line cybersecurity roles that form the backbone of every military installation, federal agency, and defense contractor.

### Cyber Defense Analyst (NICE Code: PR-CDA-001)

You monitor networks, analyze security events, and identify threats in real time. This is the classic SOC Analyst role applied to defense environments. You sit in a Security Operations Center at a military base, intelligence agency, or defense contractor and watch for adversary activity across classified and unclassified networks.

- Where you work: NSA, US Cyber Command, Army Cyber, Air Force 16th AF, Navy Fleet Cyber Command, DHS CISA, defense contractors (Raytheon, SAIC, ManTech, Leidos, Booz Allen Hamilton)
- Typical job titles: Cybersecurity Analyst, SOC Analyst (Tier 1/2), Information Security Analyst, Cyber Watch Operator, Network Security Monitor
- Salary range: $65,000 - $95,000 (GS-9 to GS-11 equivalent for federal civilian)
- Clearance: Typically requires Secret or Top Secret/SCI

### Vulnerability Assessment Analyst (NICE Code: PR-VAM-001)

You conduct vulnerability scans, analyze results, and recommend remediation across DoD networks. This role goes beyond passive monitoring. You actively probe systems for weaknesses using tools like Nessus, Qualys,

and ACAS (the DoD's vulnerability scanning platform), then work with system administrators to fix what you find before adversaries exploit it.

- Where you work: Every military branch, DISA (Defense Information Systems Agency), NSA Red/Blue Teams, Combatant Commands, defense contractors
- Typical job titles: Vulnerability Analyst, Security Assessment Specialist, ACAS Analyst, Compliance and Vulnerability Engineer, Information Assurance Vulnerability Analyst
- Salary range: $70,000 - $105,000 (GS-9 to GS-12 equivalent)
- Clearance: Secret minimum, Top Secret preferred

## RCCE Level 2 Graduates (B.S. Completers / Graduate Diploma / Advanced Certificates)

With RCCE Level 2, you qualify for advanced technical roles in the Protect and Defend (PR) and Analyze (AN) categories. These positions involve hands-on offensive operations, incident response, threat intelligence, and infrastructure defense at a senior technical level.

### Cyber Defense Incident Responder (NICE Code: PR-CDA-001)

When a military network is breached, you are the one who responds. You investigate intrusions, contain threats, perform forensic analysis, and lead recovery operations. This is high-pressure, mission-critical work. You could be responding to a nation-state intrusion on a classified weapons system or investigating ransomware on a military hospital network.

- Where you work: DoD CIRT (Computer Incident Response Teams), US-CERT, DC3 (Defense Cyber Crime Center), military branch CERTs, CISA Hunt and Incident Response Teams
- Typical job titles: Incident Response Analyst, DFIR Specialist, Cyber Incident Handler, Computer Forensic Analyst, Cybersecurity First Responder
- Salary range: $85,000 - $130,000 (GS-11 to GS-13 equivalent)
- Clearance: Top Secret/SCI typically required

### Exploitation Analyst (NICE Code: AN-EXP-001)

This is the offensive side of DoD cyber operations. You identify vulnerabilities in target systems and develop or execute exploits to gain access. You work in Offensive Cyberspace Operations (OCO) units, conducting authorized penetration testing against DoD systems or supporting national cyber mission forces. This is one of the most technically demanding and elite roles in military cybersecurity.

- Where you work: NSA Tailored Access Operations (TAO), US Cyber Command Cyber National Mission Force (CNMF), Air Force 67th Cyberspace Wing, Army Cyber Command, Navy Cyber Warfare Development Group
- Typical job titles: Exploitation Analyst, Offensive Cyber Operator, Red Team Operator, Penetration Tester (DoD), CNO (Computer Network Operations) Analyst
- Salary range: $95,000 - $155,000 (GS-12 to GS-14 equivalent)
- Clearance: Top Secret/SCI with polygraph often required

### Threat/Warning Analyst (NICE Code: AN-TWA-001)

You analyze adversary capabilities, intentions, and activities to provide early warning of cyber threats to DoD networks and missions. This role combines cybersecurity skills with intelligence analysis tradecraft. You monitor threat actor groups (APT28, APT41, Lazarus Group, etc.), produce intelligence reports, and brief military commanders on the cyber threat landscape affecting their operations.

