SOLUTION BRIEF

TREND MICRO VISION ONE™ SOCAAS

Trend Micro Vision One™ SOCaaS provides 24/7 alert monitoring and prioritization, incident investigation, and threat hunting to customers as a managed service. It leverages the resources and knowledge of Trend Micro Certified Support & Services Provider (TCSP) security experts to improve time to detection and time to respond.

This service provides teams with efficient alert monitoring, in-depth investigations into advanced threats and threat hunting via proprietary techniques.

Our threat investigators can initiate respective product response options to contain threats, while providing a step-by-step response plan on actions needed to remediate, along with custom cleanup tools, where applicable, to help recover from the threat.

SECURITY LAYER OPTIONS

EMAIL
- Cloud App Security with XDR

NETWORK
- Deep Discovery™ Inspector with XDR

SERVER AND CLOUD WORKLOADS
- Trend Micro Cloud One - Workload Security with XDR
- Deep Security software with XDR
- Third-party anti-malware with XDR

ENDPOINT
- Trend Micro Apex One with XDR
- Third-party anti-malware with XDR

SERVICE COMPONENTS AND DELIVERABLES

ANALYTICS AND AUTOMATION

Threat Inteligence | Expert Rules | Machine Learning

SOC ANALYTICS

THREAT EXPERT

SOC OPERATION

Response | Analysis and Investigation | Monitoring and Detection

Advanced

Standard

Behind the Trend Micro Vision One™ SOCaaS, it comprises of a dedicated team providing security monitoring and security operation services for our customer.

The Trend Micro Vision One™ SOCaaS team primarily focus on monitoring and detecting malicious activities on Customers environment, following as below:

24/7

- Real-time Continuous Monitoring
- SOC Cyber analyst support
- Threat Hunting support

This will help customers to improve threat detection, decrease the likelihood of security breaches, and ensure an appropriate organizational response when incidents do occur. Trend Micro Vision One™ SOCaaS teams can perform Root-cause analysis to provide an understanding of how the attack was initiated and spread and which devices were affected. In addition, the team can isolate abnormal activity on servers, databases, networks, endpoints, applications, etc., identify security threats, investigate them, and react to security incidents as they occur should the integration permits.

TREND MICRO VISION ONE™ SOCaaS BENEFITS

- **STAFF AUGMENTATION FOR COST AND RESOURCES OPTIMIZATION**

  The security operations are extended to 24/7 with security expertise without any associated expenses. It focuses on IT resources and personnel on mission critical initiatives to mitigate any threats.

- **INCREASE CYBERSECURITY OPERATIONAL EFFECTIVENESS AND EFFICIENCY**

  With the increased visibility, it centralized and connects information and reporting across security layers and customers. This provides timely detection, responses, and containment for our customer security related incidents.

- **PROVIDE INCREASED RISK VISIBILITY FOR RISK MITIGATION**

  As a Managed Serviced Partner (MSP), it enables us to deliver high value of services to our value customer. It also helps diversify risk with an "always on" approach from the solutions offered by Trend Micro Vision One™ SOCaaS beyond traditional technology.

- **THREAT INTEL INTEGRATION AND PROACTIVE THREAT SWEEPING**

  We keep up with the latest Threats out there by maintaining up-to-the-minute Threat Intelligence. With our own curated rich intel and other CTI reports, we proactively sweep your network for potential matches.

- **PERIODIC REPORTING, AND COMPLIANCE**

  With detailed and insightful weekly and monthly reports, the customers will be informed about the ongoing trends and status of incidents for the said period.

- **AUTOMATED AND TIMELY RESPONSE (USING SOAR PLAYBOOKS)**

  With SOAR Playbooks and Incident Runbooks, we work towards reducing the overall time taken to detect and respond. With defined SLA in place, this automation ensures timely response.

- **SECURITY INCIDENT RESPONSE MANAGEMENT**

  Advanced analysis and recommendations provided by our experts enables you to respond to incidents faster. This involves Malware analysis (Dynamic & Static Malware Analysis), close look into the associated processes, registry entries etc.

- **SECURITY HEALTH CHECKS**

  Regular Health Checks to ensure there are no gaps in your setup.

LICENSE DETAILS

	Trend Micro Vision One™ SOCaaS	
	Essentials	**Advanced**
Monitoring and Detection		
24*7 correlation and Prioritization	✓	✓
Proactive & On-demand IOC Sweeping	✓	✓
Proactive IOA Hunting	✓	✓
Mitre Mapping	✓	✓
Analyze and Investigate		
Complete Incident Investigation	✓	✓
Holistic approach to realize the overall Impact scope	✓	✓
Collection of artifacts	✓	✓
Sandbox analysis	✓	✓
Dynamic and Static Malware analysis	✓	✓
Respond and Remediate		
Access to SOC analyst	✓	✓
Threat Containment and Response	✓	✓
Remediate plans and Preventive measures	✓	✓
Cleanup tools wherever applicable	✓	✓
Third Party Products Response		✓
Further Reporting and Monitoring		
RCA Reports in cases of breach	✓	✓
Incident Reporting	✓	✓
Executive Summary	✓	✓
Guided/Full Threat remediation actions	✓	✓
Weekly Report	✓	✓
Monthly Report -Detailedand Executive Summary Report	✓	✓
On-demand Health check	✓	✓

TREND MICRO VISION ONE™ SOCaaS LIFE CYCLE

ONBOARDING:

The Trend Micro Vision One™ SOCaaS is onboarded in three phases which are Kick-off, Fine Tuning and Steady state, each covering broader milestones, Key Tasks with Responsibility matrix and Timelines projections

Kickoff: This phase includes all the tasks that are required prior on-boarding a customer to Trend Micro Vision One™ SOCaaS. These tasks range from initial stakeholder meetings to pre-requisite readiness and Health checks.

Fine tuning: This phase refers to reviewing the potential factors that might affect smooth functioning of Trend Micro Vision One™ SOCaaS. Any enrichment/enhancement of the said factors will also be carried out in this phase.

Steady State: Regular sync ups and reporting will be actively done in this phase.

DAILY OPERATIONS

Trend Micro Vision One™ SOCaaS Essential and Advance customers will provide Trend Micro Customers with cybersecurity talent who have the knowledge and skills necessary to combat cybersecurity threats. The Trend Micro Vision One™ SOCaaS partner's team will analyze and monitor the detections from Trend Micro Vision One™ Solutions. This service will help Trend Micro Vision One™ customers to improve threat detection, decrease the likelihood of security breaches, and ensure an appropriate organizational response when incidents do occur. Trend Micro Vision One™ SOCaaS partner team can isolate abnormal activity on servers, databases, networks, endpoints, applications, etc., identify security threats, investigate them, and react to security incidents as they occur.

SECURITY & COMPLIANCE

Faster, higher fidelity detections result in more timely containment and remediation. Improves the maturity of your security operations with capabilities that are essential to a modern, proactive, automated SOC.

REPORTS

Trend Micro Vision One™ SOCaaS Essential and Advance customers will receive weekly and monthly status and update reports summarizing investigated customer threat alerts, incident cases which contain details of the threat, including affected hosts, IoCs, and recommended mitigation options–wherever possible

Securing Your Connected World