Vectra AI Platform Management and Operation Training Syllabus

January.2025

Instructor information

Instructor	Email	Role
TBD	TBD	Professional Services Trainer

General information

Description

This coursework equips IT professionals with the knowledge and skills needed to manage and operate the Vectra AI platform effectively. Attendees will learn about post-deployment, system alerts monitoring, API usage, environmental considerations, disaster recovery, and gain hands-on experience within a lab environment. 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, security, and system administration.
  - Familiarity with terms like IP addresses, subnets, firewalls, and network protocols.
- 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.
- Virtual Lab Environment (VMware):
    - Various efforts within this coursework call for hands-on experience, so a virtual lab accessible internally to attendees is required. The virtual lab should accommodate the following minimum requirements (see documentation for resource requirements and specifications):
        - Vectra Brain
        - Vectra Sensor
        - SFTP or SCP server, or access to one (for configuring and restoring backups)
        - Syslog or Email destination (for receiving test alerts)
        - Access to DNS and firewall systems for Vectra deployment and disaster recovery testing
- 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** • **Introduction to Vectra AI** • **Lab environment preparation**	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 Lab Environment Preparation ○ Lab environment setup and validation
Session 2 **Duration: 4 hours** • **Documentation and Deployment** • **System Alerts Monitoring** • **API Usage** • **Environmental Considerations** • **Disaster Recovery Preparedness** • **Resources and Escalation** • **Hands-On Labs and Practical Exercises**	Documentation and Deployment ○ Creating comprehensive internal documentation for Vectra deployment. ○ Documenting installation procedures, configuration settings, and best practices. ○ Managing deployment across different environments (on-premises, cloud, hybrid). System Alerts Monitoring ○ Configuring and fine-tuning alert thresholds. ○ Understanding different alert types (e.g., behavioral, anomaly-based, threat-specific). ○ Investigating and prioritizing alerts effectively. API Usage ○ Exploring Vectra's REST API capabilities. ○ Leveraging standard APIs for data retrieval, alert management, and system health checks. ○ Utilizing health APIs for monitoring platform performance and stability. Environmental Considerations ○ Assessing network architecture and topology. ○ Identifying critical assets, network segments, and communication patterns. ○ Adapting Vectra deployment to fit specific network environments. Disaster Recovery Preparedness ○ Developing a disaster recovery plan for Vectra AI. ○ Backup and restoration procedures for platform data. ○ Failover strategies and continuity measures.

Sessions & Topics	Exercises
	Resource Utilization and Escalation Points Leveraging available resources: ○ Stored Documentation: Accessing knowledge bases, user manuals, and support articles. ○ Subject Matter Experts (SMEs): Collaborating with experts within the organization. ○ Escalation Points: Knowing when and how to escalate issues to higher levels of support. Hands-On Labs and Practical Exercises ○ Deploying Vectra AI in a lab environment. ○ Simulating alerts, investigating incidents, and managing system health. ○ Role-playing disaster scenarios and practicing recovery procedures.