



SERVICE DESCRIPTION

**Managed SIEM as a
Service with Security
Monitoring**

Executive Summary

Thrive Managed SIEM as a Service with Security Monitoring

Service Definition

Thrive's Managed SIEM as a Service (SIEMaaS) with Security Monitoring 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 initial triage is performed by the Thrive Security Operations Center. Remediation service is dependent on the ultimate source of the event and the management level Thrive has for the affected device or system or platform.

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

Services Scope

The service shall include:

- Implementation of SIEM tenant and SIEM log and data collectors
- 7x24x365 log collection and security monitoring
- Alerting and notification on legitimate security Incidents and events
- Standard and Custom rules for alerting
- Ongoing alert optimisation
- Allowance of 10 Events Per Second per logged device or SaaS application
- Remediation guidance from Thrive Security Operations Center on actionable Incidents
- 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 24x7x365 Security Monitoring. Thrive will analyse and assess each Incident created by the SIEM platform and assign a severity level to the Incident. Response times and methods of notification by the Thrive Security Operations Center are defined as follows:

Incident Severity Level	Incident Severity Criteria	Initial Response	Method of Notification
High	High likelihood of a security breach or attempted breach in progress	Within 15 minutes of Incident Analysis	Telephone and Incident Ticket via Email
Medium	Multiple blocked non-impacting attempts or abnormal user behavior	Within 4 Hours of Incident Analysis	Incident Ticket via Email
Low	Single non-impacting events	Within 24 hours of Incident Analysis	Incident Ticket via Email

- Thrive shall provide review of log volume and log collection and implement event filtering as required.



- Thrive shall provide alerting and notification on legitimate security events. Events will be grouped by severity. Thrive shall configure email alert notifications to customer defined email recipients and/or distributions lists.
- Thrive shall escalate High severity alerts to the Client via email and/or telephone notification and provide remediation guidance.
- 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.
- Thrive shall provide threat remediation for all devices and SaaS applications contracted for Thrive Managed Services. Remediation is dependent on the ultimate source of the event and the access Thrive has to the appliance or server. Thrive shall provide remediation guidance to the Client for any devices not contracted for Thrive Managed Services.
- Remediation shall be defined as:
 - Firewall
 - Updates to access rules
 - Updates to security services configuration
 - Geo-IP Filters
 - IPS/IDS Updates
 - Gateway Antivirus
 - Updates to firmware
 - Servers
 - Windows Operating Systems Updates
 - Recommendations for Authentication improvements
 - Server Hardening Consulting
 - Networking (Wired and Wireless)
 - Firmware updates
 - Access rule updates
 - Additional log configurations
 - Recommendations for intra-vlan segmentation
 - SaaS Applications
 - Account deactivation
 - Account modification
 - Application modification
 - Notifications for end users who may have been compromised while protected by MDR service



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 below 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 advise Thrive on any addition or removal of devices that require log collection.
- Client shall configure their firewalls with the necessary network protocols to allow the collector to communicate with the Thrive Security Platform.
- Client shall provide escalation contacts to Thrive for high severity event notification. These are currently limited to the email and phone-based escalation communication. Client is responsible for notifying Thrive of any changes to the escalation contact information.
- 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

Salesforce CRM Monitoring

- Thrive shall monitor the Salesforce CRM platform for the following events:
 - Salesforce Failed Logon Activity

Additional Salesforce CRM logs will be collected and available through SIEM reports.

Managed Services Billing Activation

Billing of Managed SIEMaaS with Security Monitoring 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 with Security Monitoring Service Definition above is considered optional and may be provided under separate agreement for an additional fee.