



Technical Comparison



RCCE COMPETITOR COMPARISON

The Modern Certification for the Modern Times



SUCCEED

Rocheston
Certified
Cybersecurity
Engineer



THE PROBLEM

1. For too long, the cybersecurity training and certification industry has wallowed in **outdated methodologies and content** that barely addresses the complexities of modern cybersecurity threats.
2. Many providers have been **repackaging ancient materials** as new, in a sector where innovation should be leading the charge.
3. This stagnation has significantly **diluted the value of such certifications**, especially considering the often exorbitant fees, which can reach upwards of \$6,000.
4. It's a scenario that has left many yearning for a more effective and impactful learning experience.

QUALITY AND EXCELLENCE

1. **Our training programs stand out** for their depth, quality, and relevance, diverging sharply from the competition.
2. **We don't produce run-of-the-mill courses;** instead, we craft comprehensive, avant-garde content tailor-made for addressing today's cybersecurity challenges head-on.
3. **Offering round-the-clock access to our labs** underscores our dedication to facilitating continuous, hands-on learning. This dedication is what propels our offerings from mere educational tools to foundational pillars of a new epoch in cybersecurity training.

CYBERSECURITY ENGINEERS



Cybersecurity engineers, identify threats and vulnerabilities in systems and software, then apply their skills to developing and implementing high-tech solutions to defend against hacking, malware, ransomware, insider threats and all types of cybercrime. They'll serve as a go-to team member for security policies and procedures.



RCCE DOD 8140 JOB ROLES



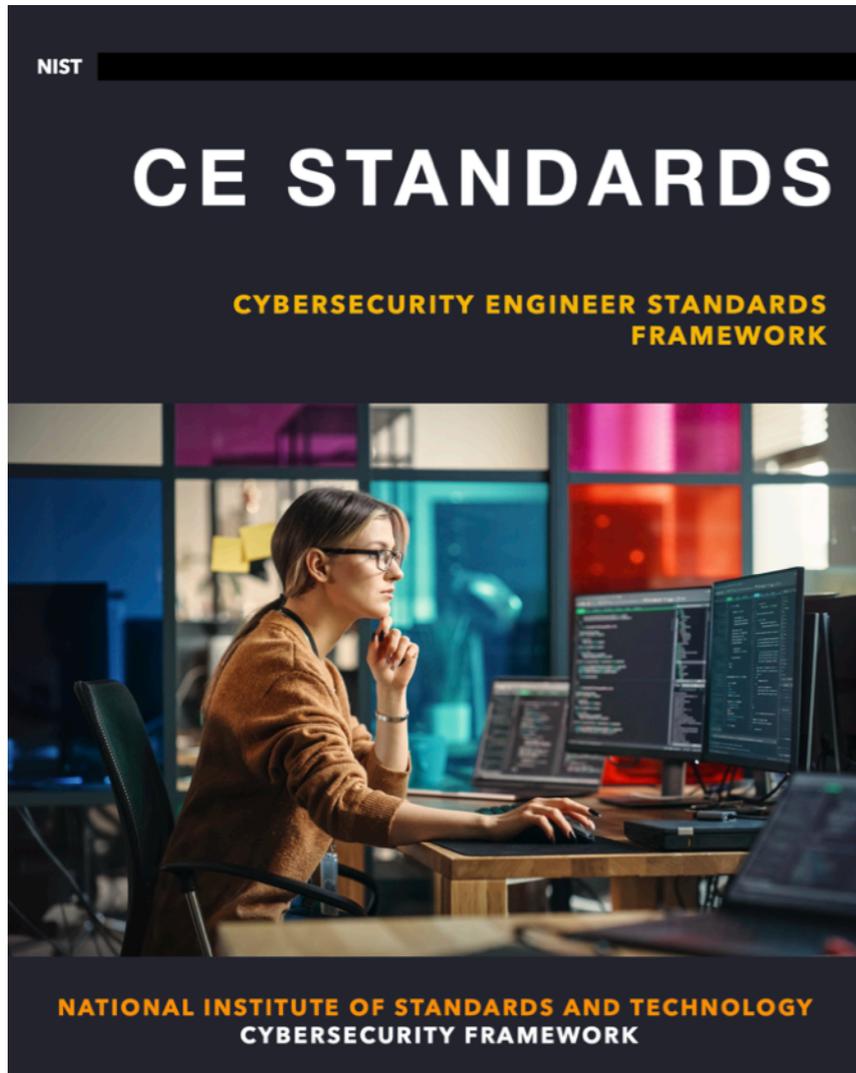
AMERICAN

ROCHESTON CERTIFIED CYBERSECURITY ENGINEER

RCCE IS ON THIS LIST

IASAE I	IASAE II	IASAE III
CASP+ CE CISSP (or Associate) CSSLP RCCE	CASP+ CE CISSP (or Associate) CSSLP RCCE	CISSP-ISSAP CISSP-ISSEP CCSP RCCE
CSSP Analyst ¹	CSSP Infrastructure Support ¹	CSSP Incident Responder ¹
CEH CFR CCNA Cyber Ops CCNA-Security CySA+ ** GCIA GCIH RCCE GICSP Cloud+ SCYBER PenTest+	CEH CySA+ ** GICSP SSCP CHFI CFR Cloud+ RCCE CND	CEH CFR CCNA Cyber Ops CCNA-Security CHFI CySA+ ** GCFA RCCE GCIH SCYBER PenTest+

