Security Operations Centre (SOC)

Service Definition Document

December 2025

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
14/05/2022	Rebecca Gilmour	0.1	Initial Draft
18/05/2022	Rebecca Gilmour	1.0	Final Release
01/05/2024	Jonny Zammer	1.01	Updates for G-Cloud 14
05/05/2025	Jonny Zammer	1.02	Updates for G-Cloud 15
29/10/2025	Rory leanord	1.03	QA
22/12/2025	Jonny Zammer	2.0	Release

Table of Contents

Contents

1. Service Overview

Maple Networks 24x7x365 SOC Service is built on a next generation remote logging security service offered to improve Customers' security awareness of their infrastructure and application environments.

The Maple Networks SOC Service is designed to meet the customer's requirement to store, analyse and triage data from infrastructure, operating system, application logs, end point devices and cloud platforms.

This Service provides the customers with the remote collection and analysis of logs, using an industry-leading cloud native Security Information and Event Management solution (SIEM) alongside proactive threat hunting and remediation. This provides customers with a service that delivers improved mean time to detection and remediation.

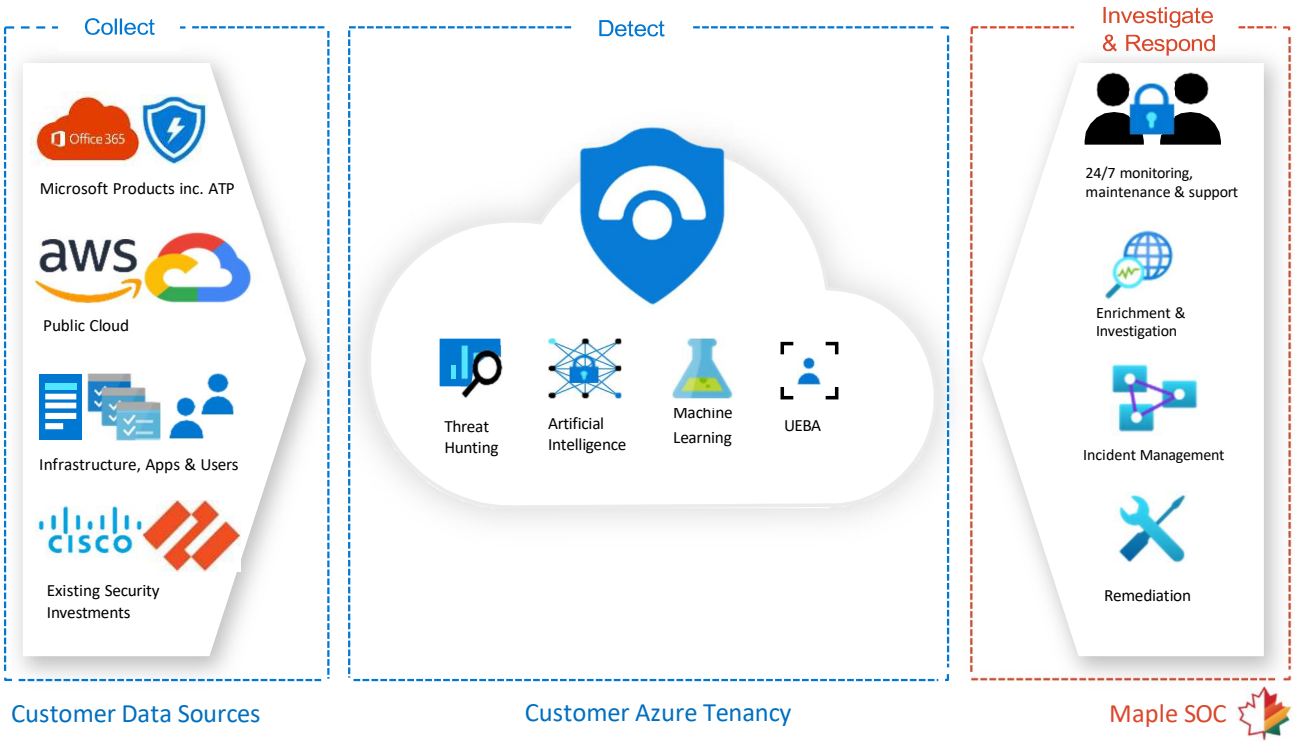
The service simplifies the correlation, consolidation and comprehension of events recorded in transient, disparate and widely dispersed system logs to deliver:

- Visibility of what events are taking place across the IT infrastructure
- Alerts for unexpected events
- Extended and flexible storage of usually transient log data
- Prioritisation of logs by risk scoring
- Real-time information surrounding log data and events
- Historical reporting and performance log analysis produced by the Security Operations team
- Proactive Threat Hunting that is industry specific and relevant to the customer

Maple Networks 24x7x365 SOC Service provides security guidance and advice to the customer's IT team and/or other nominated representatives. Maple's Security Operations Centre (SOC) becomes a cost-effective virtual member of the customer's security and IT operations team, reducing the workload of the customer's IT team, by notifying of high-risk events and remediation advise.

The environment in scope is analysed for suspect activity and abnormal events. Maple Networks then advises the customer on appropriate steps to be taken to prevent suspect activities from both escalating and occurring or being a threat in the future.

