CLOUD SECURITY FUNDAMENTALS AND INCIDENT RESPONSE

SAISH VIJAY DHIWAR | Sanjivani University, Kopargaon

DIYINTERNSHIP
Learn by doing yourself

Internship Overview

Program

DIY Internship: Cloud Security Fundamentals & Incident Response

Duration

11 Weeks (June - August 2025)

Objective

Gain hands-on knowledge of cloud security concepts and incident response processes.

Key Focus Areas

Cloud Environment Setup

AWS/GCP configuration.

IAM & Storage Security

Identity and Access Management, cloud storage security.

Network & WAF

Network security and WAF configuration.

Vulnerability & Encryption

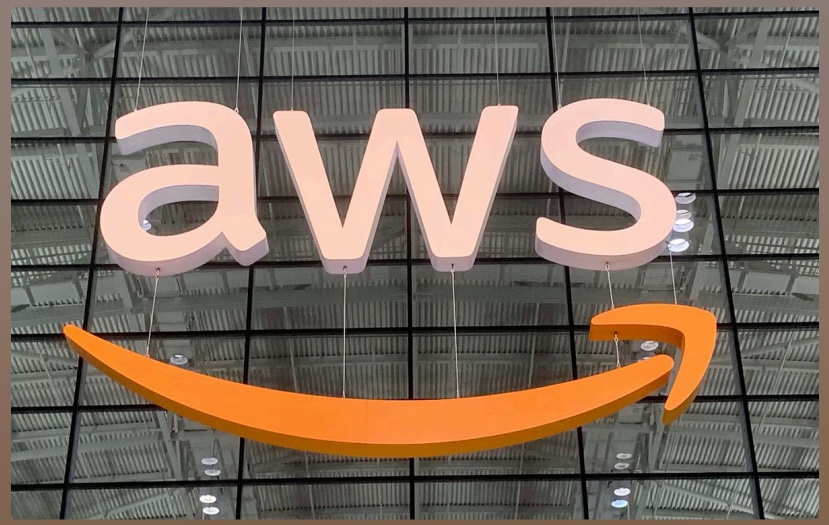
Scanning, remediation, data encryption.

Compliance & Auditing

Cloud compliance and auditing.

Incident Response

Handling security incidents.



Tools & Platforms Used

Cloud Platforms

- AWS (EC2, S3, IAM, CloudTrail, WAF, Config, Inspector)

Security Tools

- Cloudflare
- Vulnerability scanners

Monitoring Tools

- CloudWatch
- CloudTrail

Weekly Milestones: Weeks 1-4

Week 1-2: Cloud Environment Setup

1

Created AWS Free Tier Account, launched EC2 Instance, and configured basic setup.

Week 3: Cloud Storage Security

2

Configured S3 Bucket with security controls, applied access policies, and enabled security features.

Week 4: Logging & Monitoring

3

Enabled CloudTrail for auditing and configured alerts for suspicious activity using CloudWatch.

Weekly Milestones: Weeks 5-7

1

Week 5: Network Security

Configured Security Groups & Firewall Rules, blocked unnecessary ports, and hardened network security.

2

Week 6: Web Application Firewall (WAF)

Deployed WAF Solution (AWS WAF / Cloudflare) to mitigate OWASP Top 10 Threats and improve web application security.

3

Week 7: Cloud Vulnerability Scanning

Performed vulnerability scans, identified security gaps, and implemented remediation steps.

Weekly Milestones: Weeks 8-10

1

Week 8: Simulated Attack & Incident Response

Simulated compromise, detected activity via CloudTrail/CloudWatch, and performed response/containment actions.

2

Week 9: Compliance & Governance

Configured AWS Config rules, applied tagging policies, and generated compliance reports.

3

Week 10: Incident Response & Recovery

Conducted mock security breach scenarios, isolated compromised resources, and applied recovery steps.

Week 11: Final Cloud Security Audit

Comprehensive Review

Examined all cloud resources, IAM policies, network, and storage security.

Identified Misconfigurations

Highlighted risks, open ports, and policy deviations.

Final Audit Report

Prepared detailed report summarizing security posture and remediation steps.

Key Learnings & Deliverables

Key Learnings

- IAM & Access Control
- Cloud Security Monitoring
- Vulnerability Management
- Incident Response
- Compliance & Auditing
- Documentation Skills

Deliverables

- Weekly task documentation with screenshots
- Security audit reports
- Final presentation (submitted to company and GitHub)

Conclusion

Hands-on Experience

Gained practical skills in AWS/GCP setup, IAM, storage security, WAF, monitoring, vulnerability scanning, and incident response.

Developed Skills

Proficient in securing, monitoring, auditing, and remediating cloud resources, along with documentation and GitHub management.

Future Readiness

Prepared for real-world cloud security challenges and advanced certifications.

Thank You