NorthStar

A BETTER WAY
TO MANAGE VULNERABILITIES

As RBVM programs have begun to mature, there has been a shift from older CVSS only based programs towards vulnerability prioritization by the incorporation of external threat intelligence. However, many organizations that have adopted this style of vulnerability management program have come to the same conclusion: Simply adding in threat intelligence does not equate to true prioritization.

The key to unlocking the power of threat intel lies within the context of business importance.

With business importance, organizations are able to better reduce the number of lower priority vulnerabilities and distill out an actionable and effective remediation plan. The following is an example of this evolution in vulnerability management:

VULNERABILITY MANAGEMENT

CVSS

Vulnerability Data

PRIORITY CLASSIFICATION	# VULNERABILITIES PRESENT (On 25k assets)
High (7.0 - 10.0)	162,113
Medium (4.0 - 6.9)	491,250
Low (0.0 - 3.9)	569,850

% OF VULNERABILITIES REQUIRING IMMEDIATE ACTION **13%**

VULNERABILITY PRIORITIZATION

NorthStar Immediate ROI

Vulnerability Data + Threat Intel

PRIORITY CLASSIFICATION	# VULNERABILITIES PRESENT (On 25k assets)
1 Exploit Now	3,341
2 Exploit Past	1,376
3 Exploit Exists	42,444
4 Exploit None	1,176,053

% OF VULNERABILITIES REQUIRING IMMEDIATE ACTION **0.27%**

RISK-BASED VULNERABILITY MANAGEMENT

NorthStar Longterm Value

Vulnerability Data + Threat Intel + Business Context

PRIORITY CLASSIFICATION	# VULNERABILITIES PRESENT (On 25k assets)
1 Exploit Now & High Organizational Value	36
2 Exploit Past & High Organizational Value	798
3 Exploit Now & Medium Organizational Value	303
4 Exploit Past & Medium Organizational Value	578
5 Exploit Exists & High/Medium Org. Value	1,537
6 Exploit Now/Past/Exists & Low Org. Value	38,616
7 Exploit Exist/None & Compliance/Audit Scope	2,849
8 Exploit Now/Past & Exception	1,365
9 Exploit Now/Past & Compensating Controls	1,079
10 Exploit None	1,176,053

% OF VULNERABILITIES REQUIRING IMMEDIATE ACTION **0.068%**

*SAMPLE ORGANIZATION WITH 25,000 ASSETS
*TOTAL # OF VULNS DISCOVERED = 1,223,214

From a starting size of 1.23 million unique instances of vulnerabilities in this sample organization, NorthStar was able to determine only 0.068% (834) of the vulnerabilities discovered in the environnment were of a critical priority and required immediate action. This significant reduction highlights the impressive flexibility of the NorthStar model and empowers vulnerability management efforts by breaking down the large list of vulnerabilities into a manageable, laser-focused list that shows how to drive action to best protect the organization.

NorthStar Navigator was created to maximize the effectiveness of remediation efforts by focusing organizations on the problems that really matter and providing clear, actionable paths to remediation and lower overall risk.

WHERE NORTHSTAR SHINES

Prioritize vulnerability and exposure remediation based off of risk to YOUR business

- **Gain key insight** into the business importance of individual assets and business services
- **Leverage the flexibility** to decide what business and technical factors are most important to your organization
- **Provide visibility into exposures** beyond vulnerabilities, such as coverage gaps and misconfigurations across security tooling and compensating controls

Provide a complete and accurate inventory of all devices and all exposures

- **Gain visibility into** the variety, severity, and age of exposures existing in their environments
- **Enrich existing asset** inventory and management systems with relevant business and data classifications
- **Assist in data hygiene efforts** to accurately map the complex relationships betweeen assets and business services

Address the visibility gap that inherently exists between IT Security and IT Operations

- **Provide automated correlation** of vulnerability and patch information
- **Accelerate remediation efforts** by integrating with IT Management and Service Desk systems
- **Provide valuable insights** to IT incident response teams before, during, and after IT-related security events

Provide simple, powerful, and dynamic reporting

- **Validate that the most important issues** have been remediated
- **Slice and dice dashboards and reports** that fit the needs of your organization – by line of business, location, business services, etc.
- **Delivers out of the box dashboards,** and easily customizable dashboards configured through the front-end UI
- **Enforce robust role** based access control and dataset security