SafeBreach

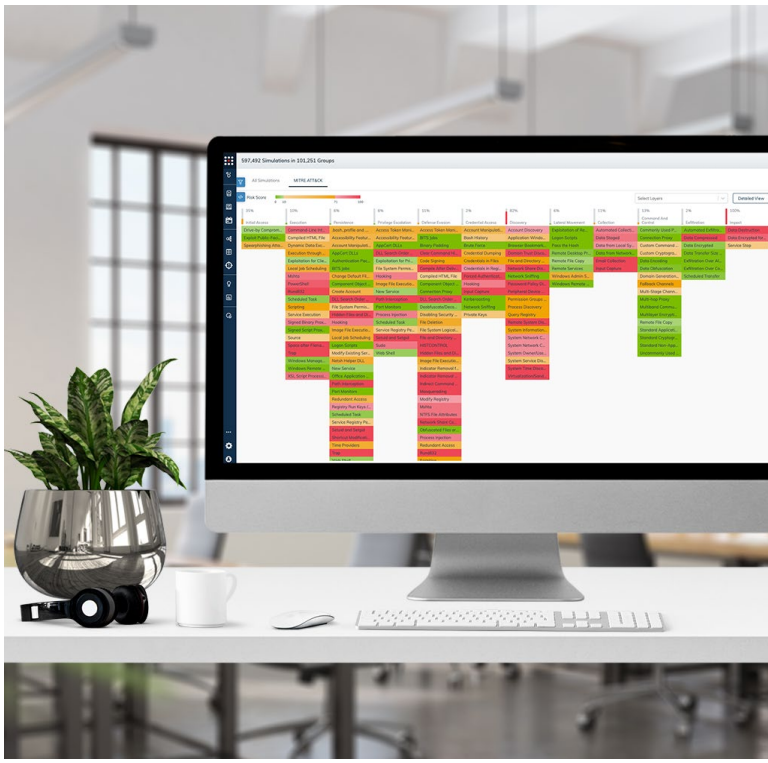
Supercharging Vulnerability Prioritization: A Risk-Based Approach

Table of Contents

Executive Summary

The biggest challenge in the vulnerability management (VM) world is prioritization. VM teams want to fix the vulnerabilities that pose the highest risk to the business first. However, while the security team might have thousands of vulnerabilities in their environment, a cyber attacker only needs one vulnerability to breach the network and get access to your critical assets. What criteria do VM teams use to determine prioritization?

Through its integration with VM tools, the SafeBreach solution can reveal the organization's actual security posture in terms of accessibility and exploitability of existing vulnerabilities. By continuously and safely executing attacks in your environment, SafeBreach calculates the risk of both network-based and host-based attacks. By combining SafeBreach insights with VM scan results, security teams can prioritize the remediation of the vulnerabilities that pose the greatest risk of accessibility and exploitation by a potential adversary. Quite simply, SafeBreach takes the guesswork out of vulnerability patching.



> **More security controls do not make your enterprise more secure.**

The Challenge with Traditional Vulnerability Prioritization

VM tools help teams understand which systems need to be patched, but they cannot help with determining which patches will have the biggest impact on the organization's security posture. Vulnerability patch prioritization is key to successful VM efforts. VM tools identify vulnerabilities but lack insights into real world threat exposure and, most importantly, lack the business-specific context needed to properly prioritize mitigation and remediation efforts.

Relying solely on VM tools, security teams lack the visibility needed to determine which network or system vulnerability can have the most impact on their security posture. For example, one vulnerability may be marked as "critical" but reside in an inaccessible location. That vulnerability shouldn't be prioritized as high as another "critical" vulnerability that is readily accessible to an external adversary. Additionally, misconfigured security controls can allow adversaries to gain access to the business' crown jewels.