- Where you work: DIA (Defense Intelligence Agency), NSA, CIA Cyber Center, Military Intelligence units, Combatant Command J2 (Intelligence) cyber divisions, CISA
- Typical job titles: Cyber Threat Intelligence Analyst, Cyber Warning Analyst, All-Source Cyber Analyst, Threat Researcher, Intelligence Analyst (Cyber)
- Salary range: $80,000 - $130,000 (GS-11 to GS-13 equivalent)
- Clearance: Top Secret/SCI required

### Cyber Defense Infrastructure Support Specialist (NICE Code: PR-INF-001)

You design, deploy, and maintain the security infrastructure that protects DoD networks. This includes firewalls, intrusion detection/prevention systems, VPN concentrators, proxy servers, email security gateways, and endpoint protection platforms across military installations worldwide. You ensure that security tools are properly configured, updated, and functioning across networks that may span continents.

- Where you work: DISA, military base Network Enterprise Centers (NECs), Regional Cyber Centers, defense contractors supporting DoD network operations
- Typical job titles: Cybersecurity Infrastructure Engineer, Network Security Engineer, IA Engineer, Boundary Protection Specialist, Security Systems Administrator
- Salary range: $85,000 - $140,000 (GS-11 to GS-13 equivalent)
- Clearance: Secret minimum, Top Secret for classified networks

## RCCE Level 3 Graduates (Master's Degree Completers)

With RCCE Level 3, you qualify for senior leadership and management roles in the Oversee and Govern (OV) and Securely Provision (SP) categories. These are the positions that set strategy, make authorization decisions, design enterprise architectures, and lead cybersecurity programs across entire organizations.

### Information Systems Security Manager / ISSM (NICE Code: OV-MGT-001)

You are the senior cybersecurity authority for a program, system, or enclave. You oversee the security posture of one or more information systems, ensure compliance with DoD security policies (RMF, STIGs), manage Authorization to Operate (ATO) packages, and serve as the primary cybersecurity advisor to program managers and commanding officers. This is the CISO equivalent within the DoD structure.

- Where you work: Every DoD agency, military installation, weapons program office, defense contractor program office
- Typical job titles: Information Systems Security Manager (ISSM), Cybersecurity Manager, Program Security Lead, Cyber Program Manager, Deputy CISO
- Salary range: $120,000 - $185,000 (GS-13 to GS-15 equivalent)
- Clearance: Top Secret/SCI typically required

### Security Architect (NICE Code: SP-ARC-001)

You design the security architecture for new DoD systems, networks, and applications. When the military builds a new weapons platform, satellite communication system, or battlefield network, you are the person who determines how it will be secured. You define security requirements, select controls, design network segmentation, specify encryption standards, and ensure the architecture meets DoD security mandates before a single line of code is written.

- Where you work: DoD CIO, DISA architecture teams, military program offices (PEOs), NSA IA Directorate, defense contractors (Lockheed Martin Skunk Works, Northrop Grumman Mission Systems, Boeing Defense)
- Typical job titles: Security Architect, Enterprise Security Architect, Cybersecurity Solutions Architect, IA Architect, Chief Security Architect
- Salary range: $140,000 - $220,000 (GS-14 to GS-15/SES equivalent)
- Clearance: Top Secret/SCI, sometimes with SAP access

### Authorizing Official / AO (NICE Code: OV-AUTH-001)

You are the executive who makes the formal decision to authorize a DoD information system to operate. This is one of the most senior cybersecurity roles in the DoD. You review the risk assessment, evaluate the security controls, and accept the residual risk on behalf of the organization. Your signature on an Authorization to Operate (ATO) means you are personally accountable for the security posture of that system. This role is typically held by Senior Executive Service (SES) civilians, General/Flag Officers, or their designated representatives.

- Where you work: DoD agency headquarters, military service CIO offices, Combatant Command headquarters, major program executive offices
- Typical job titles: Authorizing Official, Designated Authorizing Official (DAO), Senior Information Security Officer, Risk Executive
- Salary range: $160,000 - $250,000+ (GS-15 to SES equivalent)
- Clearance: Top Secret/SCI required

### Cyber Workforce Developer and Manager (NICE Code: OV-SPP-001)

You build and manage the DoD's cybersecurity workforce. You develop training programs, establish qualification requirements, manage cyber workforce development budgets, and ensure that military and civilian cyber personnel have the skills needed to defend the nation. This role is critical because the DoD faces a persistent shortage of qualified cybersecurity professionals, and you are the person responsible for closing that gap.

