Cyber Security Monitoring and Device Management

QinetiQ Digital Resilience

Organisations face a growing challenge to protect their digital assets from cyber-attacks and to detect compromises when they happen. Many organisations have invested heavily in security technologies, but often see no value from these platforms and have very limited visibility as to the potential security incidents that are ongoing across their estates.

QinetiQ's Cyber Security Monitoring and Device Management Service is a managed security service that helps protect your digital systems from malicious activity. Through the collection and analysis of security information from digital systems, the service is able to look for and identify potential security breaches, highlighting these to our customers for containment and resolution. In addition the service is also able to help customers actively manage security technologies deployed across their digital estates, which increases the security effectiveness of the devices and enriches the security data supplied by them to in turn improve the quality of the monitoring service.

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

Risk & Business Alignment
In order to deliver the best value, we work with our customers to develop a shared clarity on the specific risks to be mitigated via monitoring. We customise our service to target what is important and deliver the business protection you seek. As the risks you face evolve, we keep working with you to make sure that our service is operating in the right context and aligned with your business needs.

Defence in Depth
We aim to provide you with confidence that the investment you have already made in defensive security technology is optimised and that the technology will enable our monitoring systems to help protect you.

Once we have a clear understanding of the risks you face, our experts can review both the architecture and the configuration of the technical security controls deployed across your digital assets, to ensure they are configured to best detect relevant compromise and to minimise damage from compromise. We can also provide the active management of these platforms to ensure that their configuration remains commensurate with the evolving risks you face.

Content, Analytics & Intelligence
When your defensive technologies are tuned and configured correctly to gather the relevant security information, our engineers configure our monitoring platforms to receive and analyse that information to enable the detection of threats and anomalies in real-time. We build on more traditional correlation based analysis by harnessing the power of big data and streaming analytics to automatically detect trends and patterns, presenting high-value information to our analysts.

In addition our threat intelligence cell continually scans our sources for warnings of new threats to your business. This allows our engineers to rapidly adjust the setup of our systems and adapt our service to new risks. We also consolidate intelligence garnered across our high-threat customer base. This means that our monitoring platforms remain in the optimal state to defend you against known risks.

QINETIQ

Orchestration & Automation

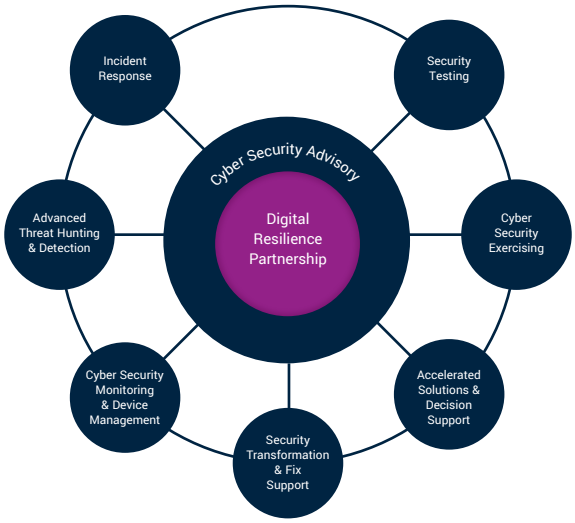
When our monitoring systems detect potential signs of compromise, you need rapid, effective response and analysis of the situation. With the use of orchestration and automation technologies our analysts are presented with a rich set of data, at the point that an alert is triggered, with which they can perform initial triage and assessment of the situation. This allows the service to be able to remove false positives and to be able to assess the incident in relation to the potential impact it has on your business, giving you a clear insight into what should be done in response to the problem.

This means that the lag between detection and response to events is minimised. It also means that we only alert you to real problems and provide you with recommendations for remedial action. You won't waste time chasing down false-positive alerts of compromise. You will receive informed advice on appropriate response to real problems instead. Where agreed, we can even take appropriate remedial action for you.

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:

- **Advanced Threat Hunting & Detection** - is enhanced by the rich data set provided by Cyber Security Monitoring & Device Management
- **Incident Response** - can be triggered and informed as a result of Cyber Security Monitoring & Device Management analysis and triage
- **Cyber Security Advisory** - complemented through sharing real time threat information about developing cyber attacks



Key Features & Benefits

Fully Managed Service Delivering 24x7x365 monitoring, alerting and device management support. Using the QinetiQ service reduces customers investment and ownership costs of implementing cyber security monitoring.

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.

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. Repeated false positives represent cost and loss of confidence; by concentrating analysts' time on critical events, QinetiQ provides a cost-effective monitoring solution.

Flexible risk-based controls Customer engagement enables analysts to continually tune the platform in accordance with the detection require-ments; they endeavour to tailor the controls based on applicable attack vectors. This improves the monitoring capability further, reducing the customer's exposure to risks.

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.

Infrastructure agnostic Deployable within on-premise, cloud or hybrid environments. This allows the service to interface with a customer's current infrastructure, reducing start-up costs.

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/19/01786

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