The Threat & Vulnerability Management Maturity Model

WHITE PAPER

Core Security
+1 617.399-6980
info@coresecurity.com
www.coresecurity.com

Organizations of all shapes and sizes, for profit and nonprofit, private enterprise and government, are facing the very significant risk that malicious individuals could breach their critical computing and data assets. And this problem is growing at an alarming rate. The 2014 PwC Global State of Information Security Survey reported the number of detected security incidents have increased 25% in the past 12 months. Similarly, the cost of security incidents increased 18% over the same time period.

This paper will introduce the Threat and Vulnerability Management (TVM) Maturity Model, along with a roadmap to take advantage of the model, as a means to manage and reduce security risk.

What is Threat and Vulnerability Management?

A formal Threat and Vulnerability Management Program is a critical component of a robust information security program. It enables an organization to understand 1) how adversaries will take action 2) what vulnerabilities exist within the organization 3) how this combination puts critical assets at risk and 4) how to manage and mitigate that risk. Generally speaking, TVM combines an understanding of the organization's assets, information technology infrastructure and systemic vulnerabilities into a coherent whole.

Breaches, Vulnerabilities, Exploits… Oh My

High profile retail organizations, restaurant chains, healthcare providers, government contractors and software companies have all been recent victims of significant security breaches. It appears that malicious actors, whether criminals, nation-states, hacktivists or disgruntled insiders, can breach any type of organization.

Although the specific mechanism for breaching security at all of these organizations varies, there are a few consistent characteristics of the modern cyber-attack. Inevitably, as we dig into these incidents, we discover that known software vulnerabilities were left unpatched, networks were exposed and sensitive business and customer data were open to attack from the Internet. These combinations create entry points and navigable paths to critical assets that are exploited by malicious actors.

As we have seen reported publicly, organizations have been breached through unintentional exposure of vulnerable systems to adversaries. This happened with Adobe, Target and Healthcare.gov, to name just a few of the many well-known breaches. In the case of Healthcare.gov, a test server that had administrative privileges was configured with a default username and password. This test server was never supposed to have network access beyond a test laboratory, but it was unintentionally connected to the public Internet. Adobe's breach was quite similar, when a network pathway from the public Internet to a Cold Fusion server was opened up without Adobe IT's knowledge. It turned out the Cold Fusion server had a low-priority, exploitable vulnerability. And the rest is history.

Most organizations have complex networks with many thousands, tens of thousands or hundreds of thousands of computer endpoints, dozens of entry points into their networks, and vulnerability reports that

are hundreds of pages long. While they may understand their networks operationally, these organizations are challenged to understand the full breadth of the threats and threat vectors they face. Without an understanding of how they will be attacked and exploited, they are unable to counter their adversaries effectively. An effective TVM program requires the ability to Think Like An Attacker™ – view your IT environment as your adversaries do.

Introducing the Threat & Vulnerability Management Maturity Model

Core Security has tremendous experience in security testing, penetration testing and vulnerability management. We have been doing this work since 1996. We have implemented several highly mature security programs for our customers over the past ten years and combined this experience to create a maturity model to advance TVM capabilities for any information security program.

The Maturity Model is a combination of asset analysis, vulnerability scanning, patch management, process implementation and metrics that enable the step by step implementation of a TVM program to meet the needs of any organization. We use a traditional Carnegie Mellon Maturity (CMM) model to understand the continuum of capability that an organization can implement. This is a significant departure from the current approach to vulnerability management, which basically calls for implementing a vulnerability assessment product, establishing a few basic measurements to prioritize patch management and includes few, if any, means of measuring the efficacy of the program. In fact, today's typical vulnerability management program will be somewhere around Level 1, perhaps Level 2, in the TVM Maturity Model (Figure 1), suffering from peak data overload and very unlikely to be able to effectively counter adversaries.

