proofpoint.
certified guardian

DATA SHEET

Collaboration Security Analyst for the AI Era

The Proofpoint Collaboration Security Analyst recommended learning course builds expertise in utilizing Proofpoint's comprehensive suite, including Email Protection, Targeted Attack Protection, Threat Protection Workbench, Threat Response, and Proofpoint's AI Satori Abuse Mailbox Agent to skillfully manage incident response, from initial detection and analysis to post-incident activities. With a strong emphasis on practical application, this course will utilize Proofpoint's products to secure organizations against the most sophisticated threats. This course provides hands-on experience focusing on Collaboration Security Analyst skillsets, along with a classroom lab environment for configuring these services and features. This course is the foundation for many Proofpoint technologies in the cybersecurity space.

Course Syllabus

Incident Response and the Threat Landscape: In this lesson, you will learn how to:

- Distinguish between events, alerts, and incidents, and understand the incident response lifecycle
- Explain the relationship between vulnerability, threat, risk, and incident, and the role of information security frameworks
- Define the threat landscape and identify common threat actor types, motivations, and attack vectors
- Explain how threat intelligence supports prioritization, investigation, and response

COLLABORATION SECURITY ANALYST

Format:

Virtual Instructor Led Training (VILT), Onsite Training At A Customer's Facilities (OS)

Duration

3

days

Intended Audience:

Messaging and Security Analysts

Product Overview: In this lesson, you will learn how to:

- Identify the core products in the Collaboration Security platform
- Explain the role of Email Protection, TAP, Threat Response, and Workbench
- Describe how these products work together during investigations and response
- Understand the purpose of operational checks and data retention
- Recognize how the platform supports analyst workflows

Email Threats, Filtering and Investigation: In this lesson, you will learn how to:

- Identify common email attack types, such as phishing, BEC, and account takeover, and use threat intelligence to stay current
- Describe the SMTP email flow and how Email Protection filtering processes messages
- Explain SPF, DKIM, and DMARC, and how authentication results support spoofing analysis
- Use Smart Search to investigate suspicious email activity and interpret message metadata
- Leverage threat intelligence and Smart Search data to support threat hunting

Threats and the TAP Dashboard: In this lesson, you will learn how to:

- Explain the purpose of Targeted Attack Protection (TAP) and how it protects against URL, attachment, and message threats
- Prioritize and interpret detected threats, evidence, and attack progression using the Threats page
- Identify impacted and at-risk users, and analyze condemnation sources and forensic evidence
- Identify high-risk users using the People page and reports, including VAPs and account takeover activity
- Use custom URL blocklists, TAP notifications, and reports to support investigations and response

Collaboration Protection and Supplier Threat Protection: In this lesson, you will learn how to:

- Explain the risks associated with collaboration tools and how Collaboration Protection blocks malicious URLs
- Investigate malicious collaboration threats using Workbench and TAP data
- Explain how Supplier Threat Protection identifies compromised third parties
- Prioritize suspected compromised supplier accounts and analyze business relationship and traffic context
- Identify employees who communicated with suspected compromised accounts and assess supplier-related risk

Threat Response and Remediation: In this lesson, you will learn how to:

- Explain the purpose of Threat Response and TRAP, and how they work with TAP
- Interpret quarantine statuses and troubleshoot common remediation failures
- Review and prioritize incidents and messages in Cloud Threat Response
- Document investigation findings and prepare incidents for escalation and remediation
- Export Smart Search results to Threat Response and use manual workflows, including CLEAR verdicts and mail bombing remediation

The Threat Protection Workbench: In this lesson, you will learn how to:

- Navigate the Threat Protection Workbench interface
- Perform threat hunting and investigations using Workbench
- Analyze messages, senders, threats, and campaigns during an investigation
- Use Query Builder, Email Insights, ThreatFlip, Satori, and other Workbench tools to support investigations
- Perform investigation and remediation actions from a single analyst workspace

Dealing with False Positives and False Negatives: In this lesson, you will learn how to:

- Differentiate false positives from false negatives
- Review evidence before reporting detection errors
- Use TAP, Workbench, and support options to report issues
- Understand how PTIS and analyst support can help validate detections
- Apply corrective actions to improve detection quality

Incident Documentation and Proofpoint APIs: In this lesson, you will learn how to:

- Identify the data required for post-incident reporting
- Explain the purpose of key Proofpoint APIs
- Use APIs and platform data to collect incident evidence
- Support post-incident review and lessons learned activities
- Describe what should be included in an incident report