NETWORK DETECTION AND RESPONSE
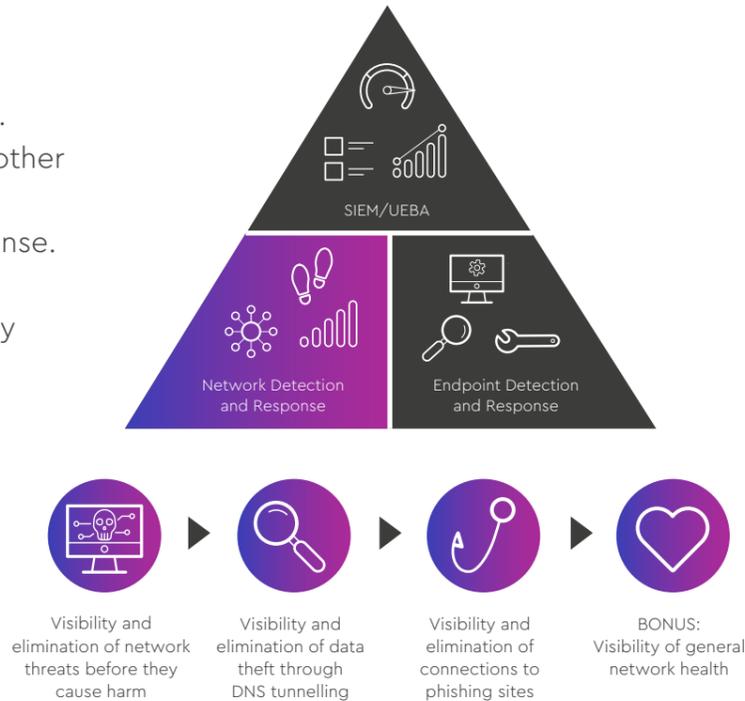
NOMINET CYBER SECURITY

The Gartner SOC visibility triad states your security solution should have three key areas. SIEM, SOAR or UEBA sits at the top, and the other two sections are Endpoint Detection and Response and Network Detection and Response.

Network Detection and Response is a security solution category used by organizations to detect and prevent malicious network activity, investigate and perform forensics to determine the root cause and then respond and mitigate.

SIEM/UEBA

Network Detection and Response

Endpoint Detection and Response

Visibility and elimination of network threats before they cause harm

Visibility and elimination of data theft through DNS tunnelling

Visibility and elimination of connections to phishing sites

BONUS: Visibility of general network health

Nominet's network detection and response solution, NTX, cuts through the sea of data your teams are working with and gives you immediate visibility of threats and anomalies to preserve the integrity of your network.

Using patented machine learning techniques, NTX analyzes vast volumes of DNS traffic to predict threats, identify infected devices and pinpoint malicious behavior, alerting your security teams so that action can be taken before these threats become a problem.

This foundational layer of security provides proven supply chain security assurance, while a scored and managed proprietary threat feed with event prioritization drives SOC team efficiency.

Predict, detect & block infections

Identify DNS hijacking

Prevent data theft

Improve network efficiencies

Threat hunting

Easy deployment

In-depth forensics

The statistics behind the performance of NTX make for a compelling reason to speak with us today:

Intercepts malicious domains at zero hours

Identifies previously unknown malicious websites, on average, seven days faster than other intelligence solutions

Only 0.05% false positives

NOMINET PROTECTS GOVERNMENTS AND ENTERPRISES GLOBALLY

With more than two decades of experience in network analytics and protection, our technology was built to help us understand and protect activity on the UK internet, so we know it works.

Nominet is chosen by the National Cyber Security Centre to be part of their Active Cyber Defence program in the UK, providing a Protective DNS service to the UK public sector.

We also help enterprises by enabling their DNS to detect and block cyber threats, strengthening their security capabilities.

Chosen by UK Government to run a Protective DNS Service across UK public sector organizations.

In a period of a year the service was able to:

Analyze more than

68 BILLION queries

Proactively block in excess of

57 MILLION suspicious events

Here are just some of the institutions we protect:

HM Government

Haas F1 Team

RS

GWR

FIND OUT MORE   Contact us for more information on how Nominet can help secure your business.

info@nominetcyber.com | nominetcyber.com

1.01