Quorum Cyber

Service Description
Clarity CTEM
G Cloud 15

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

Table of Contents

Service Overview

Background

Operating systems and applications have always contained vulnerabilities. Over time, these have been exploited and, in recent years, increasingly weaponised by attackers with very low skill levels.

Organisational and employee requirements of IT systems are in a constant state of flux. This places incredible pressure on any organisation to understand its attack surface and where its real weaknesses are concealed. Many organisations are siloed and if they use vulnerability management platforms then they suffer from having:

- Hundreds of thousands of rarely actioned vulnerability and exploit suggestions
- A long list of generic remediations that do not take business context into account
- A lack of appetite to invest in a mitigation workflow system to achieve these actions.

Vulnerability management has evolved from the classic approach of scanning for public exploits against known vulnerabilities. It now uses additional sources of threat exposure information and combines them with context-aware intelligence to sharpen remediation efforts. The result is a significantly stronger security posture that is improved over time as the Continuous Threat Exposure Management process is followed.

Quorum Cyber's Solution

Our Continuous Threat Exposure Management (CTEM) service utilises Microsoft Defender XDR (notably Defender for Endpoint & Server), Defender External Attack Surface Management and external threat intelligence monitoring. and weaving these toolsets into the CTEM process as shown below.

With CTEM, our team of experts improve your organisation's security posture by implementing a process that evolves over time.

Our Threat Intelligence teams will assess and review a variety of threat intelligence sources to get a perceived view on any imminent attacks against your organisation, which also includes in-depth analysis on new and upcoming attacker techniques and the exploits they relate to.

All this intelligence, context and analysis is fed into our separate CTEM team. The interrogation of relevant threat intelligence informs the decision tree process when estimating and prioritising fixes for our customers. They analyse, threat hunt and create a monthly report that summaries the top issues affecting your organisation and how they can be mitigated. The following months report will then have a follow up on how far this mitigation process (the mobilise section from above) has proceeded. If you utilise Microsoft Intune, then the CTEM team will create remediation packages for you that can be deployed using Intune.

Differentiators

- Threat Intelligence driven prioritisation of remediation activities.
- Utilisation of Microsoft security tooling without the need for additional third party scanning solutions
- Dedicated CTEM team of experts

Service Features

With CTEM, our team of experts improve your organisation's security posture by implementing a process that evolves over time.

- Scope Definition: Covering all your internal assets, your internet footprint and proactively scanning your critical assets such as web farms, application servers and public-facing application programming interface (API) libraries.
- Discovery: Continuous active and passive scanning of internal and external facing assets, (including operating systems and software versions) to build a complete inventory and provide you with an accurate risk review of every connected device.
- Prioritisation: Using our knowledge of your infrastructure and organisation we make informed decisions and recommendations about which systems and parts of your IT infrastructure need updating first.
- Validation: Our service tracks key metrics including your top risky machines, vulnerabilities and security recommendations to protect critical resources, and we track your exposure score over time to demonstrate how the service is improving your security posture.
- Mobilisation: Continual improvements to your security posture as your business evolves, when new projects, departments or business units are brought into scope, or when your risk appetite changes.
- Threat Landscape: In addition to internal threat and vulnerability information from an agent (not required for Windows 10 & 11 machines) the CTEM service also takes a feed from an external view of your infrastructure using Defender External Attack Surface Management. This is what an attacker will first see when carrying out reconnaissance of your Internet presence.

Service Benefits

Leveraging Microsoft Defender External Attack Surface Management and Attack Surface Intelligence, Quorum Cyber's CTEM service includes:

- A fully automated inventory of all IP connected assets, with full vulnerability management information for assets enrolled into the service.
- Measurement of your risk exposure and its improvement over time.
- Recommendations of the most important mitigation actions your business needs to take.
- Validation that security recommendations are being actioned.
- Visibility of what an attacker can see from the internet and how to minimise your exposure.
- A monthly report highlighting your exposure score and top vulnerabilities.