MANAGED SECURITY OPERATIONS (SIEM) - SERVICE GUIDE

Last Modification Date: 05/13/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 OVERVIEW

Managed Security Operations is a managed Security Incident and Event Management (SIEM) Service that collects log and event data from covered devices and processes that data to identify and detect security and compliance events. Managed Security Operations Manager delivers deep insight into your security and compliance posture without the expense and complexity of doing this in-house.

Managed Security Operations Manager Services provide automated incident alerting, incident reporting, daily log reviews, log analysis and customized escalation procedures. The platform is driven by an enterprise-class, cloud-based SIEM engine that consumes log and event data via remote collectors. The managed services SIEM platform is operated from a Security Operations Center (SOC) that is staffed by certified security analysts. Customer support to the SOC is available 24/7 via t he Hosted Cafe Support portal.

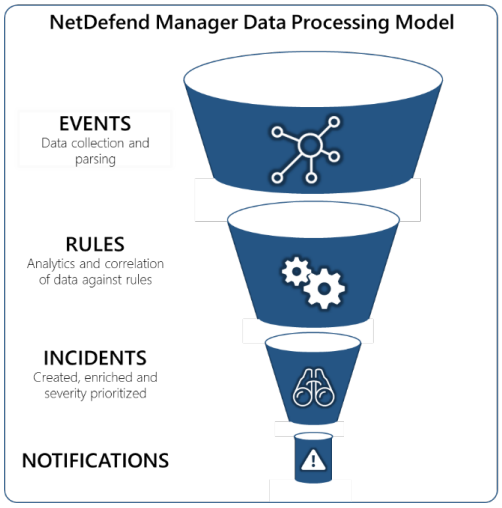
Managed Security Operations Manager provides users an easy-to-use web interface with dozens of dashboard elements, reports, and rapid search capabilities. The Managed Security Operations services team provides onboard training and assistance with utilizing the SIEM platform. While this is a powerful tool, expert knowledge of how to use a SIEM platform is not necessary to get the value from this service.

Managed Security Operations service team configures the SIEM rules engine and tunes the service to fit your environment, captures incidents, and determines which incidents are most important that require attention. Critical and important alerts are sent via e-mail and all other interesting data is available via reporting and also via the web portal. A dashboard on the web portal provides a quick view of your security posture and important risks and threats.

2 HOW IT WORKS

Client infrastructure log and event data is collected by a local log data collection appliance (virtual or physical) and then forwarded via a secure encrypted transit to the Managed Security Operations Manager Security and Incident Management (SIEM) platform. The Managed Security Operations Manager platform is an advanced analytics and correlation engine. Paired with innovative security rules and a threat intelligence database, Managed Security Operations Manager determines which events represent a security or compliance-related incident. The SIEM engine essentially distills millions of events down to a manageable level of actionable alerts.

Events from client systems are funneled through the Managed Security Operations Manager rules engine to create incidents that are then enhanced with meaningful data and assigned a severity level. Based upon the severity level, incidents may result in a ticket and client notification. All incidents, regardless of severity level, are captured and available for review in the Managed Security Operations monitoring portal via dashboard widgets, searches, and reports.



3 INSTALLATION AND CONFIGURATION

Data collection software will be installed on a customer provided virtual machine or physical server to provide data collection services in the customer environment. The Managed Security Operations service team will assist with the installation of collector software, add monitored devices to Managed Security Operations Manager, apply monitoring and alert templates, initiate delivery of reports, and set up customer response plans to alert both notification and escalation contacts.

Through the Managed Security Operations Manager platform, it is possible to recognize specific device behavior and to modify incident reporting and notification policies. The Managed Security Operations service team will work with the client to identify device behavior that may be generating false positives and work to implement specific policies for the client environment to optimize incident notification policies. It is recommended that this occur during implementation.

Changes to the client's network or policy devices are not included in the standard installation engagement. Optional Professional Services engagements may be utilized to redesign or reconfigure the network, security appliances, or application architectures if necessary.

4 SERVICE OPERATIONS

The Managed Security Operations service team (SOC) is responsible for Managed Security Operations Manager operations and maintenance. The SOC team will continually tune the platform, monitoring templates, rules engine, and threat intelligence databases. The SOC team will remotely manage data collectors, be responsible for all operating systems, software licensing, and providing maintenance on the collector. The collector needs to be sized-right and potentially changed from time to time based on changes to the client's network environment and software updates.

