Advanced Threat Hunting and Detection

QinetiQ Digital Resilience

As the threat landscape continues to evolve at a staggering pace, organisations are taking more steps to protect their data and information assets. It's estimated that 50% of network traffic is now encrypted, and threat actors are using increasingly evasive and sophisticated methods to compromise systems leading to an increased gap between attacker actions and security visibility.

QinetiQ's Advanced Threat Hunting and Detection service is an extension of its Cyber Security Monitoring service and really allows QinetiQ to provide a much deeper insight into the threats and attacks occurring within an organisation. More importantly, it allows QinetiQ to apply its knowledge of threat actors and their Tools, Tactics and Procedures (TTPs) to proactively hunt for threats across an organisation.

Taking this proactive, enhanced approach to threat detection reduces attacker dwell time, accelerates incident detection and response and greatly reduces the impact of security incidents when they occur. In addition it also provides organisations with increased confidence in their digital resilience in the knowledge that proactive threat hunts are ongoing across their digital systems, and they are not solely reliant on comparatively passive alarm triggers to identify security problems.

The service follows four key principles to personalise the service and deliver exceptional security value. They are:

Analyst Driven

With the ever increasing sophistication of cyber attackers and attack methodologies, traditional correlation based monitoring capabilities struggle to identify security issues.

QinetiQ's Threat Hunting service builds on our Cyber Security Monitoring and Device Management capability, to provide a proactive, human led capability that constantly looks for developing threats, across an organisation's digital systems. Drawing on available intelligence about threats actors, their methodologies and the tools that they use, the service can target hunting activity to root out and identify more sophisticated attacks.

Enriched Security Information

QinetiQ has a long and demonstrable history of operating Security Operation Centres (SOC) across government and industry, and with that experience, have observed how attacks are now more complex and sophisticated than ever before. To address this, QinetiQ has introduced capabilities that enhance our visibility, improve our detection capability and accelerate our response.

Using market leading technologies, QinetiQ's capabilities reach much further than ever before. Enhanced endpoint visibility now allows for QinetiQ to observe malicious behaviour on the endpoint as it occurs in real time, assess the risk and take decision actions to contain the threat and reduce the risk fast.

The service provides clear visibility of what is happening across an organisation's digital systems by making use of both statistical information and raw network packets.

Data Sciences

With the increased amount of security information from security logs, endpoint process data and network traffic the service is able to apply statistical based analysis to look for patterns and trends over time.

The service is also able to make use of automation through machine learning capabilities to continually assess the large data sets.

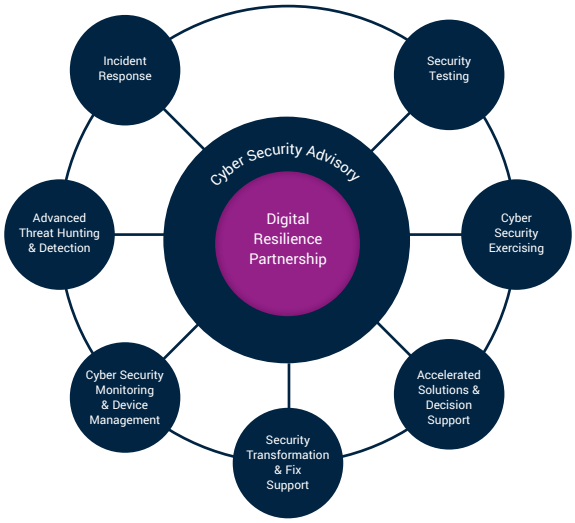
This gives QinetiQ a much greater insight into the activity taking place across an organisation's digital systems, and to identify developing security issues that may previously have gone unnoticed.

QINETIQ

Digital Resilience

This service forms part of a wider service portfolio, which seeks to help organisations mature their digital resilience and to help build confidence in their ability to deal with cyber-attacks, through a holistic approach. The main integration points for this particular service are:

- **Incident Response** - Ability to trigger managed incident response process as a result of incident triage
- **Cyber Security Advisory** - Real time threat information about developing cyber-attacks helps to tailor security advice to organisations



Key Features & Benefits

Fully Managed Service Delivering 12x7x365 Threat Hunting support. QinetiQ's service represents a cost-effective method for an organisation to benefit from these advanced capabilities without having to invest in its own bespoke capabilities.

Intelligence-led QinetiQ's extensive exposure to a variety of targeted industries provides us with an excellent insight across the cyber threat landscape. Leveraging this breadth and depth of knowledge enables QinetiQ to employ defensive capabilities throughout the cyber kill-chain, detecting the compromise before attackers have achieved their objectives. This provides customers with a wider range of protection capability at lower overall cost.

Incident Identification - Gives organisations greater confidence that sophisticated cyber-attacks can be identified, triaged and alerts raised.

Reduction of Dwell Time - As attack methodologies become more sophisticated, new methods of bypassing traditional defence approaches are used, often going unnoticed for prolonged periods. This service helps to identify these early and thus reduce an attacker's time to exploit them on digital systems.

Analyst-driven Seasoned Cyber Security Analysts are supported by a next-generation Security Information and Event Management (SIEM) toolset. Automated analytics reduce noise, allowing analysts to focus on high priority investigations. Whereas repeated false positives represent cost and loss of confidence, by concentrating analysts' time on critical events, QinetiQ provides a more cost-effective monitoring solution.

Actionable Incident reports typically encompass raw log data, analyst commentary, and, crucially, recommendations on what action should be taken. Routine service reports incorporate pertinent trend analysis and Situational Awareness reporting relevant to the monitored environment. This combination of tactical and strategic level information provides an essential contribution to the customer's management of risk.

Collaborating with QinetiQ

At QinetiQ we bring organisations and people together to provide innovative solutions to real world problems, creating customer advantage.

Working with our partners and customers, we collaborate widely, working in partnership, listening hard and thinking through what customers need. Building trusted partnerships, we are helping customers anticipate and shape future requirements, adding value and future advantage.

www.QinetiQ.com

QinetiQ/19/0173

For further information please contact:

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
customercontact@QinetiQ.com
www.QinetiQ.com