proofpoint.
cybersecurity academy

Threat Protection Analyst Course

The Proofpoint Threat 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 Threat 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.

Threat Protection 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

Messaging and Security Administrators

proofpoint.
certified guardian

Course Syllabus

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

- Threat 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

©Proofpoint, Inc. 2025

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 Threat 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

proofpoint®

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

DISCOVER THE PROOFPOINT PLATFORM →

©Proofpoint, Inc. 2025