SKYBOX™ SECURITY
Total Visibility. Focused Protection.™

It's Time for a Smarter Approach: Threat-Centric Vulnerability Management

Use knowledge of your network and the threat landscape to align remediation with your biggest risks

EXECUTIVE SUMMARY

Your approach to vulnerability management may be putting your organization at greater risk. Just dealing with vulnerabilities that a vendor said were "critical" isn't enough and may still leave you susceptible to an attack. Attackers are embracing ransomware and other forms of distributed cybercrime made readily available as packaged exploit kits and services on the dark web. These attacker tools target low-hanging fruit by exploiting a surprisingly small number of vulnerabilities, many of which wouldn't be tagged as a high priority in a purely vulnerability-centric approach.

Threat-centric vulnerability management (TCVM) offers an innovative and smarter approach for your organization's vulnerability management program that will remain effective even as the threat landscape evolves. TCVM takes into account the context of your environment, including each asset's exposure and importance to your business, the details of your current vulnerabilities, your IT environment and real-time intelligence on available and active exploits. TCVM can tell if any instance of a vulnerability in your environment is already shielded by existing security controls and, if not, whether urgent action is needed to prevent exploitation. With TCVM, you have enterprise-wide visibility into the current status of vulnerabilities and the intelligence to manage them effectively. You also have the ability to immediately identify issues and task the appropriate personnel or systems with addressing them.

> **TCVM takes into account the context of your environment, including each asset's exposure and importance to your business, the details of your current vulnerabilities, your IT environment and real-time intelligence on available and active exploits.**

Given the sheer volume of vulnerabilities and assets to manage in most enterprise networks, TCVM relies on technology to automate most of the work, including data gathering and normalization, network modeling, attack vector analysis, prioritization, remediation guidance and tracking. Organizations that adopt and integrate TCVM technology will see a major return on investment.

- TCVM technology minimizes reliance on security professionals and reduces labor by operations personnel and others involved in remediation efforts.
- Most importantly, using a TCVM approach greatly reduces the chances of successful attacks that will damage your organization.

VULNERABILITY MANAGEMENT FOR A CHANGING THREAT LANDSCAPE

For many years, organizations have relied on vulnerability management tools that prioritize patching based on the relative severity of each vulnerability—largely based on estimates of the potential impact on confidentiality, integrity or availability of affected assets. Unfortunately, standalone analysis of each vulnerability isn't enough to tell security personnel how to focus efforts where they are most needed.

Even though there are thousands upon thousands of known vulnerabilities, the majority of today's attacks exploit a very small number of "popular" vulnerabilities, and attacks often target older vulnerabilities that don't get the attention of newly discovered vulnerabilities (see figure 1).[1] If you knew what the 10 most commonly exploited vulnerabilities were, you could

[1] Verizon 2015 DBIR, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf; 2016 DBIR, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

look for those in your environment and focus your remediation efforts on them. Patching just the 10 most commonly exploited vulnerabilities throughout the last ten years would have prevented exposure to hundreds of millions of instances of malware and other threats.

Old vulnerability management approaches have other significant weaknesses. They don't take organizational context into account — for example, a vulnerability with a high CVSS score [2] may not be exploitable in a particular network, because the network architecture and security policies provide sufficient defense. Or, a high-severity vulnerability that puts a low-value asset at risk is less important to fix than a moderate-severity vulnerability on a high-value asset. Hosts should be analyzed to identify potential attack vectors and account for the mitigating controls already in place. When a new vulnerability is identified, this contextual analysis should be used to determine if the existing controls provide sufficient protection or if patching or other mitigation strategies — such as changing firewall rules or intrusion prevention system policies — are needed.

[2] https://www.first.org/cvss/specification-document

Finally, vulnerability management can't neglect the "other" vulnerabilities — the ones not actively targeted in wild. These should be remediated over time because they could quite easily turn into the exploited vulnerabilities of tomorrow. Three consecutive Verizon

> **Overall vulnerability risk should be monitored and systematically addressed to minimize the attack surface and the potential impact of new threats.**

Data Breach Investigations Reports, DBIR (2015, 2016 and 2017[3]), point to the fundamental importance of a vulnerability management approach that includes ongoing patching of those other vulnerabilities. For example, in its 2016 report, Verizon states that the top 10 vulnerabilities in 2015 accounted for 85 percent of successful exploit traffic, but that security folks should not forget the other 15 percent which include more than 900 vulnerabilities that are also being actively exploited in the wild. The 2016 report also shows that

