Squad Augmented Protection Services Training Course

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the current digital era, cyber threats are escalating at an alarming rate, and email remains the most vulnerable communication channel for organizations. Squad Augmented Protection Services Training Course equips IT professionals, cybersecurity analysts, and corporate staff with cutting-edge skills and methodologies to implement robust email security systems. This program focuses on advanced protection techniques including email threat detection, phishing defense, anti-spoofing protocols, and AI-powered filtering tools, ensuring your organization remains resilient against evolving attacks.

Through hands-on learning, case studies, and expert-led modules, participants will gain comprehensive knowledge in deploying augmented protection systems tailored to enterprise-level email infrastructures. This course is designed to enhance proficiency in email encryption, zero-trust architecture, email anomaly detection, automated incident response, and cloud-based security integration. With a strong emphasis on real-world application, learners will be empowered to fortify email gateways and proactively mitigate threats using machine learning and behavioral analytics.

Programme Curriculum

Squad Augmented Protection Services Training Course

Introduction

In the current digital era, cyber threats are escalating at an alarming rate, and email remains the most vulnerable communication channel for organizations. Squad Augmented Protection Services Training Course equips IT professionals, cybersecurity analysts, and corporate staff with cutting-edge skills and methodologies to implement robust email security systems. This program focuses on advanced protection techniques including email threat detection, phishing defense, anti-spoofing protocols, and AI-powered filtering tools, ensuring your organization remains resilient against evolving attacks.

Through hands-on learning, case studies, and expert-led modules, participants will gain comprehensive knowledge in deploying augmented protection systems tailored to enterprise-level email infrastructures. This course is designed to enhance proficiency in email encryption, zero-trust architecture, email anomaly detection, automated incident response, and cloud-based security integration. With a strong emphasis on real-world application, learners will be empowered to fortify email gateways and proactively mitigate threats using machine learning and behavioral analytics.

Course Objectives

1. Understand the landscape of modern email-based cyber threats.
2. Implement phishing-resistant authentication protocols (e.g., SPF, DKIM, DMARC).
3. Utilize AI and machine learning to enhance threat detection accuracy.
4. Deploy real-time email anomaly detection tools.
5. Integrate zero-trust architecture into email systems.
6. Create automated workflows for incident response.
7. Understand cloud-based email security platforms (e.g., Microsoft Defender, Google Workspace).
8. Analyze and respond to advanced persistent threats (APTs) via email.
9. Conduct forensic analysis of compromised email accounts.
10. Develop and enforce email encryption and data loss prevention (DLP) policies.
11. Perform email risk assessments and audits.
12. Optimize email security awareness training across teams.
13. Evaluate vendor-based augmented protection services for organizational needs.

Target Audiences

1. IT Security Professionals
2. Cybersecurity Analysts
3. Email System Administrators
4. Corporate Communications Teams
5. Risk and Compliance Officers
6. Government ICT Departments
7. Cloud Security Architects
8. Managed Security Service Providers (MSSPs)

Course Duration: 5 days

Course Modules

Module 1: Email Threat Landscape and Risk Mapping

- Overview of email-borne threats and vectors
- Evolution of phishing and ransomware via email
- Mapping organizational exposure to email threats
- Key vulnerabilities in email infrastructures
- Risk scoring and prioritization
- **Case Study**: Analysis of a ransomware breach caused by email phishing

Module 2: Authentication Protocols and Spoofing Prevention

- Understanding SPF, DKIM, and DMARC protocols
- Configuration and validation of DNS records
- Anti-spoofing mechanisms for domain protection
- Reporting and monitoring policy compliance
- Best practices for email domain reputation
- **Case Study**: Implementing DMARC to prevent domain impersonation

Module 3: AI-Driven Email Threat Detection

- Machine learning algorithms for spam and malware
- Behavioral analytics for anomaly detection
- Signature vs heuristic-based filtering
- Integration with SIEM platforms
- Continuous learning systems for adaptive protection
- **Case Study**: Enhancing detection rates with AI in Office365

Module 4: Incident Response and Automation

- Email security incident lifecycle
- Setting up automated response playbooks
- Integrating SOAR tools for email incidents
- Alert prioritization and escalation paths
- Cross-team collaboration for faster mitigation
- **Case Study**: Automated quarantine of malicious attachments

Module 5: Zero Trust and Email Security Architecture

- Principles of zero-trust in email communication
- Role-based access and least privilege enforcement
- Micro-segmentation of email flow
- Conditional access and multi-factor authentication
- Architectural designs for secure email gateways
- **Case Study**: Deploying zero-trust email framework in a healthcare firm

Module 6: Cloud-based Email Security Integration

- Overview of major cloud email providers' security
- Microsoft Defender for Office 365 & Google Workspace security
- Secure API integrations for monitoring
- Sandboxing and link rewriting
- Email routing and third-party tool support
- **Case Study**: Migrating to a cloud-secure email environment

Module 7: Email Forensics and Investigation

- Techniques for email header and log analysis
- Identifying signs of compromise
- Chain-of-custody and evidence preservation
- Toolkits for forensic analysis (e.g., MailXaminer, Xplico)
- Generating reports for stakeholders
- **Case Study**: Post-incident forensic analysis of credential theft

Module 8: Policy Design, Training & Vendor Evaluation

- Drafting and enforcing organization-wide email policies
- Designing DLP strategies for sensitive information
- Awareness training frameworks and simulation campaigns
- Evaluating and benchmarking security vendors
- ROI and effectiveness measurement
- **Case Study**: Enhancing email security posture through policy and vendor alignment

Training Methodology

- Interactive instructor-led sessions

- Real-life simulations and incident walkthroughs
- Hands-on lab environments with guided tasks
- Group-based problem-solving exercises
- Case studies with guided analysis
- Access to toolkits, templates, and post-training support

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com