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security CND Network+ CE SSCP RCCE	CCNA Security CySA+ ** GICSP GSEC Security+ CE CND RCCE SSCP	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH RCCE CCSP
IAM Level I	IAM Level II	IAM Level III
CAP CND Cloud+ GSLC Security+ CE HCISPP RCCE	CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO RCCE HCISPP	CISM CISSP (or Associate) GSLC CCISO RCCE



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

RCCE REPLACES THESE CERTIFICATIONS



Level 1



Level 2



DoD 8140 Job Role Comparison

Comparison

CEH DOD JOB ROLE

1. Network Operations Specialist
2. Cyber Defense Infrastructure Support Specialist
3. Vulnerability Assessment Analyst
4. Cyber Defense Analyst
5. R&D Specialist
6. System Testing & Evaluation Specialist

RCCE DOD JOB ROLE

1. All-Source Analyst
2. Warning Analyst
3. Forensics Analyst
4. Cyber Defense Forensics Analyst
5. Cyber Operations Planner
6. Systems Security Analyst
7. Cyber Defense Analyst
8. Cyber Defense Incident Responder
9. Vulnerability Assessment Analyst
10. Secure Software Assessor
11. Research & Development Specialist
12. Program Manager
13. IT Project Manager
14. Product Support Manager
15. IT Program Auditor

DoD 8140 Job Role Comparison

Comparison

PENTEST+ DOD JOB ROLE

1. Forensics Analysis
2. Cyber Defense Forensics Analyst
3. Cyber Defense Analyst
4. Cyber Defense Infrastructure Support Specialist
5. Cyber Defense Incident Responder
6. Vulnerability Assessment Analyst
7. Security Controls Assessor

RCCE DOD JOB ROLE

1. All-Source Analyst
2. Warning Analyst
3. Forensics Analyst
4. Cyber Defense Forensics Analyst
5. Cyber Operations Planner
6. Systems Security Analyst
7. Cyber Defense Analyst
8. Cyber Defense Incident Responder
9. Vulnerability Assessment Analyst
10. Secure Software Assessor
11. Research & Development Specialist
12. Program Manager
13. IT Project Manager
14. Product Support Manager
15. IT Program Auditor

NICE FRAMEWORK RESOURCE CENTER

The NICE Framework is a fundamental reference for describing and sharing information about cybersecurity work.



1. *Research & Development Specialist*
2. *Cyber Defense Analyst*
3. *Vulnerability Assessment Analyst*
4. *Threat/Warning Analyst*
5. *Cyber Defense Incident Responder*
6. *Exploitation Analyst*
7. *Network Operations Specialist Technical*
8. *Support Specialist System Administrator*
9. *Systems Security Analyst*

RCCE Certification is now mapped to *NICE Framework Job Roles*

GOVERNANCE & RISK MANAGEMENT

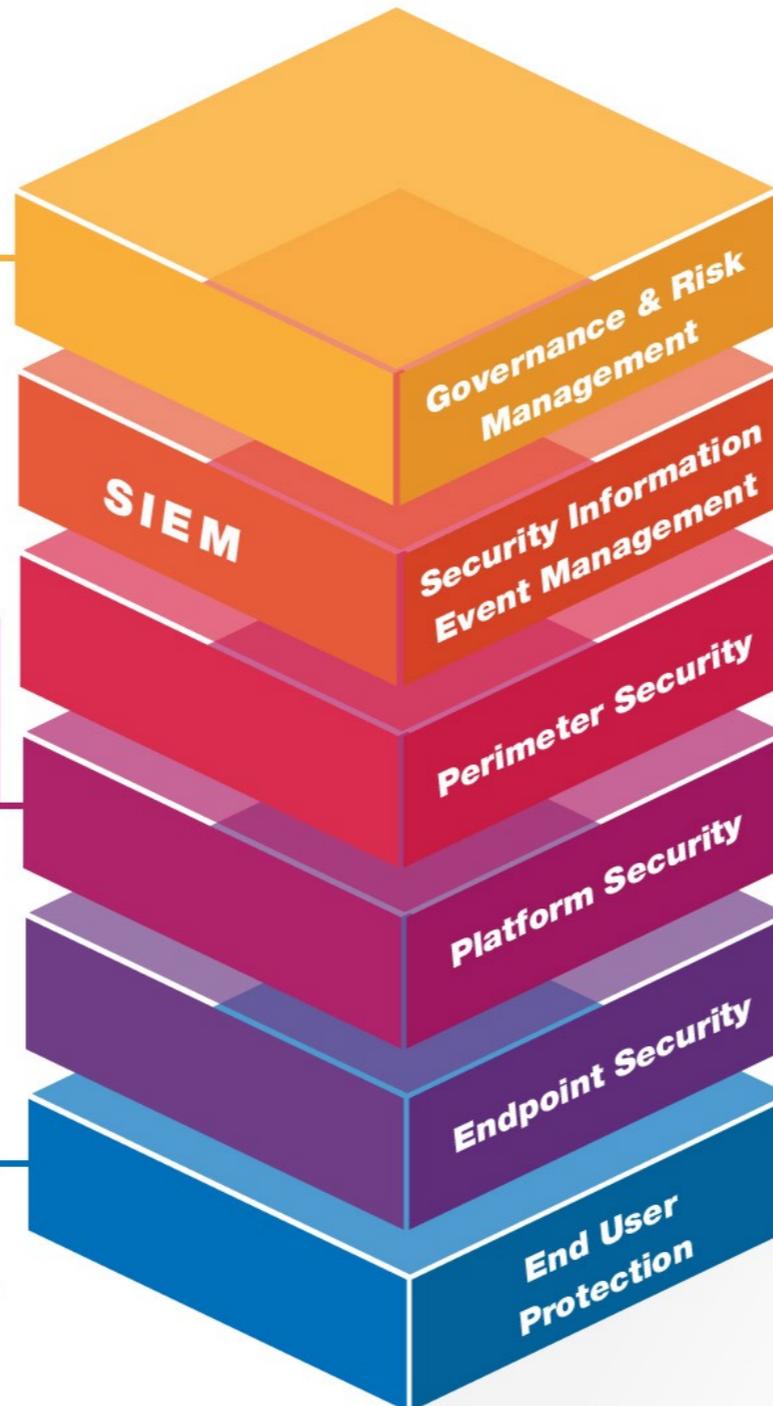
- ISO 27002 Compliant
- Center for Internet Security (CIS) Controls
- 3 Annual Pen Tests
- Privacy Shield Certified
- GDPR/CCPA Compliant
- Enterprise Risk Register
- NIST SP 800-53 Compliant
- SSAE 18 SOC 1 Type 2 Certified
- Standard Information Gathering (SIG)
- Information Security Audit Reports
- Enterprise Incident Response