[3] Verizon 2015 DBIR, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf; 2016 DBIR, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf; 2017 DBIR, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

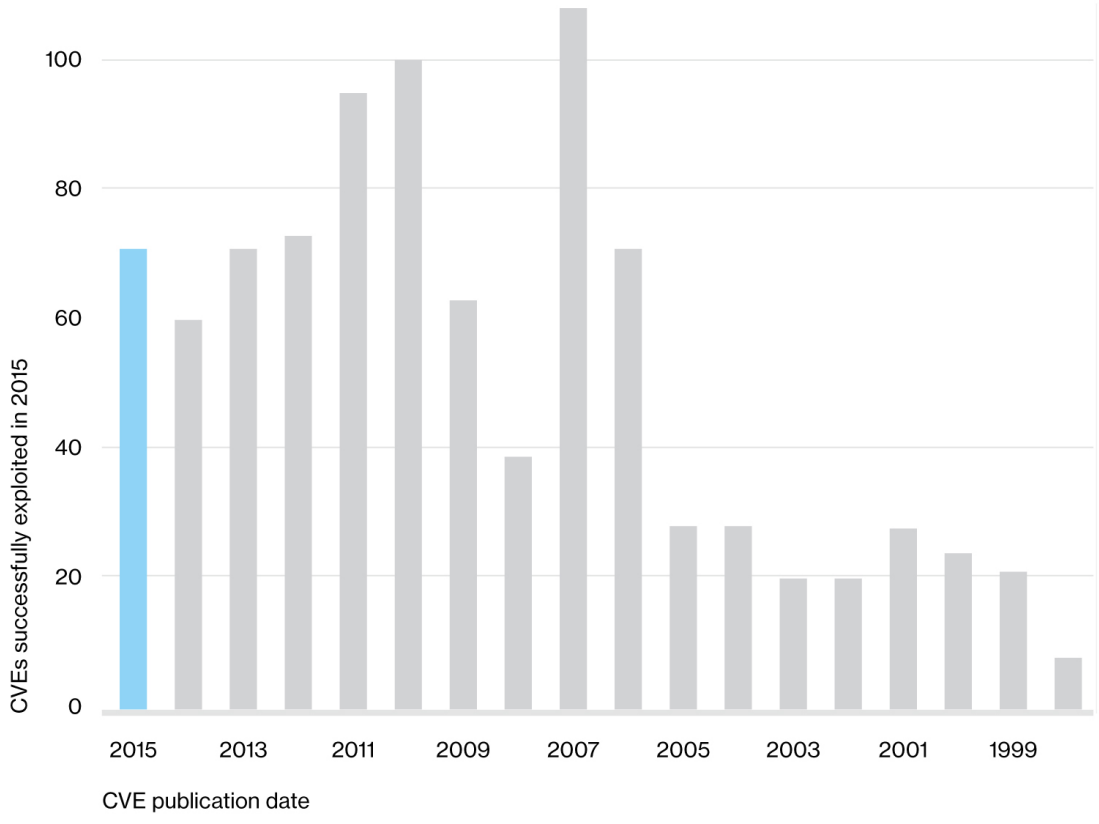

Figure 1: Count of CVEs exploited in 2015 by CVE publication date. Source: 2016 Data Breach Investigations Report, Verizon.

successful exploits in 2015 targeted a large number of vulnerabilities that were as much as five years old (See Figure 1). And, the 2017 report again affirms that "you want to fix findings before the actors start exploiting." The message: good vulnerability management happens when overall risk is monitored and systematically addressed to minimize the attack surface and the potential impact of new threats.

It's time for a smarter approach to vulnerability management. You need to rethink and revamp how your people, processes and technology work together to manage vulnerabilities, looking for a solution that will work no matter how the threat landscape changes. Fortunately, you don't have to be an expert in malware creation, attack vector analysis or vulnerability prioritization techniques to figure out how to do this.

A FUNDAMENTALLY NEW APPROACH: THREAT-CENTRIC VULNERABILITY MANAGEMENT

Old vulnerability management approaches were, for lack of a better term, vulnerability-centric. They paid attention to the relative severity of each vulnerability only. Some approaches added asset-centric techniques, which started to consider how an asset's function and exposure to attack influences the risk posed by its vulnerabilities.

