Secureworks®

WHITE PAPER

Contextual Prioritization:

An Introduction to Ranking a Vulnerability’s Priority Based on its Unique Network Context

Introduction

There have been a few uninspired attempts to quantify the risk of individual vulnerabilities in the security community, most notably, the CVSS risk score offered by the National Vulnerability Database. Others have attempted to assign a vulnerability risk score based on factors independent of – or external to – an organization's unique network architecture. Seasoned IT and security professionals, however, understand that a vulnerability's criticality can't be meaningfully assessed without accounting for its context: where it lies in the network, what machine it's running on, how it's connected to other services and devices, if it hosts any web applications (and how large and vulnerable they are), if it's on the Internet, its importance to the business, etc. Building remediation priorities through the lens of not only external factors, but also more importantly, the specific environment in which the vulnerabilities reside, is called Contextual Prioritization.

This paper will introduce a modern approach to vulnerability risk scoring that accounts for this nonnegotiable element of meaningful vulnerability risk analysis, and consequently its ramifications for determining priorities in the remediation process.

Exploitability Prediction is Something; Context-Based Prediction is Everything

Often, the sheer complexity of IT systems, rapid changes in technology, under-staffing, and business decisions that rarely include IT and Cyber Security's input can make it very difficult for IT teams to keep up. This can result in a large number of exposed application services and an array of convoluted and misconfigured infrastructure, leaving doors open for attackers to exploit.

Certainly, robust vulnerability management is a key aspect of any serious cyber security program. It is also one of the first steps to consider for small and medium size businesses (SMBs) building a security strategy. In recent years, thanks to the disclosure of major breaches in a variety of both public and private organizations, attention to vulnerability management has become an increasingly important part of the cyber security landscape.

This increasing awareness of the risk posed by network assets vulnerable to exploitation has grabbed the attention of major vendors, driven the focus on so-called Zero Day vulnerabilities, and prompted the development of tools to predict the exploitation of these very fresh vulnerabilities. Yet, there is an argument to be made that this conventional approach is not the most effective for the vast majority of organizations.

"Priority is a function of context."
– Stephen R. Covey

Predictive exploitability – projecting which recently-discovered vulnerabilities attackers will most likely choose to exploit and assigning a risk score based on that factor alone - has been the topic of many published papers[1]. It therefore comes as no surprise that it is the current state-of-the-art in legacy vulnerability management tools. But most of the time, it is not through Zero (or even fewer) Day vulnerabilities that companies are breached. Rather, it is older, forgotten, and poorly configured resources – known

[1] https://arxiv.org/abs/1707.08015, http://users.umiacs.umd.edu/~tdumitra/blog/2015/08/02/predicting-vulnerability-exploits/#USENIX-SECURITY-2015

as "N-Day" vulnerabilities - that are exploited by well-established and easily-accessible techniques.[2]

"N-day vulnerabilities are a goldmine for attackers because the hard work has already been done. In certain cases, active exploits may already exist and be readily available from public disclosure documents. Compare this with zero-days, which are time-consuming and expensive to find and exploit — the reason why their use is declining among criminal groups."[3]

Unfortunately, the sole focus of predictive exploitability as the primary strategy for remediation prioritization continuously distracts the attention of already scarce resources.

A Question of Strategy

It's important to understand that finding vulnerabilities is not the problem. It's the "easy" part. The problem comes from the overload of such vulnerabilities encountered in a company's technology stack, and the inevitable need to manually research and prioritize low risk items before starting any remediation.

An efficient and effective remediation strategy should therefore focus on:

- Discovering and understanding what is valuable for the organization (context)
- Identifying what is a plausible target
- Filtering through this information overload
- Correcting the highest risk vulnerabilities

In reality, however, many organizations waste time and resources on esoteric vulnerabilities that may, in a vacuum, appear dangerous from the perspective of conventional predictive exploitation analysis. These seemingly critical exposures, however, may contribute significantly less risk to the enterprise when a holistic, contextual approach to prioritization is embraced. Only after addressing truly high-risk vulnerabilities should a mature organization shift its focus to resolving the vulnerabilities at the far edge of technology. In a nutshell, today's focus on Zero-Day vulnerabilities and predictive exploitability as the foundational elements of contemporary vulnerability management is flawed. Not only is the vulnerability management community's uncritical acceptance of the virtues of predictive exploitability technically unsound, it is potentially dangerous. This one-size-fits-all approach can provide enterprises with a false sense of security, or divert precious resources to low-risk remediation activities at the expense of genuinely critical ones.

[2] https://www.thehaguesecuritydelta.com/media/com_hsd/report/57/document/4aa6-3786enw.pdf
[3] "The Overlooked Problem of 'N-Day' Vulnerabilities." Dark Reading. March 2018.

There's a better way: Contextualized Prioritization. The way to do it meaningfully? Artificial intelligence.

Let's take a quick look at how this can be done to enable efficient vulnerability management that ultimately results in optimized risk reduction for the resources invested.

In a nutshell, today's focus on Zero-Day vulnerabilities and predictive exploitability as the foundational elements of contemporary vulnerability management is flawed.

Understanding Context: Scrutinize, Recognize, Prioritize

As discussed previously, most companies today face the same challenges: too many assets and not enough resources and people to address all identified security issues practically. Moreover, traditional vulnerability assessment tools generate too much data, are often off the mark, inaccurate or simply wrong (e.g. false positives). Surely, the reporting of vulnerabilities is inherently of little value if we can't put these vulnerabilities into context. Sadly, inferring context is knowingly difficult and seldom done correctly, if done at all.

But that shouldn't be the case. Understanding context is a very human and intuitive thing to do. It is also the Holy Grail of artificial intelligence. Understanding the context of an object means inferring the situation in which the object exists. More than that, it means being able to usefully relate the object and its environment.

In vulnerability management, this is much more than an academic exercise. Here, context means not only finding a security issue, but understanding the causes and implications of the issue. Context in vulnerability management includes the use of the underlying asset, the potential vectors of attack that could enter this hole, the surroundings of the asset, the business line affected by a potential breach, among other factors. To put it bluntly, it is impossible to meaningfully quantify the risk of a given vulnerability without accounting for its context.

Learning Context

...it is impossible to meaningfully quantify the risk of a given vulnerability without accounting for its context.

Unfortunately, inferring all of the specific attributes at each level of abstraction throughout an organization is a practically impossible task. But what if we could approximate this with a sufficient level of accuracy? An approach accurate enough to enable an efficient and risk-centric remediation prioritization strategy? One executed systematically, without the need for expensive consultants or a team of security experts?

The solution to this problem is to combine three areas of insight:

1. Cross-sectional Data Aggregation
2. Automated Statistical Analysis
3. Domain Expertise

One useful analogy is the impressionist style of painting. For example, take a look at Vincent van Gogh's "The Starry Night." Even though any local point is not depicting a perfectly accurate element of reality, when we take in the whole picture, it is possible to appreciate the object in perspective.

Contextual prediction works the same way. By aggregating specific facts from individual models - different remediation behaviors, comparing various naming schemes, website content and network pattern complexity, asset and tool usage - it is possible to paint a realistic picture of what should be important for a given organization. And with today's technology, all this can be accomplished without active human interaction.

Putting it all Together

After the aggregation step, we can correlate this knowledge with industry-wide practices for similar organizations, anonymized cloud-based remediation data, and human security expertise. Once this is done, we can, for example, differentiate between an interesting target and one that is surely not, which asset is underestimated or overestimated, or which has most probably been forgotten or intentionally left unresolved. We can infer elements such as network context, business line priorities, or likely or unlikely scenarios of attack. It even enables an improvement in detection reliability.

With such knowledge of the vulnerabilities and business context in hand, the path to a risk-based, efficient remediation program becomes a lot shorter.

Secureworks®

Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs.

With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp