Threat Detection and Response Service

What is it?

The **norm.** Managed Threat Detection and Response service constantly monitors your network, services and devices in order to identify suspicious activity and threats. When potentially malicious activity is detected, the **norm.** 24/7/365 SOC team isolate the device or service concerned. Traffic and activity are analysed and correlated with multiple threat intelligence feeds and against threat use cases to identify cyber-attacks and malicious behaviour.

The service's purpose is simple:

- To provide near real-time security monitoring of your corporate environment, including networks, services and endpoints.
- To immediately identify and isolate threats using telemetry, threat intelligence feeds, use cases and play books.
- To minimise the impact of a cyber security breach by providing actionable incident notification and recommendations.
- To give near real-time visibility of the service via our online Visualiser portal.

Why now?

With so many users now working remotely, the attack surface has grown, meaning greater risk of exposure to unknown cyber threats.

One of the biggest threats to businesses today is Advanced Persistent Threats. These sophisticated attacks are specifically designed to bypass traditional security measures and remain undetected for as long as possible. The perpetrators of such attacks – cyber criminals, hackers and more recently state actors – commonly use this type of attack for financial, commercial and political gain.

The longer they remain undetected, the greater the opportunity the perpetrator has to steal sensitive and personal data, and the longer it takes to recover from the breach.

Currently, the average time a breach remains undetected is 197 days. The impact of such an attack goes beyond a direct commercial blow, as brand value, reputation and share price will suffer. This is in addition to the immediate operational and financial penalties.

What's included?

- Access to the **norm.** Managed SOC, SIEM and security analysts to continuously monitor corporate environments for known and unknown threats, suspicious and malicious behaviour
- Near real-time alerts and response to threats from the SOC team
- In-depth, broad visibility and detection across the entire corporate environment, wherever it may be deployed, via key telemetry feeds:
  - Network Sensor
  - Services Sensor
  - Endpoint Sensor (EDR)

The service includes 600 pre-defined event use cases to help identify possible threat events through a combination of your corporate telemetry feeds and our constantly updated global threat intelligence. Monthly reports are provided through the **norm.** Visualiser portal, which also provides near real-time reporting.

Want more detail?

For the full Service Description of our Threat Detection and Response Service <<ClickHere>>.
To register your interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

***Reassuringly dull cyber security**

norm.

In a nutshell…

The **norm.** Managed Threat Detection and Response service offers a comprehensive, proactive defence against sophisticated cyber-attacks – both known and unknown. It acts to continuously monitor activity across multiple elements of your technology environment, and constantly updates according to the latest threat intelligence data. Near real-time visibility via the **norm.** Visualiser portal means that organisations have clear visibility into their cyber security status.

How does it work?

The **norm.** Managed Threat Detection service uses various sensors, threat intelligence feeds and tools to continuously monitor activity on corporate networks, services and endpoints. It is able to identify suspicious and malicious behaviour in real-time.

Information is recorded and analysed for both internal and external attacks. The end-to-end analysis is supported by a range of innovative technologies, including machine learning, behavioural analysis and multiple threat intelligence sources. In the case of the endpoint sensor (EDR), it can also isolate and deflect attacks from internal and external sources.

Once a threat has been positively identified, an incident ticket is created, and an alert is sent to the nominated contact within 15 minutes. As part of the incident ticket, our analysts will give details of the threat and recommended remediation measures.

How do the key telemetry feeds work?

- **Network Sensor** - monitors internal corporate network traffic for known threats and Indicators of Compromise (IoC).
- **Services Sensor** - monitors the activity from business applications and operational infrastructure including Office 365, DNS, Active Directory, Remote VPN / SSL, web gateways and corporate applications.
- **Endpoint Sensor** – monitors the activity across endpoints such as laptops, desktops and servers. Unlike many other security monitoring tools such as anti-virus and unified threat management, EDR looks for unknown threats and malicious behaviour that doesn't have a defined signature (such as Zero Day attacks) offering additional protection for your devices, data and users. In agreement with the client, the Endpoint Sensor can also take automated intervention measures when it encounters an identified threat event.

FAQs…

I already have the EDR service from you, is this an upgrade?

Yes, this adds additional layers of security on top of the Endpoint Detection and Response service. By adding network and service sensors alongside EDR you benefit from more comprehensive cyber security protection.

Is this something I can do myself?

Yes, with the required skills and experience. Deploying and integrating endpoint, network and service sensors takes a high level of cyber security competency. It also needs to be managed and monitored on an ongoing basis. Our service combines these sensors and is maintained by our 24/7/365 Security Operations Centre, staffed by a team of highly skilled cyber security engineers.

What's involved in getting this up and running and how quickly can the service be set up?

Once we've deployed the network, service and EDR sensors, the service can be up and running in a matter of days, ensuring your users and your business are protected as quickly and comprehensively as possible.

Do I need cyber security trained staff to benefit from this service?

No, we know how hard it is to recruit and retain good cyber security staff, that's why we have our highly trained team. They do all of the complex technical work on your behalf. Visibility into service activity and performance is accessed via the clear and simple portal, giving you all of the information you need in a format everyone can understand.

I already have a firewall, VPN, anti-virus and email filtering – do I need this service?

Traditional IT security products rely on signatures and rules that have been created to identify known threats and vulnerabilities. The **norm.** Managed Threat Detection Service complements your existing security solutions by looking for unknown threats and correlating events which in isolation may seem innocuous, but in conjunction are suspicious.

How does this service support my core business operations?

Businesses are adapting to a new normal – working and technology practices have changed and will continue to do so. A highly dispersed workforce means an expanded attack surface, and regardless of where your employees are located, unprotected endpoints or devices are vulnerable to a cyber security breach. A breach can effectively cripple your business - both financially and in terms of brand reputation.

norm.

Copyright © NormCyber Limited. All Rights Reserved.