Quorum Cyber

Service Description Automated MDR G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

Frontline employees are a critical part of most organisations. They are responsible for day-to-day operations and delivering key business services. If they are impacted, your business and your customers are also impacted, so it is vital to empower these staff to work effectively, safely and securely. However, they often interact with IT systems and data differently than 'core' office employees and this can present challenges with more traditional cyber security approaches and services. With a vast student population studying at any hour on any device and a widely dispersed community of researchers, the higher education sector shares similar security challenges to frontline workers.

Challenges with traditional cyber security approaches to securing frontline employees and students include:

- Access: Limited, sporadic, or less predictable access can make it harder to rely on organisation-wide conditional access policies or to detect 'unusual' events
- Devices: Personal devices, which are more difficult to secure, may often be used
- Awareness: Limited awareness and less time in a traditional office setting may result in mistakes such as trusting phishing emails, links, or sharing credentials
- Compliance: There can be a tendency to share, download or copy data for ease of access which can present challenges with regulatory compliance.
- Cost: Traditional cyber security, especially managed services, can be priced per user which can make the cost of monitoring these employees prohibitive compared to office staff.

Quorum Cyber's Solution

At Quorum Cyber we aim to provide comprehensive and flexible security that meets every need in an effective and affordable way. By leveraging industry-leading solutions from Microsoft Security and our highly skilled SOC and Engineering teams, we have developed solutions tailored specifically for frontline employees and students. By combining these with our full Clarity MDR and optional MXDR services across your users, data and core systems you gain a truly flexible, leading, comprehensive detection and response and management solution at a considerably reduced cost.

We deploy and assess a number of identity focused detection rules (analytics) in Microsoft Sentinel covering your frontline users and/or students. Response automations are then performed based on different priorities of alert from these rules. Response actions are taken within Microsoft Entra ID and we will provide recommendations on which actions to apply to each alert type after analysis of alert volumes, tuning, and assessment of the fidelity of the alerting (i.e. the likelihood of true versus false positive alerts).

By addressing this additional group of people, business processes which govern them, and the technology which underpins their work, we ensure that our solution is comprehensive and takes into account the unique needs and challenges they present. This holistic and flexible approach helps maintain security and compliance while enabling frontline employees and students to work efficiently and effectively.

Differentiators

- Unique and custom built solution, developed and created by Quorum Cyber to supplement our Clarity MDR services
- Monthly reporting and near real-time visibility through integration with our Clarity Portal
- SOC handling to any major events such as an increase in alerts or response actions in a short time, indicating a possible serious attack.

Service Features

- **Advanced, identity-based, behavioural analytics**: Expertly designed analytics to detect unusual account activity, enriched to provide deeper insight into the activity. This includes monitoring data access, which alongside the full MDR service, supports regulatory compliance.
- **Intelligent response automations**: Unleashing the power of Microsoft Sentinel, Defender, and Azure, to provide rapid and tailored responses to suspicious events to protect your data and systems from malicious threat actors, such as revoking or enforcing secondary checks on an unexpected access to your data or systems.
- **Underpinned by threat intelligence**: We consider the most likely threats for your business and estate to ensure the most appropriate level of protection and response – context is critical.

Service Benefits

- **Cost effective**, threat focused, coverage of your frontline: Advanced threat led detections and intelligent containment automations offer protection for your frontline at an effective price point compared to traditional MDR services.
- **Reduced burden on your teams**: We take on handling the tide of alerts that frontline and student identities can create, ensuring you can focus where it matters.
- **Comprehensive protection**: Combined with our full Clarity MDR service protecting your endpoints, data, applications, cloud and core identities, this service covers 1000s of additional identities with access to your estate.
- **Reduced risk of cyber-attacks**: By adding monitoring of these identities, attacks are caught earlier in the attack lifecycle, lowering your risks and chances of attackers being able to cause an impact.
- **Regulatory compliance**: By extending your monitoring to cover all identities, and including access to sensitive data and systems, this enhances your regulatory compliance.