PLATFORM SECURITY

- Next Generation Firewalls
- Antivirus For Servers
- AES 256 Encryption at Rest
- Segregated Active Directory & VLANS
- Privileged Account Vaulting
- Continuous Vulnerability Scanning & Patch Management
- Secure Data Backups and Disaster Recovery
- Operating Systems Hardening

END USER PROTECTION

- Cybersecurity Awareness Training
- Multifactor Authentication
- Role-Based Access Control
- Simulated Phishing Campaigns



SIEM

- Raw Logs, Endpoint Data & Network Traffic Analytics
- Unified Log Data
- User Behavior Analytics (UBA)
- Suspicious Activity Detection & Alerts

PERIMETER SECURITY

- External Firewalls
- Remote Access
- Spam Filtering
- Threat Intel Feeds
- Remote Authentication Reporting
- Brute Force and DoS Detection
- Data Center Physical Security

ENDPOINT SECURITY

- Automated Microsoft Windows and 3rd Party application Patch Management
- Antivirus and Endpoint Detection & Response (EDR)
- Remote Monitoring & Management System
- Local Admin Password Solution
- Full Disk Encryption
- Mobile Device Management
- Group Policy Enforcement
- Password Complexity
- Brute Force Prevention

RCCE COVERS ALL OF THESE TECHNOLOGIES

RCCE JOB ROLE = **CYBERSECURITY ENGINEER**

RCCE COVERS ALL OF THESE TECHNOLOGIES

**Extreme
Hacking**

**Penetration
Testing**

**Risk
Assessment**

**Incident
Handling**

**Vulnerability
Management**

**Network
Defense**

**Cloud
Security**

Linux Skills

**Python/Ruby
PHP Rust Skills**

**Governance
And
Compliance**

Kubernetes

**Infrastructure
Security**

Zero Trust

**Identity
Management**

IaaS Security

**Malware
Analysis**

**Cybercrime
Investigations**

**Forensic
Analysis**

**Container
Security**

CyberLaw

**Web
Applications
Security**

**Red Team /
Blue Team**

IoT

**AI, Machine
Learning**



VINES

ROCHESTON TRAINING

SOLUTION WITH VINES

VINES



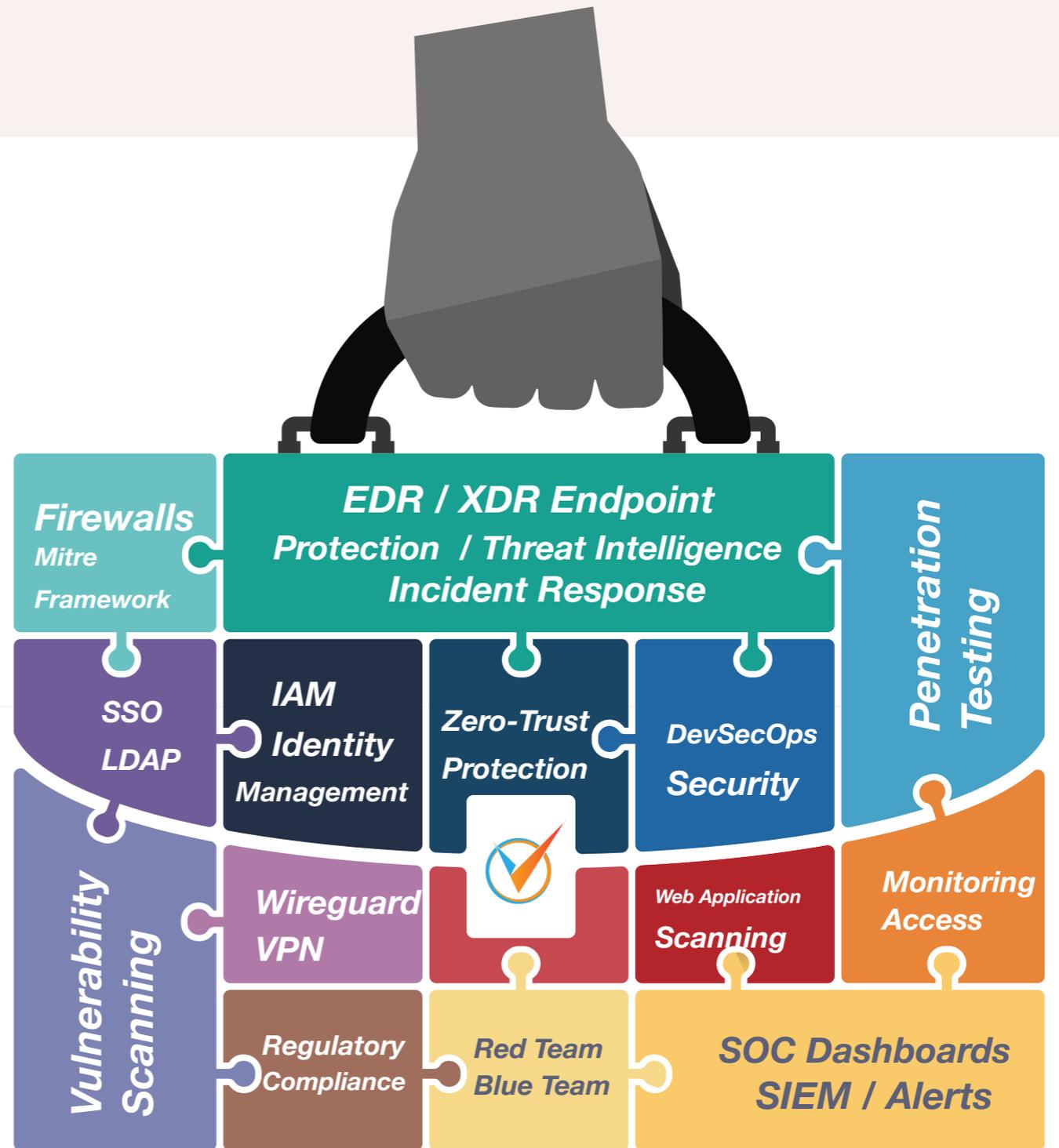
VINES

VINES

VINES

VINES CONTAINS
ESSENTIAL

TECHNOLOGIES TO
PROTECT AND SECURE



Everything an organization needs is here.



ROCHESTON VINES

Real-time monitoring

Points Counter **Power Consumption** Management



3 5123 7 1132 4 3451 8 2451

- Secondary Options
- Settings

Inputs

0	224
224	224
224	151



Summary data

75%

25%

25%

02

75%

Summary data

April

SUN	MON	TUE	WED	THU	FRI	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Events:

- FRI 16:21 am Pick up documents from a friend
- TUE 18:01 am Pick up documents from a friend

Timeline:

2014 2015 2016 2017 2018 2021 2022

Summary data

900

February

01

02

03

04

05

06



**Asset
Discovery**

Launch



**Vines
Manager**

Launch



**Application
Deepscan**

Launch



**Vines
Firewall**

Launch



**Red Team
Blue Team**



**Vulnerability
Database**



**Attack
Map**



**Wazuh
EDR**



**Monkey
Island**



**SSH
Shell**



**Threat
Intelligence**



**Live
Threats**



**Incident
Response**



**SOAR
Cortex**



**Mitre Attack
Visualizer**



**DevSecOps
Jenkins**

VULNERABILITY VINES

RCCE DOMAINS

1. Cybersecurity Threats, Attacks and Defenses
2. Reconnaissance, ML and Artificial Intelligence
3. Cyber Vulnerabilities
4. Web Application Attacks
5. Webshells, Spywares and Trojans
- 6 Denial of Service Attacks
7. Log Management and Network Analyzers
8. Identity and Access Management
9. Wireless and 5G
10. Firewalls, Endpoint Detection and Response
11. Hacking Frameworks
12. Cryptography
13. Malware Analysis
14. IoT Security
15. Virtualization and Data Centers
16. Android hacking
17. Blockchain and Cryptocurrency
18. Quantum Computing
- 19: Cybersecurity Policies and Governance
- 20 Risk Assessment
21. Risk Management
22. Incident Response and Handling
23. DevSecOps
24. Patch Management
25. Cloud Security with AWS, Azure and GCloud
26. Rocheston Cybersecurity Framework
27. Zero Trust Architecture

RCCE Comparison

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
ANSI ISO/IEC 17024 Accredited	✓	✓	✓	✓	✓	✓
DoD 8570 Approved	✓	✓	✓	✓	✓	✓
100% Cloud based training	✓	✗	✗	✗	✗	✗
100% Linux based training	✓	✗	✗	✗	✗	✗
Covers Hacking Skills	✓	✓	✗	✗	✓	✗
Covers Latest Technologies in Cybersecurity	✓	✗	✗	✗	✗	✗
Covers Incident Handling	✓	✓	✓	✓	✓	
Covers Network Defense	✓	✗	✗	✗	✗	✗
Covers Risk Management	✓	✗				✓
Covers Compliance and Governance	✓	✗	✗	✓	✗	✓
Covers Kubernetes Deployments	✓	✗	✗	✗	✗	✗
Covers Azure, AWS, Google Cloud	✓	✗	✗	✗	✗	✗
Covers Blockchain and Cryptocurrencies	✓	✗	✗	✗	✗	✗
Covers Quantum Computing	✓	✗	✗	✗	✗	✗
Covers Red Team / Blue Team Engagements	✓	✗	✗	✗	✓	✗
Cyber Range Sphere	✓	✗	✗	✗	✗	✗
Covers Virtualization Technologies	✓	✗	✗	✗	✗	✗
Covers Data Centers	✓	✗	✗	✗	✗	✗

