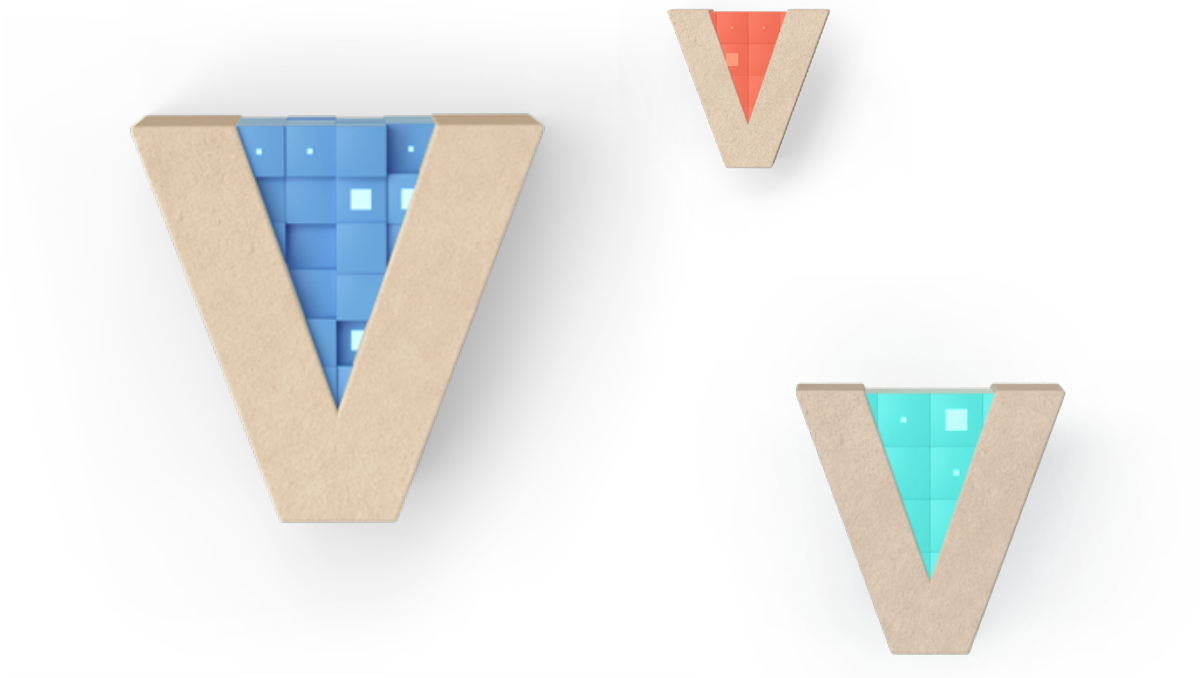
VULCAN.

A STEP-BY-STEP GUIDE TO

achieve vulnerability and risk lifecycle management maturity

Table of contents



Introduction

As IT environments become more complex and the potential for risk continues to grow, enterprises are struggling to prioritize and mitigate vulnerabilities at scale in diverse asset environments that are deployed across highly distributed architectures. Traditionally, vulnerability management dealt primarily with on-premises servers and hosts running in the company's data center. Today, vulnerability and cyber risk management has been extended to encompass cloud-native environments with virtual machines running in every cloud, code repositories and container images, and storage and network infrastructure.

Further complicating matters is the fact that organizational structures have also become highly siloed, with different specialized groups working to maintain a competitive edge in the modern economy. As a result, vulnerability and risk mitigation workflows span diverse teams (security operations, DevOps, application development, etc.), each with its own business mandates, unique processes, and preferred operating technologies.

These issues, combined with the fact that vulnerabilities and exploits continue to rapidly proliferate, mean modern enterprises are constantly challenged to ensure vulnerability and risk management programs achieve their business-critical outcome:

Effective and timely vulnerability and risk lifecycle management that enhances a company's security posture while consuming minimal resources.

This eBook establishes a useful vulnerability and risk lifecycle management maturity model to advance several stages beyond simple vulnerability scanning or prioritization. It outlines a comprehensive maturity model for full vulnerability remediation defining the mandate for organizations to drive cyber risk management programs to higher levels of maturity and analyzing the elements that comprise transformative, end-to-end vulnerability remediation.

