Mighty Guides



WHEN ORGANIZATIONS ARE OFF BALANCE WITH VULNERABILITY MANAGEMENT

Sponsored by

RISKSENSE

INTRODUCTION

Building a strong vulnerability management practice requires balancing key functions that include scanning and discovery, security analysis, prioritization, remediation workflow, and patch verification. Failure to balance these functions weakens the vulnerability management effort.

This eBook looks at strategies for developing a regular cadence of action, including orchestrating scanning, triage, remediation, and patch verification in a way that reduces the impact of an occasional disruption. Automation and orchestration are powerful tools for effective vulnerability management.

Regards,
David Rogelberg
Publisher, Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

MEET THE EXPERTS

DAVID EMERSON
Vice President, Deputy CISO, Cyxtera Technologies

HUMAYUN ZAFAR
Associate Professor of Information Security and Assurance, Kennesaw State University

ADITYA CHIKKALA
Director, Security Operations, LogMeIn

David Emerson, Vice President, Deputy CISO, Cyxtera Technologies

David Emerson works at Cyxtera Technologies, a secure platform for connecting and protecting dedicated infrastructure, private clouds, and public clouds. On the side, he advises Flux Mopeds as they capture the utilitarian SEV market, and provides technical advisory services through refmark LLC. Before that, he was at Liquidity Services building eCommerce marketplaces for the reverse supply chain, Harris Associates building and maintaining critical trading infrastructure, Vassar doing a bit of everything at campus-scale, Apple representing their (former) HPC products in higher education, and Tulane bringing formal systems administration to the Newcomb College Center for Research on Women.

"Difficulty in balancing resources and tasks will negatively affect the remediation workflow followed by patch verification."

In today's busy and dynamic IT environments, security teams are often stretched to their limits. A large part of a security practice requires setting and balancing priorities. This is just as true when it comes to vulnerability management. Building a strong vulnerability management practice requires balancing key functions that include scanning and discovery, security analysis, prioritization, remediation workflow, and patch verification.

Failure to balance these functions weakens the vulnerability management effort. Humayun Zafar, associate professor of information security and assurance at Kennesaw State University, notes that effective vulnerability management depends on getting a lot of things right. "In today's threat environment, it is important to recognize the integrated nature of vulnerability management that is a part of a holistic security program in an organization. A limited focus on any one of its key functions would ultimately affect the entire security footprint of a firm. After all, when we talk about security only being as good as its weakest link, we must not forget that it applies to its security processes as well as its people." Aditya Chikkala, director, security operations (cyber incident response, vulnerability management and threat intelligence) at LogMeIn, says that when organizations struggle to balance resources, remediation often suffers.

Humayun Zafar, Associate Professor of Information Security and Assurance, Kennesaw State University

Dr. Humayun Zafar is an associate professor of information security and assurance at Kennesaw State University. His cyber security research has been published in numerous journals and conferences, and has regularly appeared in various media outlets to talk about threats businesses face in this area.

"In today's threat environment, it is important to recognize the integrated nature of vulnerability management that is a part of a holistic security program in an organization."

"In reality, no team or organization has enough resources to achieve all the results that both the security teams and its stakeholders are passionate about. Difficulty in balancing resources and tasks will negatively affect the remediation workflow followed by patch verification because they both go hand in hand."

David Emerson, vice president, deputy CISO at Cyxtera Technologies, points out how easy it is to fall behind the curve in an ongoing process like vulnerability management. "When an organization has difficulty balancing resources and tasks, those activities that require a regular cadence of action will suffer most," he says. "Patch management, for example, is an activity that requires a regular cadence of action because patches are released almost continuously. Software that is not patched on a correspondingly regular cadence falls further behind every day, becoming more and more vulnerable. An activity such as patch management can be sporadically addressed from a backlog when other priorities take precedence, but operating in this way will limit the effectiveness of a patch management process. Among the key functions of vulnerability management, of which patch management is a subset, there are very few practices that do not require a regular cadence of action."

