Vectra AI Essentials Training Syllabus

January, 2025

Instructor information

Instructor	Email	Role
TBD	TBD	Professional Services Trainer

General information

Description

This coursework equips Vectra users with the Essential knowledge and skills needed to perform day to day operations within the Vectra AI platform effectively. Attendees will learn basic user interface fundamentals, fundamentals of the various Vectra products depending on your environment. Prerequisites include a fully deployed and operational Vectra environment, 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:

- Fully Deployed Vectra environment:
  - The Vectra Platform should be fully deployed, validated and operational before training begins.
- 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.
- 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

RUX

Duration: 4 hours

- **Introduction to Vectra AI**
- **Prioritization**
- **Respond UX**

Exercises

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

Prioritization

- Discussion on entity scoring and analyst focus

Respond UX

- Overview of the functionality of Respond UX
- Familiarize the analysts with each page of the Respond UX
- Discuss use cases and purpose of each page
- Investigations

Sessions & Topics	Exercises
Quad UI **Duration: 2 Hours** • **Introduction to Vectra AI** • **Host Scoring** • **Quad UX**	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 Host Scoring ○ Understanding Host scoring in Quad UX Quad UX ○ Overview of the functionality of Quad UX ○ Familiarize the analysts with each page of the UX ○ Discuss use cases and purpose of each page

Sessions & Topics	Exercises
Recall **Duration: 2 hours** • **Introduction to Recall** • **Understanding Metadata and Zeek** • **Recall Use cases**	Introduction to Recall ○ Overview of Recall role in threat detection and response. ○ Understanding Recall architecture and components. Working with Recall ○ Understanding Metadata ○ Understanding Lucien Query language ○ Breakdown of schema Recall Use Case ○ Threat Hunting use case ○ Network Forensic use cases ○ Investigation use cases

Sessions & Topics

Stream

Duration: 2 hours

- **Introduction to Stream**
- **Understanding Metadata and Zeek**
- **Stream Use cases**

Exercises

Introduction to Stream

- Overview of Stream role in threat detection and response.
- Understanding Recall architecture and components.

Working with Stream

- Understanding Metadata
- Understanding Lucien query language
- Breakdown of schema

Stream Use Case

- Threat Hunting use case
- Network Forensic use cases
- Investigation use cases

Sessions & Topics	Exercises
IDR/CDR for Azure AD &M365 **Duration: 1 hours** • **Introduction IDR/CDR for Azure AD & M365** • **Understanding Identity Detections**	Introduction to IDR/CDR for Azure AD & M365 ○ Overview of IDR/CDR for Azure AD & M365 role in threat detection and response. Understanding Identity Detections ○ Understanding what identity detections are ○ Overview of Identity detections within Vectra

Sessions & Topics	Exercises
CDR for AWS **Duration: 1 hours** • **Introduction CDR for AWS** • **Understanding CDR for AWS Detections**	Introduction to CDR for AWS ○ Overview of IDR/CDR for Azure AD & M365 role in threat detection and response Understanding CDR for AWS Detections ○ Understanding what CDR for AWS detections are ○ Overview of CDR for AWS detections within Vectra

Sessions & Topics

CDR for Azure

Duration: 1 hours

- **Overview of CDR for Azure**
- **Understanding CDR for Azure Detections**

Exercises

Overview of CDR for Azure

- ○ Overview of CDR for Azure role in threat detection and response

Understanding CDR for Azure Detections

- ○ Understanding what CDR for Azure detections are
- ○ Overview of CDR for Azure detections within Vectra

Sessions & Topics

Vectra Match

Duration: 2 hours

- **Overview of Vectra Match**
- **Understanding Match Metadata**

Exercises

Overview of Vectra Match

- ○ Overview of Vectra match
- ○ Match Deployment Scenarios
- ○ Understanding Vectra Match role in threat hunting and Forensics
- ○ Understanding Suricata Rule Structure
- ○ Editing Suricata rules
- ○ Additional sources for Suricata rules

Understanding Match Metadata

- ○ Understanding Match Metadata
- ○ Threat Hunting and Forensic use cases for Vectra Match

Sessions & Topics	Exercises