A traditional vulnerability management program run by security teams to deliver prioritized vulnerabilities has been properly addressed by the industry and its practitioners. Collaborative, outcome-driven vulnerability and risk lifecycle management that results in cross-functional organizational efficiency and more secure IT environments remains uncharted territory for most. The latter is challenging, but achievable with fully utilized tools, willing people, and mature processes.

This vulnerability and cyber risk management maturity model establishes an end-to-end framework to help security and IT operations teams work together to achieve advanced levels of vulnerability and cyber risk management. It explains why a company must have a strategic vision of vulnerability and risk management outcomes in order to mature its program from being primarily reactive to data-driven → orchestrated → transformational. It describes how an organization must systematically optimize its vulnerability and risk management processes at each level in order to move inexorably towards its ultimate goal: data-driven, well orchestrated, and intelligent vulnerability and risk mitigation.

The need for vulnerability and risk lifecycle management

THE FOLLOWING TRENDS ARE DRIVING THE FUTURE OF THE VULNERABILITY AND RISK MANAGEMENT LANDSCAPE:

1. **A growing number of vulnerabilities year over year.**
   - More than 50 CVEs logged every day in 2021 according to Redscan Labs (a record number)
     - 90% of all CVEs discovered in 2021 so far can be exploited by attackers with limited technical skills
     - CVEs which require no user interaction, such as clicking a link, downloading a file or sharing their credentials, accounted for 61% of the total volume up to now
     - 54% of vulnerabilities so far this year are classified as having "high" availability, meaning they are readily accessible/ exploitable by attackers
   - 60% of breach victims were breached due to a patchable vulnerability

2. **The inherent complexity and scope of the enterprise environment.**
   - Cloud Security (according to Cybersecurity Insiders)
     - 95% of orgs are concerned about cloud security
     - 58% rely on periodic vulnerability and compliance reports
     - 90% use 2 or more cloud providers
   - Appsec
     - 40% have 5,000 or more security vulnerabilities that need to be addressed and that rate has quickly increased over the past 12 months
     - 68% experienced a breach in the previous 12 months due to an application vulnerability

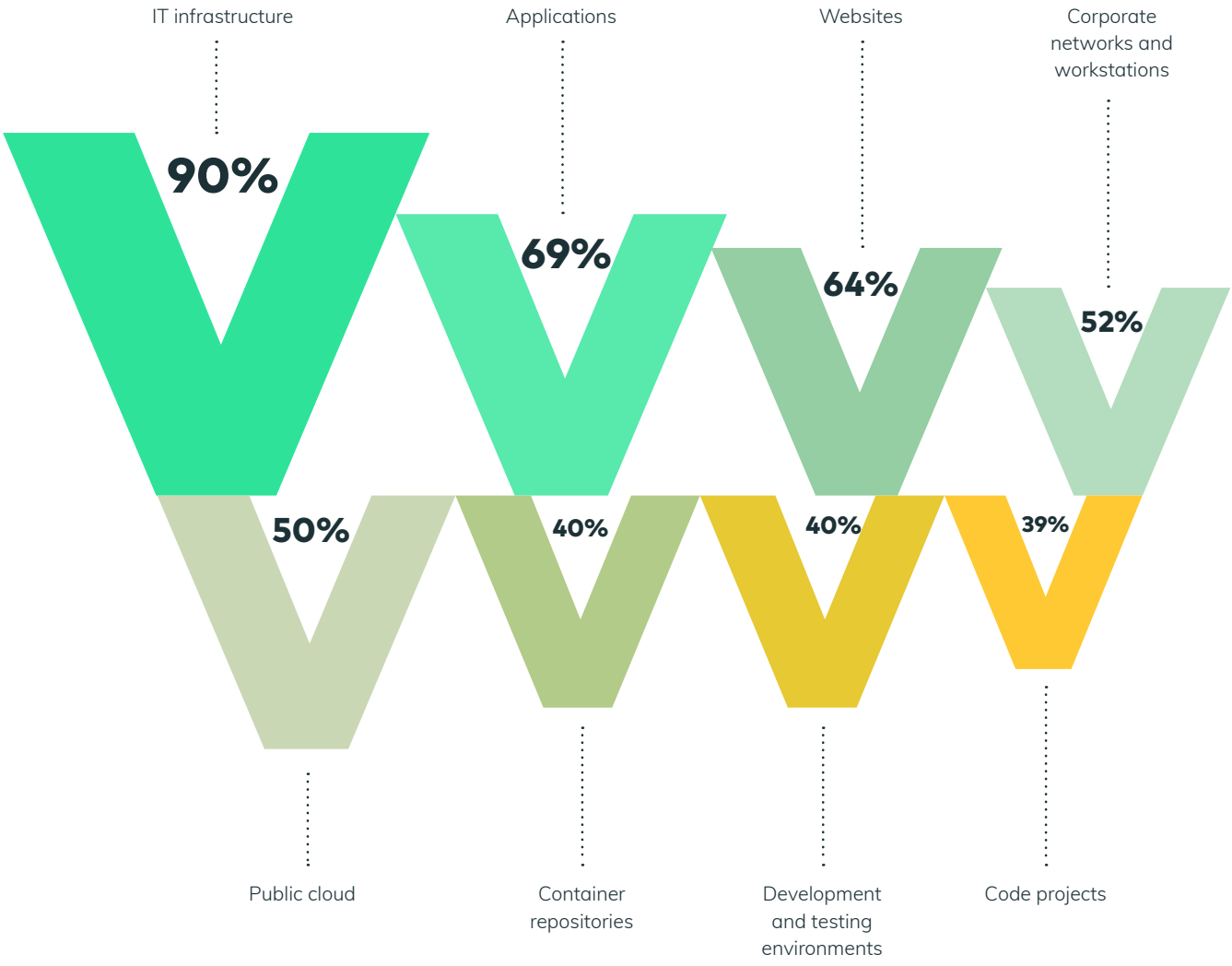
3. **There is a massive global shortage in skilled cybersecurity personnel.**
   - There were 3.5 million unfilled cybersecurity positions in 2021 (Cybersecurity Ventures)
   - Only 36% say they have enough staff to patch fast enough to prevent a breach (Ponemon/ServiceNow infographic)

