proofpoint.

Proofpoint Cybersecurity Academy

Become a Proofpoint Certified Guardian

Format:
Instructor Led Training (ILT), Virtual Instructor Led Training (VILT), Onsite training at a customer's facilities (OS)

Duration:
4 days

Intended Audience:
Customers, partners, messaging administrators, and security analyst

Recommended Learning:
Proofpoint Cybersecurity Academy Learning Path:
Email DLP for Analysts

Information Protection Analyst Course

The Proofpoint Information Protection Analyst recommended learning 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 information protection analyst's skill sets, along with a classroom lab environment for using Proofpoint Analytics to address common information protection use cases.

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.

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including 87 of the Fortune 100, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. Become a Proofpoint Certified Guardian today. More information is available at www.proofpoint.com.

proofpoint.

Information Protection Analyst Exam

Format:
Exams are available at the in-person 2024 Protect event. Please register at www.proofpoint.com/events/protect.

Duration:
90 minutes

Intended Audience:
This exam is ideal for IT professionals, security analysts, triage analysts, and incident responders seeking to elevate their cybersecurity skills and harness the full potential of Proofpoint products in the battle against cyber threats

Recommended Learning:
Proofpoint People Protection Analyst course

Exam Overview

The Proofpoint Information Protection Analyst exam equips cybersecurity professionals with the expertise to effectively utilize Proofpoint's advanced Analytics dashboard, Insider Threat Management, and Cloud DLP products. The exam will focus on key cybersecurity tasks such as sophisticated data analysis, threat containment, and incident management to provide analysts with the skills needed to defend data and detect risky behavior from careless, malicious, or compromised users.

Exam Core Components

- Incident Response Foundations: Recognize and respond to cybersecurity incidents
- Preparation: Determine what information your organization considers sensitive. Respond to potential data breaches by combining Proofpoint intelligence and organizational procedures
- Detection and Analysis: Utilize Proofpoint's solutions to determine the validity of DLP alerts and analyze violations of organizational data handling policies
- Containment, Eradication, and Recovery: Determine if an incident was prevented or automatically remediated; determine how to contain breaches and when to escalate for mitigation and recovery
- Post-incident Activity: Conduct thorough post-incident analysis to strengthen future response strategies, reduce false positives, and optimize procedures
- Operational Procedures: Implement and oversee operational best practices for ongoing security management

Exam Benefits: Gain in-depth knowledge and practical experience with Proofpoint's leading security products. Earn a certification by passing this exam to showcase your ability to defend against complex cyber threats. Be empowered with the tools and confidence to take on any cybersecurity challenge. Join a community of cybersecurity experts dedicated to protecting organizations against data loss.

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including 87 of the Fortune 100, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. Become a Proofpoint Certified Guardian today. More information is available at www.proofpoint.com.