The reality for most VM teams today is that there are far too many vulnerabilities across the enterprise's various tools and products. Teams cannot resolve them all. Therefore, any patch prioritization efforts must be reflective of the organization's risk exposure and tolerance. Current vulnerability prioritization approaches have several shortcomings, including the following:

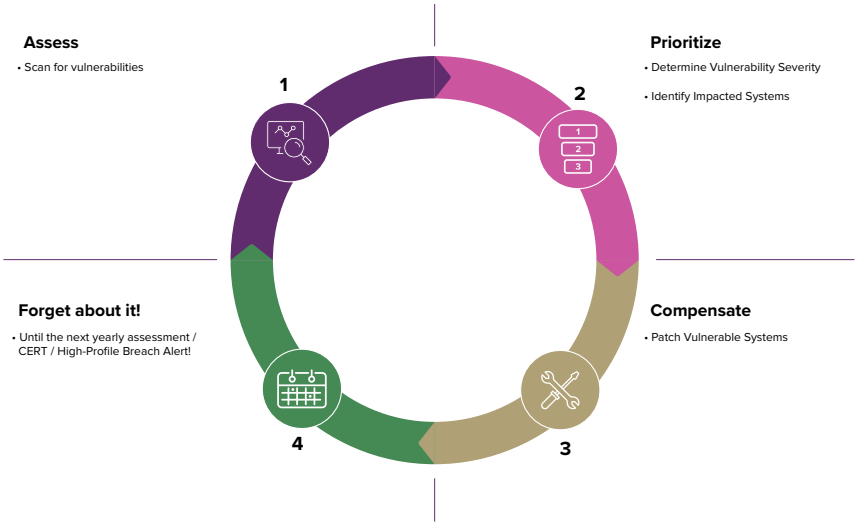
- Heavily focused on severity data alone, which leads to too many vulnerabilities being classified as critical.
- Focused on meeting compliance requirements, which leads to potential de-prioritization of exploitable vulnerabilities that may not be marked "severe" by VM tools.
- Lack of visibility into the "bigger picture." Teams have limited to no context available on business impact. For example, vulnerabilities may be classified as "non-severe" but reside at critical locations that can provide easy access to the business' crown jewels.
- Heavily focused on static, point-in-time intelligence, which means stale intelligence can contribute to incorrect prioritization.
- Reactive in nature, which means teams tend to prioritize headline-grabbing vulnerabilities for patching before other critical vulnerabilities that may pose more significant risk.

Traditional vulnerability prioritization workflows tend to include the following steps:

1. **Assess the situation**—scanning the environment for vulnerabilities.
2. **Prioritize vulnerabilities**—based on vulnerability severity (CVSS scores) and systems affected.
3. **Compensate**—patching vulnerable systems.

Then, teams tend to forget about these efforts until the next yearly assessment or the next CERT or high-profile breach alert.

Traditional Vulnerability Prioritization Workflow



Prioritizing Vulnerabilities with Threat Intelligence

A missed critical vulnerability has the potential to cause serious damage to an organization. But given the massive volume of vulnerabilities that security teams must wade through, finding that proverbial needle in the haystack can be an arduous task. Having visibility across the entire attack surface, including all security controls and configurations, is the first necessary step in identifying and prioritizing critical vulnerabilities.

Threat intelligence enhances vulnerability prioritization as it provides perspective on the vulnerabilities that are being exploited in the wild. By providing security teams with limited context into which vulnerabilities have the possibility of being exploited, this intelligence has the potential to improve vulnerability prioritization to a certain degree. However, this intelligence lacks much-needed context in terms of what impact the vulnerability can have on the organization's security posture. Given the mountainous list of vulnerabilities facing security teams, this lack of context can often lead to a flawed prioritization of vulnerabilities.