Research conducted by Pulse, Inc. and Vulcan Cyber shows that today's vulnerability landscape requires organizations to manage many and diverse vulnerabilities—not all of which are tracked by legacy vulnerability scanning—with limited skilled resources distributed across multiple, often-siloed teams.

A scanner for every surface

The top three surfaces cybersecuirty leaders scan for vulnerabilities are infrastructure (90%), applications (69%), and websites (64%). Only 39% of respondents scan their code projects.

WHAT IT ASSETS DO YOU SCAN FOR VULNERABILITIES?

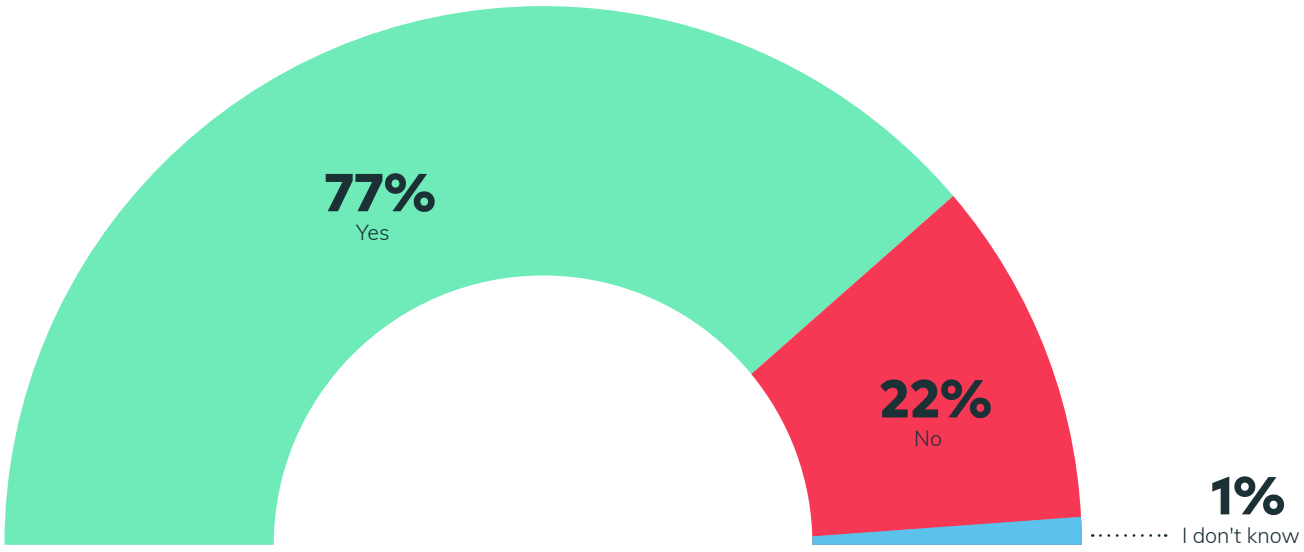


The same research shows that the need for vulnerability and risk lifecycle management is being driven by actual experience and shows that most businesses have been impacted by a security vulnerability in the past year.