2. Service Overview Diagram



3. Service Scope

This chapter identifies and describes the high-level components that make-up the service, which comprise the:

- Service package – which defines the service, capabilities and options
- Service platform infrastructure - which defines the service delivery mechanism
- Supporting services - any processes or resources that support the delivery of the service

Service Package

Objective	To provide the remote collection and analysis of logs using Security Information and Event Management (SIEM) alongside proactive threat hunting, culminating in relevant remediation guidance and assistance.
Description	The service simplifies the correlation, consolidation and comprehension of events recorded in transient, disparate and widely dispersed system logs to deliver: • Visibility of what is events are taking place across the IT infrastructure • Alerts for unexpected events • Extended and flexible storage of usually transient log data • Prioritisation of logs by risk scoring • Real-time information surrounding log data and events • Historical reporting and performance log analysis produced by the Security Operations team • Proactive Threat Hunting that is industry specific and relevant to the customer Maple Networks 24x7x365 Cyber Security Service provides security guidance and advice to the customer's IT team and/or other nominated representatives. Maple's Security Operations Centre (SOC) becomes a cost-effective virtual member of the customer's security and IT operations team, reducing the workload of the customer's IT team, by notifying of high-risk events and remediation advice.
Hosted-in	Customers owned Azure tenancy, in the Azure region of their choice.
Supported Log Sources	Logs can be collected from any device that supports one of the following protocols: • Syslog • SNMP Trap • Microsoft Windows Event Log formats • Restful API integration • Flat file collection The service also includes built-in log parsers for a wide range of industry-leading infrastructure component vendors, operating systems and applications, providing out-of-the-box best-practice log classification and correlation functionality.

	A list of available supported vendor log sources is available on request.
Supported from	All support and management are delivered remotely from the Maple Networks 24x7x365 SOC
Support level	The Maple Networks service includes the following support levels on the platform: • System Onboarding • Proactive monitoring • Proactive threat hunting • Remediation support The level of support per customer will be customised and specific to each individual customer.
Required connection types	The Maple Networks service requires internet connectivity. All connections are encrypted over the public internet.

Service Capabilities

Log monitoring	• The Maple platform monitors Customer log sources 24x7x365
Log data consolidation	• Maple handle the consolidation and storage of all logs sent by the customer assets and services in the scope of the service • Logs are viewable through the customers Azure tenancy • Logs are retained for the Customers' specified retention period
Log data classification	• All log messages are automatically classified into categories to identify the associated impact based on threat models and policies built into the platform
Entity and Log risk scoring	• As log messages are processed into the platform they are automatically associated with an 'entity'. This can be a user, device or application. The entity is continuously assigned a risk score based on the type of log messages
Log source alerts	• Maple will raise an alert if a log source fails and will contact the customer in order to work collaboratively to undertake investigation.
User Risk Profiling	• Maple shall notify the customer of suspicious user activity based on a risk scoring mechanism. Risk scoring is based on deviations from previous learned user activity in comparison to peer group activity and activity related to known insider threat vectors.
Raise security risk alerts	• Security risk alerts, identified by the Maple security team, are sent to a nominated customer contact using the chosen communications mechanism defined in the customer's Service Operations Manual.
	Maple security specialists are available to provide advice to the customer under the following circumstances. • The Investigation of security incidents: ○ The Maple security team analyse and filter the events as they are logged into the platform through correlation rules and

	threat hunting activities, to highlight suspicious or anomalous activity leading to the raising of a security incident investigation
	
	• The remediation and containment of security incidents:
	  ○ The Maple security team will provide recommendations to contain and remediate security incidents, in line with best practices provided by the associated technology vendor, relating to the application of patches, configuration changes, or other updates, required to remediate the issue and reduce any further exposure.
	  ○ The Customer is responsible for implementing recommendations provided by Maple.
	▪ Recommendations to help give the Customer an increased view-of and control-over security incidents.
	For example: Expanding the scope of the service to include additional log sources, or review and tune log sources for greater security awareness.

Supporting services

Maple Networks Service Desk	• Provides 24x7x365 support and management of the service and supporting infrastructure • Handles events, requests, queries and incidents raised by authorised users only, whether by phone, e-mail or self-service support portal • Handles Change Requests (CR) in accordance with Maple Networks' Change Management process. • Resolves problems with, applies changes to and maintains the patch state of the service platform in accordance with Maple Networks' change management process • Makes configuration changes on request (for example, changes to log feeds).
Maple Networks Self Service support portal	Maple Networks will provide customer-nominated administrators with access to a Self-service support portal through which they can: • Request additional log sources to be configured • Create new and update existing incidents for investigation • Create new and update existing changes from a change catalogue • See additional services that can be onboarded

Available Service Levels

This chapter identifies the service level measures applicable to the service.

Customers should consider these measures in the context of the general terms and conditions described in full in the Maple Networks Service Level Agreement document (available on request).

Response time	• Incidents
	  ○ P1
	  ○ P2
	  ○ P3
	  ○ P4
	• Changes
	  ○ Standard
	  ○ Normal
	  ○ Emergency
	• Service Request

Availability	*https://azure.microsoft.com/en-us/support/legal/sla/azure-sentinel/v1_0/

*The cloud native SIEM platform is hosted on Microsoft Azure therefore availability SLA's are in line with the platform SLA's provided by Microsoft.