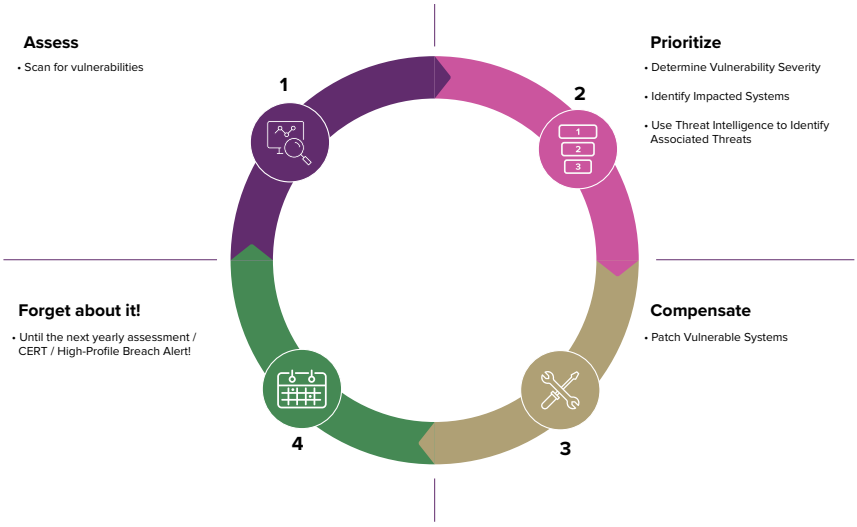
Threat intelligence can provide insights into the threat landscape, the attacks being waged, and the vulnerabilities being exploited. However, this intelligence can go stale very fast. Threat Intelligence often provides **in-the-moment context** to help security teams prioritize vulnerabilities, but it may not always be enough.

Threat intelligence-powered vulnerability prioritization workflows include the following steps:

1. **Assessing the situation**—scanning the environment for vulnerabilities.
2. **Prioritizing vulnerabilities**—based on vulnerability severity, affected systems, and threats associated with those vulnerabilities, regardless of compensating controls.
3. **Compensation**—patching vulnerable systems.

Then, teams tend to forget about these efforts until the next yearly assessment, the next CERT alert, or the next high-profile breach alert.

Threat Intelligence Powered Vulnerability Prioritization Workflow



Prioritizing Vulnerabilities with Machine Learning and Artificial Intelligence

To help teams overcome some of the challenges with vulnerability prioritization, namely sifting through large volumes of vulnerabilities to identify those that are most critical, VM tool vendors have started using machine learning algorithms. Through machine learning, tools can help teams identify the highest priority vulnerabilities that need to be patched first.

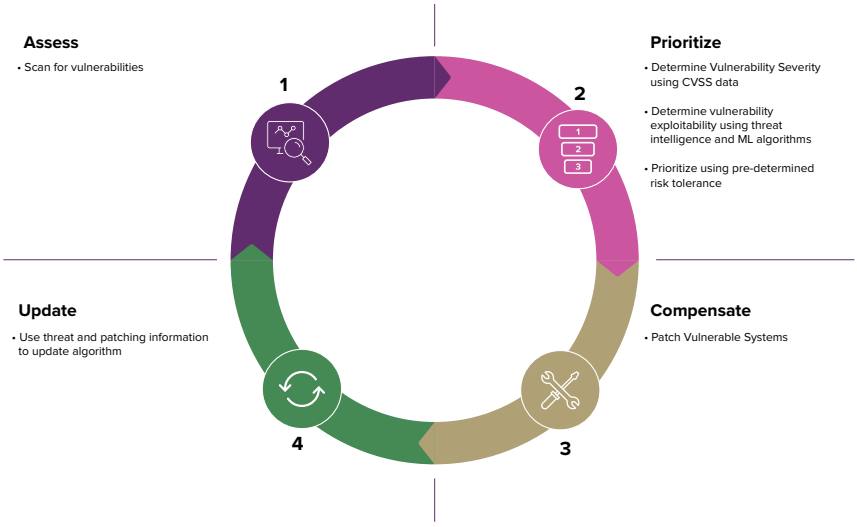
This approach makes sense when there is a large amount of past vulnerability data available that can be used to refine algorithms and identify the tell-tale signs of a highly exploitable vulnerability. However, this approach requires a lot of initial staff intervention to ensure that the algorithms employed are appropriately and accurately prioritizing vulnerabilities based on what information is available at that moment, including the latest threat intelligence.