You are not alone: 77% of businesses have been impacted by unmitigated risk

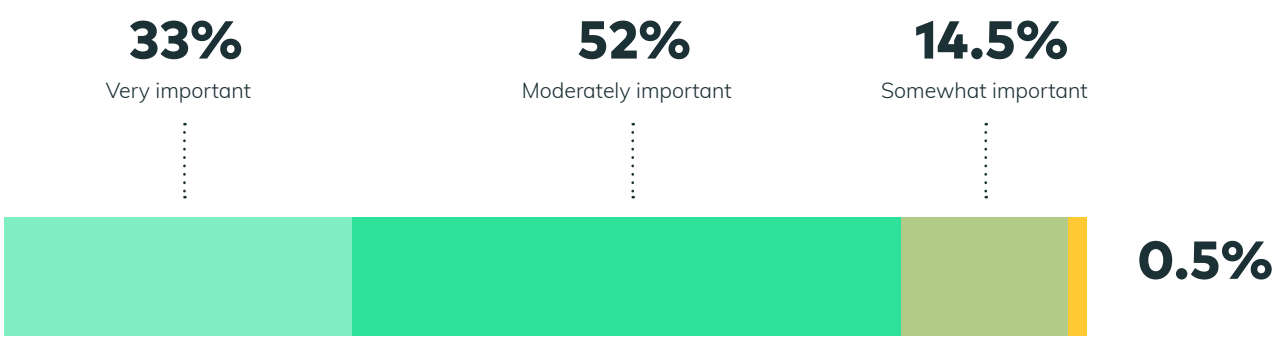
More than three-quarters (77%) of cybersecurity leaders have been impacted by a security vulnerability in the past year.

HAS AN IT SECURITY VULNERABILTY IMPACTED YOUR BUSINESS WITHIN THE LAST YEAR?



And the same research now shows that a significant majority of cybersecurity leaders recognize the importance of using a risk-based approach to vulnerability management.

HOW IMPORTANT IS RISK-BASED VULNERABILTY MANAGEMENT AND PRIORITIZATION TO YOUR ORGANIZATION?



As most cybersecurity leaders experienced a security breach recently, 85% deem it moderately or very important to manage and prioritize vulnerabilities with a risk-based approach.

Introducing the Vulcan Cyber Vulnerability and Risk Lifecycle Management Maturity Model

Vulcan Cyber has analyzed hundreds of enterprise vulnerability management program assessments, including dozens of customers who have their vulnerability and risk lifecycle management practices on our platform. We have developed the vulnerability and risk lifecycle management maturity model to describe the enterprise journey from basic vulnerability management to a transformative program that turns vulnerability and risk management into an organization-wide program and delivers significant business value and peace of mind.

STAGE 1
Reactive - Regularly scan infrastructure assets for vulnerabilities and manage remediation on a case-by-case basis using CSV scoring for basic prioritization.

STAGE 2
Data-driven - Centralize vulnerability and risk management lifecycle activities to drive actionable insights prioritized by risk using vulnerability, asset, threat intelligence and remediation data.

STAGE 3
Orchestrated - Eliminate inefficient manual processes and institutional operating silos to effectively remediate vulnerabilities and risk at scale and speed.

STAGE 4
Transformative - Rally business and product stakeholders around implementing processes that make effective cyber hygiene an organization-wide priority.

Stage 1 (Reactive)

VULNERABILITY SCANNING

Vulnerability scanners have been around for over 20 years and yet the majority of organizations continue to take a primarily reactive approach to managing vulnerability related risk. At Level 1 maturity level, an enterprise's vulnerability management program is tactical in nature. With no cross-organizational visibility across workflows and policies, effective risk-based vulnerability triage is difficult at best. Vulnerabilities are assessed on a case-by-case basis, and remediation is poorly prioritized and inefficient.

