ULTRARED

ULTRA RED
Benefit vs Value

Can you improve your cyber posture and save on resource and license costs?

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

Trying to cost justify a cyber security solution can be difficult. After all, the main reason for taking on a new technology is to lower cyber risk, not to save cost. However, sometimes solutions can offer significant savings in cyber team resource as well as in existing tool costs, while demonstrably improving cyber posture. We believe that ULTRA RED is one of those solutions and in this paper, we will cover some of the reasons why. While organizations will differ in terms of current capability, hopefully many of these benefits will resonate with you.

The External Attack Surface Challenge

Management of the external attack surface has come to the fore in recent years as cyber-attacks on Internet exposed assets now account for over 30% of all successful breaches. The ULTRA RED Threat Exposure Management Platform is a unified SaaS solution that automates the discovery and cyber management of the enterprise attack surface, enabling organizations to systematically remediate vulnerabilities and harden their attack surface.

Effective threat and exposure management requires:

- Full visibility of Internet exposed assets
- Continual discovery of potential exposures
- Validation and prioritization of those exposures
- Remediation that often involves close collaboration with other parts of the IT organization

Each of these activities is labor intensive and has historically involved the use of a variety of tools. Joining the dots to turn these activities into a consistent and repeatable process is fraught with both people and technology challenges.

In this paper we will use the discovery, detection & validation, prioritization & remediation process flow as the framework to cover the advantages of using ULTRA RED.

Streamlining the Discovery Process

Manual attack surface discovery is a highly labor-intensive process that typically produces an incomplete picture of the attack surface that is out of date as soon as it is created. Blind spots result from Shadow IT deployments, business activities such as mergers, acquisitions, and divestitures, as well as other activities that take place without the knowledge of the security team. Using point discovery and reconnaissance tools can ease the burden but do little to alleviate blind spots and can require additional work to put findings together in a standard format to create a usable asset inventory. These tools and scripts then need to be run on a regular basis, updating the asset register each time.

The ULTRA RED discovery process is fully automated and can be up and running in as little as three clicks. Utilizing recursive techniques, it discovers hosts, domains and IP addresses which are within the organization's scope, including assets and services currently unknown to the security team. Once discovered, it uses proprietary technology to check and re-check their validity, resulting in an extremely low false positive rate. It automatically

creates a rich and contextualized asset inventory and keeps that inventory up to date, so the cyber team always has a view of the current attack surface. ULTRA RED eliminates the need for other discovery and reconnaissance tools and the human resources associated with their use, saving both license costs and cyber resource.

ULTRA RED customers report average discovery time improvements of 350% compared to incumbent tools and up to 30% more assets discovered. The manual effort to consolidate findings and maintain an asset register is eliminated.

Smarter Detection and Validation

As with asset discovery, vulnerability detection and validation are resource intensive tasks that need to be done on a regular basis, as existing assets can become targets overnight due to newly published vulnerabilities. Using a vulnerability scanner to regularly scan all assets is an expensive approach as most of the scans are wasted on non-vulnerable or low vulnerability assets. Engaging in bug bounty programs and external pen testers is also costly and many organisations report that the majority of submitted vulnerabilities from these programs are of the "low hanging fruit" variety, while more sophisticated vulnerabilities can go undetected. In addition, reported vulnerabilities need to be manually verified and findings can often be difficult to recreate due to inadequate or inconsistent documentation.

ULTRA RED provides a better approach to exposure detection through its continuous vector scanning. Without the need for human intervention, all assets in the asset inventory are regularly scanned for known public vulnerabilities and cross referenced against a wide range of proprietary scanning findings and documented DarkNet references. Detected weaknesses are validated without impacting the scanned system and its security infrastructure and controls, ensuring production system continuity.

ULTRA RED's focus on vector validation eliminates time consuming false positives so that cyber teams can focus on exploitable vectors in their attack surface. For example, a high-risk CVE may not be considered a vector if there are mitigating controls that prevent it from being exploited. Each identified vector is accompanied by impacts, external references and POCs for leveraging the weakness, reducing, or eliminating the need for manual validation.

With ULTRA RED, organizations can greatly reduce their vulnerability scanner usage, eliminate, or reduce the scope and frequency of bug bounty programs and free up resource currently spent on investigating false positives and trying to recreate findings.

ULTRA RED customers report a massive reduction in the number of false positives, from 25% using other tools to less than 1%, saving hundreds of hours analyzing false-positive detections.

Consistent Prioritization and Remediation

Vector prioritization and remediation represent that last mile of the process and the one where hardening of the attack surface occurs.

ULTRA RED's prioritization scoring is based on a combination of the CVSS severity and its exploitability. 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. Continual monitoring will update the 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. Each identified vector has an actionable remediation list with required steps, allowing cyber teams to affect a smooth handover to remediation teams.

Using ULTRA RED, cyber teams can focus their efforts on remediating the vectors that present a real-world risk to their organization with a standardized process flow that lowers mean-time-to-remediation (MTTR).

ULTRA RED customers report a 50% improvement in mean-time-to-remediation.

Adopting a Standardized Approach

ULTRA RED supports Gartner's Cyber Threat and Exposure Management (CTEM) framework, standardizing the discovery, detection & validation, prioritization & remediation process flow to deliver demonstrable results month over month.

New ULTRA RED customers can show SOC operation improvements of 33% within the first 6 months, freeing up a third of staff currently working on threat and exposure management to focus on other activities.

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