THRIVE℠

SERVICE DESCRIPTION

Managed SIEM as a Service

Executive Summary

Thrive Managed SIEM as a Service Definition

Thrive's Managed SIEM as a Service (SIEMaaS) is a fully managed, hosted Security Incident and Event Management service and provides a service-oriented IT infrastructure monitoring solution which collects data from host systems, network devices, applications, SaaS and security platforms, and adds real-time context, analytics, and alerts for a more complete understanding of the environment. When a security event occurs, an Incident is created in the Thrive security platform and alerts are sent to the Client for review and analysis.

Location	Device Type	Qty	Manufacturer	Model	Operating System	Client or Thrive Owned
London	*Switch*	*3*	*Meraki*	*MS225-48*	*N/A*	*Thrive*
London	*Server*	*2*	*Dell*	*R730*	*Windows 2016*	*Client*

Services Scope

The service shall include:

- Implementation of SIEM tenant and SIEM log and data collectors
- Ongoing alert optimisation
- Allowance of 10 Events Per Second per logged device or SaaS application
- 7x24x365 log collection
- Standard and Custom rules for incident and event alerting
- Quarterly SIEM event review with Thrive Security Analyst
- Security Incident Dashboard
- Weekly PDF reports per customer specification
- 90 Day log retention. Extended retention is available for additional storage fee
- SaaS security monitoring available on some applications (optional)

Thrive Scope of Work and Deliverables

- Thrive shall deploy and configure a secure SIEM tenant on the Thrive Security Platform.
- Thrive shall configure the required SIEM collector(s) on Client premises or hosted cloud environment. A minimum of one virtual collector is required either inside the customer network or on a cloud server.
- Thrive shall provide guidance on device protocol configuration including SNMP and WMI best practices.
- Thrive shall provide and an Advanced Windows agent for each Windows server subscribed to the Managed SIEMaaS Enhanced Windows Agent service and provide agent installation guidance for servers not managed by Thrive.
- Thrive shall provide an allowance of ten (10) Events Per Second (EPS) per logged device or SaaS application. The total EPS allowance determined by the number of devices and applications subscribed for log collection. Additional EPS can be purchased if log events exceed EPS allowance. Thrive shall provide review of log volume and log collection and implement event filtering as required.
- Thrive shall configure email alert notifications to customer defined email recipients and/or distributions lists.
- Thrive shall provide quarterly SIEM event review including log source analysis.
- Thrive shall configure Security Incident Dashboards and scheduling of emailed reports.
- Thrive shall provide basic network device configuration backup.

Client Responsibilities

- Client shall provide Thrive with the list of devices and network diagram for log collection and CMDB discovery of devices.
- Client shall provide the virtual resources to install the collector at each location. Optionally, Thrive can provide a physical collector probe for an additional fee. Client shall provide the Thrive team with administrative access to the environment to install the virtual collector or provide assistance to Thrive to install the software. Each collector requires a minimum of:
    - 8GB Memory
    - 4 vCPU
    - 125 GB storage volume
- Client shall provide Thrive appropriate connectivity and administrative access to devices and applications that are required to deliver support or, provide technical assistance to Thrive to install the any required software or agent.
- Client shall configure endpoint devices for discovery. If devices are managed under Thrive Managed Infrastructure Services, Thrive will provide configuration service on covered devices.
- Client shall notify Thrive prior to making any changes to the devices that Thrive is collecting log data that may impact log collection , including external IP address changes which will prevent logs from being accepted by the Thrive Security Platform.
- Client shall configure their firewalls with the necessary network protocols to allow the collector to communicate with the Thrive Security Platform.
- Client shall provide email contact and/or distribution lists for event notifications to be delivered.
- For Windows server log collection, Client shall provide Thrive with a Windows Domain Admin account for WMI monitoring.
- For network device log collection, such as switches, routers and firewalls, Client shall provide the necessary SNMP community strings and SSH access for monitoring and the client will be responsible for any SNMP configuration on their devices such as configuring a trusted SNMP host.
- Client shall be responsible for site network connectivity to ensure collector can transmit logs the Thrive Security Platform.

Optional Services

Office 365 Monitoring

- Thrive shall monitor and log the Microsoft Office 365 platform for the following events:
  - Office 365 Successful Login from Outside the United States
  - Office 365 Failed Login
  - Office 365 User Group Management Activity
  - Office 365 Application Registration

Managed Services Billing Activation

Billing of Managed SIEMaaS recurring charges will commence as of the date Managed SIEMaaS log collection has commenced, Client portal has been configured and login credentials have made available to the Client by the Thrive Security Operations Center.

Service Exclusions

Any service not explicitly included in the Managed SIEMaaS Service Definition above is considered optional and may be provided under separate agreement for an additional fee.