ULTRARED

External Attack Surface Management

Gaining the Upper Hand

The ULTRA RED Threat Exposure Management Platform is a unified SaaS solution that automates the discovery and cyber management of your organization's enterprise attack surface. Unlike many EASM solutions, ULTRA RED continually delivers prioritized and verified vulnerabilities that can be actioned without the need for further investigation, dramatically improving exposure detection and response rates. Supporting intelligence, POCs and remediation guidance for each vector facilitate a smooth handover to remediation teams.

www.ultrared.ai

Most organizations operate in a highly competitive business environment, one where continual technology innovation is a given. When the Internet is involved, however, innovation comes at a cost.

The Ever-Changing External Attack Surface

Digital transformation initiatives, cloud migration, third party SaaS applications, supporting WFH, new Internet facing API's and IoT devices, all contribute to a rapidly expanding and constantly changing attack surface. Exploitation of the vulnerabilities hidden in organizations' attack surfaces accounts for a third of all breeches today and that percentage is rising[1].

Both the number of documented vulnerabilities and number of documented exploits continue to increase year over year. This is good news for threat actors as they have more avenues for success. Add to that new criminal business models such as the rise of Initial Access Brokers and Ransomware as a Service combined with increased geo-political tensions and nation state activity, and we have a situation that is only getting worse.

Zero-day vulnerabilities may garner much of the media attention, but threat actors more often capitalize on recently patched vulnerabilities and hunt for unpatched systems to exploit[2]. This is backed up by research showing that 4 out of the top 5 most exploited vulnerabilities were new vulnerabilities. Organizations are particularly vulnerable in the period between the public announcement of a high-risk vulnerability and the remediation of all their affected systems.

The adoption of cloud hosting and third-party SaaS applications presents unique challenges in uncovering and eliminating weaknesses. According to Gartner, the growth in the non-patchable attack surface will grow from 10% today to 50% by 2026[3].

[1] IBM X-Force Intelligence Index 2022 - https://www.ibm.com/downloads/cas/ADLMYLAZ

[2] Symantec – The Threat Landscape in 2021 - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-2021

[3] Gartner Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

A Need for Change

As we have seen, the cyber risk associated with the external attack surface is growing, putting pressure on cyber teams to increase their visibility and detection rates.

External attack surface visibility is key as you can't protect what you don't know about. Manual discovery approaches are time consuming and, in most cases, incomplete, and asset registers created in this way are obsolete by the time they are produced.

Red Teaming practitioners use a range of point solutions to uncover weaknesses and exposures in their known assets. As with asset discovery, this approach is also manually intensive and time consuming. There are often no standardized practices across the team and issues arise when trying to reproduce and validate findings of other team members. The handover to remediation teams can also be inconsistent with varying degrees of supporting documentation and remediation guidance.

Adopting a Continuous Threat and Exposure Management Approach

Cyber Teams are looking for ways to standardize and automate their activities, working smarter to identify and remediate exposures at scale. While External Attack Surface Management was seen as the domain of early adopter organizations only a few years ago, it is rapidly becoming a mainstream discipline with more organizations evaluating EASM solutions to support their cyber efforts. However, early-adopter organizations are finding that their EASM solutions generate too much noise, requiring significant resource from security teams to prioritize findings, verify vectors and investigate remediation scenarios. This can result in little or no ROI.

Gartner's Continuous Threat and Exposure Management (CTEM) framework is gaining in popularity as it outlines a standardized and repeatable process to identify and remediate attack surface weaknesses. It covers EASM but goes further to include continuous vulnerability detection and validation along with prioritization, mobilization and remediation, to create a standardized approach to tackle real threats to the organization.

ULTRA RED are Here to Help

The ULTRA RED platform was designed from the ground up to eliminate noise and deliver on ROI. It supports all phases of Gartner's CTEM framework and enables cyber teams to dramatically improve their detection and response rates.

The platform includes powerful continuous discovery and asset management capabilities but unlike many EASM solutions, ULTRA RED delivers prioritized and verified vulnerabilities with supporting intelligence and remediation guidance. As a result, vectors can be prioritized and actioned without additional overhead.

ULTRA RED's prioritization scoring is based on a combination of the CVSS severity and its exploitability. For example, a high-risk CVE may not be considered a vector as there are mitigating controls that prevent it from being exploited. A vector with a high CVSS score may have a lower ULTRA RED score if the weakness exists but cannot be exploited due to missing prerequisites. In both cases, continual monitoring will update their status and priority if the situation changes. Asset risks are categorized into logical groupings such as VPNs, development environments, admin & sensitive information. This helps managers and teams understand the potential impact of affected assets to further assist with prioritization. With ULTRA RED, cyber teams can focus on the vectors that present a real-world risk to their organization.

Each identified vector is accompanied by impacts, external references, an actionable remediation list with required steps, and POCs for leveraging the weakness. Armed with this information, cyber teams can affect a smooth handover to remediation teams, thereby lowering mean time to resolution (MTTR).

ULTRA RED's cyber experts assist customers along the way with advice and guidance; for example, in understanding new or lesser-known vulnerabilities.

Summary

The external attack surface represents significant and ever-changing risk to organizations and manual efforts to protect it fall short. The ULTRA RED platform automates the asset discovery and exposure detection process. It goes further to deliver unmatched vector validation and prioritization, allowing cyber teams to focus on addressing the vulnerabilities that matter. Full documentation for each vector dramatically improves resolutions time. ULTRA RED clients see a continual reduction in high-risk CVEs and in the number of different CVEs in their attack surface.

To find out more about the ULTRA RED Threat and Exposure Management Platform visit us at www.ultrared.ai and request a demo.