

Service Definition

Table of Contents

1	INTRODUCTION	2
2	SERVICE OFFERING	2
2.1	SOLUTION PURPOSE	2
3	SOC SERVICES	3
3.1	ON-BOARDING EXPECTATIONS FOR SOC SERVICES	4
3.1.1	SIEM Collector	4
3.1.2	Tailored Security Playbook Creation	5
3.2	COVERAGE LIMITATIONS	5
4	TECHNICAL SUPPORT AND MONITORING FOR SIEM	5
5	SERVICE LIMITATIONS	5
6	APPENDIX A – SERVICE LEVEL OBJECTIVES	7
7	APPENDIX B – SUPPORTED DATA SOURCE	8
8	APPENDIX C – HIGH/SEVERE THREAT MATRIX	9

1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's SOC as a Service.

The service definitions found herein reflect Synoptek's standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect the current Synoptek best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERING

Synoptek's SOC as a Service is the essential service in Synoptek's Managed Detection and Response Services suite.

Synoptek's Managed Detection and Response (MDR) provides 24x7 monitoring of security alerts for subscribed IT infrastructure and cloud services, as well as proactive security playbook planning and SLA-backed 24x7 containment and mitigation of detected alerts. This service enables CISO's peace of mind against the continuous threat of breach. The CISO can rest assure that they will be able to support aggressive growth and digital transformation initiatives while providing the business a risk managed response plan against actionable security threats.

SOC as a Service adds a SOC team to Managed Core IT Infrastructure, SaaS applications, and IaaS Cloud services to offer:

- **24x7 Detection** of security alerts in near-real time cross-correlated through multiple global SIEM networks connecting hundreds of organizations
- **24x7 Incident Investigation** of potentially malicious (High Severity) and/or active and imminent threats (Emergency Severity)
- **A Daily Cyber Security Review** which is an investigation of all security events for further investigation.
- **24x7 Alert Response** to act on Customer's behalf and contain and mitigate potential and active attacks.
- **Reduction of False Positive Alerts using Global Threat intelligence** via a combination of monitored alerts from our global SIEM network and data from global intelligence sources, thereby reducing the business impact of "false alarms."

2.1 SOLUTION PURPOSE

Most organizations don't have the technology or security expertise to detect cybersecurity threats, let alone investigate or remediate them. The average time between a data breach and discovery is 205 days. Simply implementing security protection tools such as firewalls or anti-virus isn't enough. This is even more true for organizations that fall under PCI, HIPAA, SOX, or FFIEC regulations. For those companies, compliance with various guidelines and mandates is critical to avoid fines or worse, breach of data and infrastructure.

Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and response. That technology is known as security information and event management (SIEM), and it provides deep security intelligence for your IT environment. A proper SIEM solution provides intelligence to help answer critical questions that are vital to your cybersecurity protection – questions such as:

- How do we determine if the employee forgot their password or whether a brute force attack is being launched?
- Was access to sensitive files on a server last night normal business use or did we just get breached?
- Which of the 864,000 events per day my firewall received important and actionable?
- Were the new wireless access points added to the network intentional?
- Are our employees going to sites – intentionally or not – that put us at risk for malware infection?
- Do we have the data needed to properly comply to regulatory compliance requirements?

Unlike other SOC as a Service offering, the burden of response is taken care by Synoptek’s SOC, EOC and NOC teams. Synoptek MDR gives your security team immediate response to mitigate and contain threats.

3 SOC SERVICES

FEATURE AND DESCRIPTION	ADDITIONAL INFO	INCLUDED
24X7X365 MONITORING, DETECTION AND INCIDENT TRIAGE	<p>Synoptek’s provides a Security Information and Event Management (SIEM) service, which includes 24x7x365 automated monitoring and alert detection through advanced log correlation, contextual analytics, big data analysis and Synoptek’s custom-tuned rule database.</p> <p>The SIEM aggregates threat intelligence from hundreds of organizations, multiple SIEM implementations around the world and provides Synoptek SOC Analysts with threat notifications for on-premise devices including firewalls, routers, unified threat management devices, switches, servers and all other applications and services for which there is a preconfigured SIEM parser.</p> <p>The list of supported event sources can be found in Appendix B.</p>	<p>Yes</p>
DAILY CYBER SECURITY REVIEW	<p>All discovered security incidents (Low, Medium, High, Severe) are reviewed daily by a SOC Analyst with further analysis to proactively hunt for hidden threats, suspicious trends, and cross organizational comparisons. Each automated alert is confirmed if they were triggered, sent, and delivered, and properly categorized. This also includes third party, non-automated intelligence gathering.</p> <p>This review also includes third party, non-automated intelligence gathering. This capability complies with major regulatory & compliance requirements requiring daily reviews such as with PCI, FFIEC, and HIPAA.</p> <p>Each event reviewed that requires awareness is documented in the monthly threat intelligence report.</p> <p>All daily reviews are completed by 8:00am Eastern Standard Time (EST).</p>	<p>Yes</p>

