AVONE – An integrated SIEM+MDR

AVONE (Government compliant) MSSP - provides scalable, extensible, resilient, and cost-effective solution with reduced manual workflow ***enhanced by FORTIDM's consulting and SOC managed services*** to help with a threat management program, vulnerability management and augmenting end point security incident detection and protection capabilities.

Objectives of AVONE's modern SIEM^{++} subscription based MSSP.

1. Prioritize threats specific to your business.
2. Centralized Visual analytics
3. Machine Learning (ML) driven threat detection.
4. Security Orchestration and Automated Response (SOAR)
5. Offers Integrated Risks and Vulnerability Assessment and SIEM that monitors, contains, remediates, and protects your assets in a single pane of glass view.

Benefits

1. **Identify the insider threats**: Uncover suspicious user activity that may indicate compromised credentials or an insider threat.
2. **Advanced threat detection:** Piece together several seemingly low-risk events to find the one extremely high-risk cyber-attack underway.
3. **Secure your Cloud:** Expose hidden risks in hybrid-multi-cloud environments and containerized workloads.
4. **Detect exfiltration:** Correlate exfiltration events, such as insertion of USBs, use of personal email services, unauthorized cloud storage or excessive printing.
5. **Centralized Monitoring:** Centralized monitoring for OT and IoT solutions to identify abnormal activity and potential threats.
6. **Integrated protection:** Unify prevention, detection, and response to combat threats at scale. Operationalize any security use case: SIEM, malware prevention, threat hunting, cloud monitoring, and more.
7. **Adhere to compliance:** Manage regulatory risk for a variety of compliance mandates, such as GDPR, PCI, SOX, HIPAA, FedRamp and more.

Operational model

AVONE SIEM will be a managed service on cloud (both commercial and Gov cloud) with the following operational model,

1. SIEM multi-cloud environment 100% MSSP managed - so clients don't need to manage patching, upgrades, availability, Disaster recovery setup and many more.
2. Clients will get the centralized SIEM Dashboard with the ability to create their own queries, timelines, lens, specific correlation-based incident etc.
3. Dozens of machine learning jobs for common security threat patterns comes OOTB.
4. Professional services may include (but not limited to) dashboard, advanced ML jobs setup, additional custom logs setup etc.
5. Automation of Vulnerability Management and SOAR and 24/7 SOC support

AVONE – An integrated SIEM+MDR

AVONE (Commercial) MSSP – Uses hosted Elastic SIEM, SentinelOne on cloud for Managed Detection and Response (MDR) with 24/7 SOC team. The capabilities of Avone are comparable for both commercial and Government in the baseline offerings. However, *the Avone SIEM/MDR commmercial SOC service is not FedRamp certified* with a competitive and simplified pricing agnostic of size of the data ingestion and/or queries performed.

Avone MDR uses machine learned, behaviour based monitoring of threats and looks for why something is happening and not just what is happening. Performs real-time response and remediation and integrates seamlesly with other security solution via API.

Avone SOC MSSP Overview

Provides SOC-supported endpoint monitoring and protection.

- Advanced Endpoint Detection & Response (EDR) with SOC monitoring & remediation

PROTECT
Static AI - Prevent attacks pre-execution

DETECT
Behavioral AI - Constantly monitors and maps each running process for incongruous behaviors

RESPOND/RECOVER
Automated EDR - Automate remediation and response—even rollback

Responsibilities of SOC

- Monitor and analyze client IT environments to protect against threats across endpoints and networks
- Identify advanced malware, exploits and script-based stealth attacks, utilizing attack forensics and intelligent automation
- Activate remediation steps when confirmed malicious attacks are in progress, including scrubbing the system of any remnant of an attack, such as malicious processes or registry keys
- Perform system rollback, if required, to restore system and data access
- Partner outreach for progress updates when needed to effectively protect against threats across endpoints and networks

Pricing: Starting at $9.20/agent/month for MDR Sentinel and $25.4 /agent/month for SIEM With 12 month commmittment and 2 hr SLA for incident respone (in actuality the typical respone time is less than 30 min). No cost during first 3 months ramp-up period.

AVONE – An integrated SIEM+MDR

AVONE **Demo**

The following presents the Demonstration of our SIEM, Vulnerability & Threat management, SOAR, EDR/MDR and UEBA capability.

Please note that the tools and technologies mentioned in this video is to show the functional capability independent of the tools. AVONE can extend these technologies to additional use cases as needed.

1. **Assessment Dashboard Demo -** This video shows the **AVONE** SIEM Dashboard capabilities as an example. Your dashboard is customizable according to your enterprise needs and priorities in maintaining your assets secured.
   https://youtu.be/9uXJvV-9xqU

2. **Overview-Asset and Vulnerability Management** - How do you make sure all your assets are accounted in monitoring and there is no compliance gap? Using Asset management tool (ITSM) integration driven configuration of **AVONE** elastic security. This demo shows an overview of the integration.
   https://www.youtube.com/watch?v=CUogQ-yOQTA

3. **AVONE Elastic Vulnerability automation lab** - **AVONE** Elastic Vulnerability automation lab
   the above link shows demo of tenable and Snipe-IT asset management integration using pipeline that enables vulnerability alert to kick start a scanning of the device in tennable.io and capture the incidents and events in **AVONE** elastic while updating the asset management database with the newly found vulnerabilities.
   https://www.youtube.com/watch?v=7VqaTfEb9eM

4. **Overview-SIEM SOAR Integration** - This video gives an overview of the SOAR integration of **AVONE** Elastic.
   https://www.youtube.com/watch?v=P54Fm6nXaHM

5. **User Entity Behavior Analytics** - this video gives an overview of the User behavior analytics and shows how insider threat was identified using **AVONE** SIEM
   https://www.youtube.com/watch?v=8sO2_9CsJJs