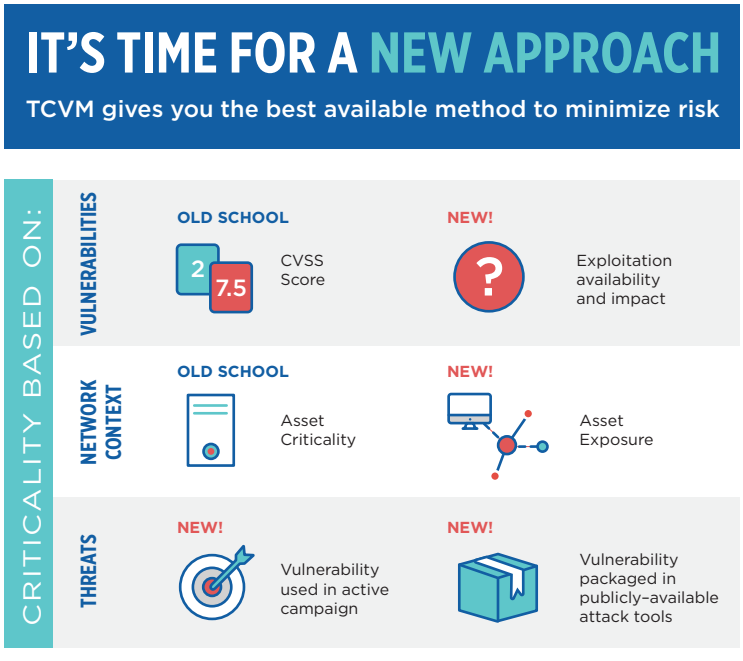

Figure 2: A New Approach: Threat-Centric Vulnerability Management

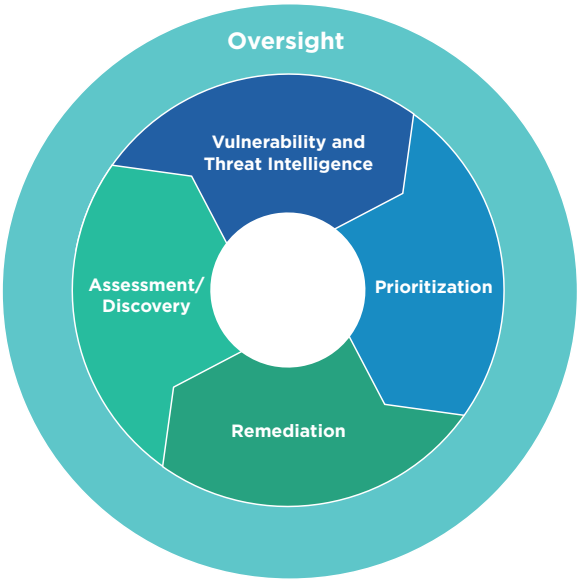

Figure 3: The five main components of TCVM

Threat-centric vulnerability management (TCVM) goes beyond these approaches by taking into account not only the characteristics of your organization's vulnerabilities, assets and topology, but also the context provided by analyzing vulnerabilities with available and active exploits correlated to your environment. TCVM also considers the characteristics of previous attacks against your organization. This establishes a much more accurate picture of the vulnerabilities that need immediate remediation and those that can be addressed later. Taking into account the context of your environment and the threat landscape will make your vulnerability management processes highly efficient and effective, with a big return on investment. TCVM has five main components (See Figure 3):

- **Assessment/Discovery:** gather data on the vulnerabilities currently within your organization's systems and incorporate them into a comprehensive model of your network and its assets
- **Vulnerability and Threat Intelligence:** use intelligence feeds and security analyst research to understand which vulnerabilities are being exploited in the wild; packaged in ransomware, malware or exploit kits sold on the dark web; or have published but inactive exploits

> Many organizations still do vulnerability management analysis and remediation planning and tracking using spreadsheets and other largely manual processes.