The following items outline service operations of the Managed Security Operations Manager Service:

- Collect, parse, normalize, correlate, and store security related logs and SNMP data from customer devices.
- Ongoing tuning of rule database and classification of security events for alerting.
- Ongoing tuning of rules to reduce false positives and negatives.
- Enrichment of security alerts with relevant service data to assist with event response, triage, or escalation steps.
- Maintain customer response and escalation plan for alert notification and procedures.
- Maintain threat intelligence database with daily updates of new threat and attack risks.
- Identifying the need to update the on-premise data collection appliance and scheduling maintenance with the client.

4.1 THREAT INTELLIGENCE

The Managed Security Operations Manager service utilizes a variety of threat intelligence sources. These sources are updated daily.

Blocked Domain Lists includes:

- Malware Domains List (MDL)
- Zeus Domains
- SANS Domains

Blocked IPs and Emerging Threat Blocked IP Lists include:

- Shadowserver C&C
- Russian Business Network (RBN)
- Spamhaus
- Zeus Blocked IP

- Dshield Top Attackers
- Feodo
- Palevo
- Brobot & Kamikazee

4.2 LOG RETENTION

Logs are accessible and retained for 400 days with a redundant copy stored in a secondary datacenter. Logs are retained on enterprise-class storage with data available via high performance solid state and disk storage through the 400-day life span of the data.

5 DAILY LOG REVIEW SERVICE

The daily log review is designed to meet compliance mandates and improve security operations. A Security Analyst will review the logs from the previous day. Log review will be performed to:

- Analyze event log data for possible security incidents.
- Identify incidents that warrant further investigation.
- Provide an audit trail for auditors and regulators.
- Continually tune event rules and notifications.

If high or medium severity security or compliance incident is identified, the SOC team will contact client with the details of the incident in accordance with the client escalation process.

Managed Security Operations Manager daily log reviews are included standard with the services. In addition to security and operational benefits of the log review service, it is designed to help clients meet compliance requirement for log reviews, a log review policy, a defined process, and log retention as defined in PCI-DSS 3.0 requirement sections: §10.2, §10.3, §10.6. This meets similar requirements outlined by HIPAA, SOX, and ISO compliance standards.

6 INCIDENT NOTIFICATION

The SOC will proactively notify the client of Priority 1 through 4 severity incidents discovered by Managed Security Operations Manager via a ticketing system. Informational-level incidents are stored in the Managed Security Operations Manager platform. All incidents, including informational-level incidents, are accessible in the Managed Security Operations monitoring portal via dashboard widgets, searches and reports. For detail regarding alerting and severity ranking please refer to the Work Order.

Note: Managed Security Operations Manager is a notification and informational service. Customers requiring assistance with network or device remediation may subscribe to Managed Network Service or Professional Services. To determine what services are offered through other Managed Network Services, see the Managed Network Service Guides and Work Order. Professional services are customized and defined per a client specific work order.

7 SUPPORT

7.1 SERVICE SUPPORT

The SOC will address Managed Security Operations Manager Service availability and performance issues in accordance to the Work Order priority definition and SLA. The SOC is available 24/7 for service requests via the Hosted Cafe' portal. The SOC will take commercially reasonable efforts to maintain continuous uptime and availability (excluding planned maintenance) of the Managed Security Operations Manager platform and web interface. In the event that the Managed Security Operations Manager platform is unavailable outside of planned

maintenance, the customer data collector will continue to collect and store logs during service disruption until connectivity to the platform is restored or the device reaches its storage capacity.

7.2 INCIDENT SUPPORT

For Priority 1 through 4 incidents, the SOC will take the following actions:

- Identify the elements involved in the incident (IPs, URLs, nature of the alert)
- Validate the severity of the incident and reclassify priority level of the automated alert as necessary
- Alert the customer with incident details and suggestions of how to proceed
- Escalate to NetDefend Security Operations Center as necessary for additional incident details
- If network or device remediation is necessary, the following actions can occur:
    - Open a Managed Network Service ticket - this is dependent upon client subscribing to Managed Network Services.
    - Open a Professional Services ticket - this is dependent upon client having Professional Services contract.
    - Refer case to customer account manager or client service manager if new services are requested.

