expel

CHAOS TO CLARITY

Risk-based prioritization in vulnerability management

Contents

INTRODUCTION

Software runs the world—and comes complete with vulnerabilities

From financial systems to electrical grids, most major business processes and infrastructure systems live and die by software and hardware computer systems, making them prime targets for attacks. A hacker exploiting a vulnerability—a security flaw, glitch, or weakness found in the code—can cripple the software's ability to control the environment and wreak havoc on an organization's operations, finances, and reputation.

Holding the line as an important part of an organization's overall security and risk management strategy is ***vulnerability management (VM),*** the ongoing process of identifying, assessing, prioritizing, mitigating, and monitoring software vulnerabilities. As a critical tool in this good fight, ***vulnerability prioritization*** helps you evaluate risks based on their severity, exploitability, and business impact so you can focus limited resources on remediating the most critical threats.

We invite you to learn more about our strategic and risk-based approach to this problem: **Expel® Vulnerability Prioritization.**

The ever-present problem of software vulnerabilities

In addition to exposing your systems to exploitation, vulnerabilities are increasing at an alarming rate, and they're hard to manage and difficult to patch.

Traditional CVSS Scoring System

Rating	CVSS Score
None	0.0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

Vulnerabilities—they're everywhere!

Software vulnerabilities are the second-most reported attack vector.* That means, as a security professional, you're wrangling an onslaught of vulnerabilities—26,448 software security flaws (to be exact) were reported in 2022. And that color-coded common vulnerability scoring system (CVSS)? More than 11% of vulnerabilities are deemed critical, with a CVSS score that's fire-engine red (between nine and ten). With critical vulnerabilities up 59% in 2022 compared with 2021, don't expect things to get any better.

Vulnerability management has ownership issues

Another issue with vulnerability management (VM) is that its ownership is split—it's controlled partly by security operations (SecOps, which deploys the vulnerability assessment tools and is responsible for determining which vulnerabilities need to be prioritized) and partly by IT operations (responsible for testing and remediating the patches). But many times, SecOps and IT aren't the only stakeholders. You may also have other teams—like dedicated vulnerability management or risk management teams—that define VM policies and processes and approve exceptions, along with various business leaders. Without consistent or shared goals across these teams, it's challenging to optimize vulnerability management.

The problem of unpatched software

Unpatched software is a beast of a problem. In fact, it's a top-three access route for hackers. And most security operations centers (SOCs) can't keep pace with the patching backlog. Two out of three (66%) security leaders report a backlog of more than 100,000 vulnerabilities. And while vulnerabilities are waiting to be patched, you can bet that threat actors know how to work the system and exploit deficiencies in patch management. Soaring vulnerability numbers, co-responsible teams, and unpatched software mean organizations must find a better way to identify and remediate vulnerabilities. We get it. For lasting value, you need a proactive approach to prioritization that's strategic, systematic, and scalable. If that seems like a tall order, it is. But read on.

*The State of Vulnerability Risk Management, 2023, Forrester Research, Inc., March 15, 2023

Why CVSS isn't getting it done for prioritization

In the past, remediation priority was tied to CVSS scores, which provide a qualitative measure of severity, ***not risk***. Since vulnerability tracking started in the late 1990s, more than 200,000 common vulnerabilities and exposures* (CVEs) have been added to the MITRE database. This is so many, in fact, that the National Institute of Standards and Technology (NIST) had to amend its CVE numbering format to add a fifth digit. To help with these booming numbers, CVSS scores were introduced to measure the severity of each vulnerability and provide a common framework for understanding potential impacts.

But then enterprises began to rely almost solely on CVSS scores to prioritize remediations—an approach that falls short for several reasons. First, CVSS scores aren't aligned with what's important to your business strategy, and they aren't able to account for an organization's unique tactical and operational objectives. For example, you must also consider attack feasibility, active threats, and other aspects of your security program, because what might be critical to one organization just isn't as important to another. Next, CVSS focuses on potential threats, not actual, so while criteria such as the use of privileged credentials or remote execution can be good indicators of possible threats, they don't consider how the vulnerability is actually being exploited or if an asset or organization is a likely target.

Finally, everything seems critical! According to the National Vulnerability Database, CVSS scored 15% of vulnerabilities as "critical" and another 43% as "high" severity.* When nearly 60% of vulnerabilities seem serious, which ones should you tackle first? Also: just because a vulnerability has a lower score, doesn't mean it can't do significant damage.