In many cases, each team works in its own silo, juggling its own fragmented scanning and management stack. For example, the security team manages a collection of technology-specific scanners for its cloud infrastructure, on-premises infrastructure, static code, open-source code, and so on. Each tool looks for specific types of vulnerabilities and operates within its own unique frame of reference with a lot of data duplication across different scanners. Remediation is often performed by different groups operating under competing priorities and using their own tools as well.

As a result, vulnerabilities are assessed on a case-by-case basis and remediation is overly reactive and slow.

Stage 1 incorporates:

1. Regular vulnerability scanning of infrastructure
2. Individualized vulnerability scoring
3. Basic process tracking and reporting

Stage 2 (Data-driven)

STRATEGIC AND INTELLIGENT VULNERABILITY MANAGEMENT

Programs that have reached Stage 2 have embraced a data-driven approach to vulnerability and cyber risk management. At this level of maturity, enterprise security teams and their allies have employed strategies and technology to consolidate diverse scanner outputs and enrich them with other internal and external data streams. This allows them to deliver accurately prioritized and actionable vulnerability insights to more efficiently identify and mitigate threats specific to their environments.

The security team's data-driven, strategic vulnerability decisions are now based on a real-time understanding of asset status and criticality, risk-specific compliance requirements, and relevant threat intelligence.

At this stage organizations begin to close the gap between necessary levels of risk reduction and the ability to execute based on available resources.

Stage 2 incorporates:

1. Asset-specific risk analysis
2. Business group contextualization
3. Threat intelligence
4. Risk-based prioritization

Stage 3 (Orchestrated)

COLLABORATIVE, AUTOMATION-DRIVEN VULNERABILITY MITIGATION

Organizations that have reached Stage 3 have implemented technologies and processes that facilitate better communication and collaboration to streamline and expedite vulnerability and risk remediation. Using an integrated security stack and automation-driven methods to break down the operating siloes between all of the vulnerability and risk management stakeholders (security, IT operations, engineering, business unit owners) delivers a highly effective and orchestrated approach to managing the vulnerability and risk management lifecycle.

As processes and practices become more transparent and individual tech stacks are integrated into an orchestrated platform, communication and collaboration are delivered via fluid, optimized, and largely automated mitigation workflows. This is critical for extending the capabilities of overburdened and under-resourced security teams and reducing mean-time-to-resolution (MTTR).

Orchestration also allows for better remediation awareness and analytics by enabling the comprehensive tracking and reporting necessary for compliance, internal auditing, board reporting, resource and capacity planning. This delivers a deep understanding of how vulnerability and risk management efforts are working over time, to improve security outcomes based on true understanding of program efficacy.

Stage 3 Incorporates:

1. Centralized management
2. Automation-driven playbooks
3. Automated collaboration
4. Remediation tracking and analytics
5. Business aligned execution

Stage 4 (Transformative)

TRANSFORMATIVE CYBER HYGIENE

Stage 4 can be considered the “holy grail” of a mature vulnerability and risk lifecycle management program. Transformative processes and technology unite multiple cross-functional teams and organizational objectives in a distributed framework in which both security and non-security teams are empowered to take responsibility for vulnerability remediation decisions. As the undisputed governing entity in extremely high risk scenarios, security may override its allies’ decisions. For the most part, however, vulnerability management at this stage is a democratized process in which stakeholders are given the tools, remedies and intelligent insight to independently make smart and correct vulnerability remediation decisions about the cyber hygiene of the enterprise.

Stage 4 Incorporates:

1. Strategic consolidation
2. Interdepartmental alignment
3. Product and business alignment
4. Business-wide adoption

Building for company-wide transformation

An enterprise's journey towards transformative vulnerability and risk lifecycle management is an iterative process. It involves a series of incremental programmatic and technology improvements that will eventually lead to enterprise-wide adoption of risk management best practices throughout the organization.

The first step in the process is understanding the need for security, operations, and application development teams to work together, while acknowledging significant differences in priorities and operating procedures. The security team is responsible for vulnerability scanning, risk analysis and mitigation planning, which is then typically communicated to the operations team and/or the application developers, depending on the specific issue. IT operations and/or DevOps teams are generally responsible for implementing most of the remediation steps that might impact production environments, while the application development teams are responsible for applying remediation recommendations to the code base.

