DATASHEET

# CRITICAL**START**® Vulnerability Prioritization

Identify and prioritize vulnerabilities based on real-world exploit weaponization.

## KEY BENEFITS

- ✓ **Seamless integration** with existing supported vulnerability management tools
- ✓ **Prioritize vulnerabilities** based on real-world threat group exploitation, not theoretical CVSS severity scoring
- ✓ **Add business context** and asset criticality specific for your environment
- ✓ **Identify hosts that are vulnerable to ransomware,** botnets, exploit kits, and advanced persistent threats (**APTs**)
- ✓ **Increase the ROI of your vulnerability scanning tools** by focusing on the most critical vulnerabilities first

As the number of vulnerabilities grows, the time to exploit shrinks, and security teams are drowning in disorganized and unprioritized data. While vulnerability scanners provide comprehensive lists of vulnerable assets and systems, the data they produce lacks the critical business and threat context to make those findings actionable. Organizations need a better way to gather actionable information so they can patch what's most important first.

CRITICAL**START**® Vulnerability Prioritization addresses these challenges by enriching vulnerability scan results with customizable business context and exploit-aware threat intelligence. With dynamic risk scoring assigned to each vulnerability, and actionable dashboards that guide data-informed decision-making, security leaders can make sense of their data and take actions that directly reduce risk.

## How it works

The Critical Start Vulnerability Prioritization integrates seamlessly with Qualys or Tenable and automates the data gathering and enrichment process. Leveraging threat data, exploitability, asset criticality, and more, Vulnerability Prioritization delivers actionable reports and rich dashboards with the data you need to accelerate patching efforts.

Vulnerability Prioritization goes beyond the Common Vulnerability Scoring System (**CVSS**) base scores to include the existence of working exploits, so you can pinpoint the systems that are at risk of ransomware, botnets, exploit kits, and APTs. Armed with data, you can rapidly navigate your next steps of remediation make the greatest impact. Critical Start's threat intelligence is backed by a team of experts who curate and monitor various sources including intelligence feeds, dark web sources, and GitHub to deliver timely advisories and information on exploits so that you can stay ahead of emerging threats.


*Figure 1: CRITICAL**START**® Vulnerability Prioritization offering prioritizes vulnerabilities based on real-world group exploitation.*

## Key Features

- **Integrate with your vulnerability management solution:** Eliminate lengthy onboarding by seamlessly integrating this SaaS solution with your existing vulnerability scanner (Qualys or Tenable). You will eliminate manual data collection and analysis, ensuring that your vulnerability data is always up-to-date and accurate.

- **Enrich scan results with cross-vector threat intelligence:** Rapidly identify which vulnerabilities persist in your network that could be used by APTs, ransomware families, botnets, and exploit kits. These findings factor in multiple data sources, including threat intelligence, public vulnerability databases, dark web forums, and GitHub repositories, NIST National Vulnerability Database (**NVD**) and the Cybersecurity and Information Security Agency Known Exploited Vulnerabilities (**CISA KEV**), and more.

- **Prioritize based on business context and asset criticality:** Customize business context and asset criticality based on your organization's unique environment and requirements. You can tag and group assets according to location, function, owner, or business impact, and assign different weights to the assets based on their importance. Vulnerability Prioritization then adjusts the risk scores of the vulnerability findings to reflect the potential impact of each vulnerability on the organization.

- **Make remediation decisions based on data:** Vulnerability Prioritization delivers results that automatically factor in asset criticality, vulnerability severity, exploitability, exposure, and threat intelligence. You'll have actionable risk scores assigned to each vulnerability finding that let you identify and fix the most pressing issues first .

- **Choose your view based on your role:** Are you in charge of vulnerability management, needing clear prioritization based on risk score, exploitability, and weaponization? Or are you tasked with remediation or IT asset management, in need of asset views and prescriptive patching guidance? Or is your role compliance or leadership, demanding aging criteria so you can articulate findings and remediation over time? For all these roles and more, Vulnerability Prioritization has views to get the job done.

- **Streamline cross-functional communication:** View dashboards and generate reports that contain the information that matters to each key stakeholder. Prioritized vulnerabilities are visualized through actionable dashboards, including views that sort by vulnerability, asset, risk score, and exploit potential. Report views include By Asset, By CVE, or By Vulnerability so that stakeholders can track and communicate vulnerability-based risks to the organization.

- **Unify preemptive and reactive security for greater risk reduction:** Vulnerability Prioritization is a SaaS offering delivered on top of the Critical Start Cyber Operations Risk and Response™ (**CORR**) platform. This critical preemptive security offering complements and enhances other services and capabilities offered by Critical Start, such as Managed Detection and Response for Endpoint, Security and Information Event Management (SIEM), User, Identity, and Cloud; Endpoint Coverage Gaps; SIEM Coverage Gaps, MITRE ATT&CK Mitigation Recommendations; and Risk Assessment risk posture and industry peer benchmarking.

**CONTACT US TODAY TO GET STARTED!**

criticalstart.com/contact/




CRITICALSTART®