- Where you work: DoD CIO Cyber Workforce Division, military service cyber schoolhouses (Army Cyber School, Navy Information Warfare Training Command, Air Force Cyber Technical Training), CISA National Initiative for Cybersecurity Education (NICE), defense contractor training organizations
- Typical job titles: Cyber Workforce Program Manager, Cybersecurity Training Director, Cyber Education Specialist, Workforce Development Lead, Cyber Human Capital Manager
- Salary range: $110,000 - $175,000 (GS-13 to GS-15 equivalent)
- Clearance: Secret to Top Secret

# WHERE DO RCCE GRADUATES WORK? MAJOR DOD & FEDERAL EMPLOYERS

The RCCE's DoD 8140 approval opens doors to the largest cybersecurity employer in the world: the United States Department of Defense and its supporting contractor ecosystem. Here are the primary organizations that hire for these work roles:

## Direct Federal Employment

- National Security Agency (NSA) - Fort Meade, MD and global locations
- US Cyber Command (USCYBERCOM) - Fort Meade, MD
- Defense Information Systems Agency (DISA) - Fort Meade, MD and regional offices
- Defense Intelligence Agency (DIA) - Joint Base Anacostia-Bolling, DC
- Department of Homeland Security / CISA - Nationwide
- FBI Cyber Division - Nationwide field offices
- Army Cyber Command - Fort Eisenhower, GA
- Air Force 16th Air Force (Cyber) - Joint Base San Antonio, TX
- Navy Fleet Cyber Command / 10th Fleet - Fort Meade, MD
- Marine Corps Forces Cyberspace Command - Fort Meade, MD
- Space Force / Space Delta 6 (Cyber Operations) - Peterson SFB, CO
- Defense Cyber Crime Center (DC3) - Linthicum Heights, MD

## Major Defense Contractors (DoD 8140 Compliance Required)

- Booz Allen Hamilton - 15,000+ cyber positions across DoD contracts
- Raytheon / RTX - Cyber defense for weapons systems and military networks
- Lockheed Martin - Cyber for F-35, satellites, and classified programs
- Northrop Grumman - Cyber operations and intelligence support
- General Dynamics Information Technology (GDIT) - DoD network operations
- Leidos - Intelligence community and DoD cyber support
- SAIC - Military cyber operations and training
- ManTech International - Defense and intelligence cyber services
- Peraton - Intelligence community cyber operations
- CACI International - DoD and IC cyber support

## Why DoD 8140 Approval Matters to Your Career

DoD Directive 8140 replaced the older DoD 8570 mandate and requires every person performing cyberspace work roles within the Department of Defense to hold an approved baseline certification. Without an approved certification, you cannot be hired for, assigned to, or continue working in a DoD cyber position. Period.

The RCCE is one of the select certifications that satisfies this requirement. This means that every graduate who earns their RCCE through an RCU partner program walks out with a credential that is not just a resume line item. It is a legal requirement for employment in the largest cybersecurity workforce on the planet. No RCCE (or equivalent approved cert) means no DoD cyber job. With RCCE, you have cleared that gate before you even submit your first application.

Combined with a security clearance (which your employer will typically sponsor), the RCCE opens access to tens of thousands of cybersecurity positions that most civilian-only certifications cannot reach.

# 16. Faculty Qualifications & Staffing Model

## RECOMMENDED FACULTY QUALIFICATIONS

Partner universities should staff cybersecurity programs with faculty who meet the following minimum qualifications. Rocheston provides faculty training and certification support to help institutions meet these standards.