- **Prioritization:** starting with the model and current information on exploits and previous attacks, use attack vector analytics and simulations to understand how attacks could play out, assessing the true risk of each vulnerability in your environment and prioritizing their remediation
- **Remediation:** apply patches or other compensating controls (IPS, access rules, segmentation changes, etc.) to prevent exploitation; remediation urgency is aligned with the threat posed by each vulnerability
- **Oversight:** track remediation to ensure threats are neutralized and progress is made in reducing overall risk; monitor unmitigated vulnerabilities in case their threat level escalates

As you can imagine, there are some significant obstacles to TCVM. Identifying the enormous volume of vulnerabilities throughout an enterprise and handling the resulting complexity in assessing, prioritizing, and remediating all of those vulnerabilities is mind boggling — not to mention monitoring all of that work. TCVM is even more difficult for organizations with siloed information and processes because there is no single vantage point for the enterprise, no easy sharing of vulnerability and threat intelligence or environment context and no centralized management tools.

Many organizations still do vulnerability management analysis and remediation planning and tracking using spreadsheets and other largely manual processes. On top of all that, the threat landscape continues to evolve. For example, more than 44,000 ransomware variants were discovered in 2016.[4]

However, there are solutions to overcome these obstacles. Technology is now available to automate the vast majority of TCVM processes for you, especially all the data gathering and analysis that's incredibly time consuming for people. Automation transforms TCVM from an overwhelming challenge to something that's not only completely achievable, but is also a necessity to effectively deal with current and future threats in a large organization. Let's look at each of the TCVM components in more detail to better understand how they would work for your organization.

> Technology is now available to automate the vast majority of TCVM processes for you, especially all the data gathering and analysis that's incredibly time consuming for people.

Assessment/Discovery

Most organizations already have many potential sources of information on the current vulnerabilities in their systems. For example, your organization probably

[4] https://securelist.com/files/2016/12/KSB2016_Story_of_the_Year_ENG.pdf

Asset Coverage

Most organizations currently scope their vulnerability management processes to handle their traditional IT assets, including servers, desktops and laptops. Setting a similar scope for your organization's initial transition to TCVM is certainly reasonable. However, be aware that eventually your organization will need to include a much broader set of computing assets in its TCVM processes. Achieving a TCVM approach for your enterprise truly means having visibility over all computing assets, including cloud and virtual environments and other network zones often left out of traditional vulnerability assessments.

Two prime examples of assets often left out of enterprise vulnerability management are mobile devices and industrial control systems such as SCADA systems. Although these types of devices are vastly different from each other, they have one thing in common: they usually can't be patched using the same technologies and processes that work well for traditional IT devices. Remediation options other than patching are also usually quite limited too. This is all the more reason why TCVM is needed: to make the most of the available resources.

has an assortment of patch management systems, network–based vulnerability scanners, host–based vulnerability assessment tools, endpoint agents and other security controls that each see part of the full set of vulnerabilities.

The assessment/discovery component of TCVM heavily leverages these systems, but for TCVM to be successful, two additional things need to happen.

One is that any gaps in vulnerability discovery must be identified and corrected so that no systems or major commercial applications are left out. The other is that all the vulnerability information needs to be brought together, correlated and assessed to ensure the vulnerability inventory is as accurate and as up to date as feasible at all times. This requires the use of TCVM technology to automate continuous vulnerability data collection, correlation and analysis.

Prioritization

Prioritization is the aspect of vulnerability management where a TCVM approach makes the biggest improvement compared to earlier approaches. It uses vulnerability and threat intelligence combined with network context to understand the intersection of your environment and the exploits of the current threat landscape. To do this, TCVM vulnerability prioritization uses five types of inputs:

- **Information on your organization's current vulnerabilities.** This comes from the assessment/discovery component of TCVM discussed above.
- **Vulnerability intelligence.** This comes from extensive databases of information on known vulnerabilities for all operating systems and applications. Vulnerability intelligence is used by TCVM to better understand the implications of the organization's current vulnerabilities. Important information in vulnerability intelligence includes the availability and use of exploits for each vulnerability, the exposure of each vulnerability to threats and the potential impact on your organization if exploitation is successful, such as ransomware installation forcing a shutdown of operation, the loss of a key server disrupting internal network functionality or unauthorized access by an attacker causing a HIPAA violation.