24X7X365 SECURITY ALERT INVESTIGATION AND RESPONSE	<p>Synoptek will investigate and perform analysis for all High and Severe Alerts detected by our SIEM.</p> <p>For every incident received, our analysts draw on their expertise, external sources of intelligence and the context of the network before taking an informed action on the threats faced. Investigation activities include detailed log analysis and looking for suspicious trends. The result is a near zero false-positive rate to ensure business continuity of mission critical IT infrastructure.</p> <p>Upon notification of an event or a detected or ongoing High or Severe Threat event, Synoptek SOC Analysts will start investigating within the “First Response” SLO and respond within the “First Activity” SLO in accordance with the agreed upon Security playbooks.</p> <p>The Service Level Objectives are described in Appendix A.</p>	Yes
MONTHLY THREAT INTELLIGENCE REPORTING	<p>Synoptek will deliver a threat intelligence report of security events discovered by our SIEM and reviewed on a daily basis. One hour of advisory report overview is provided following the distribution of the report.</p>	Requires SIEM Threat Intelligence Add On

3.1 ON-BOARDING SERVICES

3.1.1 SIEM Collector Deployment

Synoptek is responsible for detecting network anomalies and eliminating the false positive traffic patterns that show up on our screens in near real-time. An initial 4-6 weeks of tuning are required before the system becomes optimized. Ongoing tuning, which is inclusive in the service, progressively provides improvement in data quality reporting.

The implementation of the *SIEM Collector* is dependent on the Customer’s environment architecture, which may require deployment of a Virtual Appliance. The SIEM collector is capable of operating on a variety of hypervisors and cloud services. If the target environment does not currently support virtualization and hardware needs to be procured to facilitate installation of the Collector, the hardware expense will be in addition to the SOC-as-a-Service offering.

Scheduling of the implementation will be arranged and is expected to occur within a 4-hour service delivery window and is non-disruptive to your production environment. The collector’s minimum requirements are:

- 2 core CPU
- 4GB of memory
- 40GB of disk space

A single appliance can handle multiple sources of network traffic and cover up to tens of thousands of individual devices, depending on peak traffic volumes and network segmentation.

3.1.2 Tailored Security Playbook Planning

Synoptek will work with customers to define actions Synoptek can take on the Customer's behalf. The baseline security playbook is developed from over 150 alerts of type Severe Threat (Alert Level 10) and High Threat (Alert Level 9).

Customer input is required to tailor the playbook, most importantly, for IT or application services that need to be taken offline following detection of a Severe/High Threat security event. Generally, Synoptek aims to be least disruptive to preserve business continuity but aims to deliver an appropriate level of response based on the security risk.

The Threat Severity Matrix for all Severe and High Threats can be found in Appendix C.

3.2 COVERAGE LIMITATIONS

This service includes investigation for all incidents with threat indicators of either High Threat (Ticket opened as P2) or Severe Threat (Ticket opened as 'P2 – User Expedite').

Due to the unique nature of each security incident investigation, Synoptek's objective is to address and take action, totaling no more than 5 hours per incident. Any additional work to restore availability of services (e.g., IT infrastructure services) require Synoptek Managed IT services or billable time and material.

Synoptek's requires full visibility with its SIEM and other services in order to comprehensively investigate the scope of the incident. Any appliances, devices, systems, applications, and services (e.g., sources) that are not subscribed to the SOC-as-a-Service will produce inconclusive analysis (e.g., endpoints that are only subscribed to ITaaS Standard services and not required SOC services, will not provide any alerts to the SIEM, nor the SOC team). Any investigative requests for other sources will require billable time and material.

