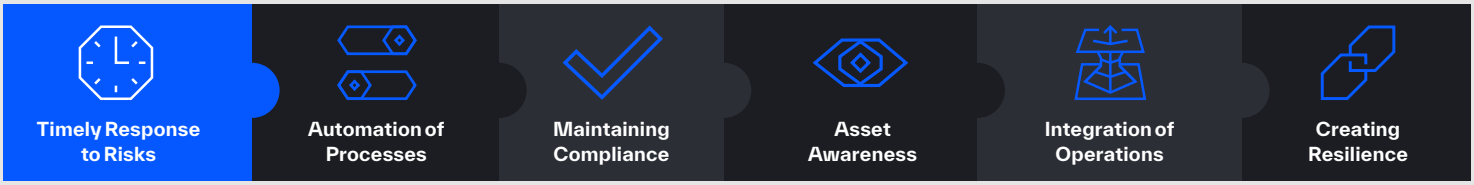
Advisory Spotlight Series

Overcoming Security Program Challenges

Developing the strategies and capabilities to address CVE's is an important step toward better defending your organization from data breaches. It's only a piece of the puzzle however, and complements a number of other challenges faced by defenders.

This spotlight is the first in a series on overcoming common security program challenges. Read all the currently published spotlights at www.bluevoyant.com.



Challenge 1: Timely Response to Risk

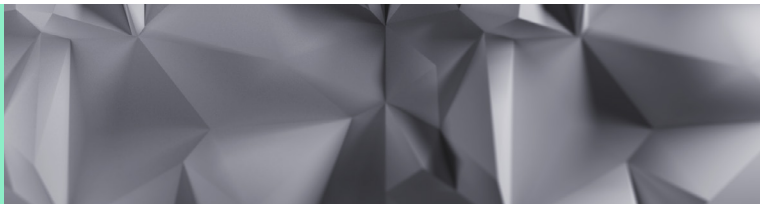
Actioning CVE Data: How should you be thinking about CVEs as a security practitioner?

A Common Vulnerabilities and Exposures (CVE) entry represents a publicly known security vulnerability or exposure in software or hardware. Managed by the CVE Program, sponsored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), these entries provide a standardized method for identifying and cataloging vulnerabilities to improve the speed and efficiency of security responses. Each CVE entry receives a unique identifier, which aids organizations in tracking and addressing specific vulnerabilities across different systems and platforms.

While CVEs facilitate faster and more efficient security responses by providing unique identifiers for tracking vulnerabilities, they also pose challenges related to volume, response times, and prioritization. This article presents a strategic approach to help security practitioners effectively manage CVEs, enhancing security without being overwhelmed by complexity.

Common Challenges with CVEs

Organizations, particularly smaller ones, often struggle to keep up with the pace of discovery of new vulnerabilities. This challenge underscores the need for efficient processes to manage, patch, and mitigate these vulnerabilities. Limited resources, both in terms of personnel and budget, exacerbate the issue, leaving many organizations vulnerable to exploitation. Additionally, the complexity of modern IT environments, with a diverse array of software and hardware components, makes it difficult to prioritize and address vulnerabilities effectively. As a result, organizations must adopt strategic and scalable approaches to vulnerability management to safeguard their systems and data.



Volume and Frequency

Response Time

Prioritization

1. Volume and Frequency of CVEs

The volume of CVEs reported annually presents a formidable challenge. With thousands of vulnerabilities discovered each year, organizations face difficulties in keeping up, especially smaller companies that may lack the dedicated cybersecurity resources available to larger enterprises. In 2023, over 28,000 vulnerabilities were reported, with that number rising sharply to over 40,000 in 2024. All of this underscores the growing scale of the challenge for companies trying to patch, monitor, and mitigate risks effectively.

Compounding this issue is the fact that not all vulnerabilities are created equal; some may have immediate and severe implications, while others pose minimal risk. The rapid pace of technological advancement further complicates the landscape, as new software and hardware releases can introduce unexpected vulnerabilities. This dynamic environment necessitates not only an efficient process for addressing known vulnerabilities but also a proactive approach to anticipate and defend against emerging threats.

2. Response Times

When a CVE is disclosed, it initiates a race between attackers and defenders to address the vulnerability. The speed at which organizations can respond varies significantly based on the maturity and readiness of their security operations.

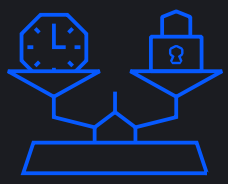
This delay between disclosure and response can provide attackers with a critical window of opportunity to exploit the vulnerability, often even before a full CVE entry is published. Consequently, the need for rapid and efficient action is paramount to prevent potential exploitation and mitigate risks effectively.

3. Prioritization and Resource Allocation

Not all CVEs present the same level of risk, so effectively prioritizing vulnerabilities is essential. Factors like severity scores, exploitability, potential impact, and specific threat contexts need to be considered. The Common Vulnerability Scoring System (CVSS) provides a standardized severity score for each CVE, but prioritization can still be complex and challenging, especially as severity does not always equate to immediate risk. Companies often lack the resources to address every vulnerability, requiring robust processes to identify, prioritize, and address those that pose the highest potential impact.

To enhance prioritization, organizations can incorporate threat intelligence feeds and real-time data analytics to better understand the active exploitation trends and align their efforts with the most pressing threats. Additionally, fostering collaboration between IT and security teams can ensure that vulnerability management aligns with broader business objectives and risk management strategies.





