S|3 SPECIALIZED SECURITY SERVICES

BUILDING STRATEGIC RESILIENCE

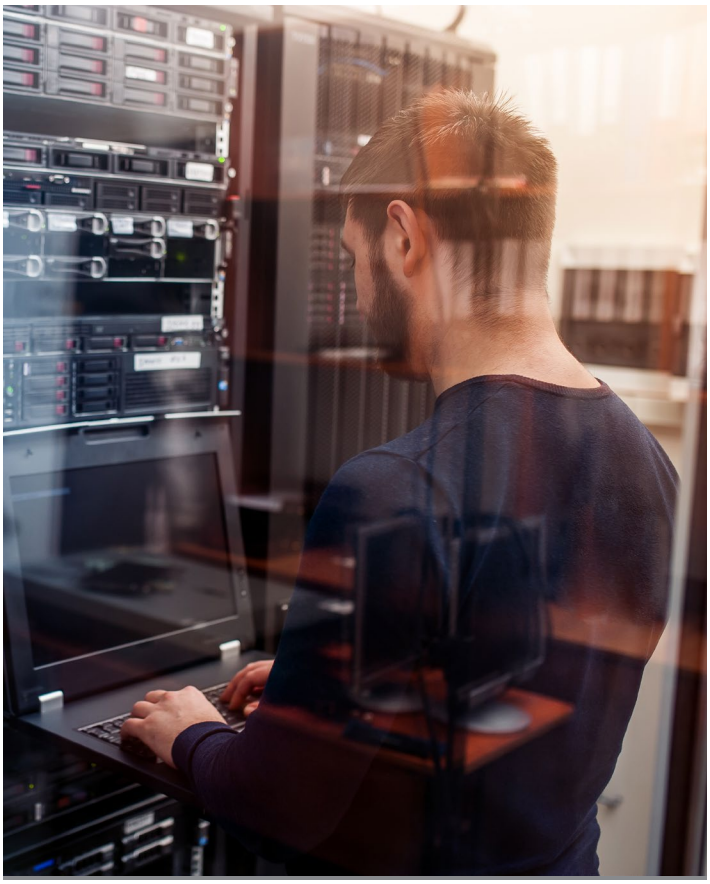
ELEVATE YOUR SECURITY PROGRAM

As cyberattacks become more frequent and damaging, the importance of effective vulnerability management to organizational security and resilience cannot be overstated.

Vulnerability management programs provide organizations with a comprehensive, proactive approach to security that reduces the risk of security breaches and helps ensure the protection of assets and data. However, in the fast-evolving landscape of cybersecurity, the traditional approach to vulnerability management is proving inadequate as cyberthreats become more frequent and severe. Security and risk leaders are grappling with challenges such as failing audits, ineffective metrics and a general sense of being overwhelmed by the sheer number of vulnerabilities.

S3 Security is a trusted partner for vulnerability management. For the past 25 years, S3 Security experts have worked side-by-side with clients to help maintain compliance and protect against cyber-attacks. We are committed to providing straightforward guidance for proactive cybersecurity programs that support business goals, build trust and deliver peace of mind.

Our cybersecurity experts not only know the most common vulnerabilities cybercriminals exploit but the most effective strategies to combat them. We can help you build a Risk Based Vulnerability Management (RBVM) program that will actively combat ongoing threats and satisfy compliance requirements.



CHALLENGES WITH VULNERABILITY MANAGEMENT

The challenges organizations face in vulnerability management are multifaceted and can impact the overall effectiveness of their cybersecurity posture.

Treating Vulnerability Management as a Process Issue

Organizations often view vulnerability management as a routine process rather than an integral component of a comprehensive risk-based security program.

Impact: This mindset may result in a reactive rather than proactive approach, where vulnerabilities are addressed as isolated incidents instead of a broad, strategic risk management initiative.

Routine Scanning and False Positives/ Negatives

Issue: Regular vulnerability scanning is essential, but it comes with the risk of generating false positives or false negatives.

Impact: False results can lead to misallocation of resources with teams focusing on non-existent issues or overlooking real threats. This can hinder the efficiency of remediation efforts and expose the organization to unnecessary risks.

Overwhelming Volume of Vulnerabilities

Issue: The sheer volume of vulnerabilities discovered regularly poses a challenge in determining which ones are most critical and require immediate attention.

Impact: Without a robust prioritization mechanism, organizations may struggle to focus resources on addressing the most severe vulnerabilities, leaving critical assets exposed to potential exploitation.

Rapidly Evolving Threat Landscape

Issue: The constant emergence of new vulnerabilities and evolving threat landscapes make it challenging for organizations to keep up with the latest risks.

Impact: Delays in identifying and remedying vulnerabilities expose the organization to a higher risk of exploitation. This lack of timely response can result in security gaps and potential breaches.