### Full-Time Faculty (Tenure-Track)

- Doctoral degree (Ph.D. or D.Sc.) in Cybersecurity, Computer Science, or closely related field
- Minimum 3 years of industry experience in cybersecurity roles
- At least one industry certification (RCCE, CISSP, or equivalent)
- Active research program with peer-reviewed publications
- CyberRange proficiency certification (provided by Rocheston during onboarding)

### Industry Practitioners (Adjunct Faculty)

- Master's degree minimum (exceptions for exceptional industry credentials)
- Minimum 5 years of hands-on cybersecurity experience
- Currently employed in relevant security roles (SOC, Red Team, CISO, etc.)
- RCCE Level 2 or higher certification
- Demonstrated teaching ability through guest lectures, training delivery, or mentorship

### Recommended Faculty-to-Student Ratios

- Lecture courses: 1:30 maximum
- Lab courses: 1:15 maximum (critical for hands-on supervision)
- Capstone advising: 1:5 maximum
- Graduate thesis supervision: 1:3 maximum

# 17. Student Career Outcomes & Employer Partners

## TARGET CAREER PATHWAYS BY PROGRAM

| Program | Entry-Level Roles | Mid-Career Roles (3-5 Years) |
|---|---|---|
| **B.S.CE** | SOC Analyst, Jr. Penetration Tester, Security Engineer I, Vulnerability Analyst | Senior Penetration Tester, Security Architect, Threat Hunter, Red Team Operator |
| **B.S.CDI** | Cyber Threat Analyst, Digital Forensics Examiner, Intelligence Analyst | Senior Threat Intelligence Analyst, DFIR Lead, Counterintelligence Specialist |
| **M.S.CDS** | Security Manager, GRC Analyst, Senior Security Engineer | CISO, VP of Security, Director of Cyber Risk, Principal Security Architect |
| **M.S.AISAS** | AI Security Engineer, ML Security Researcher | Head of AI Security, AI Red Team Lead, AI Governance Director |
| **GD Offensive** | Penetration Tester, Red Team Operator | Senior Red Team Lead, Offensive Security Manager |
| **GD GRC** | GRC Analyst, Compliance Specialist | GRC Director, Chief Compliance Officer, Risk Manager |
| **Cert Foundations** | SOC Analyst Tier 1, Help Desk Security | SOC Analyst Tier 2, Security Operations Lead |

## SALARY BENCHMARKS (US MARKET, 2025)

Based on data from Bureau of Labor Statistics, CyberSeek, and Rocheston employer partner surveys:

- Entry-Level SOC Analyst: $65,000 - $85,000
- Penetration Tester: $85,000 - $130,000
- Security Engineer: $100,000 - $160,000
- Senior Security Architect: $150,000 - $220,000
- CISO (Mid-Market): $200,000 - $350,000
- CISO (Enterprise/Fortune 500): $350,000 - $700,000+
- AI Security Engineer: $140,000 - $250,000

## TARGET EMPLOYER CATEGORIES

- Defense & Intelligence: Department of Defense, NSA, CIA, FBI, DHS, defense contractors (Lockheed Martin, Raytheon, Northrop Grumman, Booz Allen Hamilton)
- Big Tech: Google, Microsoft, Amazon, Apple, Meta, NVIDIA
- Financial Services: JPMorgan Chase, Goldman Sachs, Bank of America, Visa, Mastercard
- Consulting & Advisory: Deloitte, PwC, EY, KPMG, Accenture, Mandiant (Google Cloud)
- Healthcare & Pharma: UnitedHealth, CVS Health, Johnson & Johnson, Pfizer
- Critical Infrastructure: Duke Energy, Southern Company, Exelon, major water utilities

- Security Vendors: CrowdStrike, Palo Alto Networks, Fortinet, SentinelOne, Zscaler

# 18. Admissions, Tuition & Financial Aid Framework

## ADMISSIONS REQUIREMENTS BY PROGRAM

### Bachelor of Science Programs (B.S.CE / B.S.CDI)

- High school diploma or equivalent (GED)
- Minimum 3.0 GPA (2.8 with conditional admission and summer bridge program)
- SAT: 1100+ or ACT: 22+ (test-optional policy available)
- Personal statement (500 words): Why cybersecurity?
- Letter of recommendation from STEM teacher, employer, or mentor
- No prior cybersecurity experience required

### Master of Science Programs (M.S.CDS / M.S.AISAS)

- Bachelor's degree in STEM field from accredited institution (3.0 GPA minimum)
- OR: Bachelor's degree in any field + 3 years of professional cybersecurity experience
- GRE scores: Recommended but not required
- Professional resume
- Statement of purpose (750 words)
- Two professional or academic references
- M.S.AISAS additionally requires: Python proficiency + basic ML coursework or equivalent