What this approach primarily lacks is the enterprise's environmental context—including the effectiveness of security controls and the external accessibility of the crown jewels. Additionally, these machine learning algorithms depend on probability models that intend to predict the exploitability of a particular vulnerability. However, because these tools lack environmental context, they can potentially generate false negatives or false positives, causing security teams to miss important issues or waste their time and efforts in patching vulnerabilities that may not need patching right away.

Machine learning-powered vulnerability prioritization workflows include the following steps:

1. **Assessing the situation**—scanning the environment for vulnerabilities.
2. **Prioritizing vulnerabilities**—based on vulnerability severity and algorithm-ranked vulnerability likelihood.
3. **Compensation**—patching vulnerable systems.
4. **Updating algorithms** for future use.

Machine Learning Powered Vulnerability Prioritization Workflow



Using a Risk-Based Approach for Vulnerability Prioritization

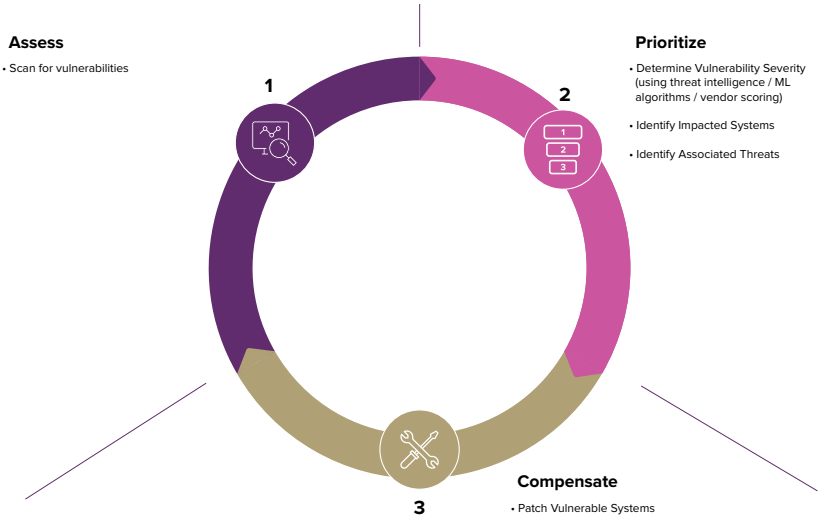
A vulnerability is only as bad as the threat exploiting it and its impact on the organization. Vulnerabilities should be rated/prioritized based on risk to improve VM program effectiveness. By not considering the business risk, teams may ignore an easily exploited, "low priority" vulnerability that can potentially cause more damage than a "high priority" vulnerability that may be more difficult to exploit. Risk-based vulnerability management (RBVM) is an approach that seeks to address these limitations.

RBVM is the process of organizing and prioritizing vulnerabilities based on the level of risk they pose to an organization's specific environment and security posture. RBVM elevates the traditional VM approach by mapping specific business risks to the vulnerabilities and exploits in systems. This allows security teams to focus on vulnerabilities that are at the highest risk of being exploited. Using a risk-based approach for vulnerability prioritization allows security teams to:

1. Understand how current threats can impact their specific organization and security posture.
2. Identify ways to prioritize remediation of vulnerabilities based on their business impact.

However, this approach also fails to take into consideration the existing security infrastructure and controls in place and the level of protection they offer. As the threat landscapes change, security controls get updated. So, a severe vulnerability that is protected by an existing security control should not be prioritized over a vulnerability that is not protected. This is one of the biggest shortcomings of using RBVM to prioritize vulnerabilities. To be complete and effective, RBVM needs to consider the organization's security controls and protections, and the overall attack surface across the organization. The diagram below offers a depiction of a typical RBVM workflow.