RCCE Comparison

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Covers Infrastructure Security	✓	✗	✗	✗	✗	✗
Covers Linux Programming	✓	✗	✗	✗	✗	✗
Covers Vulnerability Management	✓	✓	✗	✓	✓	✗
Covers DevSecOps	✓	✗	✗	✗	✗	✗
Covers Artificial Intelligence / Machine Learning	✓	✗	✗	✗	✗	✗
Covers DarkWeb	✓	✗	✗	✗	✗	✗
Covers Cloud Backups and Patch Management	✓	✗	✗	✓	✓	✓
Covers Ethics, Policies and Standards	✓	✗	✗	✗	✗	✓
Rocheston Rose Linux OS (1tb Tools)	✓	✗	✗	✗	✗	✗
Rocheston Macsys	✓	✗	✗	✗	✗	✗
Rocheston Maya (Instructor Portal)	✓	✗	✗	✗	✗	✗
Rocheston Be	✓	✗	✗	✗	✗	✗
Rocheston Winston (Forensics OS)	✓	✗	✗	✗	✗	✗
Azure Based Labs	✓	✗	✗	✗	✗	✗
Rocheston Rosecoin (Own Cryptocurrency)	✓	✗	✗	✗	✗	✗
Rocheston Search (Own Search Engine)	✓	✗	✗	✗	✗	✗
Rocheston Data Centers (Own Data centers)	✓	✗	✗	✗	✗	✗
Rocheston Vines (Own Scanner)	✓	✗	✗	✗	✗	✗