The real challenge in facilitating effective collaboration is that each team is typically evaluated by different KPIs. The security team is measured by vulnerability management and security outcomes. If there is a security breach, it is the security team that will be held accountable. The operations team, on the other hand, is measured by infrastructure uptime, availability, and reliability. If business continuity is disrupted by a remediation task, such as deploying a patch, the operations team will be held accountable. And application development and DevOps teams are focused on adding business value in very short cycles. If their rapid development and deployment pipelines are slowed down by having to go back and fix bugs or secure code, they have a difficult time achieving their mandate.

In essence, the vulnerability remediation maturity model is a step-by-step strategic blueprint for closing the human, technological, process and operational gaps created when vulnerability remediation takes place across siloed teams. As shown in the figure below, each level consists of several foundations that represent the key outcomes to be achieved. Although the model maps a clear pathway toward vulnerability remediation, the process does not have to be strictly linear. The organization gains immediate and quantifiable vulnerability remediation benefits as it optimizes foundations at all different maturity levels. As mandate owners, the security team gains incremental tool, process and team buy-in to actually deliver cyber hygiene but only by working with engaged and empowered DevOps, IT operations, and business unit teams in seamless, collaborative vulnerability remediation workflows.

01

Stage 1 (Reactive)

1. Regular infrastructure scanning
2. Individual vulnerability scoring
3. Basic process tracking and reporting

02

Stage 2 (Data-driven)

1. Asset-specific risk analysis
2. Business group contextualization
3. Threat intelligence
4. Risk-based prioritization

03

Stage 3 (Orchestrated)

1. Centralized management
2. Automation-driven playbooks
3. Automated collaboration
4. Remediation tracking and analytics
5. Business-aligned execution

04

Stage 4 (Transformative)

1. Strategic consolidation
2. Interdepartmental alignment
3. Product and business alignment
4. Business-wide adoption

The following sections of this paper describe the vulnerability management foundations for each level within the Vulcan Cyber vulnerability and risk lifecycle management maturity model. While Stage 1 activities are still critical components of vulnerability and risk lifecycle management, most organizations have successfully deployed them.
This ebook will focus on Stages 2-4.

Data-driven vulnerability and risk management

02

Stage 2 (Data-driven)

1. Asset-specific risk analysis
2. Business group contextualization
3. Threat intelligence
4. Risk-based prioritization

There are four key foundations for the security team to optimize at the data-driven vulnerability management maturity stage:

1. **Asset-specific risk analysis.** The enterprise maps and maintains the status and risk attributes of every asset within the organization (hosts, servers, cloud compute and storage, code repositories, and so on) and ensures that all assets are being scanned and managed for Vulnerabilities relevant to the specific asset type.
2. **Business group contextualization.** The enterprise can define, analyze and calculate risk based on business context to set security policies and align risk management strategies to compliance mandates and business requirements. This allows organizations to focus on vulnerabilities and risk that is most likely to have a critical impact on the business.
3. **Threat intelligence.** The enterprise incorporates relevant threat context that helps them better understand the true severity of a vulnerability, including whether or not it has been exploited in the wild, the likelihood that it will be successful at exploiting their environment, etc.
4. **Risk-based prioritization.** Vulnerabilities are prioritized based on information provided by multiple data points, including threat intelligence, asset configuration data, available vendor solutions, and an understanding of the business impact of each possible remediation workflow. Risk algorithms should be customizable to the business for maximum efficiency.

As these foundations undergo optimization, the enterprise benefits from data-driven vulnerability assessment and prioritization that takes into account the organization's unique asset, infrastructure, compliance, and business requirements. The security team can confidently identify the vulnerabilities that are truly high risk for the specific enterprise, allowing them to stay focused on remediation execution that targets their true organizational risk. Further, the organization can now take a strategic approach to its remediation campaigns, deciding when to be vulnerability-driven (solving a single vulnerability across all assets), when to be asset-driven (remediating all vulnerabilities affecting assets that impact the organization's security posture), and when to be solution-driven (patching an OS across the entire organization).

