proofpoint.
cybersecurity academy

Data Security Analyst Course

The Proofpoint Data Security Analyst course equips cybersecurity professionals with the expertise to effectively utilize Proofpoint's advanced Analytics dashboard, Insider Threat Management, and Cloud DLP products. Focusing on key cybersecurity tasks such as sophisticated data analysis, threat containment, and incident management, this course enables analysts with skills needed to defend data and detect risky behavior from careless, malicious, or compromised users. This course provides hands-on experience focusing on the data security analyst's skillsets, along with a classroom lab environment for using Proofpoint Analytics to address common Data Security use cases.

Data Security Analyst Course

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

DURATION
3 days

INTENDED AUDIENCE
Customers, Partners, Messaging Administrators, and Security Analyst

RECOMMENDED LEARNING
Proofpoint Cybersecurity Academy Learning Path: Email DLP for Analysts

proofpoint.
certified guardian

Course Syllabus

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

- How the Proofpoint Information Protection solution provides tools to identify, prevent, and remediate information leaks
- Proofpoint Endpoint DLP, Insider Threat Management (ITM), Cloud App Security Broker (CASB), and Email DLP products
- The Incident Response Life Cycle and why following accepted guidelines is good for your organization

The Preparation Phase:: In this lesson, you will learn:
- Key resources that may be available to you, including what goes into a runbook
- How to find Proofpoint training, documentation, and knowledge resources
- How to increase confidence by preparing for security incidents before they occur

Detection and Analysis: In this lesson, you will learn how to:
- Identify system or communications issues that may affect your ability to detect suspicious activity
- Identify activity and alerts that indicate common use cases for information protection
- Use the Analytics application to identify significant activity and determine the triage order of alerts and activity
- Determine if activity meets your organization's definition of risky behavior
- Determine if an alert is an active risk or already resolved
- Identify trends in false positive alerts that may be preventable with changes to the environment or monitoring rules
- Use Analytics' workflow tools to track the status, owner, escalation, and timeline of alerts

Containment, Eradication, and Recovery: In this lesson, you will learn how to:
- Prepare incident reports and show the trends over time
- Make recommendations regarding the installation, configuration, and maintenance of security tools
- Present a completed incident report detailing the activity and alerts associated with incidents, including the timeline, users, devices, and tactics involved
- Present recommendations on ways to avoid future events

Post-Incident Activity: In this lesson, you will learn how to:
- Preserve evidence related to an information protection incident and build a timeline for the after-event writeup
- Review alert or activity trends that may help prevent the incident in the future
- Suggest changes to rules, dictionaries, or policies to improve the platform's efficiency
- Generate reports on Endpoint DLP and Cloud DLP activity

This course and related exam are based on the NIST SP800-61 r2 Computer Security Incident Handling Guidelines. This information should be transferable to other guidelines such as SANS Incident Response or ISO 27001 and 270035.

proofpoint.

https://www.proofpoint.com/us/cybersecurityacademy

DISCOVER THE PROOFPOINT PLATFORM →