Exclusions:

- Service and event notification outside of the Customer Response Plan.
- Support is limited to the devices supported by Managed Security Operations Manager Platform.
- Products not on the Supported Products list.

8 HOSTED CAFÉ MONITORING PORTAL

Customers are provided access to the Hosted Café monitoring portal in which the Managed Security Operations Manager SIEM capabilities are available. This will allow security logs, events, rules, incidents and reports to be viewed. The portal is accessible via https://health.hostedcafe.com[1]

9 HOSTED CAFÉ SERVICE PORTAL

The Hosted Café service portal provides for the creation, tracking, and review of service tickets. All service ticket information in available via this portal and enables tracking of implementations, changes, releases, and trouble issues. This portal is accessible via https://support.hostedcafe.com[2]

10 REPORTS

The SOC will set up and configure a library of standard reports during service implementation. The reports provide incident details, trends, and summary data related to covered devices. Incident reports include access attempts, policy changes, incident details, incident/alert statistics, events by devices, network traffic, URL access, application connections, infected files, blocked connections, and compliance reports.

Below is a current list of the available reports, as of the publication date of this Service Guide. Reports names may vary slightly from this document to the portal.

Active Directory Catalog Changes

All High Incident Count – Detail

All Incident Count – Detail

1 https://health.hostedcafe.com/
2 https://service.hostedcafe.com/

All Managed Security Operations Incidents that Create Tickets – Detail

Blocked Web Browser Activity

Change: Audited File Added/Deleted

Change: Audited File Attribute Modifications

Change: Domain Groups Modified

Change: Domain User Accounts Created

Daily Log Review: Detailed Failed Login

Daily Log Review: Devices Added to CMDB

Daily Log Review: Firewall Admin Activity Details

Daily Log Review: Firewall Config Changes

Daily Log Review: Network IPS Events

Daily Log Review: Top Security Incidents by Severity

# of Incidents

# of High Incidents

# of Medium Incidents

# of Low Incidents

# of Raw Events

Detailed Domain or Server Account lockouts

Detailed Failed Login at Any Device

Domain Groups Modified

Inbound Cleartext Password Usage Detected

Incidents – High Incidents by Source IP

Incidents with Notification Sent by Count

Logon: Failed Database Server Logon Details

Logon: Failed Firewall Admin Logon Details

Logon: Failed Router Admin Logons

Logon: Windows Domain Authentication Details

Privileged Windows Server Logon Attempts Using the Admin Account

Successful VPN Logon from Outside My Country

Top Blocked Network Attacks

Top Blocked Destinations by Connection Count

Top Blocked Inbound Connections by Count

Top IPs with Malware Found by IPS and Firewalls

Top Permitted Uncommon Services by Connections

Top Security Event Severity by Count

Top Security Incidents

Top Web Sessions by Bytes

Top Web Users by Bytes

Top Web Users, Denied Sites and Categories by Connections

Users Added to Domain Group

Report availability may be dependent upon the type of devices monitored and data collected. This list of reports can change at any time, and reports may be added, altered or removed.

Specific report bundles can be created upon request including reports for compliance including GLBA, HIPAA, PCI-DSS, and other industry or regulatory standards.

Additional custom report requests will be accommodated on a best-effort basis. Depending upon the request, custom report creation may be an additional one-time service fee.

11 CUSTOMER RESPONSIBILITY

Customer setup and data collector maintenance requirements:

- Provide accurate and complete network information including IP addresses, domain names, diagrams, SNMP string information and other information as needed for configuration and function of the service.
- Configure monitored devices as required for the service to collect event information.
- Provide required CPU, memory, storage space, and power resources to run the data collector per Managed Security Operations specifications.
- Provide device authentication and credential information as required for service delivery.

Service Operations:

- Ensure monitored systems/devices are running properly.
- Ensure monitored networks are running properly.
- Ensure adequate and reliable connectivity to the data collector appliance and on premise devices, including appropriate bandwidth.
- Promptly notify of any changes to Customer security policy, firewall, devices and/or notification contacts.
- Notify of any planned maintenance or outage that will impact the covered device(s) at least 48 hours in advance.

Incident remediation:

- Client is responsible for incident response, resolution, and remediation or obtaining additional services for remediation assistance.
- It is strongly recommended that customer maintain Managed Network Services for each Managed Security Operations monitored device.

