Managed Threat Detection Service – Services Sensor

Norm's Managed Threat Detection Service - Services Sensor is a module from Norm's Cyber Security as a Service (CSaaS) offering.

The Managed Threat Detection Service - Services Sensor provides cloud-based monitoring of your corporate services traffic and activity such as O365, DNS, Active Directory, Remote VPN, Application Logs, etc which is then scrutinised and analysed 24/7/365 by our Security Operations Centre (SOC).

This service module focuses on the Technology element of Norm's holistic trinity of cybersecurity - People, Process and Technology. Its purpose is simple:

- Continuous real-time security monitoring of your corporate services activity
- Automatically alerts during an identified threat event
- Delivers total visibility of all threats and alarms that occur within your IT applications/services and/or public cloud environments

The Services Sensor takes security telemetry feeds from your corporate services and is ingested into Norm's Threat Detection service. Services Sensors include all corporate business applications and operational infrastructure, including public cloud environments that can provide a telemetry/log feed.

The Services Sensor constantly monitors your corporate services activity, looking for suspicious or threatening behaviour enabling an immediate response from our SOC Team. The information collected from the monitoring process is recorded, analysed and investigated to enable response.

Service Features

You will gain access to the following features:

- Services Sensor is a telemetry feed from your corporate business applications and operational infrastructure within your corporate/cloud environment that continuously sends activity information to Norm's Threat Detection service. The service collates all telemetry feeds with our global threat intelligence looking for known threats, Indicators of Compromise (IoC) and suspicious / threatening behaviour.
- Services Sensors include all corporate business applications, public/private cloud environments and operational infrastructure that can provide a telemetry feed including Office 365, DNS, Active Directory, Remote VPN / SSL, Web Gateways, Corporate Applications or Services, etc
- It provides in-depth visibility and detection across all the organisation's corporate service(s), monitored for threat detection.
    - Detect threats across the organisation's services and infrastructure
    - Automated threat detection and correlation process
    - Significantly reduced time to detection
    - Enabling rapid incident response times

On-Boarding Process

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process, outlining who will be responsible for each element of the installation, and introduce you to your Norm technical lead. The onboarding process will include:

- Providing you with our service handbook detailing our service operational processes, SLA and contacts
- Work with your IT / Network team(s) or provider(s) to integrate and digest your Service Sensor telemetry feed(s) into Norm’s Threat Detection Service and SOC
- Providing access to Norm’s Visualiser platform

Once the service is fully deployed our customer experience team will provide you with access to the Norm visualiser. This visualiser will provide you with an overview of all the threats detected within your services environment, as well as a log of all incidents and remediation.

The SOC will be available to provide technical advice and assistance on cyber-security queries or issues should this be required.

Technical Requirements

The Service Sensor(s) are any corporate application/service/operational infrastructure that can send telemetry/activity information externally to Norm’s Threat Detection services.

Telemetry feeds from your Corporate Services can be sent to Norm in the following methods/formats:

- Syslogs
- APIs

The Services Sensor will passively monitor your corporate service activity and traffic and will seamlessly work with any pre-existing firewall, VPN or internet gateway solution you might have, providing a security in-depth approach.

Service's Prerequisites

The customer must subscribe to Norm's Threat Detection Service to access the Services Sensor module.

Service Availability

The service is managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Customer Experience team is available during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

The Customer Experience and SOC teams will be available to provide technical advice and assistance on any queries or issues in regard to the integration of your Service Sensor feeds should this be required.

Customer Responsibilities

- The Customer will be responsible for configuring the telemetry/log feed from their corporate applications and infrastructure to Norm's Threat Detection service.
- The Customer shall nominate an administrator internally for the Norm Visualiser.
- The Customer shall be responsible for user administration within the Norm Visualiser.