No drama, no compromise*

norm.

*Reassuringly dull cyber security

Managed Threat Detection Service

Norm’s Managed Threat Detection Service is a module from Norm’s Cyber Security as a Service (CSaaS) offering. Norm’s Managed Service underpins three key security modules:

- Endpoint Sensor
- Network Sensor
- Services Sensor

The Managed Threat Detection service provides cloud-based monitoring of your corporate applications/services, network traffic and endpoint devices which is scrutinised & 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 environment; Network, Services and Endpoints**
- **Automatically alerts and reacts to an threat event using your Telemetry, Threat Intelligence, Use cases and Play Books**
- **See the Results with monthly management reports and real-time reporting**

The Managed Threat Detection service constantly monitors your corporate information technology infrastructure and activity allowing for immediate response from our SOC Team. The service includes monthly easy to digest reporting as well as access to real time reporting.

Service Features

You will gain access to Norm’s managed service offering the following features:

- Access to Norm’s Managed SOC, SIEM and Security Analysts who will continuously monitor your corporate environment for Known and Unknown threats, suspicious and malicious behaviour.
- Real-time response to threats. Many threats can bypass traditional and advanced security in the time it takes for a human to respond to the activity.
  - Detect threats across the organisation
  - Automated threat detection and correlation process
  - Significantly reduced time to detection
  - Enabling rapid incident response times
- In-depth and broad visibility and detection across all your organisation's corporate environment through gaining key telemetry feeds:
  - Network Sensors includes a network appliance or appliances hosted within your corporate environment that continuously monitors your corporate network traffic for known threats and Indicators of Compromise (IoC).
  - Services Sensors include all corporate business applications and operational infrastructure that can provide a telemetry feed including Office 365, DNS, Active Directory, Remote VPN / SSL, Web Gateways, Corporate Applications etc. The service collates all telemetry feeds with threat intelligence looking for known threats, Indicators of Compromise (IoC) and suspicious / threatening behaviour.

  - Endpoint Sensor is based upon EDR software that is hosted on Endpoint devices such as Laptops, Desktops and Servers which monitors and detects suspicious or threatening activity. Unlike many other security monitoring tools such as AV, SPAM and UTM, EDR looks for unknown threats and malicious behaviour that doesn't have a defined signature (also known as Day Zero attacks) offering additional protection for your devices, data and users.

- The service includes 600 pre-defined Event Use Cases to help identify possible threat events from your corporate telemetry feeds combined with our Global Threat Intelligence. The service also includes the ability to create custom Event Use Cases to tailor against any unique situation in your corporate environment.

- For the Endpoint Sensor, Norm's SOC can provide intervention/automatic responses upon an identified threat event. These actions/responses are defined in Playbooks which are created and agreed with you before going live.

- Norm's monthly reports summarise all the events, alarms and incidents that have occurred within your environment over the past month, including any remediation recommendations/and or steps taken.

- 12 months of log data retention.

- Norm's online visualiser provides access to the monthly reports, but also the technical details of all the alarms and incidents in real-time.

How the Managed Threat Detection service works

Norm's Managed Threat Detection service using various Sensors, Threat Intel feeds and tools to continuously monitor activity on Endpoints, Corporate Network(s) and Service(s), to identify suspicious or threatening behaviour in real-time. The service is managed from Norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year.

Information is recorded and analysed for internal or external attacks. The end-to-end analysis is supported by a range of innovative technologies, including machine learning and behavioural analysis. In the case of Endpoint Sensor (EDR), it can isolate and deflect attacks from internal and external sources, protecting endpoint devices from risks immediately and prevents the attack from propagating throughout the rest of your environment.

Once a threat has been positively identified, Norm's SOC will create an incident ticket and will alert your IT/Security team within 60 minutes. As part of the incident ticket, Norm's SOC will provide your IT/Security team with details pertaining to the identified threat and our recommendations for your team's response/remediation activities including:

- Affected Device(s)
- Time / Date of incident
- Nature of Threat
- Threat criticality
- Our recommendations on how to manage and remediate the incident

Once a threat is identified there are two primary paths the incident can follow: -

Automated Isolation (Endpoint Sensor Only)

If a threat from your playbook is identified, the Endpoint agent on the device will respond accordingly as soon as the threat is identified; this may include isolating that device. When a device is isolated a custom message is displayed requesting that the user does not power off the device and contacts your IT team or outsourced ICT provider.

After isolating any threat, a member of our SOC will co-ordinate with your organisation’s IT Team or outsourced provider to mitigate any effects caused by an incident.

Manual Incident Handling

If the threat identified is not in your playbook, a member of our SOC will contact your nominated representative(s) within 60 minutes to discuss the incident details, our recommended next steps and ask for a decision.

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 our service handbook detailing our service operational processes, SLA and contacts
- Providing you with your Sensors and integration through co-ordinated installation with your IT/Network team(s)
- Defining your Corporate Event Use Cases[1] and response Play Books
- Enrolling your Sensor(s) into Norm’s 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 on your network, as well as a log of all incidents and remediation. A list of all endpoints will also be available to give you full visibility of your protected environment.

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

[1] Customer specific use cases are available upon request

Technical Requirements

The service requires a local telemetry collector/aggregator which collects all customer logs/telemetry feeds and securely sends to Norm's managed SOC Sensor. The collector is based upon Fortinet's FortiSIEM Collector and will require to be hosted within the customer's corporate environment. The FortiSIEM Collector has the following technical requirements:

	FortiSIEM Collector
Hypervisor	ESXi, Hyper-V, AWS, Azure
Host Resources	2vCPU, 8GB RAM, 100GB HDD
Access Requirements	N/A
Outbound Access	Port 443
Image Size	5GB
OS	CentOS 6.10

The FortiCollector Image is provided by norm. The Collector can be deployed onsite in a virtualised stack or in an enterprise cloud environment providing all log sources can reach the Collector as a syslog destination. The Collector also requires outbound access on port 443 to establish an encrypted connection with the SIEM platform.

The Collector receives log messages from various sources, in particular the FortiGate IDS, parses the log into a format readable by the Norm SIEM platform and then forwards the traffic up to the SIEM in the cloud where the SIEM runs aggregation, correlation and analytical engines to detect threats.

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 operate during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

Software updates and patching for the FortiCollector will be automatically managed by the Norm platform. Software support will be available 24x7 and provided through Norm's SOC.

The Customer Experience and SOC teams will be on hand to provide technical advice and assistance for any queries or issues should this be required.

Customer Responsibilities

- Customer will be responsible for hosting the FortiSIEM Collector within their corporate environment including suitable server or virtualised platform.
- The customer shall provide a network connection to the FortiSIEM Collector and allow onward access to Norm's SOC.
- The Customer shall nominate an administrator internally for the Norm Visualiser.
- The Customer shall be responsible for user administration within the Norm Visualiser.