RCCE Comparison

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
<i>Rocheston Niles (NFT Tokens)</i>	✓	✓	✗	✗	✗	✗
<i>Rocheston Jerico (Blockchain crypto exchange)</i>	✓	✓	✗	✗	✗	✗
<i>Rocheston Cyberbook (Own laptop hardware)</i>	✓	✗	✗	✗	✗	✗
<i>Rocheston Hackathon (Hacking competition)</i>	✓	✗	✗	✗	✗	✗
<i>Rocheston Ramsys (Remote proctoring)</i>	✓	✓	✗	✗	✗	✗
<i>Rocheston Glass (Own virtual meeting platform)</i>	✓	✗	✗	✗	✗	✗
<i>Rocheston Labs (Cybersecurity R & D)</i>	✓	✗	✗	✗	✗	✗
<i>Rocheston Threat Intelligence Center</i>	✓	✗	✗	✗	✗	✗
<i>Course Content Updated weekly</i>	✓	✗	✗	✗	✗	✗
<i>Reasonably priced</i>	✓	✗	✗	✗	✗	✗
<i>Beautifully Designed Training Materials</i>	✓	✗	✗	✗	✗	✗
<i>Interactive Labs</i>	✓	✗	✗	✗	✗	✗
<i>Labs Migration to Own Cloud</i>	✓	✗	✗	✗	✗	✗
<i>Downloadable Labs</i>	✓	✗	✗	✗	✗	✗
<i>Cutting-Edge Technologies</i>	✓	✗	✗	✗	✗	✗
<i>Rocheston Search (Own Search Engine)</i>	✓	✗	✗	✗	✗	✗
<i>Prepares for Job role Cybersecurity Engineer</i>	✓	✗	✗	✗	✗	✗
<i>Limited and Prestigious</i>	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Cybersecurity Policies and Governance	✓	✓	✗	✓	✗	✓
Risks/Threats/Vulnerability Assessment	✓	✓	✗	✗	✗	✓
Risks/Threats/Vulnerability Management	✓	✗	✗	✗	✗	✓
Security Incident Response and Recovery Plan	✓	✗	✓	✗	✓	✗
Cybersecurity Threats, Attacks and Defenses	✓	✓	✗	✗	✗	✗
Reconnaissance, ML and Artificial Intelligence	✓	✗	✗	✗	✗	✗
Cyber Vulnerabilities	✓	✓	✓	✓	✓	✗
Web Application Attacks	✓	✓	✗	✗	✓	✗
Webshells, Spywares and Trojans	✓	✓	✗	✗	✓	✗
Denial of Service Attacks	✓	✓	✗	✓	✓	✗
Log Management and Network Analyzers	✓	✓	✗	✓	✓	✓
Identity and Access Management	✓	✗	✗	✗	✗	✗
Wireless and 5G	✓	✗	✗	✗	✗	✗
Firewalls, Endpoint Detection and Response	✓	✓	✗	✓	✓	✗
Hacking Frameworks	✓	✓	✗	✓	✓	✗
Cryptography	✓	✓	✗	✗	✓	✗
Malware Analysis	✓	✓	✗	✓	✓	✓
IoT Security	✓	✓	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Virtualization and Data Centers	✓	✓	✗	✗	✗	✗
Android Hacking	✓	✓	✗	✗	✗	✗
Blockchain and Cryptocurrency	✓	✓	✗	✗	✗	✗
Quantum Computing	✓	✗	✗	✗	✗	✗
Cybersecurity Policies and Governance	✓	✓	✗	✗	✗	✓
Risk Assessment	✓	✗	✗	✓	✗	✓
Risk Management	✓	✗	✓	✗	✗	✓
Incident Response and Handling	✓	✗	✓	✗	✓	✗
DevSecOps	✓	✗	✗	✗	✗	✗
Patch Management	✓	✗	✗	✗	✓	✗
Cloud Security with AWS, Azure and GCloud	✓	✗	✗	✗	✗	✓
Rocheston Cybersecurity Framework	✓	✗	✗	✗	✗	✗
Zero Trust Architecture	✓	✗	✗	✗	✗	✗
Introduction to Penetration Testing.key	✓	✗	✗	✗	✗	✗
Penetration Testing Methodologies	✓	✗	✗	✗	✗	✗
Legal and Ethical Issues in Penetration Testing	✓	✗	✗	✗	✗	✗
Rules of Engagement	✓	✗	✗	✗	✗	✗
Network Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
<i>Vulnerability Assessment and Exploitation</i>	✓	✗	✗	✗	✗	✗
<i>Web Application Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Wireless Network Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Physical Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Database Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Source Code Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Social Engineering in Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Cyber Threat Intelligence in Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Mobile and IoT Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Cloud Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Firewalls & IDS in Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Report Writing in Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Active Directory (AD) Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Administrative Interface Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Anti-Malware Efficacy Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Apache2 and nginx Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Multi-factor authentication (MFA) Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Network Mapping Penetration Testing</i>	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Ongoing Tests Penetration Testing	✓	✗	✗	✗	✗	✗
OWASP Top 10 Penetration Testing	✓	✗	✗	✗	✗	✗
Best Practices Penetration Testing	✓	✗	✗	✗	✗	✗
Password Cracking Penetration Testing	✓	✗	✗	✗	✗	✗
Password Strength Penetration Testing	✓	✗	✗	✗	✗	✗
Patch Management Penetration Testing	✓	✗	✗	✗	✗	✗
Penetration Testing from Various Locations	✓	✗	✗	✗	✗	✗
Phishing Attack Simulation Penetration Testing	✓	✗	✗	✗	✗	✗
Post-Exploitation Techniques	✓	✗	✗	✗	✗	✗
Privilege Escalation Penetration Testing	✓	✗	✗	✗	✗	✗
Race Condition Bugs Penetration Testing	✓	✗	✗	✗	✗	✗
Ransomware Attacks Penetration Testing	✓	✗	✗	✗	✗	✗
Real-time Alerting Penetration Testing	✓	✗	✗	✗	✗	✗
Reconnaissance Penetration Testing	✓	✗	✗	✗	✗	✗
Red Teaming Penetration Testing	✓	✗	✗	✗	✗	✗
Regulatory Compliance Penetration Testing	✓	✗	✗	✗	✗	✗
Remote Access Penetration Testing	✓	✗	✗	✗	✗	✗
Rogue Device Detection Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