Security remediation, defined as taking steps to prevent and/or eliminate future threats to IT infrastructure and systems, is not included in this service. Security remediation is offered by Synoptek as a separate billable project service.

4 TECHNICAL SUPPORT AND MONITORING FOR SIEM

Synoptek manages and maintains the support for the SIEM collector. In addition, Customers can submit a web-based ticket where Synoptek will track, take action and update SIEM collector related issues.

Synoptek will remediate issues related to the SIEM collector appliance, identified either via monitoring and notification, or those initiated through contacting the Service Desk. In all cases, a service ticket will be created and prioritized based on the severity. The service desk will take necessary resolution steps required to resolve the issue remotely, escalating as required. If the issue cannot be resolved remotely, a field technician will be dispatched.

5 SERVICE LIMITATIONS

Synoptek's Security Operation Center Services are an excellent addition to an organization's strategy of defense in-depth approach. The sophistication of attacks as they evolve, may circumvent detection by the SIEM. The industry recommendation is to architect a security defense that complements an array of protection measures. Undetectable patterns that can be identified by SIEM require full network visibility.

Furthermore, this service differs from a threat prevention service in that it is meant to detect the threats that manage to bypass your other security systems and protective barriers. While this service cannot prevent any intrusion, its utility is in early detection, and investigation so that you, or other Synoptek services can take preventative action.



Customers will not have access to the SIEM product as a strict security policy, but can request an export of their event data.

6 APPENDIX A – SERVICE LEVEL OBJECTIVES

Threat indicators will be assessed, and incidents will be categorized into three levels of severity:

- Alerts Level 10 (Severe Threat)
- Alert Level 9 (High Threat)
- Alert Level 1-8 (“Interesting” Events)

The most urgent threats are categorized with the type “Severe Threat” (ST), and for those, Synoptek will gather and document the necessary context and activity logs required to act. Notification will be provided in writing to the customer’s designated alert contact.

<u>Severity Icon</u>	<u>Description</u>
	<p><u>Severe Threat</u> Any incident (ongoing or detected) that has been determined to have the potential for severe commercial, legal and/or operational impact.</p> <p>Severe Threats are those that should be raised to the executive level immediately as data and/or resource confidentiality, integrity and/or availability are at significant risk.</p>
	<p><u>High Threat</u> Any incident (ongoing or detected) that has been determined to have the potential for moderate commercial, legal and/or operational impact.</p> <p>High Threats are those that could indicate malicious use of corporate resources, are active infections or are otherwise placing the organization’s data and/or resource confidentiality, integrity and/or availability at moderate risk.</p>

The SOC-as-a-Service provides 24x7 response according to the following SLO matrix:

Type	Ticket Priority	First Response (Alert Acknowledgement) (SLO Target = 95%)	First Activity (Live Acknowledgement) (SLO Target = 95%)	Communication Updates	Explanation
Incident - Critical Event (Multiple Customer)	P0 – Critical	15 minutes	15 Minutes	Every 30 minutes	Severe Threat detected or ongoing across multiple customers. Service interruption or breach of critical infrastructure, processes, systems, networks, assets, technologies critical to customer operations.
Incident – Major Event (Single Customer)	P1 - Major	15 minutes	15 minutes	Every 30 minutes	Severe Threat detected or ongoing across one customer. Service interruption or breach of critical infrastructure, processes, systems, networks, assets, technologies critical to customer operations.
Incident - Single User (Critical Impact)	P2 – User Expedite	15 minutes	60 minutes	60 minutes	Severe Threat detected or ongoing for one user with critical functions impacted.

Incident – Single User (High Impact)	P2 – User Expedite	15 minutes	60 minutes	60 minutes	High Threat detected or ongoing for one user with critical functions at risk.
Low to Moderate SIEM Alert (Level 1-8)	P3 – Moderate to P4 - Functional	Every 24 hours	Every 24 hours	Every 24 hours	Low to Moderate Threats reviewed on a daily basis, are typically no cause for immediate action, but may be actioned on subject to SOC Analyst decision.

Synoptek will open a ticket for each incident in accordance with the above matrix. Service Ticket priority levels may change during the course of Synoptek’s investigation.

Definition of Possible Actions:

- First Response: Detection of an alert and automated alert notification by the SIEM to an incident management system (i.e., a ticket delivered to an ITSM system).
- First Activity: The first investigative actions by a Synoptek SOC Analyst leading up to a formal containment action by Synoptek. Note: Not all alerts require formal containment and therefore need not be communicated as no action is.

