



Vulnerability & Threat Trends Report 2024

Unprecedented Vulnerabilities
Expose Critical Gaps in
Traditional Vulnerability
Management Approaches



This past year has emerged as a watershed moment for cybersecurity,

setting unprecedented records in the volume and complexity of challenges faced by organizations worldwide. The landscape has been markedly transformed by an unparalleled increase in identified vulnerabilities, with the National Vulnerability Database (NVD) recording over 30,000 new Common Vulnerabilities and Exposures (CVEs). Notably, half of these vulnerabilities were classified as high or critical severity, creating a significant challenge for organizations in prioritizing and mitigating these threats.

Additionally, the exploitation timeline has tightened, with the mean time from CVE publication to exploit at just 44 days, and 25% of CVEs exploited on the same day they are published. Meanwhile, the Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR) vulnerabilities remains over an inadequate 100+ days.

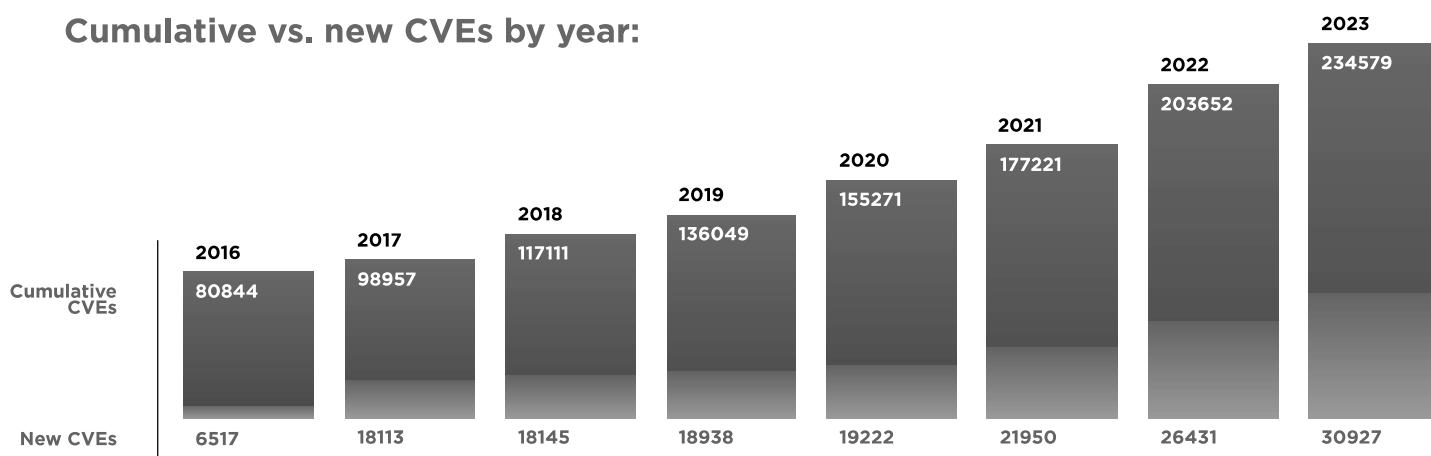
Amidst this backdrop, sectors such as financial services, manufacturing, and utilities find themselves at the nexus of heightened cyber threats, grappling with the financial and operational repercussions of data breaches and targeted attacks. Additionally, the increasing legal accountability of Chief Information Security Officers (CISOs) signals a paradigm shift toward more rigorous governance and compliance demands in cybersecurity management.

This 2024 Vulnerability and Threat Trends Report unravels the complexities of the cybersecurity ecosystem, highlighting key trends, sector-specific challenges, and the imperative for new approaches to identifying, prioritizing, and mitigating vulnerabilities in the face of an increasingly hostile digital environment.