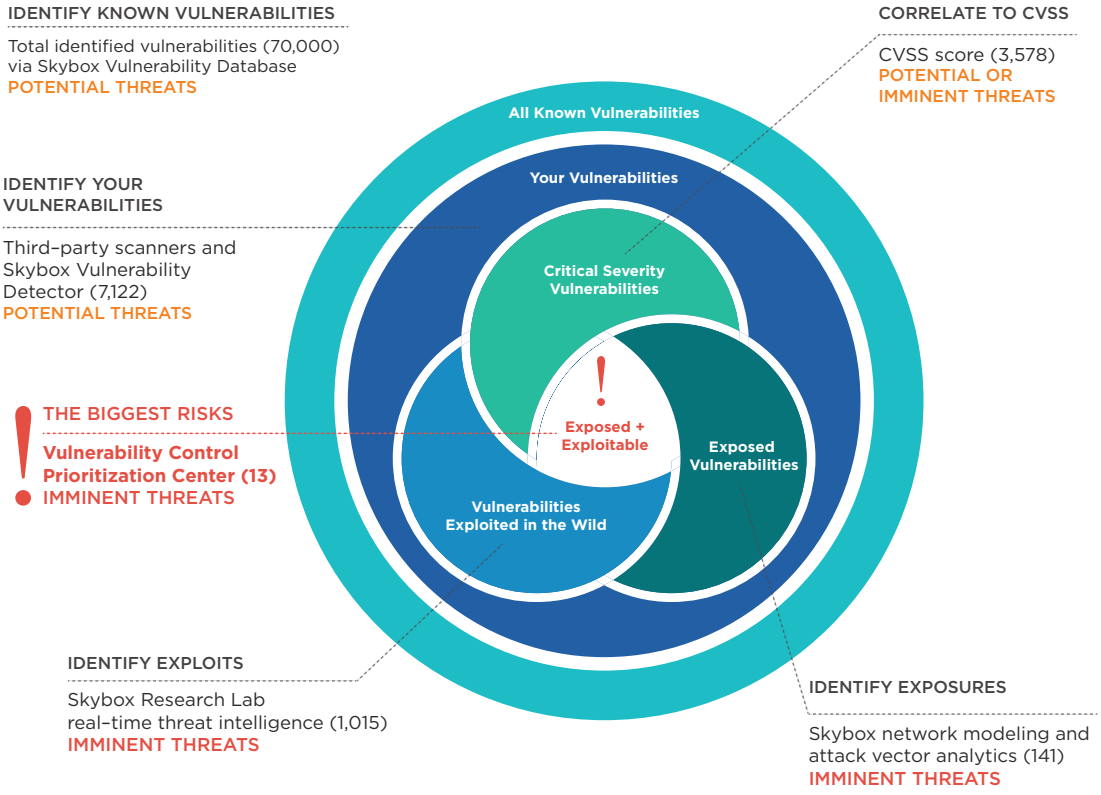

Figure 4: TCVM provides a systematic process for analyzing the thousands — even millions — of vulnerabilities in your environment (including cloud and virtual), making it possible to pinpoint those that are truly putting your organization at risk. Quickly narrow down "known" vulnerabilities that are potential threats to a smaller, manageable number of vulnerabilities that are identified as imminent threats — exposed vulnerabilities known to be exploited in the wild. In addition, TCVM enables a systematic approach for ongoing, gradual risk reduction of potential threats that could escalate in the future.

- **Threat intelligence.** Most people who are familiar with threat intelligence have experience with threat intelligence feeds that provide blacklists of IP addresses, domains, URLs or other entities associated with malicious activity. However, TCVM relies on a much deeper understanding of threats that goes far beyond simple blacklists. TCVM ingests information on the characteristics of active, in–the–wild exploits and exploits packaged in distributed exploit kits, crimeware, etc., including the geographic locations and industries being targeting by active attacks. Threat intelligence is acquired from both public and private sources on an ongoing basis.
- **Information on your organization's assets and networks.** As mentioned earlier, this information is needed to provide context for the environment around each asset and its vulnerabilities. From a security standpoint, information is needed on the composition of your organization's networks and the exposure to threats of each asset on each network, such as attack vectors and the existing security controls mitigating threats against those attack vectors. This enables TCVM to understand the nature of the attack surface for the entire organization. Also, from a business standpoint, TCVM needs to know the business criticality of each asset—how important is each asset to the mission of your organization? Knowing the network criticality of each asset is also important, such as identifying which other assets will lose network access if the asset becomes unavailable.
- **Your organization's attack history.** Information on previous attacks — both successful and failed — that exploit vulnerabilities within an environment can indicate the strength of mitigating security controls against those attacks as well as the impact of successful attacks. On a larger scale, information on previous attacks indicates which assets and software on those assets are targeted most often. Your organization can probably collect the necessary information on attack history and the targeted vulnerabilities through your existing enterprise security controls, such as your security information and event management (SIEM) system, intrusion prevention system (IPS) or endpoint protection solutions.