### Graduate Diplomas

- Bachelor's degree from accredited institution
- OR: 2+ years of professional IT/security experience with relevant certifications
- Professional resume and statement of intent

### Professional Certificates

- Foundations Certificate: No prerequisites (open enrollment)
- Advanced Certificates: RCCE Level 1 or equivalent experience

## SUGGESTED TUITION FRAMEWORK

Partner universities set their own tuition rates. The following are recommended ranges based on market analysis of comparable programs:

| Program | Total Program Cost (Suggested) | Per Credit/Module |
|---|---|---|
| **B.S.CE / B.S.CDI (In-State)** | $48,000 - $72,000 | $400 - $600/credit |
| **B.S.CE / B.S.CDI (Out-of-State)** | $80,000 - $120,000 | $667 - $1,000/credit |
| **M.S.CDS / M.S.AISAS** | $36,000 - $54,000 | $1,000 - $1,500/credit |

| | | |
|---|---|---|
| **Graduate Diplomas** | $18,000 - $28,000 | $750 - $1,167/credit |
| **Professional Certificates** | $8,000 - $15,000 | Per program |

## FINANCIAL AID & SCHOLARSHIPS

- Federal Financial Aid (FAFSA): Available for B.S. and M.S. programs at accredited partner institutions
- GI Bill / Military Benefits: All programs approved for VA educational benefits
- Rocheston Merit Scholarships: Up to $10,000/year for B.S. students demonstrating exceptional aptitude through CyberRange challenge scores
- Diversity in Cybersecurity Scholarship: $5,000/year for underrepresented students
- Women in Cyber Scholarship: $5,000/year for female-identifying students
- Career Changer Grant: $3,000 towards Professional Certificate tuition for career switchers
- Employer Tuition Reimbursement: Most Fortune 500 employers reimburse RCCE-aligned programs
- Income Share Agreements (ISA): Select partner institutions offer ISAs for Professional Certificates

## APPLICATION DEADLINES

- Fall Semester: August 1st (Priority: March 15th)
- Spring Semester: December 15th (Priority: October 1st)
- Summer Sessions: April 15th
- Professional Certificates: Rolling admissions (cohorts start quarterly)
- Graduate Diplomas: Rolling admissions with monthly start dates

---

**ROCHESTON UNIVERSITY PARTNERSHIP**

Curriculum and Labs powered by Rocheston University (RCU)



ANAB Accredited | ISO/IEC 17024 | US DoD 8140 Approved

**www.rocheston.com**

# Important Disclaimer

## SAMPLE DOCUMENT

This is a sample document intended to demonstrate the scope and depth of the Rocheston Cybersecurity Academic Framework (RCF). The programs, course codes, credit structures, and institutional details presented herein are illustrative examples designed to showcase what a partner university can build using the RCF platform.

### ABOUT ROCHESTON CYBERSECURITY UNIVERSITY (RCU)

Rocheston Cybersecurity University (RCU) is not a real university and does not offer degrees, diplomas, or academic credentials. RCU is a brand and educational content platform owned and operated by Rocheston LLC. RCU does not have institutional accreditation and is not authorized to grant academic degrees or diplomas of any kind.

### WHAT RCU PROVIDES

RCU supplies comprehensive cybersecurity curriculum content, educational technology platforms (including Cybernotes™, CyberRange Sphere™, CyberSim™, AI-Tutor™, and Nexus™), and professional certification pathways such as the Rocheston Certified Cybersecurity Engineer (RCCE). These are content and training resources only.

### PARTNER INSTITUTION RESPONSIBILITIES

Any degrees, diplomas, certificates, or academic credentials are issued exclusively by accredited partner educational institutions that license RCU's content and platforms. Partner institutions maintain full responsibility for their own institutional accreditation, academic governance, degree-granting authority, student enrollment, faculty oversight, and all academic policies. Students are enrolled in and receive all academic credentials from the partner institution, not from RCU or Rocheston.

### NO REPLACEMENT OF ACCREDITATION

RCU's curriculum and technology platforms do not replace, substitute, or transfer any institutional accreditation. Partner institutions must obtain and maintain their own accreditation through recognized accrediting bodies independent of any relationship with RCU or Rocheston. RCU functions solely as a curriculum content provider and educational technology vendor. All academic credentials, transcripts, and degrees bear the name and authority of the partner institution only.