Trellix

EDUCATION SERVICES

Network Detection and Response ANALYST course

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

This course is intended for system administrators, security personnel, auditors, and/or consultants concerned with Systems administration. A working understanding of networking and network security, knowledge of Wireshark as well as a basic understanding of computer security concepts is 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 course covers the fundamentals and concepts of Network Traffic Analysis. This course is targeted to help Network Analysts learn how to search, filter, analyze, reconstruct, and preserve network traffic; and to apply techniques to conduct a Network forensics investigation utilizing the Network Detection and Response (NDR) solution.

This course combines lectures and practical lab exercises with significant time allocated for hands-on interaction with all user interfaces.

Learning Objectives

After completing this course, learners should be able to:

- Discuss Network Detection and Response (NDR) solution
- Differentiate between full packet data, network flow data, and payload data
- Customize the analysis environment with dashboards, network visualizations, scheduled queries, and lists
- Reconstruct artifacts from network data and submit them for malware analysis
- Review aggregated alerts and pivot to related traffic
- Search for anomalies on network traffic and Investigate leads based on alerts and anomalies
- Analyze network flow data, metadata, and payload data
- Investigate an advanced persistent threat (APT) attack, based on aggregated alerts and network traffic anomalies

Who Should Attend

Network security professionals and incident responders who use Trellix Packet Capture and Investigation Analysis appliances to analyze cyber threats through packet data..

Course Outline

1. Introduction to NDR
2. Network Traffic Analysis Foundations
3. NDR Alerts
4. Advanced Detection and Analysis
5. Investigation Workshop
6. Starting with Leads
7. Queries, Reconstruction, and Alerts with Investigation Analysis
8. Threat Hunting with NDR
9. Investigating Leads
10. Conclusions and Summary

Visit Trellix.com to learn more.

022024-15