| Datasheet – TrendAI Vision One for Administrators and Operators Training

TrendAI Vision One for Administrators and Operators Training

Course Description:

During this two-day instructor-led training cyber security professionals will learn how to effectively run TrendAI Vision One in their organisation.

Learning Objectives:

1. Configure and onboard TrendAI and third-party security solutions to TrendAI Vision One™ for consolidated XDR and protection coverage.
2. Collect and leverage telemetry from endpoints, email, web, and network sources to enhance threat visibility across the environment.
3. Apply Agentic SIEM and XDR capabilities by using Workbenches and XDR Data Explorer to investigate threats and locate relevant security artifacts.
4. Automate incident response using Security Playbooks.
5. Manage cyber risk exposure by using Cyber Risk Exposure Management (CREM) to identify high-risk assets, ongoing attack activity, and contributing risk factors.

Target Audience:

TrendAI Customers

Prerequisites:

Knowledge of networking concepts, security principles, and cloud technologies are required.
Participants are required to bring a laptop with a recommended screen resolution of at least 1980 x 1080 or above and a display size of 15" or above. A second screen is advantageous for labs i.e. lab guide on one screen and virtual environment on the other..

Training Outline:

Extended Detection and Response (XDR)

- **Overview** – Unified XDR architecture and operating model within Trend Vision One.
- **Telemetry & Sensor Deployment** – Collection of telemetry from endpoints, servers, email network, cloud, identity, and web sources. Native sensors, third party integrations, and Service Gateway usage.
- **Security Events vs Activity** Data – Understanding detection events versus behavioural activity telemetry and their role in correlation.
- **Observed attack techniques** – Visibility into attacker behaviour mapped to MITRE ATT&CK tactics and techniques.
- **Workbench & Incidents** – Alert correlation, incident grouping, timelines, graphs, and impact analysis.
- **Targeted Attack Detection** – Identification of ongoing attack campaigns and multi-stage attacks.
- **Thread Investigation** Tools – Use of Workbenches, XDR Data Explorer, execution profiles, network analytics, and forensics.
- **Response Actions –** Endpoint, account, email, and object-based response actions with centralized tracking.
- **Security Playbooks –** Automated and semi-automated response workflows with approval and governance controls.
- **Third Party Integrations** – Integration with firewalls, IAM, SIEM/SOAR, vulnerability management, BAS, and ITSM platforms.
- **API Usage & Automation** - API-based access for investigation, response, reporting, and custom integration.

Cyber Threat Intelligence (CTI)

- **Overview** – Integration of threat intelligence into XDR-driven security operations.
- **Intelligence Reports** – Threat actor activity, campaigns, and industry-relevant intelligence.
- **Sweeping vs Threat Hunting** – Indicator sweeping across historical data versus hypothesis-driven threat hunting.
- **Suspicious Object Management** – Management of Ips, domains, URLs, and file hashes across internal and external sources.
- **Sandbox Analysis** – Static and dynamic analysis to enrich detections and investigations.
- **Third Party Interlligence Integrations** – STIX/TAXII feeds, MISP, and Service Gateway-enabled intelligence sources.

Cyber Risk Exposure Management (CREM)

- **Cyber Risk Exposure Management** Overview – Risk-based security approach focused on continuous exposure management.
- **Cyber Risk Index** – Centralized risk scoring derived from exposure, attack activity, and configuration factors.
- **Attack Surface Discovery** – Identification of internet-facing assets, identities, cloud resources, and shadow IT.
- **Asset Risk Assessment** – Risk visibility across devices, accounts, applications, and cloud assets.
- **Continuous Risk Management** – Ongoing assessment of vulnerabilities, misconfigurations, and attack paths.
- **Cyber Attack Prediction** – Identification of likely attack vectors based on exposure and behaviour.
- **Security Posture Management** – Posture and configuration insights across hybrid environments.
- **Compliance Management** – Visibility supporting regulatory and framework-aligned security requirements.
- **Compliance Management** – Visibility supporting regulatory and framework aligned security requirements.
- **Security Awareness & Human Risk** – User behaviour risk, training effectiveness, and continuous improvement.

Role-Based Access Conrtol (RBAC)

- **Role Definition** – A role defines a grouping of permissions and a management scope within TrendAI Vision One.
- **User Assignment** – Users are assigned to a single role that determines their responsibilities and access level.
- **Operational Flexibility** – Allows customers to define responsibilities that align with their operational structure.
- **Application & Module Access** – Roles control high-level access and visibility across TrendAI Vision One applications and modules.
- **Granular Resource Control** - Fine-grained access controls for endpoints and servers.
- **Scope Management** – Scopes define what a role can see and manage across the console, inventories, and applications.
- **Separation of Responsibilities** – Supports both high-level and granular separation of duties across the platform.
- **Customer-Defined Role Design** – Enables organisations to design roles that fit their internal processes and governance model.