SOLUTION QUICK CARD

Vulnerability Prioritization for Leadership and Compliance

Critical Start Vulnerability Prioritization

KEY BENEFITS

- Use the vulnerability management tools you already have in place
- Enrich scans with expertly curated, timely cross-vector threat intelligence
- Quickly see which assets contain vulnerabilities that are being actively exploited
- Collaborate with cross-functional teams to achieve greater impact in less time
- Make sound, data-driven decisions to decrease exposure

Do You Know the State of Vulnerabilities in Your Environment?

Vulnerability prioritization is a crucial step within vulnerability management that focuses on ranking discovered weaknesses based on their potential impact and exploitability. Even small IT environments can have tens of thousands of vulnerabilities, but not all vulnerabilities are created equal. Knowing which assets contain vulnerabilities – including CVE, non-CVE, and weaponized vulnerabilities – is the first step in sound asset and vulnerability management.

CRITICAL**START**® Vulnerability Management provides asset and vulnerability management leaders with detailed "By Asset" and "By CVE" views so that leadership and compliance teams gain a comprehensive view of their potential points of exposure, length of exposure, and related risks of ransomware and exploitability.

Ideal Use Cases

Vulnerability Prioritization streamlines and accelerates analysis and mitigation by:

- Determining the most vulnerable hosts by number of vulnerabilities present.
- Finding specific vulnerabilities present on each host.
- Clearly seeing all hosts that contain weaponized vulnerabilities or are at risk for Ransomware.
- Check for hosts that were not scanned in the last month.
- See the aging of each vulnerability in your environment.
- Recommend remediation steps based up-to-date risk-based prioritization.

How it works

Critical Start Vulnerability Prioritization provides View by Asset, which offers CVE and non-CVE vulnerabilities present on each asset in the environment. In the CVE view, users see deduplicated and normalized views of CVEs discovered by all available vulnerability management sources. In each view, users see vulnerabilities associated with a host, along with relevant asset information like IP, OS, hostname, etc. Each row clearly shows asset criticality, corresponding risk scores, and the last date the vulnerability was detected on that asset. In the grouped view, each row represents data from all vulnerability management sources, including the total number of vulnerabilities, CVEs, and weaponized vulnerabilities associated with each host.

These view options give security leaders and compliance teams the data they need to track and manage risks and decide on the best actions that they can take to further protect their organizations from exposure.