SOLUTION QUICK CARD

Effective Ransomware Exposure Mitigation

Critical Start Vulnerability Prioritization

KEY BENEFITS

- Use the vulnerability management tools you already have in place
- Enrich scans expertly curated, timely cross-vector threat intelligence
- Quickly see which assets are vulnerable to ransomware attacks
- Collaborate with cross-functional teams to achieve greater impact in less time
- Demonstrate risk reduction with rich reports geared to each stakeholder

Do You Know Which of Your Assets are Vulnerable to Ransomware Attacks?

Ransomware threat actors only need one vulnerable asset to find their way inside your network. Failure to patch or mitigate vulnerabilities can leave you exposed to attacks, resulting in significant financial losses, downtime, and reputational damage. Vulnerability scan results can keep you informed of potential exposures across your organization, but do you know which of those are prime targets for ransomware attacks?

Critical Start Vulnerability Prioritization answers that question for you with game-changing insights that let you fix the most critical vulnerabilities first.

Ideal Use Cases

Vulnerability Prioritization solves the challenge of ransomware exposure mitigation for customers who:

- Receive false or inaccurate ransomware signal from Qualys or Tenable.
- Suffered a ransomware attempt or attack in the past despite having a vulnerability management tool in place.
- Rely primarily on Common Vulnerability Scoring System (CVSS) scores to determine patching priority.
- Need to demonstrate effective risk reduction to leadership and boards.

How it works

Critical Start Vulnerability Prioritization integrates seamlessly with Qualys or Tenable and automates the data gathering and enrichment process. Leveraging threat data, exploitability, exploit probability, asset criticality, and more, Vulnerability Prioritization delivers actionable reports and rich dashboards with the data you need to identify and mitigate vulnerabilities related to real-world ransomware activity.

Vulnerability Prioritization also goes beyond the ransomware threat, giving you insights into potential exposure to botnets, exploit kits, and APTs as well. Because results are prioritized with your unique business context and asset criticality in mind, you can rapidly navigate your next steps of remediation to make the greatest impact. Critical Start's threat intelligence is backed by an expert team that curates and monitors various sources, including intelligence feeds, dark web sources, and GitHub to deliver timely advisories and prescriptive patch lists for potential ransomware exploits so that you can stop threat actors before they take hold of your assets.

Learn more about Critical Start Vulnerability Prioritization Service by scheduling a demo at: www.criticalstart.com/contact/request-a-demo/