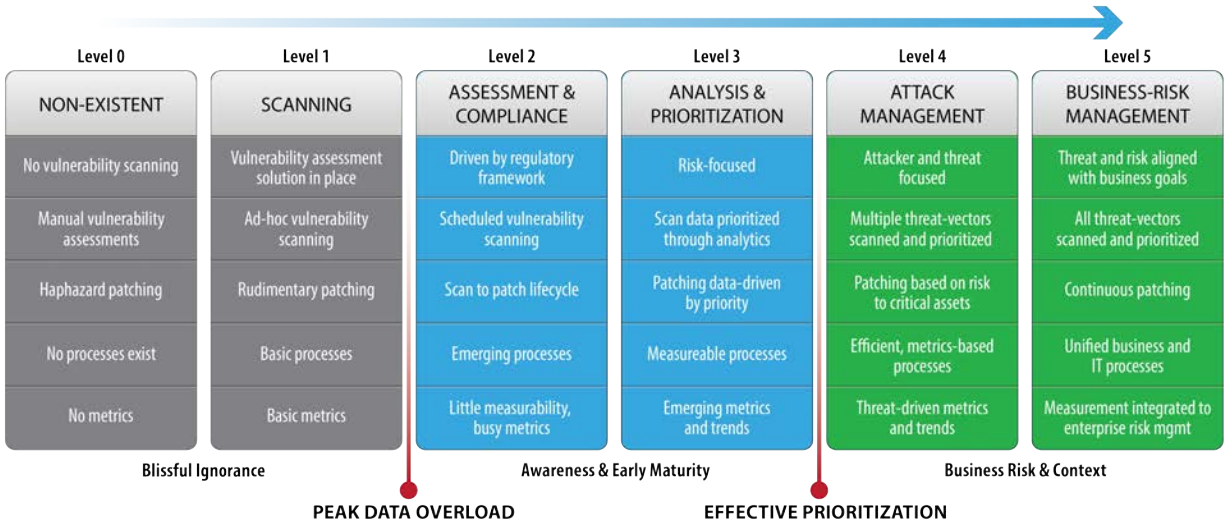

Figure 1. The Threat and Vulnerability Management Maturity Model

A Roadmap to Maturity

Reduce the Risk of a Breach

We can characterize the risk of breach as inverse to the maturity of a TVM program. The less an organization understands about who will attack them, how they will be attacked and what vulnerabilities and attack paths can be exploited to reach critical assets, the greater the chance that a damaging breach will occur. The single most effective way for an organization to reduce the risk of breach is to increase the maturity level of their TVM program.

Level 0: Non-Existent

This is the most nascent level of any TVM program. Organizations at this level have no automated vulnerability assessment (VA) solution in place; everything is done manually system by system. This, of course, is not reasonable for any but the smallest organizations. The most proactive patching at this level is the weekly "Patch Tuesday" push from Microsoft. At this level, patches are implemented on a haphazard basis, with little regard to information security.

Recommendation to advance: Acquire a vulnerability assessment solution and create processes to patch operating systems.

Level 1: Scanning

Those organizations that mature out of Level 0 into Level 1 realize several major improvements to their emerging TVM program. At this level, there is a vulnerability scanner in place, ideally covering both web and network vectors in addition to scanning for device misconfigurations. However, implementing a VA solution without first establishing some initial policies and process is like driving a car aimlessly with no destination or directions. It's relatively pointless.

To avoid scanning on a random, ad-hoc basis, it's important to start thinking about when scans should run. Should they be run on a quarterly basis? Perhaps in preparation for a compliance audit? Or maybe scans should be run more frequently as a measure to lower overall risk. Further, and arguably more important, patching efficiency and accuracy gradually becomes an issue. As more and more vulnerability data is being consumed, effective prioritization and timely remediation becomes more challenging.

Recommendation to advance: Adopt compliance frameworks, create and report metrics, implement vulnerability prioritization (probably CVE) and conduct penetration testing.

Level 2: Assessment & Compliance

The journey from Level 1 to Level 2 could be considered the most difficult adjustment, and most often where organizations become complacent. At this point, a vulnerability assessment solution is solidly in place feeding scans, most likely from multiple types of scanners from several vectors. With this new source of vulnerability data, comes the question of what to fix first – i.e. what vulnerabilities impact critical business assets and have

the particular combination of characteristics that make them dangerous. At this point, these organizations are commonly overloaded by vulnerability data to the point of paralysis. Too much data, not enough context, "busy" metrics, and insufficient prioritization capabilities leave dangerous vulnerabilities hidden in plain sight.