<i>Scan Open Ports Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Secure Token Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Security Policy Compliance Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Security Tool Efficacy Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Security Training Efficacy Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Server Misconfigurations Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Server Security Headers Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Server-side Request Forgery Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Session Hijacking Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Session Management Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Shadow IT Detection Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Social Media Footprinting Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Spear Phishing Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>SSL-TLS Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Wordpress Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Third Party and Supplier Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Third-party Software Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Threat Hunting Penetration Testing</i>	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Token Permissions Penetration Testing	✓	✗	✗	✗	✗	✗
Unauthorized Data Access Penetration Testing	✓	✗	✗	✗	✗	✗
URL Manipulation Penetration Testing	✓	✗	✗	✗	✗	✗
Use of Known Vulnerabilities Penetration Testing	✓	✗	✗	✗	✗	✗
Version Detection Penetration Testing	✓	✗	✗	✗	✗	✗
Virtual Machine Security Penetration Testing	✓	✗	✗	✗	✗	✗
VoIP Penetration Testing	✓	✗	✗	✗	✗	✗
VPN Security Penetration Testing	✓	✗	✗	✗	✗	✗
Vulnerabilities and Exposures (CVE) database Penetration Testing	✓	✗	✗	✗	✗	✗
Vulnerability Analysis Penetration Testing	✓	✗	✗	✗	✗	✗
Web Services-API Penetration Testing	✓	✗	✗	✗	✗	✗
Work from home Penetration Testing	✓	✗	✗	✗	✗	✗
Zero Trust Architecture Penetration Testing	✓	✗	✗	✗	✗	✗
Zero-day Exploit Penetration Testing	✓	✗	✗	✗	✗	✗
Mobile Application Penetration Testing	✓	✗	✗	✗	✗	✗
Man-in-the-Middle (MITM) Attacks Penetration Testing	✓	✗	✗	✗	✗	✗
Malware Analysis and Reverse Engineering	✓	✗	✗	✗	✗	✗
Logs Auditing Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Logic Penetration Testing	✓	✗	✗	✗	✗	✗
Local Network Access Control Penetration Testing	✓	✗	✗	✗	✗	✗
Load balancer Penetration Testing	✓	✗	✗	✗	✗	✗
Linux Servers Penetration Testing	✓	✗	✗	✗	✗	✗
IoT Device Penetration Testing	✓	✗	✗	✗	✗	✗
Intrusion Prevention System (IPS) Penetration Testing	✓	✗	✗	✗	✗	✗
Insider Threat Simulation Penetration Testing	✓	✗	✗	✗	✗	✗
Input Validation Penetration Testing	✓	✗	✗	✗	✗	✗
Infrastructure Configuration Review Penetration Testing	✓	✗	✗	✗	✗	✗
Information Disclosure Penetration Testing	✓	✗	✗	✗	✗	✗
Incident Response Capability Penetration Testing	✓	✗	✗	✗	✗	✗
Human Interface Device (HID) Attacks Penetration Testing	✓	✗	✗	✗	✗	✗
HTTP protocol verbs Penetration Testing	✓	✗	✗	✗	✗	✗
Firewall Configuration Penetration Testing	✓	✗	✗	✗	✗	✗
File Upload Penetration Testing	✓	✗	✗	✗	✗	✗
File system permissions Penetration Testing	✓	✗	✗	✗	✗	✗
Encryption At Rest & In Transit Penetration Testing	✓	✗	✗	✗	✗	✗
Embedded Device Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Email Phishing Campaigns Penetration Testing	✓	✗	✗	✗	✗	✗
Email Configuration Penetration Testing	✓	✗	✗	✗	✗	✗
DNS Security Penetration Testing	✓	✗	✗	✗	✗	✗
DDoS Mitigation Capability Penetration Testing	✓	✗	✗	✗	✗	✗
Database Security Penetration Testing	✓	✗	✗	✗	✗	✗
Cyberthreat Intelligence Penetration Testing	✓	✗	✗	✗	✗	✗
Cryptography for Penetration Testers	✓	✗	✗	✗	✗	✗
Cross-Site Request Forgery (CSRF) Attacks Penetration Testing	✓	✗	✗	✗	✗	✗
Cookie Security Penetration Testing	✓	✗	✗	✗	✗	✗
Content Management System (CMS) Penetration Testing	✓	✗	✗	✗	✗	✗
Codebase Review Penetration Testing	✓	✗	✗	✗	✗	✗
Code Injection Penetration Testing	✓	✗	✗	✗	✗	✗
Cloud Storage Penetration Testing	✓	✗	✗	✗	✗	✗
Cloud Container Penetration Testing	✓	✗	✗	✗	✗	✗
Client-side Security Controls Penetration Testing	✓	✗	✗	✗	✗	✗
Clickjacking Penetration Testing	✓	✗	✗	✗	✗	✗
Business Logic Penetration Testing	✓	✗	✗	✗	✗	✗
Brute Force Attacks Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
Breach Readiness Assessment Penetration Testing	✓	✗	✗	✗	✗	✗
Bot Detection Penetration Testing	✓	✗	✗	✗	✗	✗
Backup and Recovery Penetration Testing	✓	✗	✗	✗	✗	✗
Azure, AWS, GC Penetration Testing	✓	✗	✗	✗	✗	✗
Asset Discovery Penetration Testing	✓	✗	✗	✗	✗	✗
ARP Spoofing Penetration Testing	✓	✗	✗	✗	✗	✗
Application Container Penetration Testing	✓	✗	✗	✗	✗	✗
Application Behavior Penetration Testing	✓	✗	✗	✗	✗	✗
SSH Penetration Testing	✓	✗	✗	✗	✗	✗
WAF Penetration Testing	✓	✗	✗	✗	✗	✗
Blockchain Penetration Testing	✓	✗	✗	✗	✗	✗
DevSecOps in Penetration Testing	✓	✗	✗	✗	✗	✗
Identity and access management (IAM) Penetration Testing	✓	✗	✗	✗	✗	✗
Ethics in Penetration Testing	✓	✗	✗	✗	✗	✗
Tools in Penetration Testing	✓	✗	✗	✗	✗	✗
POS Systems Penetration Testing	✓	✗	✗	✗	✗	✗
Advanced Persistent Threat (APT) Penetration Testing	✓	✗	✗	✗	✗	✗
ATM Penetration Testing	✓	✗	✗	✗	✗	✗

