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:
PPS 101: Protection Server Foundations - Level 1; TRP 101: Threat Response Auto-Pull (TRAP) Foundations - Level 1; TAP 101: Targeted Attack Protection Foundations – Level 1

People Protection Analyst Course

The Proofpoint People Protection Analyst recommended learning course builds expertise in utilizing Proofpoint's comprehensive suite, including Targeted Account Protection, Threat Response Auto Pull, and Email Protection 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 People Protection 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 Foundations: In this lesson, you will learn:
- People Protection components, including Email Protection, TAP, TRAP, CTR, and NPRE
- The Incident Response Life Cycle and why following accepted guidelines is good for your organization
- The responsibilities of an incident responder based on the NIST SP800-61 r2 Computer Security Incident Handling Guidelines

The Preparation Phase: In this lesson, you will learn:
- Development of a security infrastructure
- Roles and responsibilities of an incident responder
- Incident response procedures and run books
- How to investigate event logging locations and identify escalation paths
- Various incident response tools used by analysts to monitor security events
- How changes to threat landscapes impact analysts

Detection and Analysis: In this lesson, you will learn how to:

- Identify tools and detection mechanisms used to analyze potential security incidents
- Perform operational checks on People Protection components
- Identify and report out of policy configurations and recommend system configurations in response to threat insights
- Investigate at-risk users and analyze system logs to detect suspicious activities
- Monitor system consoles for alerts, prioritize threats and escalate as required
- Identify common threats such as spam, virus, malware, BEC, commodity and phishing
- Review logs for click patterns and suggest security awareness content and targets

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

- Arrange similar threat patterns into a single investigation and assign threat urgency based on threat, context, and target
- Explain manual remediation steps of threats post-delivery and verify results of automated remediation actions
- Eliminate common false positives and open support cases when required
- Make recommendations for threat protection, including updating workflows, custom spam rules, VIP users, and custom blocklists

Post-Incident Activity: 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 this type of event in the future

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 cyber attacks. 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.

People Protection Analyst Exam

Exam Overview

The Proofpoint People Protection Analyst exam builds expertise in utilizing Proofpoint's comprehensive suite, including Targeted Account Protection, Threat Response Auto Pull, and Email Protection. The exam will focus on how to skillfully manage incident response, from initial detection and analysis to post-incident activities, along with a strong emphasis on practical application of securing organizations against the most sophisticated threats.

Exam Core Components In this lesson, you will learn:

- Incident Response Foundations: Recognize and respond to cybersecurity incidents
- Preparation: Strategize and prepare with advanced tools to stay ahead of potential threats
- Detection and Analysis: Utilize Proofpoint's solutions to detect and dissect security threats efficiently
- Containment, Eradication, and Recovery: Contain breaches, eradicate threats, and restore systems to normal operation
- Post-incident Activity: Conduct thorough post-incident analysis to strengthen future response strategies
- Operational Procedures: Implement and oversee operational best practices for ongoing security management
- Escalation and Mitigation: Escalate and mitigate threats to minimize impact on business operations

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 people and organizations.

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 cyber attacks. 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.