Actioning CVEs: Patch Management and System Downtime

While CVEs are essential for identifying risks, patching or remediating the vulnerabilities they highlight isn't always straightforward. Companies must balance the need for security with the potential disruption of system updates or downtime. Applying a patch may lead to compatibility issues or interrupt mission-critical services, which can deter organizations from rapid or automated implementation. Delays increase the opportunity a cyber threat actor can take advantage of an exposed vulnerability and increases the risk of exploitation.

To mitigate these challenges, organizations can implement a phased approach to patching, testing updates in controlled environments before wider deployment to ensure compatibility and minimize disruptions. Additionally, leveraging automated patch management tools can streamline the process and reduce human error, while maintaining a backup and recovery plan can further safeguard against potential negative impacts of patch deployment.

Alternative Options for Addressing CVE Challenges

To manage CVE-related challenges, organizations are employing several strategies, combining technical solutions with policy improvements. These include:



Automation

Automated vulnerability management systems that regularly scan for, identify, and prioritize vulnerabilities can be an option for companies. These tools can streamline the detection and prioritization process, often integrating with patch management systems to automate updates.



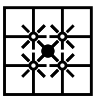
Third-Party and Cloud Solutions

For many companies, using third-party management or patching services, or shifting to cloud providers with robust patching and security measures already incorporated into their service reduces the burden of manual updates. Cloud providers typically handle patches for their infrastructure, which can streamline an organization's vulnerability management efforts.



Risk-Based Prioritization

Adopting risk-based prioritization frameworks that go beyond CVSS scores to consider business impact, exposure, and exploitability can help focus on the most pressing threats. By focusing on the vulnerabilities most likely to be exploited in their specific context, companies can make more effective use of limited resources.



Cross-Department Collaboration

Recognizing that cybersecurity is an organization-wide responsibility, companies are fostering collaboration between IT, cybersecurity, and other departments. This approach enhances CVE response, as cross-functional teams can offer diverse perspectives on risk and operational impact, leading to faster and more informed decision-making.



CVE's as applied to Third Party Cyber Risk

BlueVoyant works with enterprise and government organizations to help incorporate CVE analysis into their security programs, both for internal security as well as third party cyber risk. Experience has confirmed that CVE management is not an isolated task, but a vital component of a comprehensive cybersecurity strategy.

The BlueVoyant approach integrates automated analytics and analyst validation with a planned and well-enacted strategy to enhance the detection and management of vulnerabilities.

Volume and Frequency

Response Time

Prioritization

1. Volume Solution

It's important to determine whether a CVE directly affects your organization or its vendors. Focusing on relevant vulnerabilities will help you streamline the management process, making it easier to handle the sheer volume of CVEs reported annually. This targeted approach reduces the noise and helps organizations concentrate on the most pertinent threats.

2. Response Times Solution

As the disclosure of CVEs starts a race condition, it's important to be as responsive as possible against the publication to counter and deter threat actor exploitation of the vulnerability. Using predictive modeling and incorporating the results it generates into your program's SOC or TPRM solution have proven to help reduce the window of exposure and mitigating risks more effectively. BlueVoyant leverages a "CVSS Score Predictor" that enhances response times by accurately predicting potential vulnerabilities before they become widespread threats. This rapid awareness enables all parties to take timely and coordinated action, further minimizing the risk of exploitation.

3. Prioritization and Resource Allocation Solution

It's important to have insights into how vulnerabilities impact your organization's supply chain, to include assessing risks based on vendor connectivity. Using this information, you can prioritize CVEs not just by severity scores, but by understanding the actual business impact and exploitability within their specific context. By aligning vulnerability management with business objectives you can allocate resources more efficiently and effectively.



An Additional Solution: Maintain a CVE Catalog

With NIST no longer managing this task, maintaining a CVE catalog has become increasingly important. This in-house CVE catalogue should include data points associated with all CVEs detected, including their CVSS scores, severity and a way to notify if the CVE is included on the KEV list (Known Exploited Vulnerabilities). Some key data points to include in the CVE catalogue/library:

- List of all CVEs detected and number of monitored third parties impacted
- List of impacted companies and when the CVE was Last Observed
- List of all assets for each company impacted by the CVE
- Ensure continued reference to official CVE updates and publications

The practice assists with and simplifies all the other challenges associated with CVEs: volume, response, and prioritization.

Conclusion

CVE management is a complex yet essential part of cybersecurity that necessitates a balanced approach, combining automation, prioritization frameworks, and organizational collaboration. As the volume of CVEs continues to rise, organizations must refine their vulnerability management strategies to remain resilient against evolving threats. By proactively addressing these challenges, companies can create a secure technology environment capable of withstanding modern cyber pressures.

As part of a broader cybersecurity program, effective CVE management is crucial for safeguarding organizational assets as well as the many third parties in your extended ecosystem. By adopting a balanced approach that integrates automation, strategic prioritization, and collaboration, companies can build resilient processes capable of adapting to the evolving threat landscape. Proactively addressing CVE challenges is essential for maintaining a secure and resilient technology environment, capable of withstanding the pressures of modern cyber threats.



BlueVoyant delivers a comprehensive cloud-native security operations platform that provides real-time threat monitoring for networks, endpoints, and supply chains, extending to the clear, deep, and dark web. The platform integrates advanced AI technology with expert human insight to offer extensive protection and swift threat mitigation, ensuring enterprise cybersecurity. Trusted by more than 1,000 clients globally, and the 2024 Microsoft Worldwide Partner of the Year, BlueVoyant sets the standard for modern cyber defense solutions.