7 APPENDIX B – SUPPORTED DATA SOURCES

The SIEM collector supports a variety of data sources for aggregating security events. Examples include :



For a full list, contact Synoptek Security Services. Custom parsers may be required for unsupported data sources which requires billable time and material.

8 APPENDIX C – HIGH/SEVERE THREAT MATRIX

Severity	Incident Name
10	Backdoor Found :g:
10	Collector Signal Loss :g:
10	Compromised Host Detected :g:
10	Distributed DoS Attack detected by NIPS :g:
10	DoS Attack detected by NIPS :g:
10	DoS Attack on Network Devices :g:
10	DoS Attack on WLAN Infrastructure :g:
10	CiscoStealthWatch Worm Propagation
10	Excessive WLAN Exploits: Same Source :g:
10	FortiGate detects Botnet :g:
10	High Severity Internal Permitted IPS Exploit :c:
10	Large Supervisor JMS Request Queue :g:
10	Large Supervisor JMS System Queue :g:
10	Malicious HTML Applications Spawning Windows Shell :g:
10	Malware found by firewall but not remediated :g:
10	Mass Business File Deletion :g:
10	Outbound malware found by firewall but not remediated :g:
10	System Exploit Detected by Network IPS - Likely Success :g:
10	TCP DDOS Attack :g:
10	Cisco AMP Detected a Computer Executing Malware :g:
10	Cisco AMP High Volume of Detected Infections :g:
10	Cisco AMP Rootkit Detected :g:
10	Cisco AMP Threat Detected and Not Remediated :g:
10	Virus found but not remediated :g:
10	Virus outbreak :g:
10	VNC from Internet :g:
10	Windows Java running with remote debugging :g:
10	Windows NotPetya ransomware activity :g:
10	Windows Office Macro Spawning shell :g:
10	Windows Wannacry ransomware activity :g:

10	Windows Webservers spawning command shell :g:
10	Windows WScript or CScript Dropper :g:
10	Wireless Man-in-the-middle attack detected :g:
10	FireEye Malware Callback :g:
10	FortiSandbox detects multiple attacks from same source :g:
10	FortiSandbox detects multiple hosts with infected files :g:
10	Phishing attack found but not remediated :g:
10	Rootkit found :g:
10	SentinelOne Malware Found but not remediated :g:
9	Brute Force Login Success :g:
9	Cisco StealthWatch Bot Command Control Server
9	Cisco StealthWatch Bot Infected Host Successful Activity
9	Cisco StealthWatch High DDoS Source Index
9	Cisco StealthWatch High DDoS Target Index
9	Cisco StealthWatch High Target Index
9	Cisco StealthWatch SpamSource
9	Default Password Detected by System :g:
9	Default password usage :g:
9	Difference in Running and Startup Config :g:
9	DNS Traffic to FortiGuard Malware Domains :g:
9	DNS Traffic to Malware Domains :g:
9	DNS Traffic to Threat Stream Malware Domains :g:
9	Excessive Login Failures Followed by Successful Login :g:
9	High Severity Internal Permitted IPS Exploit :g:
9	Excessive WLAN Exploits :g:
9	Malware found but not remediated :g:
9	Executable file posting from external source :g:
9	Malware hash match :g:
9	Multiple Logon Failures: Same Src and Dest with Multiple Accounts :g:
9	Multiple Logon Failures: Same Src Multiple Hosts :g:
9	P2P traffic detected :g:
9	FortiSandbox detects Botnet :g:
9	FortiSandbox detects high/medium risk file malware :g:

9	FortiSandbox detects Malware URL :g:
9	FortiSandbox detects Network Attack :g:
9	Privilege Escalation Exploits :g:
9	Replay Exploit :g:
9	Successful Logon From Outside My Country :c:
9	Successful Office365 Logon From Outside My Country :g:
9	Successful VPN Logon From Outside My Country :g:
9	System Exploit Detected by Network IPS :g:
9	Cisco AMP Retrospective Cloud Quarantine failed :g:
9	Cisco AMP Vulnerable Application Detected :g:
9	Unapproved File Execution :g:
9	High Risk Rating Cisco IPS Exploit :g:
9	Virus found in mail :g:
9	High Severity Inbound Permitted IPS Exploit :g:
9	Weekend: User Added to Administrator Group :g:
9	High Severity Non-Cisco IPS Exploit - High Count :g:
9	High Severity Non-Cisco IPS Exploit :g:
9	High Severity Tipping Point IPS Exploit :g:
9	High Severity WatchGuard IPS Exploit :g:
9	Info Leak Exploits :g:
9	Injection Attack detected by NIPS :g:
9	Invalid TCP Flags - High Intensity :g:
9	Layer 2 Switch Port Security Violation :g:
9	Linux Buffer overflow :g:
9	Multiple Account Lockouts: Same Source Workstation / Multiple Users :g:
9	Multiple Accounts Disabled by Administrator :g:
9	Multiple Distinct IPS Events From Same Src :g:
9	Multiple Privileged Logon Failures: Server :g:
9	Multiple Windows Logon Failures: Same Src Workstation Multiple Accounts :g:
9	Outbound Traffic to Open Proxies :g:
9	Outbound Traffic to Tor Network :g:
9	Permitted Traffic from FortiGuard Malware IP List :g:
9	Permitted Traffic from Threat Stream Malware IP List :g:

9	Scanner found severe vulnerability :g:
9	Shellshock Expression in Log Files :g:
9	Spyware Found :g:
9	Suspicious Control Panel DLL Load :g:
9	Suspicious logon attempt detected :g:
9	Sustained DoS Attack detected by NIPS :g:
9	SWATFeed : DNS Traffic to Cybercrime Threat :g:
9	SWATFeed : DNS Traffic to Known Bad Address List :g:
9	SWATFeed : DNS Traffic to Ransomware Threat :g:
9	SWATFeed : Inbound Traffic from Cybercrime Threat :g:
9	SWATFeed : Inbound Traffic from Known Active Threat :g:
9	SWATFeed : Inbound Traffic from Known Bad Address List :g:
9	SWATFeed : Inbound Traffic from Ransomware Threat :g:
9	SWATFeed : Inbound Traffic from Tor Network :g:
9	SWATFeed : Large Outbound Transfer to Cybercrime Threat :g:
9	SWATFeed : Large Outbound Transfer to Known Active Threat :g:
9	SWATFeed : Large Outbound Transfer to Known Bad Address List :g:
9	SWATFeed : Large Outbound Transfer to Ransomware Threat :g:
9	SWATFeed : Outbound Traffic Attempted to Cybercrime Threat :g:
9	SWATFeed : Outbound Traffic Attempted to Known Active Threat :g:
9	SWATFeed : Outbound Traffic Attempted to Known Bad Address List :g:
9	SWATFeed : Outbound Traffic Attempted to Ransomware Threat :g:
9	SWATFeed : Outbound Traffic to Tor Network :g:
9	SWATFeed DNS Traffic to Known Active Threat :g:
9	Cisco AMP Device Flow Correlation Threat :g:
9	Cisco AMP Indicator of Compromise Detected :g:
9	Traffic to Threat Stream Malware IP List :g:
9	Transient Account Usage :g:
9	User SID History Addition or Addition Attempt :g:
9	Web Traffic to FortiGuard Malicious URLs :g:
9	Web Traffic to FortiSandbox Malicious URLs :g:
9	Web Traffic to Threat Stream Malicious URLs :g:
9	Website defacement attack :g:

9	Windows Audit Log Cleared :g:
9	Windows Backup Catalog Deleted :g:
9	Windows Certutil Decode in AppData :g:
9	Windows Code Execution in Non-Executable Folder :g:
9	Windows Command With Suspicious URL and AppData String :g:
9	Windows DHCP Callout DLL installation :g:
9	Windows DNS ServerLevelPluginDll Install :g:
9	Windows DSRM Password Change :g:
9	Windows LSASS Process Access :g:
9	Windows Malicious Service Installed :g:
9	Windows Network Connection from Suspicious Program Locations :g:
9	Windows Password Dumper Activity :g:
9	Windows PowerShell Download from URL :g:
9	Windows PowerShell using Suspicious Parameters :g:
9	Windows Remote Thread in LSASS :g:
9	Windows Suspicious Logon Failures :g:
9	Windows Suspicious Password Hash Retrieval :g:
9	Windows User Account Control Bypass via sdclt :g:
9	Windows Web shell Reconnaissance :g: