CSW Cyber SecurityWorks

Whitepaper

Risk Based Vulnerability Management-Threat-Centric Approach

Abstract— Current practices about Vulnerability Management usually focus mainly on the technological aspects of vulnerabilities. This paper explores a more effective method for Risk Based Vulnerability Management. i.e. Threat-Centric Approach. The purpose of this research is to prioritize the threats within an organization in an effective manner. Threat centric approach has been used to evaluate the impact of the threat which helps the organization to reduce the risk against their infrastructure. The proposed work replaces the traditional approach by picking the threats in public and private sectors, prioritize it and develop the countermeasures to mitigate the risk. The proposed study also helps the organization to further strengthen their security practices to prevent cyber-attacks in the future.

Keywords—weaponization, vulnerability, threats, attack

I. INTRODUCTION

A vulnerability is only as dangerous as the threat exploiting it. A vulnerability when viewed in isolation using the traditional method of treatment based on critical/high/medium/low ratings is flawed for three primary reasons:

- Threat actors pay no attention to the scoring of a vulnerability and regularly exploit lower-ranked vulnerabilities.
- The sheer volume of vulnerabilities that organizations have to deal with makes it impractical to try to remediate all critical/high vulnerabilities.
- Not all vulnerabilities have patches or can't be patched for valid reasons, like breaking overall application functionality. This traditional method has also caused significant friction between security and IT operations teams. The two teams often have competing deliverables (security vs. uptime), and this process is compounded by the uncontrollable x-factor of threat actors.

The traditional approach of risk reduction to reduce the numbers can only be an effective means of preventing breaches if organizations' first focus is eliminating the imminent risks that can cause most significant impact on the business. Prioritizing treatment of vulnerabilities commonly targeted. by exploit kits, malware, ransomware and threat

actors, while also considering asset criticality and external

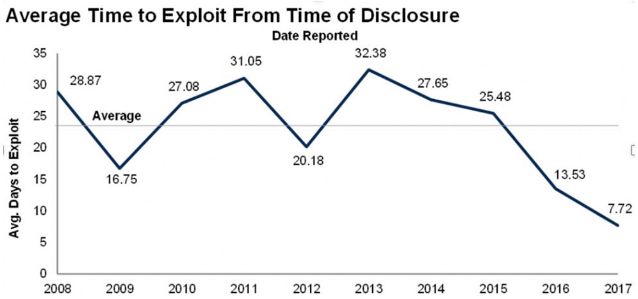

Fig. 1. Average Time to Exploit Vs Time of Disclosure (Source: Gartner August 2018)

exposure, will focus remediation on the elimination of imminent risks. This approach will result in a reduced attack surface and will provide “breathing room” for additional patch installation.

There is often a gap between the discovery of vulnerabilities and the ability and resources available within IT operations to treat these within the time frame when attackers operate. The data show (see Figure 1) that, on average, if you can’t patch or apply compensating controls in under two weeks, you are at risk of a serious breach. Threat actors know this and leverage this fact.

II. THE PROBLEM

The drive toward “Digital Transformation” is dramatically expanding the organizational attack surface with an explosion of assets. Examples include:

• Connected devices across your IT, Cloud, and IoT infrastructure

• Locks, HVAC, lighting, and other key building systems ands sensors are enterprise IoT, which 90 percent of the time are not managed by your IT team – and that’s a problem because they're on your network, and your staff / 3rd party vendors can use them to access your network – there’s numerous examples of this resulting in a successful attack (Target-HVAC, Experian-?,)

• Shadow IT results in non-approved local and cloud expansion

• Business units are often directly deploying cloud-based solutions with nothing more than a credit card

• Databases, web apps, VMs, mobile are often half internal, half in the cloud

• The problem? No consistent footprint anymore, orgs are co-managed in some cases. In some cases you don't even know what they are.

Of course, you have your IT environment where you know what's going on, right? Your server, desktop, and network infrastructure picture is becoming very complex, with multiple stakeholders, and so many moving parts, including the presence of suppliers, partners, and others on your network with whatever assets they bring in the door.

Now, on average, for each asset in an organization there are 7 critical vulnerabilities. Do the math, this adds up quickly. Many reputable studies have found that it takes about 70 days on average to remediate one of these critical vulnerabilities. And let’s not forget that we have people spending hours per week researching threat feed alarms.

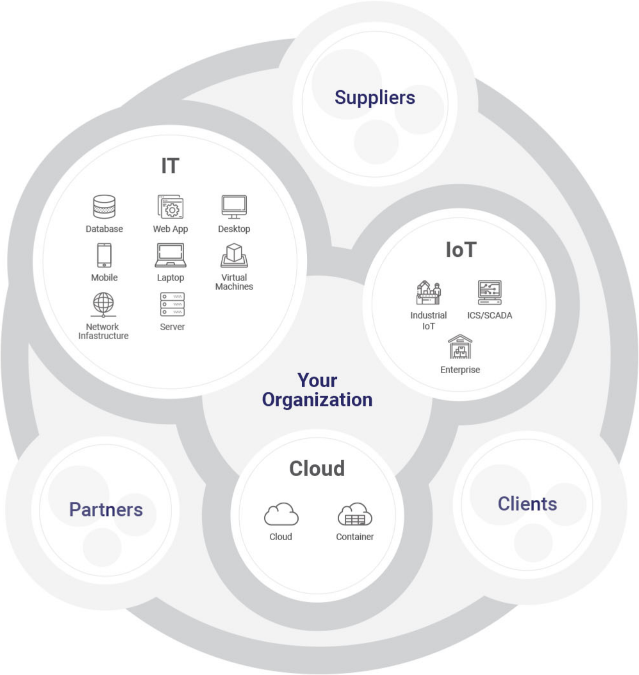

Fig. 2. Increasing IT Landscape

A vulnerability is only as bad as the threat exploiting it and the impact on the organization. Security and risk management leaders should rate vulnerabilities on the basis of risk in order to improve vulnerability management program effectiveness.

• A small number of vulnerabilities represent a disproportionately large risk to the organization, but few organizations can identify the most serious vulnerabilities.

• Organizations are confronted with the large number of vulnerabilities that are discovered by a vulnerability assessment, but have little guidance on how to reduce the risk of breaches.

• Organizations often lack a common framework and approach to vulnerability prioritization and treatment, which leads to disparate security levels across the business departments.

• Vulnerability rating schemes that don’t take into account what threat actors are leveraging in the wild can cause organizations to address less risky issues first.

• The awareness of a risk-based approach and risk analysis tools for vulnerability management is at a nascent stage. Therefore, attacks like ransomware continue to cause significant damage.

A. Typical Vulnerability Management : Unscalable & Unsustainable

So how are organizations applying people to vulnerability management? Let's walk through a day in the life, the common activities that folks engage in to gather, model, prioritize, patch, report, and communicate their cybersecurity posture.

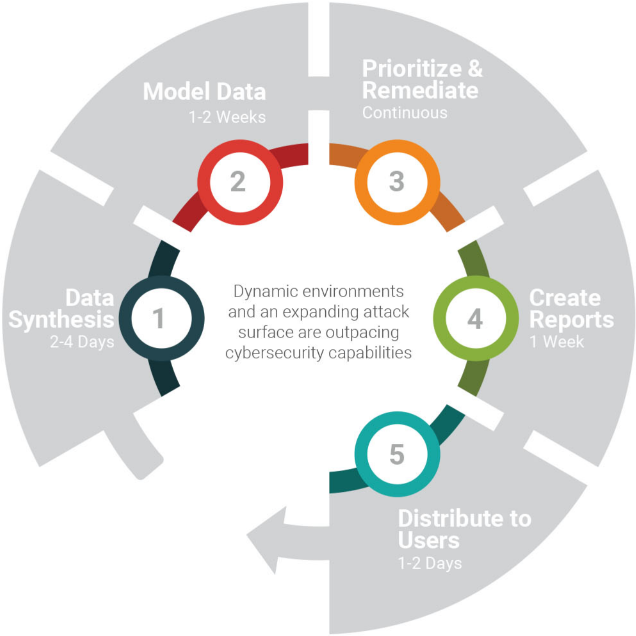

Fig. 3. Traditional Vulnerability Management Approach

- Data Synthesis

Do we have the right data? Most analysts spend 2-4 days just doing data synthesis. Gathering the data from disparate sources (network, application, database scanners, CMDB, threat intel, etc.), trying to understand what it means.

- Model Data

Once we have the data, enormous effort is expended normalizing and preparing the data for use, usually in the rage of 1-2 weeks. Remember, the data isn't all structured. Aggregation, correlation, query tuning, filter creation, visualization, defining workflows, represent a heavy lift and takes a serious amount of time to do right. Are we even looking at the data the way it should be looked at?

- Prioritize & Remediate

More of a continuous treadmill than a discreet event, it's a constant effort to perform vulnerability scans, try and prioritize what needs remediation, decide which will be patched vs. accepted, find and apply the patches, re-scan. Rinse, lather, and repeat.

- Create Reports

Usually there's a week or so of seemingly endless tweaking of reports and dashboards for multiple stakeholders.

- Distribute to Users

Last, a day or two is spent manually publishing all of these reports to the various stakeholders.

III. WEAPONIZATION

What does the world of vulnerabilities truly look like? Having a list of vulnerabilities is simply insufficient for making progress toward improving our security posture. We must be able to filter them down to a manageable and meaningful subset that provides direction as to what should be remediated first. There are 118,496 known vulnerabilities disclosed in the National Vulnerability Database (NVD). How many of these vulnerabilities are an active threat to your network?

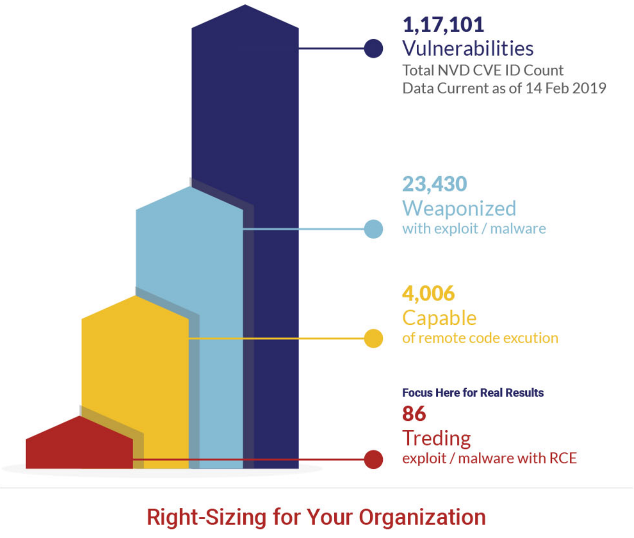

Fig. 4. Prioritization
(Source: https://risksense.com/)

If we look at which vulnerabilities that have been weaponized, meaning vulnerabilities with exploits or malware, this reduces the sample size to a large but somewhat more contained list (23,571).

Next, let's look and see which vulnerabilities in this list are capable of Remote Code Execution (RCE), as this type of exploit yields some of the highest rewards for attackers. This reduces the sample size to a smaller, more focused list (4,017). If you look at the last ten years of successful attacks, 98% of them used vulnerabilities that contained an RCE.

Now, from the list of RCE-capable vulnerabilities, further refine our view by identifying only those vulnerabilities that are trending, weaponized, and are capable of RCE (92). Trending is important because these are the vulnerabilities that are being actively used by adversaries in the wild. By focusing our attention on this important subset of vulnerabilities (less than 1/10 of a percent of all known vulnerabilities in the U.S. NVD!), we can quickly see meaningful results. But how does this corpus of known vulnerabilities relate to you and your specific business environment?

Q. What's "trending"?

A. Many data sources are considered, including:

- McAfee threat dashboard which summarizes trending vulnerabilities and threats

- AlienVault Open Threat Exchange (OTX) and IBM X-Force Exchange

- Twitter feeds, hacker forums, pen tester research, etc.

IV. THE SOLUTION

In an era where known security vulnerabilities are the leading cause of data breaches, most organizations are suffering with tools and processes that. Where does this leave us?

- Offer no/poor visibility, lack of context, and hard make it to collaborate

- Make it hard, if not impossible, to measure, manage, and control risk

- Lack meaningful prioritization and reporting to direct activities and align expectations

Let's briefly cover how can we approach managing vulnerabilities and threats to prioritize remediation to measure and control cybersecurity risk.

A. Correlation and Normalization

Consume and correlate data from tools such as Vulnerability Scanners, Application and Event Monitoring Systems, Database Security and Data Leakage Systems, Configuration Management Systems, Patch Management System, and many more.

Normalize the data and minimizes false-positives by conducting differential analysis across the different sources and unifying the data to avoid duplicates and enrich the findings.

B. Aggregation

Then, aggregate the vulnerability data provided by these sources and normalize it for common terminology, data scales, etc. mapping it to CWE, CVE, and OWASP.

C. Contextualization and Prioritization

After that, contextualize the data by correlating vulnerability relationships with multiple external threat intelligence sources (e.g., zero-day, malware, dark web, DShield, etc.), pen test results, as well as business criticality (e.g., asset classification, asset risk) delivering a complete view of the risk a given vulnerability represents to the business, expressed as a Risk Rating.

D. Risk Scoring

From this, calculate the Risk for each asset, group, and the organization itself. This facilitates both initial benchmarking and ongoing measurement, as well as meaningful prioritization of vulnerabilities and remediation activities.

E. Remediation and Tracking

Build a workflow engine or a ticketing system which allows seamless collaboration between your security and IT operations team, streamlining the remediation processes and shortening time-to-remediation dramatically.

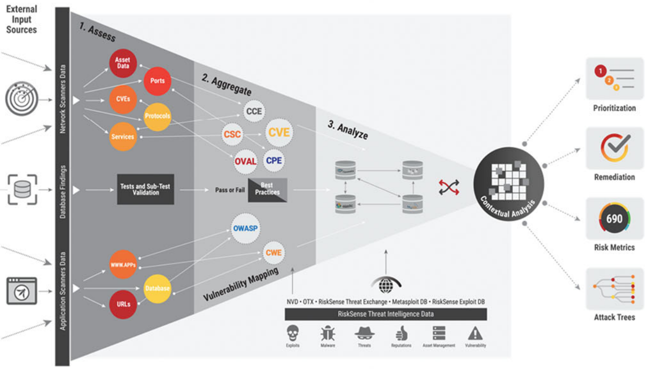

Fig. 5. Risk-based vulnerability management work flow (Source: https://risksense.com/)

V. THE CONCLUSION

The reality is that most vulnerability management programs are at an early level of maturity. So early, in fact, that they should be referred to as only "vulnerability assessment" programs instead because they are right around Level 1 (Scanning). Organizations at early levels should ask themselves where their security programs need to be and what their ultimate goal is. Is it simply being compliant? Or is it threat-centric?

It's important to understand that shifting away from a traditional approach will take time, resources, and cooperation across information security and the business. But in the end, there is a significant return on this investment.

Advancing your organization's Threat and

Vulnerability Management Program may be necessary for compliance purposes, but the process of reaching maturity yields business value far beyond your ability to "check the box." By moving through this model you will simultaneously 1) reduce your organization's risk exposure and the likelihood of the breach 2) gain ongoing visibility into your true business risk, improving future decision-making 3) align IT, information security, and the rest of your organization in the direction of strategic business goals and 4) significantly increase operational efficiency. This isn't merely an ideal model from a security perspective; it's a no-brainer for the business.

REFERENCES

[1]https://risksense.com/products/the-risksense-platform/data-integrations/

[2]https://risksense.com/products/the-risksense-platform/how-it-works/

[3]https://www.coresecurity.com/blog/the-threat-and-vulnerability-management-maturity-model

[4]https://pdfs.semanticscholar.org/39b5/6bffb6385481043974cc9f0db743057cc37b.pdf

[5]https://www.gartner.com/en/documents/3887782/implement-a-risk-based-approach-to-vulnerability-managem

CSW Cyber SecurityWorks

Cyber Security Works analysis vulnerabilities, comprehends the outcome and dynamically penetrates the networks, systems and application with our pre-eminent technology. A human hacker is recognized with precise efficacy by our patent pending technologies, it also gives proficient data mined with reliable information. We work closely with our customers and safeguard their customers from the escalating internet threats and counsel them based on all the security needs.