proofpoint.
certified guardian

DATA SHEET

Data Security Analyst for the AI Era

The Proofpoint Data Security Analyst for the AI Era course equips cybersecurity professionals with the expertise to effectively utilize Proofpoint Data Security Workbench, Data Classification, Insider Threat Management, Endpoint DLP, Cloud DLP/CASB, Email DLP, Data Security Posture Management (DSPM), and Data Security for AI. Focusing on key cybersecurity tasks such as data analysis, threat containment, incident management, AI-era data protection, and Satori-assisted alert triage, this course enables analysts with the skills needed to defend data and detect risky behavior from careless, malicious, compromised, or unsafe AI use. This course provides hands-on experience focusing on the data security analyst's skillsets, along with a classroom lab environment for using Proofpoint Data Security tools to address common Data Security use cases.

Course Syllabus

Incident Response Basics: In this lesson, you will learn:

- The difference between security events, alerts, and incidents
- How cybersecurity frameworks and the incident response lifecycle guide analyst decisions
- How threats and vulnerabilities create incident risk for users, systems, and data

DATA SECURITY ANALYST COURSE

Format:

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

Duration

3

days

Intended Audience:

Messaging Administrators and Security Analysts

The Preparation Phase: In this lesson, you will learn:

- How incident response plans, playbooks, and runbooks support consistent response
- How exercises and readiness testing prepare analysts before incidents occur
- When documentation should be updated from lessons learned, tool changes, or role changes

Platform Foundations: In this lesson, you will learn:

- How Proofpoint protects sensitive data, risky behavior, and AI interactions across channels
- How Data Security Workbench, Data Classification, Administration, DSPM, and Data Security for AI support analyst workflows
- How detectors, data classes, AI classifiers, Satori, DSPM, and Data Security for AI support AI-era data protection

Investigating Alerts: In this lesson, you will learn:

- How alerts are viewed, filtered, assigned, tagged, exported, and investigated in Data Security Workbench
- How rules, detectors, Data Classes, snippets, and workflow status support alert validation
- How analysts investigate Endpoint DLP, CASB/Cloud DLP, Email DLP, and Satori triaged alerts

Investigating Activity: In this lesson, you will learn:

- How Explorations help analysts investigate user activity and risky behavior across available channels
- How to use filters, tags, dashboard views, exports, and timelines to build investigation context
- How to document and escalate findings from an example DLP investigation

Containment, Eradication, and Recovery: In this lesson, you will learn:

- How to identify recovery options after investigation and document remediation outcomes
- How Endpoint DLP, Cloud DLP/CASB, and Email DLP remediation options help limit data exposure
- How GenAI prompt protection supports containment for AI-related data exposure

Post-Incident Activity Phase: In this lesson, you will learn:

- How to perform post-incident review activities and preserve evidence
- How to document incident timelines using user, file, device, Attack Sequence, and multichannel Exploration evidence
- How to export activity results support reports, recommendations, and future improvements

This course and related exam are based on the NIST SP 800-61 r2 Computer Security Incident Handling Guidelines. This information should be transferable to other guidelines such as SANS Incident Response or ISO 27001 and 270035.