> **. . . intelligence based on monitoring dark web activity and validating exploit and vulnerability claims (to prevent attackers from gaming the system via false claims) can be incredibly valuable in anticipating what may be the next target for attackers.**

Ideally both vulnerability intelligence and threat intelligence should include insights from dark web research. The latest exploits and vulnerabilities often appear first

Lessons Learned from CVSS

The Common Vulnerability Scoring System (CVSS) was developed over ten years ago to help organizations prioritize vulnerability remediation. Each vulnerability analyzed for CVSS receives a set of scores that take into account the likelihood and ease of successful exploitation, as well as the estimated impact of successful exploitation. The CVSS specification defines three levels of scores: base, temporal and environmental. Base scores involve the static characteristics of a vulnerability only. Temporal scores start with base scores and factor in characteristics that change over time, such as the availability of exploits. Finally, environment scores start with temporal scores and allow an organization to take into account some aspects of the context of their own environment.

This sounds like a reasonable approach to vulnerability remediation, and it was— but it was never fully implemented. Major vulnerability databases and security software vendors invested their scarce resources into producing base scores, not into maintaining tens of thousands of temporal scores on a daily basis. Without a source of temporal scores, organizations couldn't generate environmental scores. So only base CVSS scores have been used, and understandably they've been insufficient for prioritizing vulnerability remediation. TCVM takes into account the lessons learned from CVSS as well as many other observations about vulnerability management to provide far more accurate and up-to-date assessments of the priorities for remediating vulnerabilities.

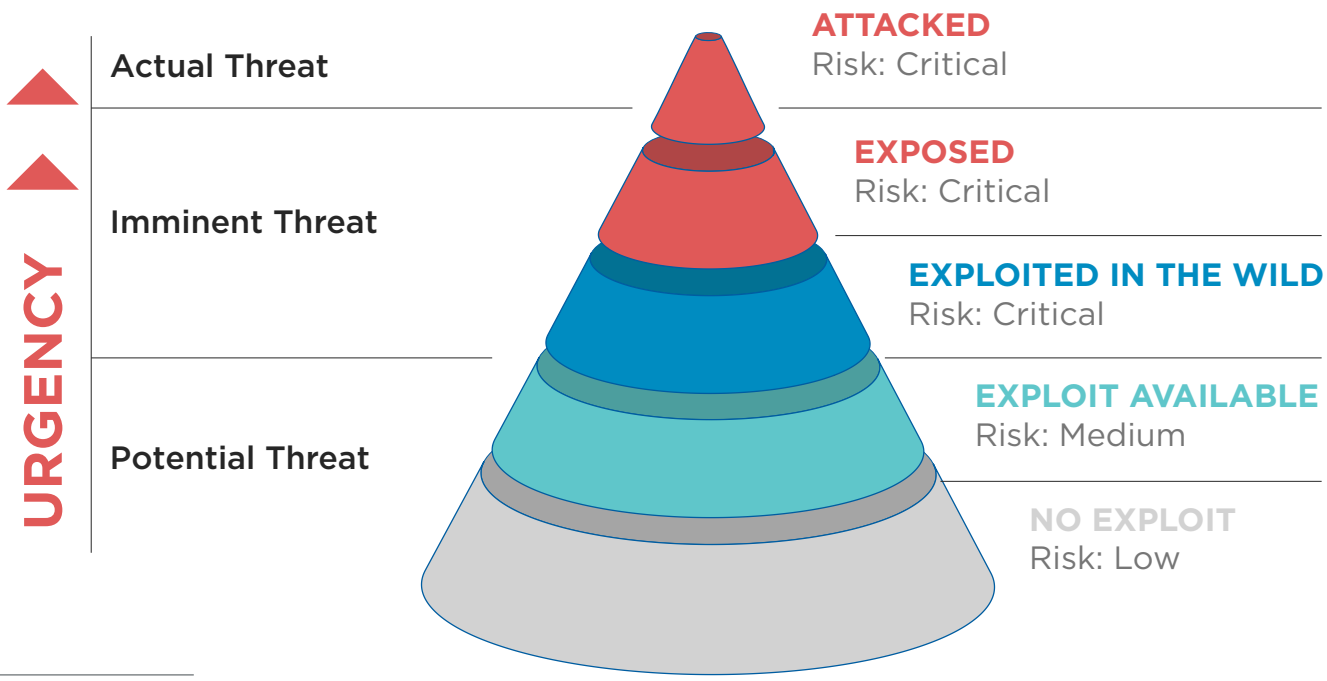

Figure 5: A New Approach:
TCVM prioritizes vulnerability according to risk of exploit.