Typical Risk Based Vulnerability Prioritization Workflow



Compared to traditional approaches, RBVM offers the following benefits:

1. **Allows for vulnerability prioritization specific to an organization's risk tolerance.**
2. **Enables security teams to map their specific business risk to the current threat landscape.**
3. **Goes beyond compliance by enabling continuous risk prioritization based on current business needs.**
4. **Enables security teams to make informed decisions between patching and compensating controls.**
5. **Empowers teams to take a proactive approach.**

Using SafeBreach's Unique Perspective to Supercharge Risk-Based Prioritization

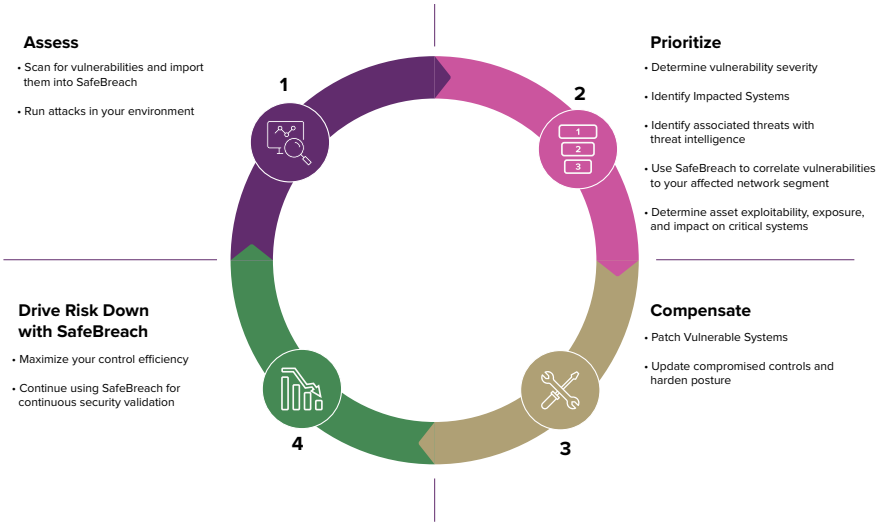
As mentioned above, the biggest drawback of an RBVM approach to prioritization is its lack of context related to an organization's security controls and their ever-changing configurations. The team at SafeBreach understands the critical importance of gaining contextual visibility into our customers' specific security controls and environments. This visibility is critical to enabling security teams to understand which vulnerabilities pose the biggest risk to their business.

Security teams must remember that there isn't a one-size-fits-all approach to organizational security posture and vulnerability management. A lower-ranked vulnerability that gives an attacker direct access to an organization's crown jewels must automatically become a high priority for a security team. To mitigate an attacker's advantage and secure enterprise assets, it is critical for teams to map attackers' intent (threat) and their ability to exploit existing defenses (vulnerability) to the specific business risk.

SafeBreach can safely and continuously validate an organization's security controls against real attacks to determine asset exploitability and accessibility. By continuously validating security controls and mapping the external accessibility of critical assets to business risk, security teams can gain the context they need to make smart prioritization decisions. SafeBreach allows security teams to effectively manage their security posture by:

1. Understanding the overall attack surface for the vulnerability
2. Determining the overall accessibility of the vulnerability
3. Assessing the impact of the vulnerability on their organization's critical assets
4. Determining adversaries' potential reach within their organization, considering the risk of vulnerability exploitation

Risk Based Vulnerability Management with SafeBreach



Using SafeBreach to Add Environment Specific Context

SafeBreach's integration with VM tools sheds light on the actual posture of an organization's environment in terms of accessibility and exploitability. By continuously and safely executing attacks in an enterprise environment, SafeBreach calculates the risk of both network and host attacks. By combining SafeBreach's contextual insights with vulnerability scan results, VM teams can focus the vulnerability remediation process on the locations that have the greatest risk of exploitation by a potential adversary.