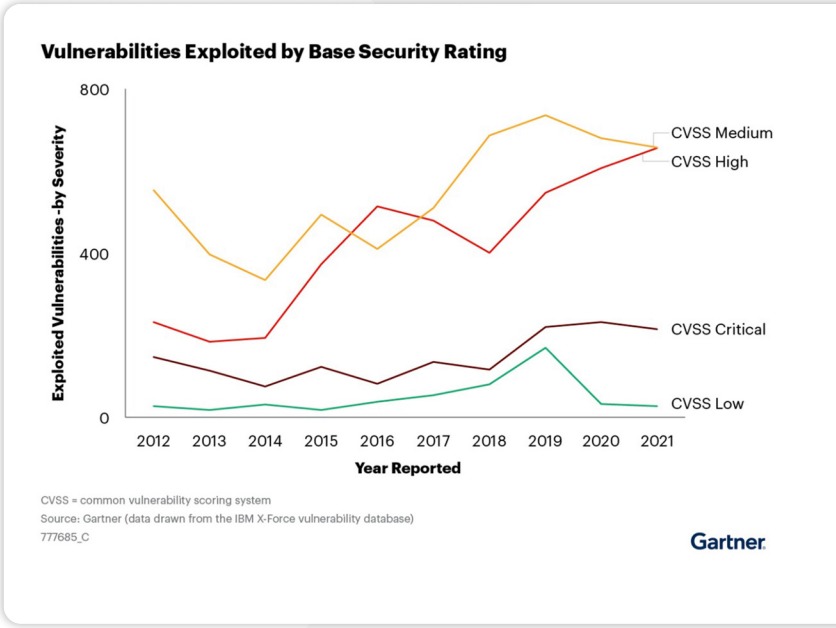
According to the National Vulnerability Database, CVSS scored **15% of vulnerabilities as "critical" and another 43% as "high" severity.** When nearly 60% of vulnerabilities seem serious, which ones should you tackle first?

*How To Strengthen Vulnerability Risk Management With Remediation Prioritization, Forester Research, Inc., December 21, 2022

Vulnerability management metrics need updating

The most common vulnerability management metrics (e.g., time-to-detection, vulnerability age, patching rate) are not risk-based and they often lead to ineffective, low-value prioritization with negative impacts and high costs. For example, neither velocity nor volume of vulnerabilities patched are effective indicators of a vulnerability management program's success.

As mentioned previously, prioritizing vulnerabilities based on CVSS scores isn't an effective strategy since many vulnerabilities rated critical or high may not have any significant relevance for your organization. Patching a vulnerability with a high CVSS score that poses little to no risk is a waste of time and resources. Conversely, threat actors often target vulnerabilities rated medium and low as a path of least resistance since lower CVSS scores aren't typically given the same level of scrutiny. For reference, see chart (right) from Gartner® report: [How to Implement a Risk-Based Vulnerability Management Methodology, By Craig Lawson, Published 20 April 2023](#).*



Using CVSS to rank vulnerabilities leaves out critical considerations, such as individual context, compensating controls, and exploit activity. Instead, security and risk management leaders should use metrics aligned with operational objectives and risk to improve their vulnerability management programs.

Risk-based metrics prioritize vulnerability treatment, with a goal of easily identifying vulnerabilities that:

- May cause **significant impact** to the organization if exploited;
- Are **most likely to be exploited** based on known threat techniques; and
- Can **be easily blocked** by other compensating controls and existing security tools.

