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:

RISK-BASED 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%

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.

NorthStar

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

NorthStar
516 N. Ogden Ave Suite 115
Chicago, IL 60642
Give us a call
312.421.3270
Send us an email:
connect@northstar.io
For more info, visit us at:
www.northstar.io

PREDICTING EXPLOITABILITY

NorthStar PREDICTION ENGINE

YES/NO FORECAST FOR VULNERABILITY MANAGEMENT

EASY ANSWERS TO HARD QUESTIONS

Is your vulnerability management program able to clearly delineate between vulnerabilities that are unexploited versus ones that are either currently being actively exploited in the wild or are predicted to be exploited in the wild?

NorthStar is the ultimate vulnerability prioritization and prediction engine.

In addition to automatically identifying vulnerabilities currently being exploited in the wild, NorthStar's vulnerability prediction engine accurately identified over 45% of the vulnerabilities that would be exploited in the wild at some point in the future, providing an average notice of around 280 days in advance.

45%

OF THE CVES ARE VALIDATED AS EXPLOITED IN THE WILD

280

DAYS ADVANCE NOTICE

HOW IT WORKS

Prediction begins with the collection of surveillance data that captures the footprint or breadcrumbs left behind on-line by attackers seeking to develop, deploy, and monetize exploits that are capable of leveraging an existing vulnerability. The appearance of these events and activities have proven reliable in determining the immediate risk posed by each vulnerability.

NorthStar's vulnerability prediction engine is a **yes/no categorical prediction**. This provides a definitive assessment on whether a CVE will eventually be exploited in the wild. Each prediction comes with a timestamp representing when the prediction was first made based on all available data at the time.

97%

REDUCTION IN THE NUMBER OF CVES TO FOCUS ON

NorthStar
516 N. Ogden Ave Suite 115
Chicago, IL 60642
Give us a call
312.421.3270
Send us an email:
connect@northstar.io
For more info, visit us at:
www.northstar.io

WHY NORTHSTAR?

Sometimes in life, it's the small decisions that create the biggest impact. Just because a CVE has an exploit, it does not mean it has ever been used in the wild. Don't get stuck relying on an exploit probability score that leaves you questioning where to draw the line.

NorthStar predicts the **application of exploit to a CVE** and our results are validated by industry leading threat intelligence feeds.

CVE	DESCRIPTION	CVE PUBLISH DATE	NORTHSTAR PREDICTION DATE	EXPLOITED IN THE WILD	CVSS CRITICALITY SCORE
CVE-2019-11510	In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.	**2019-05-08**	**2019-09-01**	**2020-09-17**	**10.0**
CVE-2019-19781	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	**2019-12-27**	**2020-01-15**	**2020-03-25**	**9.8**

NorthStar leverages active attacker tool imagery and all available vulnerability data to predict if an exploit will be created and used in the wild for a particular vulnerability. In the examples above, NorthStar predicted CVE-2019-11510 **386 days in advance** and CVE-2020-15505 **47 days in advance** of either being exploited in the wild.

Confidently anticipate future exploits with a definite **YES** from NorthStar Prediction Engine.

516 N. Ogden Ave Suite 115
Chicago, IL 60642

Give us a call
312.421.3270

Send us an email:
connect@northstar.io

For more info, visit us at:
www.northstar.io

NorthStar