SafeBreach enables teams to take a risk-based approach that provides prioritization accuracy with added context, including the likelihood of exploitability based on the validated, actual capabilities of their environment. In this way, security teams can get realistic visibility into the risk posed by vulnerabilities in their organization. This allows them to focus on threats and vulnerabilities that matter the most and ensure an appropriate response.

SafeBreach enhances RBVM by enabling security teams to:

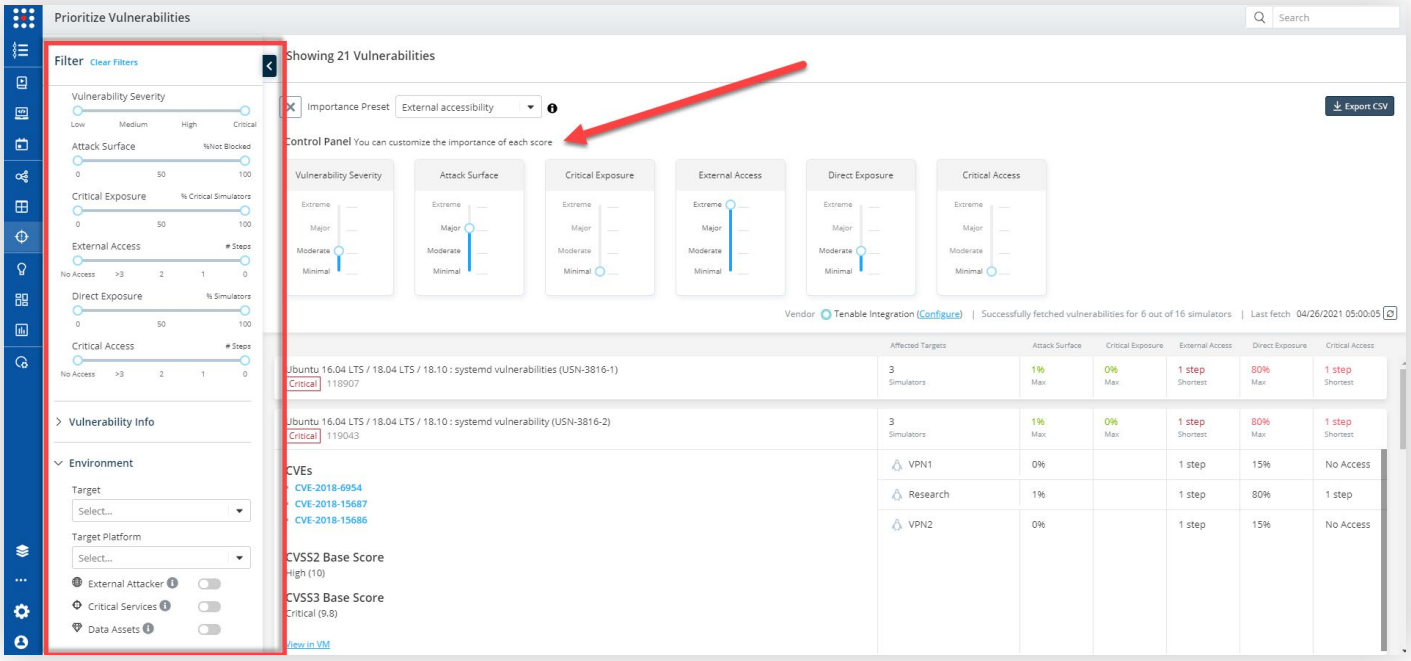
- Prioritize vulnerabilities using context based on security control effectiveness and crown jewel exposure—all validated by SafeBreach's attack simulations.
- Customize prioritization to accommodate their organization's changing security requirements.
- Communicate and share prioritization criteria and data between different teams.
- Continuously validate security controls and configurations to provide real-time contextual insight into their effectiveness against attacks.
- Make informed decisions regarding whether to patch vulnerabilities or update security controls to compensate.
- Provide the visibility and intelligence decision makers need to optimize their organizational security posture and security spending.
- Continually test their defenses, including before and after patching, to ensure maximum levels of protection.