A new risk-based approach to vulnerability management

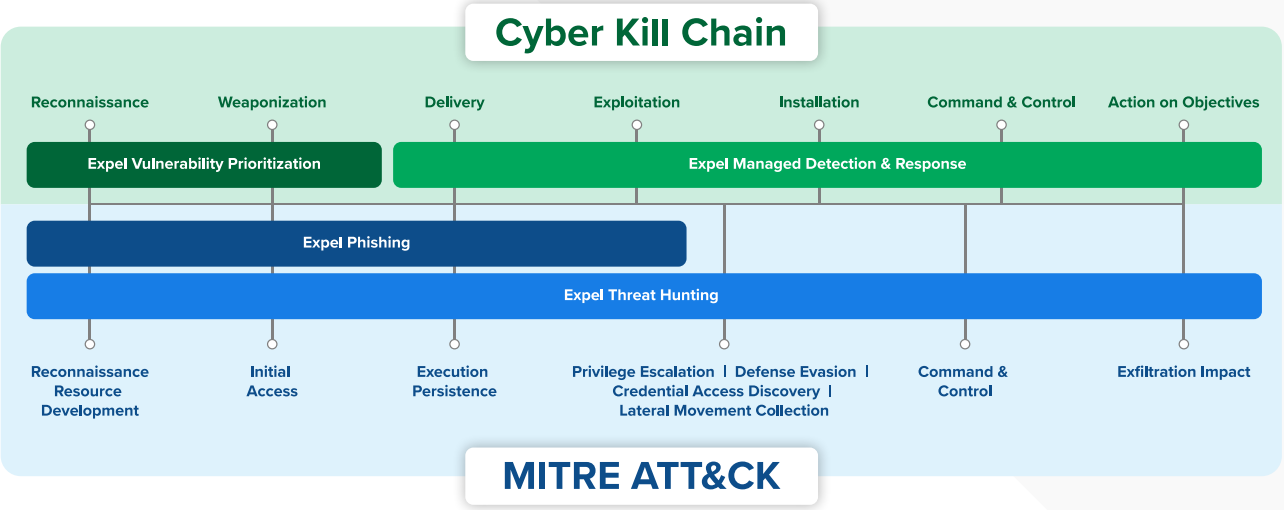
Prioritization is critical for effective risk and threat reduction. By implementing risk-based, stakeholder-specific vulnerability prioritization (like Expel Vulnerability Prioritization), you can reduce organizational risk and achieve better results. Instead of wasting resources on unimportant or low-risk vulnerabilities, Expel Vulnerability Prioritization focuses on the most-critical ones, identifying, prioritizing, and remediating based on the relative risk they pose ***to your organization***. Expel Vulnerability Prioritization accounts for the likelihood and impact of exploitation, as well as the business criticality and exposure of the affected systems, something for which vulnerability scanners don't have visibility.

To increase the effectiveness and impact of your vulnerability management efforts, industry analysts and experts, such as those at CISA, recommend you employ a risk-based, stakeholder-specific model to prioritize which vulnerabilities get put on the remediation list. This process includes enriching vulnerability findings with asset context and criticality, and correlating findings with active threats and known exploits. Analysts also recommend using a risk-based vulnerability approach that focuses effort and resources on treating relevant and exploitable vulnerabilities that pose the most significant business risk.

Simply put, you assign your resources to patch vulnerabilities that affect exposed or business-critical assets. For example, a payment card industry (PCI) scan should be completed more regularly than an end-user laptop scan. And when patching isn't practical, you must find effective compensating controls, such as endpoint and web-application security solutions—e.g., endpoint detection and response (EDR) and web application firewalls.

Vulnerability prioritization **accounts for the likelihood and impact of exploitation, as well as the business criticality and exposure** of the affected systems, something for which vulnerability scanners don't have visibility.

Expel's services aligned to the attack lifecycle



At Expel, we cover the entire threat lifecycle, so we can uncover common risks—whether from vulnerabilities or phishing attempts—as early as possible in the attack chain. We built our entire security operations platform around preventing risk upfront, while also weeding out the noise, so we can more quickly and effectively detect and respond to attacks. This ounce of prevention is worth a pound of cure—saving you a lot of headaches and reducing your risk profile.

Benefits of risk-based vulnerability prioritization

At Expel, we use threat intelligence and organizational context to enrich prioritization, helping you make faster and more confident decisions about what to patch first. We slice through the noise and cut down the hundreds or thousands of vulnerabilities piling up in your VM tools to a manageable number. We help you understand what you need to fix now and what can wait until the next remediation cycle. We provide context about each threat and targeted recommendations so you can avoid future attacks.

Our approach to vulnerability prioritization accelerates your remediation process by letting you know exactly which vulnerabilities pose the greatest risk, so you can:

- **Spend less time triaging and more time patching**. The sheer volume of vulnerabilities demands a keenly optimized approach to prioritization and remediation. We match internal context with potential exploitability, criticality, and likely impact to expedite prioritization, cutting remediation response times for identified exploits. Customers repeatedly tell us that prioritizing vulnerabilities takes many hours of research per week. What could you do with those hours back in your week?
- **Strengthen detection and response**. Vulnerability context across your environment highlights which assets are at risk, improving threat detection and response. The more context around your priority systems and VIPs you provide in our platform, the better. This context is visible to our vulnerability analysts and our MDR SOC team. As quickly as possible, we strive to identify possible risks to your organization, helping you stop threats before they attack, thereby lowering the impact and potential damage a breach would cause.

