Quorum Cyber

Service Description
Clarity OT
G Cloud 15

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

Table of Contents

Service Overview

Background

Operational Technology (OT) environments are the heart of organizations, yet the vulnerable systems often go unprotected, drastically increasing the risk of business impacting events such as ransomware attacks. This risk is amplified due to the increasing convergence of IT, IoT, and OT, with threat actors frequently using traditional IT cyber tactics to infiltrate OT systems. The lack of isolation between OT and IT services and the necessity to comply with industry regulations only add to OT cyber security challenges.

Quorum Cyber's Solution

Quorum Cyber's Clarity OT service, powered by Microsoft Defender for IoT and Microsoft Sentinel, offers advanced detection and response, specially designed to protect OT and industrial control system (ICS) devices. The service integrates seamlessly with existing Microsoft and third-party IT security solutions, providing robust threat detection, response, and vulnerability visibility capabilities across your entire OT network.

Clarity OT leverages cutting-edge Microsoft Security technologies:

- Microsoft Sentinel: Cloud-native SIEM and SOAR solution for comprehensive data analysis and correlation.
- Microsoft Defender for IoT: Uses passive deep packet inspection, behavioural analytics, and threat intelligence for robust threat detection.

Differentiators

With Quorum Cyber's Clarity OT service, you're not just protecting your critical infrastructure, you're ensuring your organisation operates with confidence in an increasingly complex and risky digital landscape.

We have a dedicated team of OT specialists ready to help with the deployment and integration of OT threat detection.

Microsoft Defender for IoT experts with enriched detections an automations to support the Clarity OT service.

Service Features

1. **24/7 threat monitoring, analysis, investigation, diagnosis, and notification** to provide continuous event monitoring and response
2. **Detection analytics subscription** As part of the service Quorum Cyber deliver a fully maintained and continually developed set of threat detection rules (analytics) which run within Microsoft Sentinel to ensure we are detecting the latest threats. These rules are regularly tuned and tailored to Customer, to ensure the alerts are reliable and relevant.
3. **Incident Response** is included within the Clarity OT Service up to the point of containment of the threat, for assets in scope.
4. **Threat Intelligence**: Quorum Cyber's threat intelligence feed is applied across all customers, ensuring we are detecting the latest IOCs. Threat intelligence also informs continuous improvement to detection rules.
5. **Web-based customer portal**. A secure portal that provides visibility, reporting, and workflow for all G Cloud 15 Security Incidents, raising service requests and other Quorum Cyber related interactions.
6. **Continuous service improvement**: This is delivered as a combination of three primary factors: Feedback from our customers on what more they would like to see from the service; our threat analysts leverage threat intelligence to update service components such as analytics; our solution teams look beyond the horizon to develop new capabilities and service lines.
7. **Health monitoring** of the Sentinel platform: Monitoring of connector and analytic health, ensuring all aspects of the service are working correctly, and notifying you of any drops of data feeds.
8. **Monthly Service Delivery Review Meetings**
9. **Advanced incident enrichment**
    a. Asset enrichment
    b. Extended properties enrichment
    c. OT Protocol function code tables
    d. User activity correlation
    e. CVE enrichment and correlation
10. **Dynamic alert learning**
11. **Incident PCAP to Sentinel ingest**
12. **OT Threat Hunting**

Service Benefits

- 24/7/365 Protection: round-the-clock monitoring and defence across your entire OT estate
- Complete Asset Visibility: gain a full inventory of all assets using passive, agentless network monitoring, with zero impact on infrastructure performance
- Increased effectiveness of security teams: highly optimised controls and Cyber OT expert-led service delivery frees up your teams to focus on business goals rather than being distracted with low-value alerts
- Real-time insights and reporting: via our customer platform, Clarity, for a clear view of your current security posture, enabling informed remediation decision-making
- Reduced Internal Workload: our service supports ongoing cyber programme maturity while alleviating the burden on your internal teams
- Always-optimised security posture: reduce the probability and impact of a security incident, and keep pace with the relevant threats facing your organisation and industry
- Threat Detection & Response: our security operations centre (SOC) and Threat Intelligence teams swiftly identify and addresses threats, continuously fine-tuning alerts to ensure consistent protection
- Unified IT/OT Protection: seamless integration with Clarity Protect for advanced visibility and protection across your entire IT and OT environments