Prioritizing Critical Vulnerabilities Using the SafeBreach Platform

The SafeBreach platform can be integrated with several market leading VM tools, including those from such vendors as Qualys, Rapid7, Tenable, and more. Through these integrations, SafeBreach can import vulnerabilities detected by the VM tool. By safely executing attacks within your environment, SafeBreach allows security teams to identify the most critical risks and the steps required to remediate them.

The solution safely executes thousands of attacks, testing all steps of a potential attack lifecycle. SafeBreach empowers security teams to establish an intelligent, data-driven way to prioritize vulnerabilities based on the specific risks to their business. Security teams can focus their patch management efforts on the specific locations and security controls that have the greatest risk of exploitation by attackers. Further, SafeBreach allows teams to revalidate their security controls after remediation efforts to ensure critical vulnerabilities have been eliminated. Rather than simply providing generic data about known vulnerabilities and threats, SafeBreach helps teams find out exactly where their most critical vulnerabilities are.

SafeBreach provides an intuitive, easy-to-use interface that makes it simple for operators to identify, filter, and prioritize which vulnerabilities pose the biggest risk to their business. SafeBreach automatically augments vulnerability data with SafeBreach risk scores, based on the results of attacks run on the affected targets.



Vulnerability Prioritization in the SafeBreach Platform

Security teams can easily filter vulnerabilities based on SafeBreach risk scores, vendor-provided severity scores, and target environments. After narrowing down the vulnerabilities, security teams can prioritize based on their specific risk tolerances and requirements, enabling faster patch management.

Security teams can either use the preset prioritization criteria included within SafeBreach or they can completely customize how they prioritize vulnerabilities. Vulnerabilities can be prioritized using the following criteria:

- **External accessibility**—This preset allows security teams to prioritize vulnerabilities based on how easily they can be accessed by an external adversary. Any assets on the network perimeter that can be easily exploited using a minimal number of steps can be identified to be patched first.
- **Nearby exposure**—This preset allows security teams to prioritize based on the number of exposed targets that surround a vulnerable crown jewel. The higher the number of exposed surrounding targets, the higher risk to critical assets.
- **Critical target proximity**—This preset allows security teams to prioritize based on vulnerabilities that appear on assets offering direct attack paths to their organization's crown jewels.
- **Custom Prioritization**—If none of the presets match their organization's risk tolerance, security teams can further customize prioritization based on what is important to them, including:
    - Severity of the vulnerability
    - Likelihood of a vulnerability being exposed to an exploitation
    - Prevalence of a vulnerability among your critical assets
    - Likelihood of a vulnerability being exploited by an external attacker
    - Likelihood of a vulnerability being exploited internally
    - Likelihood of exposure of your critical assets following an exploitation of a vulnerability

By allowing security teams to prioritize vulnerability patching based on the level of business risk they pose, the SafeBreach platform allows security teams to create a dynamic, adaptable security posture that is proactive and allows the organization to withstand a wide variety of threats while ensuring business continuity. In addition, the reports of prioritized vulnerabilities can be viewed or exported to external systems, where they can be augmented with other risk and prioritization data. The SafeBreach integration is fully automated, allowing the platform to interact with several of the leading VM tools and their APIs.

Conclusion

By integrating security control validation data from SafeBreach with data from VM tools, CISOs and VM teams can gain the complete picture they need. This combination enables RBVM that is based on the organization's actual—and current—security configuration and posture. Most importantly, it helps security teams focus on what really matters at any given moment. This can make a substantial difference in the organization's protection strategy and its overall security posture.

SafeBreach

Schedule a Demo Today

contact@safebreach.com

Here