WHAT YOU GET:

Expel Vulnerability Prioritization

- **Integration with the scanner technology you already have**, whether it's Tenable, Rapid7, or one of the other technologies we integrate with.
- **Vulnerabilities prioritized by potential risk** to remove the lengthy investigation process from your team's workload and help you focus instead on closing the gaps.
- **Real-world threat intelligence** based on attacks we're seeing across Expel's customer base.
- **A dedicated vulnerability team** that uses our prioritization model and evaluation criteria to quickly identify and inform you of "priority one" vulnerabilities.
- **Visibility across your environment** by aligning vulnerability risk and upfront prevention with your detection and response process—all in one place.
- **Detailed vulnerability guidance** from Expel Workbench™ focusing on the next steps you can take to remediate.

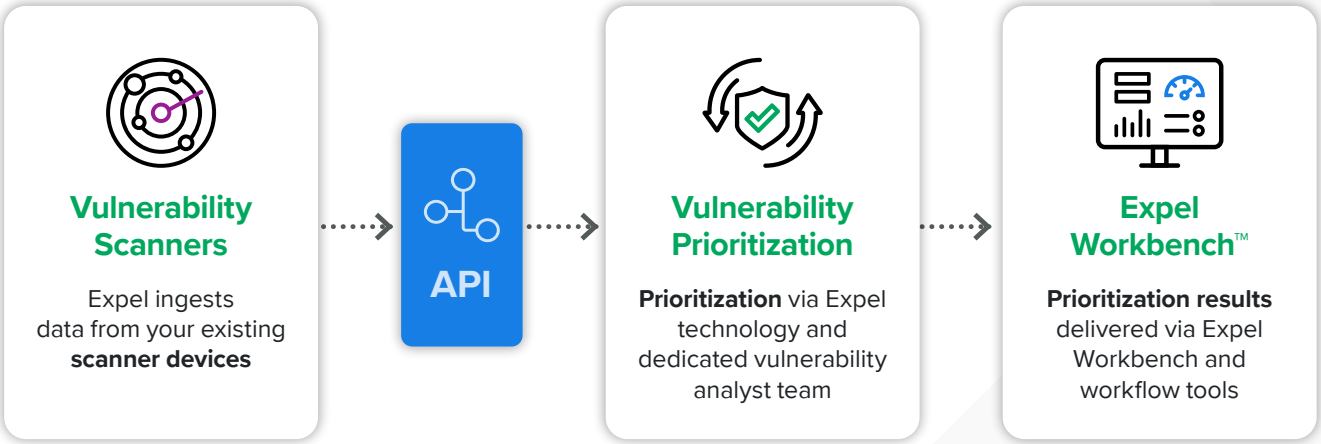
- **Improve visibility and decision making**. We provide investigation support and prescriptive guidance so you can easily communicate which vulnerabilities need to be remediated now and why. Our weekly roll-up reports with remediation guidance are also easily shared across teams, so you can keep all stakeholders better informed and aligned. With Expel you also benefit from extended visibility into real-world attacks on vulnerabilities within our customer base, but are yet to be identified publicly. In some cases, we'll tell you about a vulnerability we're seeing exploited that your VM assessment technologies haven't even picked up yet.

There are many tools out there that will give you a risk number, but with Expel you can feel confident knowing that our vulnerability analysts are reviewing your scans and qualifying which vulnerabilities should be prioritized based on the actual risk to your organization.

How we do it

Expel Vulnerability Prioritization does the heavy lifting for your SOC teams by investigating and prioritizing the most-critical vulnerabilities facing your organization. We consider your specific business and technical context, which vulnerabilities are being exploited, and our own Expel Managed Detection and Response (MDR) intelligence on attacks happening in the wild. Then we pair this with the information you're seeing within your VM assessment tools. You'll know immediately if the vulnerability requires emergency or urgent attention and what we recommend next for remediation.