12 EVENTS PER SECOND (EPS) ALLOCATION

Managed Security Operations Manager monitoring is sold based upon an allocated Events Per Second (EPS) quota. The allocated EPS for a device type is defined in the service order. In the event that the aggregate EPS exceeds the total allocated EPS, the following actions can occur:

1. The SOC will work with the customer to tune the log settings to ensure that excessive logs are not being collected and stored.
2. If tuning the log setting does not adjust the log collection and bring it into the quota level, the SOC retains the right to charge the customer for the additional events per second overage and adjust the monthly billing to reflect the proper quota allocation. Overage billing will be based upon our current EPS pricing plus 10%.

Aggregate EPS is the total average EPS across all monitored devices as observed in a one week period. The SOC takes the highest weekly average EPS in a given month to determine the EPS reported for the month.

Allocated EPS is the total allocated EPS across all monitored devices. For example, if monitoring 10 servers, 2 databases, 2 firewalls, 2 domain controllers, and 2 routers, the budgeted EPS is the total EPS as represented in the service order across all devices.

13 MANAGED SECURITY OPERATIONS MANAGER SUPPORTED ENVIRONMENTS

Managed Security Operations Manager supports the following log data formats: Syslog, SNMP, or WMI

13.1 DATABASE SERVER (ACCESS LEVEL INFO ONLY)

Microsoft SQL Server

MySQL Server

13.2 DIRECTORY SERVER

Microsoft Active Directory

13.3 MAIL SERVER

Microsoft Exchange

13.4 UNIFIED COMMUNICATION SERVER CONFIGURATION

Cisco Call Manager

Cisco Presence Server

13.5 CLOUD APPLICATIONS (ASK, REQUIRES PROSERVICES SETUP)

AWS CloudTrail API

Microsoft Azure Audit

Microsoft Office365 Audit

13.6 MANAGED ENDPOINT PROTECTION SECURITY SOFTWARE

Cisco FireAMP Cloud

Cylance Protect Endpoint Protection

FortiClient

Palo Alto Traps Endpoint Security Manager

Sophos Endpoint Security and Control (Ask)

13.7 FIREWALLS (REQUIRES EPS INFO TO QUOTE)

Check Point Firewall

Cisco Adaptive Security Appliance (ASA) / Firepower

Fortinet FortiGate Firewall

Palo Alto Firewall

13.8 LOAD BALANCERS AND APPLICATION FIREWALLS

F5 Networks Application Security Manager*

F5 Networks Local Traffic Manager*

13.9 INTRUSION PROTECTION SYSTEMS

Cisco FireSIGHT

Cisco Intrusion Protection System

Snort Intrusion Protection System

13.10 ROUTERS AND SWITCHES

Cisco IOS Router and Switch

Cisco Meraki Cloud Controller and Network Devices**

Cisco NX-OS Router and Switch

HP ProCurve Switch

Juniper Networks JunOS Switch

13.11 SECURITY GATEWAYS

Barracuda Networks Spam Firewall

Cisco IronPort Mail Gateway

13.12 SECURE NETWORK ACCESS CONTROL

Aruba Clearpass

Cisco ISE

13.13 SERVERS

Linux Server

Microsoft Windows Server

13.14 VIRTUALIZATION

HyperV

VMware ESX

13.15 VPN GATEWAYS

Cisco Adaptive Security Appliance (ASA) / Firepower

Cisco VPN 3000 Gateway

Juniper Networks SSL VPN Gateway

13.16 VULNERABILITY SCANNERS (REQUIRES PROSERVICES SETUP)

Nessus Vulnerability Scanner

Qualys Vulnerability Scanner

Rapid7 NeXpose Vulnerability Scanner

13.17 WAN ACCELERATORS

Riverbed SteelHead WAN Accelerator

13.18 WIRELESS LANS

Aruba Networks Wireless LAN

Cisco Wireless LAN

** Cisco Meraki environments requiring two-factor authentication to log into the management dashboard are not supported

14 COMMERCIAL ITEMS

The following are Managed Security Operations Manager specific orderable services.

Minimum service term starts at 1-year contract. A minimum of $1,500 monthly recurring service fees in Managed Security Services and Managed Infrastructure and Monitoring services combined is required for new service activation. New orders under this amount are not accepted.

Optional Managed Security Services services:

- Managed Vulnerability Scanning
- Managed Endpoint Protection
- Professional services – Vulnerability Assessment and Management