RCCE Modules

	RCCE	CEH	GIAC	Security+	Pentest+	CISSP
<i>RFID and Access Control Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Endpoint Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Industrial Control Systems (ICS) & SCADA Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Dark Web Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Quantum Computing Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>AI and Machine Learning Systems Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Big Data Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Biometric Systems Penetration Testing</i>	✓	✗	✗	✗	✗	✗
<i>Drone & Robotics Penetration Testing</i>	✓	✗	✗	✗	✗	✗

EC-COUNCIL - TO GET THE CYBERSECURITY ENGINEER SKILLSET



DON'T BE A SUCKER

You will need to attend all these trainings

Pay for EC-Council CEH Training - \$3,900

Pay for EC-Council CEH Practical Training \$3,900

Pay for vCPENT (Pen Test Training) \$3,900

Pay for EC-Council CND (Network Defender) \$3,900

Pay for EC-Council CBP (Blockchain Training) \$3,900

Pay for EC-Council CCISO Training \$3,900

Pay for EC-Council Incident Handling Training \$3,900

Pay for EC-Council Encryption Specialist Training \$3,900

Pay for EC-Council EDRP (Disaster Recovery Training) \$3,900

Pay for EC-Council Cloud Security Training \$3,900

Pay for EC-Council Application Security Training \$3,900

Pay for EC-Council Secure Programming Training \$3,900

↓

Annual renewal fees: \$960

Total USD \$46,000

** Prices are rough estimate, not accurate*

RCCE - TO GET THE CYBERSECURITY ENGINEER **SKILLSET**



Just take the RCCE and you are done!