At Level 2, emerging processes for assessing vulnerabilities are structured around relevant compliance regulations, rather than on an ad-hoc basis. Regulations such as PCI-DSS v3.0 explicitly state that organizations under the requirements of PCI-DSS must run network scans quarterly (at least) or whenever significant changes occur in the network. This is also true for patching, which is required within one month of the patch release.

Many recent PCI-related breaches were caused by a failure to patch systems and applications for several months. Patching in a more timely fashion, as PCI-DSS requires, would have limited the scope the breach damages in these cases.

Recommendation to advance: Implement measurable vulnerability assessment and patching processes; processes should be risk-based rather than compliance based, metrics are now focused on security improvement, and penetration testing is used to validate vulnerability and patch management activity.

Level 3: Analysis & Prioritization

The move from Level 2 to Level 3 is the point where a true TVM program begins to emerge from a simple VA program. The program looks at vulnerabilities and patching as a complete ecosystem rather than separate entities. In order for this to happen, policy libraries need to be created along with formal processes for vulnerability management as a whole. Rather than a simple scan and patch methodology, a more advanced and thorough process should be considered with penetration testing used for vulnerability validation. Example: Scan → Analyze (Consolidate & Prioritize) → Patch → Validate

A risk-based approach to patching emerges to augment typical compliance patching from the previous level. This approach helps isolate and associate high-risk business assets (PCI database, PHI data, etc) to become part of the overall TVM program, ultimately resulting in a better way of managing the data overload mentioned in Level 2. However, for this to work, both information security and IT operations have to adopt tools and processes that add value to the data, consolidate scan sources and employ more advanced prioritization. This approach will alleviate data overload issues.

This level is critical not only for the reduction of data overload, but also because these metrics truly focus on improving security (vs. "busy" metrics). Prior to this level, organizations may have become accustomed to simply identifying the number of vulnerabilities scanned and patched across endpoints, network devices, applications, and systems, which is not very useful or actionable information.

Recommendation to advance: Processes move from point-in-time to continuous, enhance metrics to show trends, focus patching on risk to critical assets, introduce multiple threat vectors, introduce red team concept for formal penetration testing, adopt processes that span information security and IT operations.

Level 4: Attack Management

An organization at this stage approaches the most mature level of any TVM program. At this level of maturity, the TVM program revolves around mitigating critical asset risk and moves farther away from a compliance-driven program. The focus has shifted from patching for compliance reasons to being attacker and threat-centric. To be truly threat-centric, a selection of additional threat vectors should be adopted such as web-to-network, network, mobile, wireless, and socially engineered attacks.

Prioritization, processes, and metrics are focused on high-risk critical assets identified in the previous level. In order for this to happen, the information security and IT operations groups build processes to jointly manage the lifecycle of vulnerabilities. This newly established process is the key to establishing a closed-loop vulnerability management program, from threat identification to remediation and validation.

At this level, organizations are mostly likely to have internal Red Teams conducting regular penetration testing of high-risk applications and systems against known exploits. Information security teams will also leverage penetration testing to validate potential threats before and after they are remediated.

Recommendations to advance: Incorporate business strategy into TVM program, align information security goals with desired business outcomes, vulnerability metrics become key risk indicators, consider all threat vectors.

Level 5: Business-Risk Management

At this point, the security and IT operations teams have moved completely away from compliance-driven TVM. They have adopted a risk management framework that focuses entirely on the risk to the business and providing early warnings to the organization when threats and vulnerabilities pose risk to business performance. Business leaders are able to make informed decisions about the best means to protect their organization's assets, maintain performance, and provide a full feedback loop involving security, IT operations and business leadership.

Vulnerability and patch management is a continuous process operating on an ongoing basis with no discernible start/stop point. Data from the TVM program is integrated into all other aspects of information security and IT operations to enable near real time adjustment of security controls, network and data center management.

Formal Red Team/Blue Team or Purple Team approaches to penetration testing and validation of TVM program activity is established. External providers are used to validate internal TVM and penetration testing programs on a regular basis.

Where Do You Go From Here?

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 TVM 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.

41 Farnsworth Street | Boston, MA 02210 | USA | Ph: +1 617.399.6980 | www.coresecurity.com
Blog: blog.coresecurity.com | Twitter: @coresecurity | Facebook: Core Security | LinkedIn: Core Security