Trellix

CYBER OPERATIONS

Threat Hunting Fundamentals

Instructor-Led Training

Highlights

Duration

4 days

Prerequisites

Students taking this course should have a working knowledge of Windows/Linux/macOS operating systems, and network technologies. Basic understanding of information security, command line syntax, malware, and analytical thinking recommended.

How to Register

This course is available for purchase at https://training-catalog.trellix.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://training-catalog.trellix.com.

This entry-level course in threat hunting and threat intelligence provides foundational knowledge in threat hunting methodologies and techniques, including the application of information security frameworks, and threat intelligence. This course employs open-source tools to perform threat hunting and analysis in hands-on labs, touching on threat hunting use cases, hunting techniques, and key tactics.

This course is part of the Trellix Cyber Operations team's Foundations in Incident Response Education (FIRE) track of general defensive security training. Learners are provided a blend of lecture, discussions, and hands-on labs.

Learning Objectives

After completing this course, learners should be able to:

- Define key terms in threat hunting and threat intelligence
- Describe the TaHiTI methodology
- Apply the MaGMa framework for use cases
- Contrast methodologies and the techniques they support
- Identify key tactics and techniques of the adversary
- Use investigative tools for threat hunting

Who Should Attend

This course is intended for beginning threat hunters, incident responders, information security staff, auditors, SOC analysts, investigators, and consultants responsible for threat hunting and threat intelligence.

Course Outline

1. Course Introduction
2. Threat Hunting Overview
3. The Adversaries
4. Analytical Thinking
5. Maturity Methodologies Techniques
6. Hunting Tools Overview
7. Hunting: Network
8. Hunting: Endpoint
9. Hunting: Application
10. Hunting: Use Cases

Visit Trellix.com to learn more.

Trellix

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 artificial intelligence, automation, and analytics to empower over 40,000 business and government customers with living security. More at https://trellix.com.

052024-31