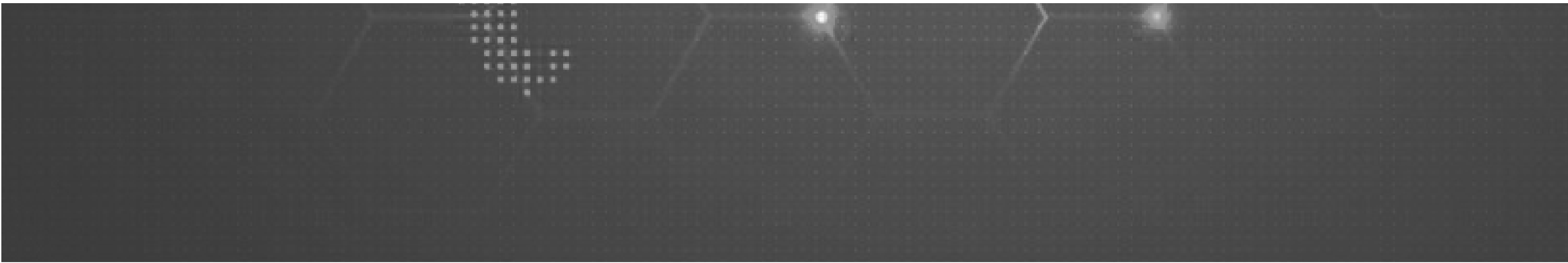
Mighty Guides

TURNING AROUND THE NEGATIVE BUSINESS OF VULNERABILITY MANAGEMENT



Sponsored by

RISKSENSE

INTRODUCTION

Modern vulnerability management practices need tight collaboration and feedback from everyone involved to enhance job satisfaction and act as a team. However, the volume of remediation tickets a vulnerability management program generates can cause friction between IT and security teams.

This eBook looks at strategies, including internal competitions, incentives, and gamification that can overcome those old 'vulnerability management blues,' and effective address problems like persistent recurring vulnerabilities.

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 CROSS
CSO, DarkSight Security

MIKE SHEWARD
Senior Director of Information Security, Accolade

David Cross, CSO, DarkSight Security

David Cross is the Principal Security Architect/Hacker for Henry Schein One. David switched mid career from architect-level development in image recognition, voice operation, and AI, to cyber security in 2001. David brings his former coding experience into the security world by contributing to new tools and technologies for making security management easier. If David isn't hacking, coding or writing about the former, he is finding practical ways to use AI in daily life.

> "Few defensive information security activities are as underappreciated as vulnerability management."

Vulnerability management can generate lots of tickets for busy IT operations staff that may not recognize their important role in managing the organization's cyber risk. This can cause friction between IT and security teams that impede effective vulnerability remediation. Ideally, a modern vulnerability management practice needs tight collaboration and feedback for everyone involved to enhance job satisfaction and act as a team. The challenge for many organizations is to inspire and sustain this level of focused collaboration.

Mike Sheward, senior director of information security at Accolade, explains why teams often struggle with key elements of vulnerability management. "Few defensive information security activities are as underappreciated as vulnerability management," he says. "It's a critical foundational activity for any security program, yet more often than not, a task that is quickly assigned to the newest, or most junior member of the security team, and subsequently passed around like a hot potato. The stigma associated with vulnerability management is that it's a process bathed in negativity and nagging. Having the same person responsible for shepherding countless tickets through the remediation tracking process does not make for a satisfying job, nor does it make that person a popular member of the security team. To overcome the 'vulnerability management blues,' a collaborative approach between the security team and those ultimately responsible for addressing vulnerabilities is key."

Mike Sheward, Senior Director of Information Security, Accolade

Mike Sheward is the senior director of information security at Seattle-based Accolade Inc, and runs a digital investigation consultancy, Secure Being LLC. He has worked in information security, primarily in incident response and digital forensics, in both the UK and US for 12 years. A published author, Mike has written books including; 'Hands-on Incident Response and Digital Forensics' and 'Digital Forensic Diaries'.

> **"For example, divide the room into two sides: attackers and defenders. Have them attack and defend the product they are responsible for."**

Of course, the big question for many organizations is how to actually overcome the 'vulnerability management blues.' Sheward suggests taking advantage of basic human nature. He says, "It turns out that teams within an enterprise can get mighty competitive when it comes to having the most secure systems. Leaderboards, scoring, and the opportunity to gain recognition and even win small prizes can serve as motivators to getting the routine, but highly necessary work of patching done. It's important to remember that, as with any security control, this strategy should be one of positive reinforcement rather than attempting to achieve security through shaming, because that never works."

David Cross, CSO of DarkSight Security, says competition can be highly effective, and he suggests other gamification strategies to make vulnerability management more fun and more effective. "Fun is motivating, while the 'usual' same-old approaches can do more harm to morale than good. You need motivated employees who don't hate the vulnerability management process. So the next time you're prepared to give a security lecture or make someone sit through a corporate security training video set with matching quizzes, consider a different approach. For example, divide the room into two sides: attackers and defenders. Have them attack and defend the product they are responsible for. Don't intervene or lecture, but do highlight comments made by people who are noticing aspects of fun and creativity.

Someone—or maybe multiple someone's—will admit a security, vulnerability, or risk issue you've never heard of before during the exercise." Cross explains how a little competitive nudge like this can change the entire dynamic around vulnerability management. He says, "Before long, you'll notice people grooming the backlog for things to fix. Managers need to ensure developers hold to their regular schedule of addressing security issues or test scripts. But also ensure that the plus side, in terms of security health scores and how it coincides with motivating factors, remains very visible." Cross makes a key point here. It is maintaining the visibility that enables everyone to see and share how doing those collaborative remediation activities removes the most dangerous vulnerabilities and improves security health.

Recurring vulnerabilities can be particularly troublesome, but gamification strategies can be applied to them as well. Sheward explains, "In the case of specific vulnerabilities that pop up en-masse and require a concerted effort to eliminate once and for all, bonus challenges packaged as specific events related to the eradication effort can provide an opportunity for teams to move up the leaderboard. As much as we ridicule 'named' and 'logoed' vulnerabilities, at least they provide us with raw material to help make these challenges more engaging. Who among us doesn't love that little ghost fella who represents the Spectre vulnerability? Depending on the structure of the organization, a contest to determine who can be the quickest to kick out a specific vulnerability over the course of a few days, or a "patching party" hosted by the security team, can really help bring teams together and build those all-important relationships."

Cross notes that when it comes to recurring vulnerabilities, it’s important to understand where they are coming from. “Recurring issues are tricky because they can be a sign of a normal software development life cycle (SDLC), or they can be a sign of smart people abusing your awesome gamification program,” he says. But he goes on to say there are ways to keep a gamification approach honest. “The secret to keeping this approach under control is using the positive mental state motivations of time off, on-the-spot nominal cash bonuses, awarding those who create a playbook for closing a recurring issue or find a way to resolve why a recurring issue occurs. This helps your security maturity, educates your team, and provides momentum in closing discouraging issues. It will also help you earn a spectacular audit score because you will be able to present auditors with evidence that your SDLC is repeatable and documented. Any negative experience not only can be, but absolutely must be, turned into a positive to grow a successful security program.” ■

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.