BAE SYSTEMS
INSPIRED WORK

Managed Detection and Response

Threat hunting, detection and response across endpoints, networks and cloud

The Problem

Organisations today face a compound and overwhelming set of pressures when trying to keep up with evolving cyber threats:

- Covering the growing volume, variety and sophistication of both external and internal threats
- Managing the proliferation of smart devices, cloud infrastructure and applications with business operations often not touching the traditional network
- Optimising existing investments in security hardware, software and services
- Reducing the time and effort it takes to triage and investigate the expanding number of alerts
- Coping with the security skills shortage and high turnover rates that imped hiring, retention, group productivity and effectiveness

Therefore, more and more organisations are looking to outsource elements of cyber security. However, traditional security outsourcers only focus on protecting against predictable threats and reacting to today's issues. Without the flexibility to support your development and a partnership model that emphasizes seamless integration with your internal security operations you and your managed security provider will always be playing catch up.

The Solution

Managed Detection and Response (MDR) from BAE Systems focuses on the importance of both the detection of, and complete response to, sophisticated attacks masquerading as legitimate activity to breach security.

Powered by BAE Systems Threat Analytics, MDR acquires as broad a set of data as possible using our expertise in Big Data. It then creates an organisation baseline and uses advanced behavioural detection analytics to detect anomalies. When combined with context from sources such as HR, financial data, Technique, Tactics and Procedures (TTP) Intelligence and risk, these analytics can be used to detect a broad set of known, modified or brand new attack techniques across all stages of the kill chain.

Our unique ability to acquire, fuse and correlate data and to run detection analytics across diverse infrastructures allows BAE Systems SOC Analysts and responders comprehensive visibility and rapid access to data to fully investigate potential threats. Aside from reducing the impact of attacks, this approach gives a wealth of data that facilitates the rapid and thorough investigation of even the most complex cyber threats.

Key coverage areas:

- Critical cloud service providers, including AWS, Azure, O365 and EPS
- Coverage of cloud infrastructure as if it was on-premise
- Comprehensive authentication and access monitoring for rogue account detection
- Anonymous access link distribution detection
- Endpoint activity, including OS and hardware details and file, memory and registry usage
- Malware-less attacks that use scripting languages including PowerShell and memory
- Data acquisition from HTTP, SMTP, packet, netflow and DNS
- Non-security data enrichment from HR, financial systems and physical security

Integrated Threat Hunting

Proactive threat hunting is a key element of the managed detection and response service. BAE Systems threat hunters act in two specific ways to combat new and innovative or novel threats.

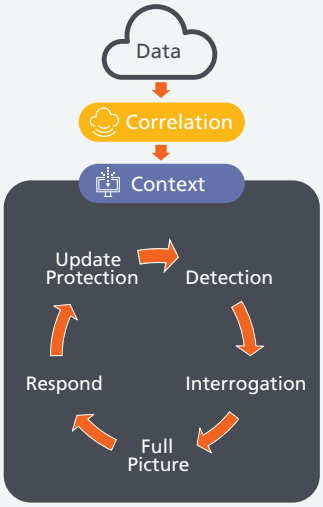
1. A team of highly trained subject matter experts search for and investigate behavioural anomalies and deviations from a customer's standard digital behaviour or baseline, which could be indicators of previously unknown attack

2. Using BAE Systems privileged access to intelligence, hunters create and test hypotheses of possible attacks. They have the ability to fuse and interrogate large disparate data sets, calling on behavioural analytics, machine learning, raw data search and visualisation tools, to uncover new patterns of malicious behaviour and adversary TTPs. Detection through hunting quickly flows into creation of new actionable threat intelligence leading to the development and enrichment of automated analytics, rules and signatures which improve existing detection and protection mechanisms

Delivering on approach

- Acquire as broad a set of data as possible
- Correlate into understandable and consumable events
- Add context and intelligence (Threat, Vulnerability, Risk)
- Detect behaviours that correlate to objectives of attack
- Interrogate data, hunt for connected anomalies
- Build out the full picture of the campaign of activity
- Respond and remediate completely
- Update and tune protection equipment

Focused Detection and Response

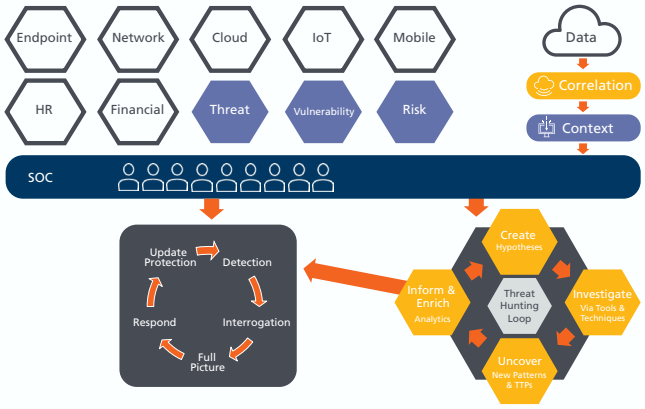


Detection and response is an area of increased investment for organisations and an area of development for security equipment vendors. This, although a step in the right direction, can lead to multiple analytic platforms and siloed response.

Each silo of detection and response requires specialist staff and specialised incident responders. Whilst the increased volume and variety of data provides more information to analyse, the inability to analyse across these data sources results in further confusion which in turn undermines the efforts to improve performance and ultimately leads to a decline in business defence.

BAE Systems has an organisation wide approach to detection and response. Agnostic to the data sources and able to deliver coordination of the output they provide, Managed Detection and Response delivers maximum context and correlation across diverse data sets and delivers detection earlier in the kill chain.
This allows more timely and accurate analyst investigation, driving down false positives and ultimately the time-to-response, minimizing the cost to your organisation and the demands placed on your internal security resources.

Organisation wide Detection and Response



BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

UK: +44 (0) 1483 816000

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai