Cyberint
Impactful Intelligence

Cyberint Argos Platform

Vulnerability Intelligence Datasheet

Cyberint's Vulnerability Intelligence module automatically detects CVEs in the publicly-visible software in your environment and provides accurate risk scoring that considers CVSS, the probability of exploitation, and threat intelligence, like mentions of a CVE on the dark web, the availability of exploit code, and active exploitation.

Challenge

In 2022, over 25,000 new entries were added to the Common Vulnerabilities and Exposures (CVE) database, representing a 400% increase in just 10 years. Coupled with the proliferation of software in an enterprise environment, this huge spike in CVEs has made vulnerability and patch management an extremely difficult project. With limited time and resources available, security leaders face a challenge in deciding how to prioritize CVEs for remediation.

Solution

Cyberint's Vulnerability Intelligence automatically detects the software and services running in your external attack surface, as well as any CVEs associated with that software and version. The module then assigns each CVE a risk score that accounts for the CVSS score, the probability of exploitation, and other threat intelligence indicators of an increased risk. Alerts are issued when new CVEs are detected or when the risk level changes significantly for known CVEs (e.g. documented exploitation of that CVE in the wild).

Key Benefits:

- Improve visibility on all the software running on your external attack surface
- Understand all of the CVEs present in the software your organization is using
- Leverage threat intelligence to see which CVEs are discussed in threat actor forums, have POC code available, and/or are actively exploited
- Receive accurate risk reporting on the CVEs discovered in your environment
- Effectively prioritize CVEs to ensure an optimal impact from the time you invest into patch management and remediation

Understand The Software & Associated CVEs In Your Environment

Cyberint continuously and automatically discovers all your external IT assets, the software and services running on each asset, and any CVEs known in the specific software you have deployed.

Gain Visibility On The Software In Use

Discover your external attack surface and all of the software and services running on your publicly visible assets.

Know Where Software Is Running

Keep an up-to-date inventory of assets and software to increase agility when a new CVE is documented or exploited.

Get An Overview Of All Your CVEs

Gain a complete overview of all the CVEs in the software and specific versions running in your environment.

Receive Immediate Alerts When A CVE Is Causing Serious Risk

Cyberint issues alerts when you have a major increase in risk: when a new CVEs is discovered, when a specific CVE is mentioned on the dark web, or when a known CVE begins to be exploited at scale.

Keep Up With New Software & CVEs

Know when new software is deployed in your environment to understand any new CVEs that are introduced.

Know When A New CVE Is Revealed

Get a notification when a new CVE is discovered in software that is running on one of your external IT assets.

Stay Ahead of CVE Exploitation

Receive alerts when a CVE in your attack surface is exploited in the wild or when exploit code becomes publicly available.

Effectively Prioritize CVEs To Reduce Risk & Prevent Breaches

Cyberint helps you to accurately and comprehensively understand the risk that each CVE introduces to your organization, helping you to optimize remediation efforts, eliminate major risks, and stay secure.

Quickly Eliminate Critical Risks

Understand which CVEs are creating the most risk for your organization so you can patch them immediately.

Prioritize CVEs To Optimize Resources

Make the most of the resources you invest in patch management with effective and optimal prioritization of CVEs.

Improve Hygiene & Stay Secure

Improve your patch and vulnerability management processes to strengthen security posture and prevent breaches.

About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.