on the dark web, so intelligence based on monitoring that activity and validating exploit and vulnerability claims (to prevent attackers from gaming the system via false claims) can be incredibly valuable in anticipating what may be the next target for attackers. Such work requires skilled and experienced researchers who can rapidly analyze threats and vulnerabilities to separate fact from fiction.

On an ongoing basis, all five types of inputs need to be correlated and analyzed to determine the true level of risk involving each vulnerability within your enterprise. This analysis, which has to take many factors into account simultaneously and weigh each factor accordingly, is not at all easy to perform. The result of the analysis is a label for each instance of each vulnerability within your organization that indicates the relative risk posed by not immediately remediating it. Your organization should adopt a simple and clear set of labels that explain the current state of exploitation and the urgency for remediating the vulnerability. Here is a possible set of labels (see Figure 5):

- **Actual threat:** Successful or failed attempts to exploit this vulnerability have already occurred or are in process on the organization's systems. Vulnerability remediation should begin immediately.
- **Imminent threat:** The vulnerability is exposed to attack based on the existing security controls and/or the vulnerability has been exploited in the wild. Vulnerability remediation should begin as soon as possible, at the latest immediately after vulnerabilities labeled as actual threats have been addressed.
- **Potential threat:** The vulnerability exists and/or an exploit has been published but not used in the wild. Vulnerability remediation should be performed based on the principle of gradual risk reduction, meaning it should be remediated after the actual and imminent threats have been addressed.

Remediation

The TCVM approach recognizes that there are many options for vulnerability remediation besides patching. For example, your organization could rely on existing security controls such as intrusion prevention systems or endpoint protection suites to stop attacks. Another option is to change network or host–based firewall rulesets to prevent attackers from reaching a vulnerable asset. In some cases, the vulnerable software itself can be reconfigured to prevent vulnerability exploitation. Or, if the vulnerable software is an old version, upgrading it to a new version may eliminate the vulnerability.

It's important to be aware of different remediation options and be prepared to use them quickly when needed instead of relying on patching alone. Patching is often disruptive to operations, requiring applications or operating systems to be restarted, unlike most other remediation options.

It's important to be aware of these options and be prepared to use them quickly when needed instead of relying on patching alone. Patching is often disruptive to operations, requiring applications or operating systems to be restarted, unlike most other remediation options. Also, installing patches on critical assets without first testing them may introduce serious operational and security problems caused by the patches themselves. In terms of speed, it would be far faster to change a single intrusion prevention signature than to patch tens of thousands of servers and end user devices. It's also important to consider that vulnerabilities are sometimes announced before patches are available, and in cases where vendors no longer support a product, patches will never become available. In these cases, using security controls to remediate the vulnerabilities is the only option.

One of the extra advantages of the TCVM approach is the value of having a comprehensive model of the organization's current attack surface. Through TCVM technology, you can see what the possible remediation options are and apply different options to see which would be the most effective and/or efficient. An attack surface model for the organization also enables you to look for unexpected consequences of remediation; for example, reconfiguring a control to block one means of attack may create a new attack vector.

Oversight

The last important component of TCVM is oversight. With so many assets and vulnerabilities, it's easy for something to be overlooked. A centralized oversight capability helps ensure 100 percent of the vulnerabilities with actual and imminent threats are remediated quickly. Organizations need to monitor and track assigned vulnerability management tasks, confirm they've been completed and escalate tasks that need to be addressed more quickly. Oversight is also needed to monitor progress on gradual risk reduction over time.

Integration Through TCVM Technology

TCVM technology integrates many kinds of analytics, which optimizes the effectiveness of each analytic technique and the efficiency and accuracy of overall analysis. In terms of preventative analytics, TCVM technology can include all of the following:

- Attack surface modeling
- Attack simulation
- Threat and vulnerability intelligence monitoring and analysis
- Correlation across numerous data sources
- Detecting previously unknown threats
- Searching for threats in archived logs
- Monitoring activities inside the network
- Investigating alerts more quickly
- Improving operations

CONCLUSION

Old vulnerability management approaches haven't kept up with changes in the threat landscape, so they've become ineffective and are wasting precious time and resources. A new approach, threat-centric vulnerability management (TCVM), takes many factors into account when prioritizing remediation within the unique context of your organization.

