Vectra AI SIEM Operations Training Syllabus

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 effectively ingest and understand Vectra Data within their SIEM. Attendees will learn how to integrate Vectra data into their existing SIEM Platform and identify avenues to integrate the Vectra AI platform into standing workflows. Prerequisites include fully deployed and operational Vectra Environment, fully deployed and Operational SIEM, full understanding of your SIEM Platform, 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.
- SIEM:
    - Have a working knowledge of the SIEM within your environment
    - Have an operational and functional SIEM Environment that either is, or will, ingest Vectra metadata. Stream and/or alerts/API.
    - 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.

Coursework

Sessions & Topics	Exercises
Session 1 **Duration: 2 Hours** • **Initial Discovery**	Initial Discovery ○ Understanding customer tools, people, and processes ○ Understand customer pain points and requirements with SIEM data ○ Setting expectations and outcomes based on customer requirements and SIEM

Sessions & Topics	Exercises
Session 2 **Duration: 4 hours** • Data Sources	Data Sources ○ What's important and what's not in your environment ○ Understanding the difference between Metadata and Detections ○ Duplicate source types/data ○ Maximizing value while minimizing footprint

Sessions & Topics	Exercises
Session 3 **Duration: 4 - 6 hours** • **Vectra Data Sources**	Workflow Integration Discussion ○ Alerts ○ Metadata ○ Detections ○ Entity scoring ○ Health API ○ Custom API ○ Vectra Match ○ Audit API

Sessions & Topics	Exercises
Session 4 **Duration: 4 - 6 hours** • **Data consumption principles**	Data Visuals ○ Visualization ○ Dashboards ○ Pre-configured and custom use case ○ Workflow best-practices ○ Automation triggers/flows ○ Compliance/regulatory uses