How Expel Vulnerability Prioritization Works



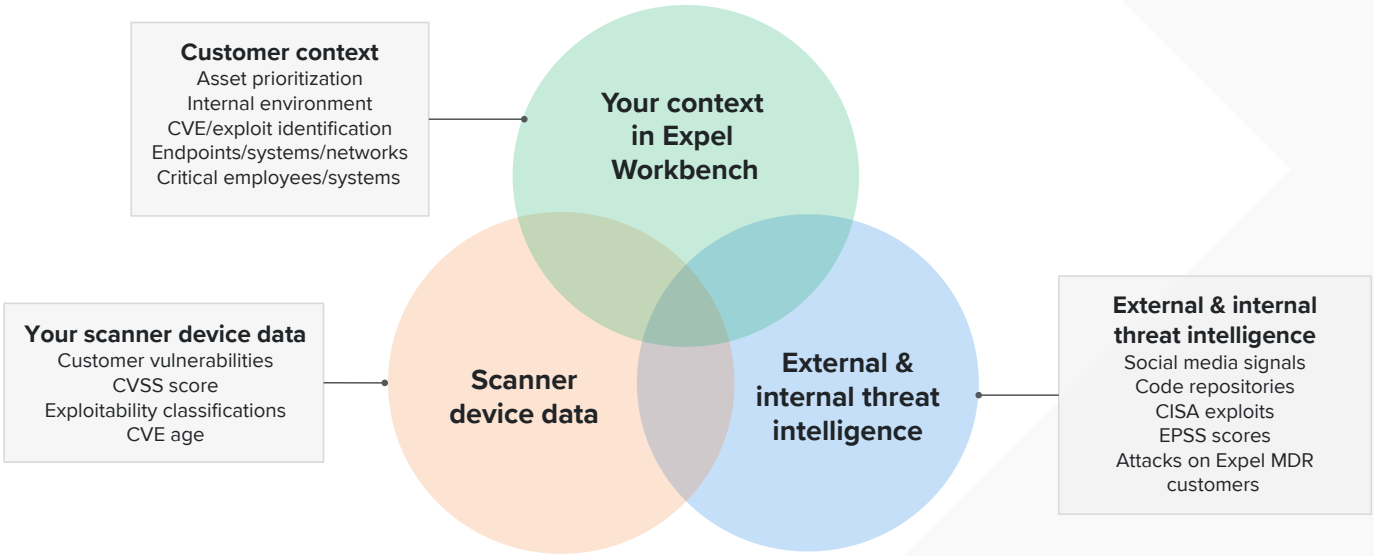
A natural extension—the Expel difference

We have a remarkable track record of reducing noise from the detection process and making sure our MDR customers promptly address incidents and alerts. Many customers told us exactly how painful and noisy they found the vulnerability management process. So we decided to tackle vulnerabilities based on that feedback. Like our MDR service, we use our security operations platform—Expel Workbench—to apply automations that help weed out much of the noise from the hundreds or sometimes thousands of vulnerabilities flagged in our customers' VM assessment tools. When we identify an active exploitation of a vulnerability from within our MDR customer base, we can also use that threat intelligence to help prioritize vulnerabilities. We understand the risks our MDR customers face, and our team quickly uses lessons learned to address vulnerabilities.

There are many tools out there that help with vulnerability prioritization by assigning a score or metric. But these tools still require your team to investigate and qualify what needs to go on the immediate remediation list. With Expel Vulnerability Prioritization, customers can feel confident that some of the same experts handling their detection and response needs are also investigating their vulnerabilities and qualifying which need urgent attention. There's no need to resource and manage a new technology, or have a team member guess what goes into a particular score and why the vulnerabilities received the score they did. Expel handles all of that on your behalf—we review your VM assessment scan results, qualify which require urgent attention and which can wait, and tell you exactly why we rated them the way we did. The context is then easily shared with internal IT stakeholders for easy prioritization and remediation.

What resources do we use? We consider numerous sources, including inthewild.io, exploit-db.com, CISA's Known Exploited Vulnerabilities Catalog, and code repositories, among other resources, to help us reliably note actively exploited vulnerabilities. We then evaluate and inform our customer base about the existing risk specific to their infrastructures and asset contexts.

What exactly goes into our prioritization model?



Learn more

So that's vulnerability prioritization 101! What's next is up to you. **To get started** prioritizing your vulnerabilities, visit us at here or request a demo.

About Expel

Expel helps companies of all shapes and sizes minimize business risk. Our technology and people work together to make sense of security signals—with your business in mind—to detect, understand, and fix issues fast. Expel offers managed detection and response (MDR), vulnerability prioritization, phishing protection, and threat hunting. For more information, visit our **website**, check out our **blog**, or keep up with us on **LinkedIn** or **X**.