TCVM uses threat intelligence and network context to prioritize the small number of vulnerabilities exposed in your environment or actively being exploited in the wild. It also ensures that all other vulnerabilities are monitored and addressed over time, thus systematically reducing your organization's attack surface.

TCVM also supports multiple remediation methods, recognizing that patching isn't always the best option—or an option at all.

Your organization can establish a robust TCVM capability that complements existing investments such as SIEMs, firewalls, IPSs and more. This will generate a significant return on investment by automating as much of your processes as possible, making vulnerability management highly efficient and effective and minimizing the workload for your scarce cybersecurity professionals and operations teams.

Implementing a TCVM approach gives your organization a proactive response to threats, greatly reducing the chance of damaging attacks and data breaches. Plus, you can monitor the impact of vulnerability management throughout the enterprise, identify and react to any issues and ultimately optimize your vulnerability management performance.

Best of all, TCVM enables your organization to have a dynamic security program that can adapt as the threat landscape evolves and your organization grow

ABOUT SKYBOX SECURITY

Skybox Security arms enterprises with the broadest set of solutions for cybersecurity management. By integrating with more than 100 networking and security technologies, the Skybox™ Security Suite provides the context needed for informed and timely action, combining attack vector analytics and advanced threat intelligence to continuously analyze vulnerabilities in your environment and correlate them with exploits in the wild. This gives the insight needed to improve and automate security operations in vulnerability and threat management and firewall and security policy management.

> **Other vendors may offer different components of TCVM processes or data inputs, but they don't provide contextual insights drawn from the correlation of your environment and the threat landscape.**

Other vendors may offer different components of TCVM processes or data inputs, but they don't provide contextual insights drawn from the correlation of your environment and the threat landscape. Only Skybox brings together the technologies that make TCVM possible, including the automation of data gathering and normalization; vulnerability prioritization based on the correlation of environment data and real-time threat intelligence; and remediation guidance and tracking. Due to the breadth of the Skybox Security Suite, users can also use contextual vulnerability intelligence to improve network security tasks such as firewall change management, proactively assessing the risk of proposed changes.

Skybox has offered context-based vulnerability prioritization and management techniques since its first Skybox product in 2004. TCVM is the latest refinement of that approach, adding real-time threat intelligence to its contextual analysis of vulnerabilities.

In addition, Skybox™ Horizon, the company's award-winning attack surface visualization solution within the Skybox Security Suite, provides new capabilities to pinpoint indicators of exposure (IOEs) influenced by TCVM, including exposed, exploited and exploitable vulnerabilities. Horizon also gives security leaders insight to how their organization's security posture is improving or diminishing over time. Users can focus on specific sites within their attack surface (geographic locations, business units, cloud, etc.) and compare current and past risk levels or view trends of risk fighting progress over time.

ABOUT SKYBOX RESEARCH LAB

The Skybox™ Research Lab is the force behind the vulnerability and threat intelligence used in TCVM. This team of security analysts scours data from more than 30 leading public and private security feeds as well as more than 700,000 sites in the dark web. The result is extremely accurate vulnerability analysis based on Skybox-certified intelligence of the current threat landscape — delivered to you daily.

While many tasks of the Research Lab are automated, the human element is key. Security analysts validate and enhance data through manual analysis, bringing their knowledge of attack trends, cyber events and the tactics, techniques and procedures of today's attackers. Their ongoing investigations determine what vulnerabilities are being exploited in the wild and used in distributed crimeware such as ransomware, malware, exploit kits and other attacks exploiting client- and server-side vulnerabilities.

The Skybox Security Suite correlates the Skybox Research Lab's threat-centric vulnerability intelligence with information gathered from your environment, such as asset exposure and criticality. With insight to how the current threat landscape impacts your organization, Skybox can quickly prioritize your most imminent threats in need of immediate remediation and monitor gradual risk reduction to ensure potential threats don't escalate. Threat-centric intelligence from the Skybox Research Lab gives you an invaluable resource to take a systematic, targeted approach to fight threats, improve vulnerability management and continuously reduce your attack surface.