REDSPECTOR

// RCCSP · ADVANCED CLOUD SECURITY

Redspector Certified
Cloud Security Professional

PROFESSIONAL PROGRAM

An elite, hands-on certification for security professionals engineering multi-cloud defense — AWS, Azure, GCP, Kubernetes, DevSecOps, and cloud red teaming.

~/redspector/rccsp

```
redspector ~$ cloud_pentest --targets aws,azure,gcp --mode red-team

> multi-cloud attack chain & detection engineering verified.
```

ENROLL NOW

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520

"Building the Next Generation of Cybersecurity Professionals"

// 01 ABOUT

Course Overview

TheRedspector Certified CloudSecurity Professional (RCCSP) program is an elite, hands-on training track for engineers and security professionals mastering enterprise cloud defense. Students learn to architect, attack, and defend production multi-cloud environments across AWS, Azure, GCP, Kubernetes, and modern DevSecOps pipelines — from IAM exploitation to detection engineering and cloud IR.

12	24	03	01
CORE MODULES	HANDS-ON LABS	BONUS TRACKS	CERTIFICATION

// WHO SHOULD JOIN

Built for Cloud Defenders & Red Teamers

Cloud Engineers
Architects and engineers securing AWS, Azure and GCP workloads at scale.

Security Analysts
SOC and blue-team professionals moving into cloud detection engineering.

Penetration Testers
Red teamers pivoting into cloud attack paths and multi-cloud exploitation.

DevSecOps Engineers
Practitioners hardening CI/CD pipelines, IaC and Kubernetes clusters.

Incident Responders
IR professionals building cloud forensics and containment playbooks.

Advanced Students
Graduates targeting elite cloud-security roles and specialization.

// 02 PATH

Learning Journey

Astructured,six-stageprogressionfromcloud architecture to enterprise red teaming.

01

CLOUD ARCHITECTURE

ZeroTrustdesign,securelandingzones, hybrid & multi-cloud

02

IDENTITY & ACCESS

Federation,SAML/OAuth,PAM, JIT access, conditional policies

03

OFFENSIVE CLOUD

MITREATT&CKforCloud,initial access, privilege escalation

04

PLATFORM ENGINEERING

AWS,Azure,GCPsecurityengineering & threat hunting

05

CONTAINERS & DEVSECOPS

Kuberneteshardening,securepipelines,supply chain security

06

DETECT · RESPOND · GOVERN

SIEMengineering,cloudIR,forensics,CNAPP & compliance

// PROGRAM CURRICULUM

Modules 01–04

Foundations—cloudarchitecture,identity and offensive cloud techniques.

MOD 01 ADVANCED CLOUD ARCHITECTURE SECURITY

- Multi-Cloud Security Design
- Hybrid Cloud Security
- Zero Trust Cloud Architecture
- Secure Landing Zones
- Cloud Security Reference Architectures

LABS
- Design Enterprise Cloud Security Architecture
- Multi-Cloud Security Assessment

MOD 02 ADVANCED IAM & IDENTITY SECURITY

- Identity Federation
- SAML & OAuth Security
- OpenID Connect
- Privileged Access Management (PAM)
- Just-In-Time (JIT) Access
- Conditional Access Policies

LABS
- IAM Privilege Escalation Detection
- Identity Attack Simulation

MOD 03 CLOUD ATTACK TECHNIQUES

- MITRE ATT&CK for Cloud
- Initial Access Techniques
- Cloud Persistence
- Defense Evasion
- Privilege Escalation
- Lateral Movement

LABS
- Attack Path Mapping
- Cloud Red Team Operations

MOD 04 AWS SECURITY ENGINEERING

- IAM Exploitation
- Cross-Account Attacks
- S3 Bucket Exploitation
- Lambda Security
- EC2 Hardening
- KMS Security

LABS
- AWS Misconfiguration Exploitation
- AWS Threat Hunting

// PROGRAM CURRICULUM

Modules 05–08

Platformengineering—AWS,Azure,GCP, Kubernetes & DevSecOps.