Orchestrated vulnerability and risk management

03

Stage 3 (Orchestrated)

1. Centralized management
2. Automation-driven playbooks
3. Automated collaboration
4. Remediation tracking and analytics
5. Business-aligned execution

At this stage, the enterprise's remediation efforts go beyond the security team and establish cross-organizational workflows for more effective vulnerability and risk mitigation strategies. The key foundations to be optimized at this level are:

1. **Centralized management.** Application, cloud, and infrastructure vulnerability management is analyzed and managed in one place, allowing risk managers to more effectively coordinate risk management activities track program efficacy.
2. **Automation-driven playbooks.** Continuously design and implement effective vulnerability and risk management processes that are as automated as possible. Build and maintain playbooks that leverage data-driven recommendations and task statuses as triggers to drive workflows forward.
3. **Automated collaboration.** Align the different vulnerability and risk mitigation stakeholders (security, IT operations, DevOps, application developers, business unit owners, etc.) to determine how they fit into and operate within the enterprise's chosen vulnerability remediation framework.
4. **Mitigation tracking and analytics.** Ensure that all stakeholders can track the mitigation workflows across teams, tools, and diverse processes. At the task and workflow levels, define clear success criteria that can be used to verify that the remediation campaign effectively closed the detected vulnerability gaps.
5. **Business-aligned execution.** Establish how quickly different vulnerabilities need to be addressed by different teams, product lines, environments, asset groups, and type of problems.

When the enterprise has optimized its vulnerability and risk management orchestration capabilities, cybersecurity hygiene will be better upheld because vulnerability remediation is now far less disruptive to the IT operations, DevOps, and business teams. In addition, the overhead of manual work drops dramatically at this level. Non-security stakeholders are empowered to make responsible vulnerability remediation decisions within the framework of their unique mandates and responsibilities. And, the remediation workflows themselves are clear, transparent, and as seamless as they can possibly be.

Transformative vulnerability and risk lifecycle management

04

Stage 4 (Transformative)

1. Strategic consolidation
2. Interdepartmental alignment
3. Product and business alignment
4. Business-wide adoption

Now that the enterprise's vulnerability and risk lifecycle management program is data-driven and orchestrated, it can proceed to the transformative maturity stage, in which management functions within the organization can make informed cybersecurity decisions.

1. **Strategic consolidation.** Relevant risk management personnel have access to comprehensive, consolidated analytics for all attack surfaces allows organizations to plan and adopt proactive vulnerability and risk mitigation strategies across all surfaces in tandem, for more efficient and secure growth.
2. **Interdepartmental alignment.** The organization has acquired the tools and processes required to empower IT, SecOps, DevOps and AppDev to work together and make smart risk management planning decisions.
3. **Product and business alignment.** The C-suite and board have access to user-friendly vulnerability management reports and dashboards that help them make decisions about where to invest resources in order to improve the organization's cybersecurity outcomes. Product management teams can insightfully align their roadmaps with high priority security issues.
4. **Business-wide adoption.** Business group owners receive dynamic tools that let them quickly understand their cyber-risk profile and compare their security performance with their peers', both within and outside of the organization, turning the entire organization into active risk managers.

At this transformative maturity stage, security teams provide their allies with reports, dashboards, and insights that align with their native work environments and business vocabularies, empowering them to make smart decisions independently. Organizations leverage real-time insights into their vulnerability and risk lifecycle management program in order to make informed decisions about investments in product development, security tools, skills and training, policies, and processes that will further align and enhance business and security outcomes.

Conclusion

As enterprises strive to optimize their vulnerability and risk management and remediation programs, a good first step is to benchmark their current practices and outcomes against the Vulcan Cyber vulnerability and risk lifecycle management maturity model described in this paper. For each foundation in each level, it is important to honestly assess whether an enterprise's processes are still largely manual, semi-automated and siloed, or fully optimized for automation-driven processes and organization-wide collaboration and orchestration. The resulting map provides the basis for a strategic plan that gradually but inexorably drives the organization towards a fully mature vulnerability and risk lifecycle management program that contributes to business-critical outcomes.

The Vulcan Cyber cyber risk management platform has been built from the ground up to deliver transformative outcome-driven vulnerability and risk lifecycle management. Vulcan Cyber integrates all of the relevant teams and their native tools to make vulnerability and cyber risk management processes a seamless collaborative effort with high levels of automation and orchestration. Highly contextual, risk-based vulnerability prioritization and remediation intelligence ensure that an enterprise's risk management efforts provide maximum business impact.

See how Vulcan Cyber can accelerate your company's vulnerability and risk management maturity.

REQUEST A DEMO

VULCAN.