Expert Q&A: How Can Your Organization Embrace Modern Vulnerability Management for Compliance?

Security teams have never needed to cover so much ground. Cloud migrations, AI deployments, IoT devices – not to mention rapid development cycles – create new vulnerabilities everywhere you look. Meanwhile, traditional infrastructure still demands attention, and supply chain risks lurk in every third-party integration.

It's not just about finding vulnerabilities anymore. It's about making sense of an overwhelming flood of security data. Which vulnerabilities pose real risk? Which ones warrant immediate action? And how do you prove to auditors that you're making the right calls?

In this Q&A with NopSec's Michelangelo Sidagni, CTO, we explore how enterprises should be tackling these challenges. From cutting through the noise to aligning security and IT teams, and building vulnerability management programs that work, here's how organizations can stay compliant and secure.

Q: From your experience working with security teams, what's their biggest compliance challenge?

A: You know, I hear the same story from almost every team I work with. They're drowning in vulnerability alerts while trying to satisfy multiple compliance requirements – whether it's PCI, HIPAA, Fed and OCC requirements, something else, or all of the above. What makes this even harder is the constant back-and-forth between security identifying critical issues and IT teams trying to balance patches with system stability. The real struggle isn't finding vulnerabilities. It's figuring out which ones actually matter from both a risk and compliance perspective.

I was talking with a CISO recently who put it perfectly: "I can't tell my board that we're compliant because we fixed 1,000 low-risk vulnerabilities while missing the three critical ones that could actually cause a breach." That's the heart of the challenge – transforming all this vulnerability data into something meaningful that both reduces risk and satisfies auditors.

Q: You just alluded to the friction between security and IT teams. What are some best practices for fostering collaboration to advance compliance efforts?

Collaboration between security and IT teams is often the linchpin of a successful compliance strategy. One of the most important best practices is establishing clear, shared objectives. Both teams need to understand not just the technical priorities but also the organizational goals they are working toward – whether that's reducing cyber risk, meeting specific regulatory requirements, or improving overall operational resilience.

Regular communication is also crucial. Many teams benefit from structured workflows, such as standing weekly meetings to review vulnerabilities, progress on remediation, and potential bottlenecks. Bringing IT into the prioritization conversation early helps ensure that remediation plans align with operational realities.

Another best practice is defining ownership and accountability. Too often, teams encounter delays because it's unclear who is responsible for specific actions. Clearly assigning roles – and documenting those responsibilities – creates accountability and reduces friction.

Lastly, investing in education across teams can be transformative. When IT understands the security implications of delaying a patch, and security appreciates IT's operational constraints, the focus shifts from finger-pointing to problem-solving. That shift, more than anything, creates the alignment needed to meet compliance challenges head-on.

Q: How is automation changing the game for these teams?

A: It's really about giving teams their time back while improving their compliance posture. Look, nobody gets into security because they love documentation, right? But that's what compliance demands. The beauty of automation is that it can handle the heavy lifting -- gathering the data, prioritizing what matters, and maintaining those audit trails -- while security teams focus on actual security work.

The real game-changer is moving from that reactive "scan and patch" cycle to actually understanding your risk exposure. When you can automatically correlate vulnerability data with real-world threat intelligence and business context, you create priorities that both security and IT teams can agree on. Those better security decisions naturally lead to better compliance outcomes.

Q: What should teams prioritize when looking at automated solutions?

A: Having worked with countless security teams, I've learned that simplicity is key. Yes, you need comprehensive visibility across your environment, but what teams really need is clarity. They need solutions that can take all that vulnerability data -- from their infrastructure, cloud services, applications, you name it -- and tell them "here's what you need to worry about first."

The most successful teams I work with look for tools that fit into their existing workflows and bridge the gap between security and IT. Because let's face it, you're not going to completely change how these teams operate just to accommodate a new tool. The automation should enhance what you're already doing, not force you to rebuild everything from scratch.

Q: We hear a lot about context in vulnerability management. Why is it so crucial for compliance?

A: This really hits home for me. Early in my career, I was that person generating massive vulnerability reports and trying to explain to auditors why we prioritized certain fixes over others. The truth is, a high CVSS score alone doesn't tell the whole story. Is the vulnerable system customer-facing? Is there active exploitation in the wild? Do you have compensating controls in place?

These are the questions auditors ask, regardless of which compliance framework they're working from. They want to see that you understand your risk landscape and are making informed decisions. When you have automation providing this context automatically, those audit conversations become much easier. Instead of defending your choices, you're walking auditors through your well-documented, risk-based approach.

Q: How do you recommend teams handle the workflow side of compliance?

A: I always tell teams to start with their biggest pain point. For most, it's the back-and-forth between security identifying vulnerabilities and IT handling remediation. Throw compliance documentation requirements into that mix, and you've got a real headache.

The key is building workflows that create compliance evidence as a natural byproduct of your security operations. Your vulnerability management system should automatically track who made what decisions and why. When an IT team, for example, needs to delay a patch for operational reasons, the workflow should capture that justification automatically.

Q: What's your advice for teams struggling to demonstrate compliance effectiveness?

A: First, take a deep breath. Every security team I've worked with has struggled with this at some point. The key is shifting from a check-the-box mentality to telling your security story effectively. Whether you're dealing with Fed and OCC examiners or other auditors, they all want to see the same fundamental things: that you have a handle on your risks and a systematic approach to managing them.

Document your wins, but be honest about your challenges. Auditors actually appreciate seeing how you've identified and planned to address gaps in your program. It shows maturity and continuous improvement, which is what they're really looking for.

Q: Looking ahead, how do you see vulnerability management compliance evolving?

A: The future is definitely moving toward continuous monitoring and assessment. The days of point-in-time assessments are numbered. I'm seeing this shift across all compliance frameworks – they're increasingly focused on how organizations maintain ongoing visibility into their risk posture.

But here's the encouraging part: As we move toward more continuous approaches, automation becomes even more powerful. Teams that embrace automated, risk-based vulnerability management now will be better positioned for whatever comes next. It's about building resilient security programs that can adapt to evolving threats and regulatory expectations.

The bottom line? Focus on building a strong, risk-based vulnerability management program that keeps security and IT aligned around shared priorities. Good compliance almost always follows good security practices.