How to Implement a Risk-based Approach to Vulnerability Management

Ditch the spreadsheets and move beyond counting closed vulns
The traditional approach to vulnerability management—counting closed vulnerabilities—doesn’t suffice in a world where hacker sophistication is constantly expanding the threat landscape. According to the Identity Theft Resource Center (ITRC), the first three quarters of 2017 resulted in 1,120 total breaches and more than 171 million records exposed—a considerate increase over the 1,039 breaches and just over 36.6 million records exposed in all of 2016.

Unfortunately, so long as organizations continue to count closed vulnerabilities as their modus operandi, there will continue to be high-profile breaches and dissatisfied executives. But there’s an easier way to manage vulnerabilities that will both improve the organization’s security posture and give both you—and upper-management—confidence in your efforts.
What’s Wrong with Counting Closed Vulnerabilities?

Let’s face it: No one in your organization wants to be the next data breach headline. Unfortunately, reams of scanner data make it difficult to prioritize remediation efforts. So, instead of closing vulnerabilities that are most likely to be exploited, security teams remediate as many vulnerabilities as they can with the hope that they’ve closed the right ones.

But that’s all the security team is left with—a faint hope. And faint hope doesn’t stand up in the boardroom when executives ask what the numbers mean.

To make matters worse, the security organization can’t go it alone. While Security often has all of the responsibility for vulnerability management, it must be a team effort to be successful. After all, Security doesn’t have the purview to apply patches, fix code, or update systems. Security teams, however, often have limited success in getting the cooperation from IT operations and DevOps.

“The number of exploited vulnerabilities year over year for the last decade is actually flat, despite the number of breaches increasing and the number of threats appearing. Essentially, more security threats are leveraging the same small set of vulnerabilities.”

— Gartner, “Focus on the Biggest Security Threats, Not the Most Publicized”
Vulnerability and Risk Management Unite

Security teams must shift their focus from counting vulnerabilities to managing risk. Adopting a risk management approach means focusing on the issues that pose the greatest danger to the business. By doing so, security teams can ensure that they’re focusing their limited resources on the vulnerabilities that matter most. A risk management approach also enables teams to monitor their efforts and make progress towards the ultimate goal of reducing the likelihood of making the news headlines.

To succeed, risk management must be incorporated into operations across the organization. When this happens, the critical efforts that need to happen do happen, and everyone benefits:

**Security Teams** can start measuring real risk and understand how best to reduce it. Security becomes more effective at strengthening the organization against threats and at-risk vulnerabilities.

**Executive Teams** gain a clear understanding of the company’s security posture, including how it’s changing, as well as the efforts and investments needed for continued improvement. Businesses ultimately profit from stronger security and improved productivity across a number of different business groups.

**Remediation Teams** can continue to work with existing tools, processes and platforms while gaining increased visibility into the risks facing the business. With a risk-based approach, remediation teams are able to focus their efforts on the most strategically impactful actions—say, the top three things they can do to significantly strengthen security—versus running on the vulnerability treadmill and not making any real progress. In addition, remediation teams can make more effective use of their time, as they no longer have to sift through giant reports or hunt down fixes.

---

**Key Definitions**

**Risk**
A calculation of the probable frequency and magnitude of future loss.

**Threat**
A negative event that results in the loss, damage or exposure of an asset.

**Vulnerability**
A weakness that makes a negative event possible or more significant.
Step 1: Establish Meaningful Metrics

Having the right metrics in place is one of the key components of any risk management strategy. The best metrics focus on risk both in terms of the likelihood of vulnerability exploitation and its potential business impact.

Metrics should track progress in reducing risk across both of these attributes by factoring in associated assets. Key components include an asset’s importance and impact to the business, processes associated with an asset, mitigating controls that are in place, and the most common forms of attack targeting the asset.

While optimal metrics can depend on the nature of the specific business and its IT environment, a few best practices exist. Consider the following:

- Remediation rate of high-risk vulnerabilities and the number of these high-risk vulnerabilities in a specific environment
- Median time to remediate a high-risk issue
- Median time to discover a high-risk issue
- Number of high-risk assets

Operationalizing a risk-based approach to vulnerability management involves three steps:

- Remediation rate of high-risk vulnerabilities and the number of these high-risk vulnerabilities in a specific environment
- Median time to remediate a high-risk issue
- Median time to discover a high-risk issue

Metrics to Avoid:
- Total open vulnerabilities
- Average vulnerability age
- Total vulnerabilities open longer than X days
Step 2: Integrate Risk Management Into Operational Processes

Instead of creating new operational processes, focus on integrating risk management into existing processes. When organizations use one system to manage development work and another to manage security issues, security will always take a back seat. It’s just too difficult to balance and prioritize work across functional areas. However, using common tools, workflows, and language will help everyone focus on the right thing.

The key to success is to find opportunities to integrate risk management into existing tools and workflows. For instance, find out how to feed your prioritized risks into the development team’s bug tracking system. Likewise, weaving remediation efforts into the operations team’s existing service desk, ticketing systems, change management platforms, and workflows can also help achieve desired results.

Step 3: Embrace Opportunities to Become Predictive

Once organizations integrate a risk-based approach to vulnerability management into core operations, they can transition from being proactive to predictive. Organizations can apply machine learning and predictive modeling technologies to their data set to determine the likelihood that a new vulnerability will be weaponized and exploited. These insights can then be integrated into the risk score, enabling teams to prioritize remediation of future threats within the context of today’s threats. With the right tools and strategies in place, teams can preempt both current and future threats with risk metrics that keep them data-driven, authoritative and in control.
Organizations face two fundamental challenges when it comes to proactively managing cyber risk: leveraging data and ensuring collaboration. To be successful, security teams need access to advanced data science (to generate risk scores) and a solution that coordinates efforts between teams. The Kenna Security Platform can help.

Risk operations with the Kenna Security Platform are proactive, measurable, and most importantly – effective. The platform helps teams move beyond spreadsheets by automating the analysis, correlation, and prioritization of vulnerabilities. The platform leverages threat intelligence and advanced data analytics to generate a single risk score around which all teams can rally. But the platform goes beyond simply telling you what to fix.

The Kenna Security Platform was built on the premise that cyber risk must be managed as an enterprise-wide effort that transcends divisions, roles, and tools. The platform serves as a foundation for a centralized risk management environment, seamlessly integrating with your existing workflows, processes and systems. The right vulnerabilities get to the right people, along with actionable data to help guide remediation efforts.
Benefits of the Kenna Security Platform

- Reduce cyber risk by proactively focusing on high-risk vulnerabilities
- Increase IT efficiency by automating vulnerability analysis, correlation, and prioritization
- Obtain continuous, real-time visibility into the organization’s risk posture
- Make data-driven investment decisions based on objective risk metrics
- Eliminate spreadsheets and home-grown apps with automated reports
- Monitor risk and measure improvement over time