MOD 05 AZURE SECURITY ENGINEERING

- Azure AD Attacks
- Managed Identity Abuse
- Azure RBAC Exploitation
- Azure Defender Operations
- Azure Sentinel

LABS

- Azure Security Assessment
- Azure Incident Response

MOD06 GOOGLE CLOUD SECURITY ENGINEERING

- GCP IAM Security
- Service Account Abuse
- Cloud Run Security
- Kubernetes Security
- SCC Operations

LABS

- GCP Threat Hunting
- GCP Security Review

MOD 07 KUBERNETES & CONTAINER SECURITY

- Kubernetes Hardening
- RBAC Security
- Container Escape Concepts
- Supply Chain Security
- Admission Controllers
- Runtime Security

LABS

- Secure Kubernetes Cluster
- Container Security Assessment

MOD 08 DEVSECOPS SECURITY

- Secure CI/CD Pipelines
- GitHub Security
- GitLab Security
- Jenkins Security
- Secret Detection
- Artifact Security

LABS

- Pipeline Attack Simulation
- CI/CD Hardening

// PROGRAM CURRICULUM

Modules 09–12

Detect,respondandgovern—SIEMengineering, IR, AI security & CNAPP.

MOD 09 CLOUD DETECTION ENGINEERING

- SIEM Engineering
- Detection Rule Development
- Cloud Log Analysis
- Threat Intelligence Integration
- Security Analytics

LABS
- Build Cloud Detection Rules
- Create Detection Dashboard

MOD 10 CLOUD INCIDENT RESPONSE & FORENSICS

- Cloud Forensic Acquisition
- Memory Analysis
- Log Correlation
- Ransomware Response
- Incident Containment

LABS
- Cloud Breach Investigation
- Forensics Report Creation

MOD 11 AI & LLM CLOUD SECURITY

- Secure AI Infrastructure
- LLM Threat Models
- Prompt Injection Risks
- AI Data Leakage Prevention
- Secure AI Deployment
- Model Supply Chain Security

LABS
- Secure LLM Deployment
- AI Security Assessment

MOD 12 ENTERPRISE CLOUD SECURITY OPERATIONS

- CSPM
- CWPP
- CIEM
- CNAPP
- Governance & Compliance
- Cloud Risk Management

LABS
- Enterprise Cloud Security Audit
- Compliance Assessment

// APPLIED LEARNING

Capstone & Bonus Tracks

Production-grade capstone and mastery modules to complete certification.

FINAL ENTERPRISE CAPSTONE

Build & Defend Enterprise Cloud

Students architect and defend a complete enterprise cloud environment across three providers.

01 AWS + Azure + GCP Deployment

02 Zero Trust Architecture

03 Kubernetes Cluster

04 Secure CI/CD Pipeline

05 SIEM & Threat Detection

06 Incident Response Playbook

07 Compliance Framework Mapping

08 Executive Security Report

BONUS EXPERT MODULES

Elite Specialization Tracks

CLOUD RED TEAM OPERATIONS
- Cloud Reconnaissance
- Privilege Escalation Paths
- Persistence Techniques
- Attack Chain Development

CLOUD PURPLE TEAM
- Adversary Emulation
- Detection Validation
- ATT&CK Mapping

CLOUD SECURITY AUTOMATION
- Terraform Security
- Security as Code
- Automated Compliance
- Automated Incident Response

~/redspector/capstone

```
redspector ~$  deploy --capstone "multi-cloud-defense" --env production

> status: certification requirements met. RCCSP eligible.
```

// CERTIFICATION

Benefits, Value & Contact

An industry-ready credential built for elite cloud security roles.

CERTIFICATION BENEFITS

- Professional RCCSP Certification
- Multi-Cloud Red & Blue Team Credentials
- Production-Grade Cloud Security Skills
- Elite Career Advancement Track
- Portfolio of Real Capstone Builds
- Verifiable Industry Recognition

WHY REDSPECTOR?

- Industry-Focused Training
- Practical Learning Approach
- Expert-Led Curriculum
- Real-World Methodologies
- Career-Oriented Skill Development
- Professional Certification Program

REDSPECTOR

CONTACT US

Start Your Cloud Security Journey

WEBSITE
www.redspector.com

EMAIL
team@redspector.com

PHONE
+91 80783 28520

"Building the Next Generation of Cybersecurity Professionals"

REDSPECTOR

// RCCSP · CLOUDSECURITYPROFESSIONAL

"Building the Next Generation of Cybersecurity Professionals"

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520