Trellix

EDUCATION SERVICES

Trellix® Insights Essentials: Investigation

Self-Paced Online Training

Highlights

Duration

45 minutes

Prerequisites

Students taking this course should have a working knowledge of Microsoft Windows administration, system administration concepts, and a basic understanding of computer security and internet services. It is also necessary to have prior experience using Windows CLI commands and ePolicy Orchestrator.

How to Register

Here is the Academy Course link. Click Enroll to sign up.

This investigation course equips participants with the essential skills to effectively prioritize and respond to threats using Trellix Insights and EDR capabilities, enabling them to use the Campaigns dashboard and “Requiring Attention” list to prioritize threats and understand their global/local impact. Learners will master the IOCs table, interpret Determinism/Lethality scores, and pivot to Real-Time Search in Trellix EDR for rapid investigation. The course also covers how to analyze affected endpoints, manually resolve events, and leverage Hunting Rules (Yara, Snort, Sigma) for proactive defense, culminating in the ability to identify and reconfigure insufficient endpoint security policies to improve the Security Posture Score (SPS).

Learning Objectives

After completing this course, learners should be able to:

- Analyze affected endpoints, manually resolve events, and leverage Hunting Rules (Yara, Snort, Sigma).
- dentify and reconfigure insufficient endpoint security policies to enhance the Security Posture Score (SPS).
- Use the Campaigns dashboard and “Requiring Attention” list to assess global/local impact and prioritize threats.
- Master the IOCs table, interpret Determinism/Lethality scores, and pivot to Real-Time Search in Trellix EDR for investigation.

Who Should Attend

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.

Course Outline

INTRODUCTION

1. About the Course
2. Learning Objectives
3. Useful Links
4. Disclaimer
5. Copyright

PRODUCT INTRODUCTION

6. Module Introduction
7. Campaign Analysis and Prioritization
8. Advanced Threat Intelligence and IOCs
9. Remediation and Security Posture
10. Insights Countermeasures
11. Reporting and Status
12. Troubleshooting

CONCLUSION

13. Summary
14. Course Exam

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.

Copyright © 2025 Musarubra US LLC

022024-15