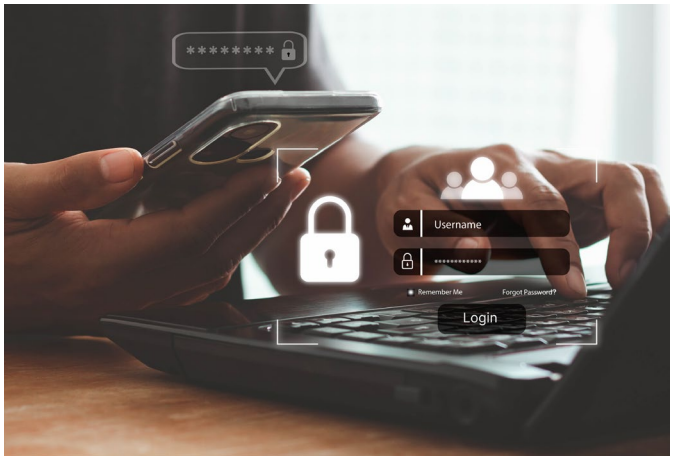
Changing Compliance Requirements

With PCI DSS v4.0, vulnerability scans must now include internal authenticated vulnerability scans. (Requirement 11.3.1.2 March 31, 2025)

Resources for Internal Authenticated Scans

Issue: Authenticated scans can be resource-intensive, making it difficult to choose the proper tools to ensure scans are being performed correctly – especially on large networks or systems with numerous assets that may not be able to support authenticated scanning.

Impact: This can lead to performance issues and if the organization is not prepared, they might struggle to assemble the resources needed to conduct and prioritize comprehensive internal authenticated scans.



RISK-BASED VULNERABILITY MANAGEMENT

As we confront the challenges posed by traditional vulnerability management, it becomes evident that there is a gap between its intended purpose and the practical feasibility for many security teams. This is where implementing Risk-Based Vulnerability Management (RBVM) is highly effective.

RBVM enhances traditional vulnerability management by focusing on genuinely exploitable vulnerabilities. It leverages threat intelligence to identify potential risks, generating scores based on the likelihood of exploitation. Perhaps most importantly, it considers the business context, recognizing that the impact of an intrusion may vary across different network segments.

This strategy focuses patching efforts on the vulnerabilities most likely to be exploited, residing on the most critical systems. The result is a balanced approach that prioritizes the most significant risks while accepting a measured level of risk in certain areas.

KEY COMPONENTS

Vulnerability Assessment
This can be performed in many ways, such as active scanning, passive scanning, using agents or using APIs. The goal is to assess the organizational assets to understand the state of the software, firmware and configuration of these assets.

Risk Prioritization
This phase leverages the vulnerability assessment report to identify where these vulnerabilities intersect with the prevailing threat landscape as well as other compliance mandates, thus calculating the risk associated with a particular vulnerability or asset on the organization's overall risk posture.

Patching or Compensation
Patching is ideal, but not always feasible. Patches may not be available, can't be applied without affecting other applications and/or can't be applied at the same time scale as threat actors are operating (zero days). IPS, WAF, segmentation and strong authentication are all excellent, mature examples of compensating controls that help deal with vulnerabilities and their exploitation. Other practices, including enhanced monitoring and analytics (such as UEBA), can also help compensate for other shortcomings in your environment.

RBVM not only provides gains in efficiency but also establishes a proactive stance in mitigating risks before exploitation occurs. By understanding the factors that make a vulnerability more likely to be exploited, security teams can enhance their overall risk posture.

PREPARING YOUR ORGANIZATION

Strategize Your Approach

- **Review Your Current Solutions**
  Evaluate your current process. Is it working? How could you start prioritizing differently?

- **Consider Pivoting to a Risk-Based Approach**
  Read more about Risk-Based Vulnerability Management and reach out to colleagues currently using it. Speak with your QSA or other assessor to learn how this approach might impact your compliance. Evaluate what, if any, workload can be outsourced.

- **Create a Strategic Game Plan**
  Evaluate what, if any, workload can be outsourced. Perform an Asset Inventory, identifying which systems are external facing, have business implications and/or priority applications. Identify and outline your approach for prioritizing vulnerabilities, engaging your QSA/Assessor and cybersecurity providers for review of and assistance with your program.

PROPELLING YOUR BUSINESS FORWARD

Cyberthreats are here to stay and S3 Security is here to help you create a multi-layered program that reduces risk and satisfies your compliance requirements. We're your trusted partner for implementing and managing an RBVM program, going beyond the traditional "scan, patch, rescan" process.

We not only understand the challenges you face but appreciate the fact that one of the greatest benefits of vulnerability management is professional peace-of-mind. Our goal is to enhance your organizational efficiency, security and profitability in the long haul.

Contact us today. Our team of world-class assessors, consultants and engineers will be happy to walk you through new updates to process, testing procedure guidance and prioritization. Let us show you how RBVM can mature your security program by addressing evolving security risks, promoting security as a continuous process and supporting technological innovation.