Aditya Chikkala, Director, Security Operations, LogMeIn

Aditya Chikkala is the Director for Security Operations at LogMeIn and manages a team of security professionals responsible for Incident Response & Threat and Vulnerability Management. His background has been in Incident Response, Threat Intelligence and Vulnerability Management. His past experiences have been managing an Incident Response Team at EMC, Senior Security Analyst with companies like Target and DTCC and he holds a MBA degree from University of Massachusetts at Amherst and a Masters Degree in Infrastructure Assurance from University of Texas at San Antonio.

The good news is that some tools can address these issues to ensure that all phases of a vulnerability management practice have the support they need. Emerson says, "Much of the vulnerability management practice can be automated. Scanning, initial triage, some remediation, and most patch verification can be orchestrated in a way that reduces the impact of an occasional disruption in staff attention. Automation and orchestration as a cultural practice, often referred to as 'DevSecOps,' is the most powerful single tool in the arsenal of a security practitioner when attempting to reconcile the activities of, and collaboration between, IT, security, and business owners. What is automated is often forgotten, not because it is ineffective, but because it does not continuously represent a drain on resources, a distraction from revenue-generating activities, and a hobbling of administrative rights and processes."

Humayun Zafar emphasizes the role of top management in setting priorities and building a collaborative culture in the organization. "Top management is fundamentally responsible for pushing down its vision of what it considers to be its security posture in regard to vulnerability management processes and how they relate to rank and file employees. Management should focus on making these processes opportunities for each employee to have a stake in ensuring a security posture and making it a shared responsibility for all. Once that occurs, collaboration between all units—be it IT or business owners—will improve." Aditya Chikkala also believes support from executive management is important. "Executive management support is the key to an efficient vulnerability management program.

Executive managements' acceptance of risks—for instance, the risk of patching the infrastructure, supporting new products' feature rollouts, and its potential negative effects on infrastructure availability, versus the risk acceptance of not patching critical findings—will influence the fears of the patching efforts affecting a business process. A well-documented plan with the different stakeholders (IT, business owners, and so on) is the key to resource allocation and buy-in, which will also drive an effective vulnerability management process."

David Emerson advises that the way you balance your vulnerability management workflow for optimum risk management must ultimately be a business decision. "It's important to take a careful, and if possible, quantitative, measurement of risk and risk tolerance. No security program will be without cost constraints, and no business will tolerate a program out of proportion with the scale of risks that business experiences. Security practitioners would do well to understand this relationship and to calibrate their programs in a way that advocates for risk mitigation that is in line with the business-described tolerance for risk." ■

CLOSING THOUGHTS

Without a doubt, you struggle with prioritizing the plethora of threats and vulnerabilities that hit your organization. Penetration testing findings add to the problem. There are never enough hours in the day, nor enough staff to remediate all of the possible exposure on both your internal and external IT infrastructure.

Shift your thinking. Narrow down the threats and vulnerabilities to the ones that have active exploits, are dangerous with remote code execution capabilities, and are trending with active threats in the wild. This is impossible if you don't have a platform that takes in all of your vulnerability scanner data, across your dynamic attack surface: network, endpoints, database, applications, cloud, and IoT devices. Leverage human intel, combined with AI and machine learning to achieve prescriptive prioritization in minutes. Security and IT teams can focus on what matters the most with a new efficiency to manage cyber risk.

This article illustrates the value of risk-based vulnerability management to predict, prioritize, and take control of your most dangerous vulnerability and risk findings.

Regards,
Srinivas Mukkamala
CEO and Co-Founder, RiskSense

RISKSENSE

RiskSense®, Inc. provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness.

The company delivers a fully-informed picture of group, department, and organizational cybersecurity risk with our credit-like RiskSense Security Score (RS3). The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals.

By leveraging RiskSense threat and vulnerability management solutions, organizations significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, lower costs, and ultimately reduce attack surface and minimize cyber risks. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.