**SAVE Time & Money
Become a real
CyberSecurity Engineer**

EC-COUNCIL COSTS 50 TIMES MORE THAN RCCE

THAT IS SMART



Annual renewal fees: \$80

Save \$\$\$\$

** Prices are rough estimate*



HOW DOES RCCE COMPARE WITH OTHER CERTIFICATIONS

RCCE IS ELITE

The Rochester Certified Cybersecurity Engineer (RCCE) program distinguishes itself as a superior leader in the cybersecurity training landscape for several well-founded reasons. Here's an in-depth comparison showcasing its superiority over competing programs.

FORWARD-LOOKING

The Rochester Certified Cybersecurity Engineer (RCCE) program offers a comprehensive, forward-looking, and hands-on approach to cybersecurity training that is distinct from other certifications.

Its inclusion of advanced and emerging technologies, combined with the depth of hands-on real-world lab experience and a broad, vendor-neutral curriculum, positions RCCE as a premier certification for professionals seeking to advance their expertise in cybersecurity.

RCCE IS PROGRESSIVE

- *While certifications like Security+, CISSP, and CEH hold value and recognition within the industry, RCCE's unique blend of features caters to a rapidly evolving cybersecurity landscape, preparing professionals not just for today's threats but for the challenges and innovations of tomorrow.*
- *The cybersecurity arena is replete with numerous certifications, each designed to cater to different facets of the field. The Rocheston Certified Cybersecurity Engineer (RCCE) program, however, sets itself apart through its encompassing, progressive, and immersive curriculum and training methodology.*

STATE-OF-THE-ART CYBER RANGE LABS

- *Hands-On Learning Experience: RCCE training incorporates state-of-the-art cyber range labs, providing participants with a unique hands-on learning experience that closely simulates real-world cybersecurity scenarios.*
 - *This practical approach contrasts sharply with programs that rely heavily on theoretical knowledge. The immersive cyber range labs facilitate a deeper understanding of how to counteract and defend against complex cyber threats effectively, making RCCE training exceptionally practical and applicable.*
-

CYBER RANGE SPHERE

Client Name	Client Type
Aina	Desktop Clients
Apex Node	Cyber Range
Aqua	Desktop Clients
Binary Phantom	Cyber Range
Chrome	Desktop Clients
Chrono Lock	Cyber Range
Cipher Nexus	Cyber Range
Circles	Desktop Clients
Code Angis	Cyber Range
Crypto Engine	Cyber Range
CUDA	Artificial Intelligence
Cyber Beacon	Cyber Range
Data Sphere	Cyber Range
Debian Bookworm	Cyber Range
Docker Jammy	Cyber Range
Docker Jammy	Cyber Range
Doom	Cybersecurity Games
Echo Matrix	Cyber Range
Firefox	Desktop Clients
Ghost Circuit	Cyber Range
Horizon Watch	Cyber Range
Infection Monkey	Cyber Range
Jungle Jammy	Desktop Clients
Kali Linux	Extreme Hacking
Macsys	Desktop Clients
Maltego	Extreme Hacking
Malware and Exp...	Extreme Hacking
Matrix Scanner	Cyber Range
Nebula Keeper	Cyber Range
Nexus Core	Cyber Range
Nova Defender	Cyber Range
Nova Scanner	Cyber Range
Orbit Guard	Cyber Range
Parrot OS	Extreme Hacking
Photon Sentry	Cyber Range
Pixel Shield	Cyber Range
Planet Earth	Desktop Clients
Plasma Monitor	Cyber Range
Pulse Shield	Cyber Range
Quantum Grid	Cyber Range



FORWARD-THINKING CURRICULUM

- *Emphasis on Emerging Threats and Technologies: The cybersecurity field is rapidly evolving, and RCCE stays ahead of the curve by incorporating the latest trends, threats, and technological advancements into its curriculum.*
 - *This forward-thinking approach ensures that RCCE-certified professionals are not just prepared for today's cybersecurity landscape but are also equipped to adapt to future challenges, a benefit not always guaranteed in other programs.*
-

CURRICULUM DEPTH AND SCOPE

- *While CISSP is revered for its extensive coverage, emphasizing managerial perspectives alongside technical aspects, it may not immerse learners in the practical, hands-on experiences that are pivotal in today's cybersecurity landscape. RCCE fills this gap with a curriculum that is both broad in knowledge and deep in practical application.*
 - *CEH focuses predominantly on offensive security skills. In comparison, RCCE takes a more balanced approach, educating individuals on both offensive tactics and defensive strategies, ensuring a full-circle understanding of cybersecurity challenges and solutions.*
-

REAL-WORLD APPLICATION AND CYBER RANGE LABS

- *A distinguishing feature of RCCE is its cyber range labs, which simulate complex real-world cybersecurity scenarios, offering learners an unparalleled immersive experience.*
 - *Unlike Security+ and CISSP, which may lean more towards theoretical learning, RCCE emphasizes practical, hands-on experiences, catapulting learners into the thick of cyber warfare in controlled environments.*
-

EMPHASIS ON FUTURE-READY SKILLS

- *RCCE distinguishes itself by focusing profoundly on futuristic and evolving technologies.*
 - *It doesn't just prepare learners to address current security challenges but equips them with the knowledge to anticipate and mitigate future vulnerabilities, a feature not specifically highlighted to the same extent in Security+, CISSP, or CEH.*
-

**RCC
CE**

Cybersecurity Engineer