Vectra AI SOC Analyst Training

January, 2025

Instructor information

Instructor	Email	Role
TBD	TBD	Professional Services Trainer

General information

Description

This coursework equips Security Operations Center (SOC) professionals with the knowledge and skills needed to respond to alerts in the Vectra AI platform effectively. Attendees will learn basic system architecture, fundamentals of prioritization of entities, how to analyze and assess detections, API usage, and identify avenues to integrate the Vectra AI platform into standing workflows. Prerequisites include basic IT knowledge, cybersecurity fundamentals, and proficiency in networking and system administration. The course emphasizes practical exercises, collaboration, and continuous learning.

Expectations and Prerequisites

To make the most of this training content, attendees should meet the following expectations and prerequisites:

- Basic IT Knowledge:
    - Attendees should have a foundational understanding of IT concepts, including networking fundamentals, protocols, security, and system administration.
- Cybersecurity Fundamentals:
    - A grasp of cybersecurity principles is recommended. Attendees should understand concepts like threat detection, incident response, and risk management.
    - Knowledge of common attack vectors (e.g., phishing, malware, insider threats) is helpful.
- Networking Proficiency:
    - Attendees should be comfortable with network architecture and protocols.
    - Understanding network traffic flow, segmentation, and communication patterns will enhance their learning experience.
- Security Tools Familiarity:
    - Prior exposure to security tools (e.g., SIEMs, IDS/IPS, firewalls) will be advantageous.
    - Understanding how these tools contribute to threat detection and prevention is valuable.
- Critical Thinking and Problem-Solving:
    - Attendees should possess analytical skills to interpret alerts, investigate incidents, and troubleshoot issues.
    - Logical reasoning and the ability to connect the dots are crucial.
- Documentation Discipline:
    - A willingness to create and maintain thorough documentation is essential.
    - Attendees should be comfortable documenting deployment steps, configurations, and troubleshooting procedures.
- Collaboration and Communication:
    - Attendees will benefit from collaborating with colleagues and subject matter experts.
    - Effective communication skills are necessary for escalations and knowledge sharing.
- Resourcefulness:
    - Attendees should proactively seek out additional resources beyond the coursework.
    - Utilize stored documentation, engage with community forums, and explore online resources.

Required attendee materials

- Computer or Device:
  - Ensure you have access to a reliable computer or laptop with internet connectivity.
  - Make sure your device is compatible with Microsoft Teams.
  - Test connectivity with required internal network resources and lab environment(s).
- Internet Connection:
  - A stable and reasonably fast internet connection is essential for participating in virtual sessions.
- Microsoft Teams:
  - Online training will be conducted through Microsoft Teams. Ensure that necessary software is installed and up to date.
  - Familiarize yourself with Teams features like chat, video calls, and screen sharing.
- Vectra AI Documentation:
  - Review Vectra's official documentation (found on support.vectra.ai) to understand the platform and its features.
  - Access the REST API guides for any API-related tasks.
- Time Management:
  - Allocate time for attending virtual sessions, setting up your lab, and practicing exercises.
  - Remember to actively participate, ask questions, and explore the Vectra AI platform during the coursework.

Sessions & Topics	Exercises
Session 1 **Duration: 4 hours** • **Introduction to Vectra AI** • **HostID** • **Prioritization** • **RUX UI Overview** • **Respond** • **Hunt** • **Grouping**	Introduction to Vectra AI ○ Overview of Vectra AI's role in threat detection and response ○ Understanding the platform architecture and components. ○ Familiarization with Vectra AI's documentation and support HostID ○ Introduction to HostID and its importance ○ Familiarize with how Vectra AI platform utilizes HostID and Host Artifacts Prioritization ○ Introduction to entity scoring and analyst focus RUX UI Overview ○ Overview of the functionality of RUX UI ○ Familiarize the analysts with each page of the UI ○ Discuss use cases and purpose of each page Respond ○ Familiarize the analysts with the Respond page ○ Demonstrate searches and filters in UI Hunt ○ Familiarize the analysts with the Hunt page ○ Demonstrate searches and filters in UI Grouping ○ Introduction to Grouping - how and why ○ Familiarize the analysts with Grouping ○ Demonstrate Grouping in UI ▪ Creating ▪ Search ▪ Manage

Sessions & Topics	Exercises
Session 2 **Duration: 4 hours** • **Triage** • **Tags and Notes** • **Assignments** • **Investigate** • **Instant Investigation** • **Integrations and API**	Triage ○ Introduction to Triage ○ Familiarize the analysts with Triage ○ Demonstrate Triage in UI Tags and Notes ○ Introduction to Tags and Notes ○ Familiarize the analysts with Tags and Notes ○ Demonstrate Tags and Notes in UI Assignments ○ Introduction of Vectra User Assignments ○ Familiarize the analysts with Vectra User Assignments ○ Demonstrate Assignments in UI Investigate ○ Introduction of RUX Investigate ○ Familiarize the analysts with RUX Investigate ○ Demonstrate RUX Investigate in UI Instant Investigation ○ Introduction of RUX Instant Investigation ○ Familiarize the analysts with RUX Instant Investigation ○ Demonstrate RUX Instant Investigation in UI Integrations and API ○ Introduction to Vectra's REST API and capabilities ○ Familiarize the analysts with Vectra REST API ○ Leveraging APIs for data retrieval, alert management, and system health checks ○ Utilizing health APIs for monitoring platform performance and stability ○ Demonstrate Vectra REST API

Sessions & Topics	Exercises
Session 3 **Duration: 4 hours** • **Detections** • **Workflow Integration Discussion** • **Platform Consolidation**	Detections ○ Deep dive into Vectra AI detections ○ Discussions include; ▪ Meaning of the detections ▪ How to analyze ▪ What to consider for validation and/or remediation ○ Command & Control ○ Reconnaissance ○ Lateral Movement ○ Exfiltration ○ Botnet Workflow Integration Discussion ○ Current workflow ○ Identify workflow integration points Platform Consolidation ○ Analyze prioritized Entities ○ Assess Triage requirements ○ Create Groups and Triage Filters ○ Practice workflow integration points

Sessions & Topics	Exercises
Session 4 **Duration: 4 hours** • **Investigate** • **Network Protocols** • **Threat Hunting** • **PCAP Analysis**	Investigate ○ Understanding the Investigate capability within RUX ○ Difference between Investigate tab and instant investigate **Introduction to Network Protocols/Network Traffic & Metadata** ○ Network Protocols in-depth ○ Differentiating Network Traffic and metadata in Vectra Platform ○ Metadata deep dive **Threat Hunting** ○ Threat hunting components and best-practices ○ Threat hunting in investigate PCAP Analysis ○ Detection PCAP Analysis using Wireshark ○ Detection PCAP Analysis using tcpdump