2023: A Milestone Year in Cybersecurity Vulnerabilities

2023 marked an unprecedented period in the cybersecurity landscape, underscored by a record-setting surge in newly identified vulnerabilities. With the National Vulnerability Database (NVD) documenting 30,927 new Common Vulnerabilities and Exposures (CVEs) within the year, the frequency and severity of these security flaws reached new heights. This volume of vulnerabilities represents a significant uptick of 17% year-over-year, highlighting an accelerating trend in the identification of potential security risks.

Cumulative vs. new CVEs by year:



Since the NVD's inception, 234,579 CVEs have been cataloged over 30 years, yet astonishingly, half of these were discovered in just the past five years, indicating a dramatic escalation in vulnerability detection efforts and capabilities.

Half of all CVEs were published in just the last five years.

- SKYBOX RESEARCH LAB

The pace at which these vulnerabilities are being published is equally startling, with a new CVE emerging approximately every 17 minutes, averaging around 600 new vulnerabilities per week. While this number alone is shocking, the rapid rate of discovery underscores both the increasing sophistication of threat actors and the expanded complexity of modern software and systems; together, these create a fertile ground for vulnerabilities – and a lot of opportunity for cybercriminals.

A particularly concerning aspect of the 2023 data is that half of the new CVEs were classified as high or critical severity. This poses a significant challenge for organizations, as it dilutes focus from the most critical risks due to the sheer volume of vulnerabilities requiring attention, leaving security teams with a “focus gap.” The difficulty in prioritizing vulnerabilities effectively jeopardizes the ability of organizations to safeguard their systems against the most severe threats within their environment, potentially exposing them to significant security breaches.

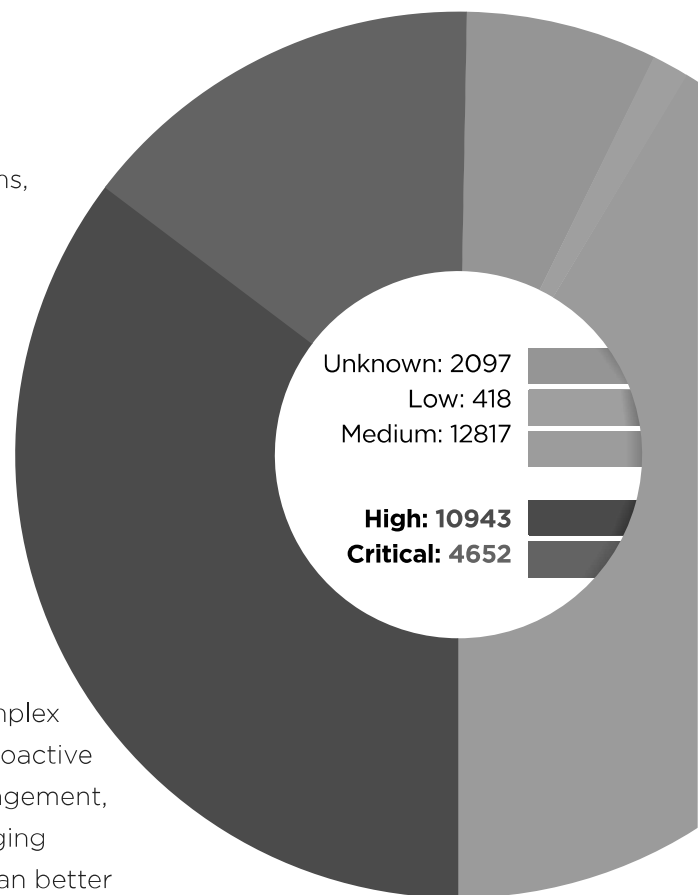
“A new vulnerability is published every 17 minutes”

- SKYBOX RESEARCH LAB

Several factors contribute to the rising trend in vulnerabilities:

- + The proliferation of interconnected devices and systems, expanding the attack surface for potential exploits.
- + The complexity of software has grown exponentially, with dependencies on multiple third-party libraries and components that may harbor undiscovered vulnerabilities.
- + The increased focus and investment in security research have also contributed, as more resources are dedicated to uncovering and documenting vulnerabilities.

The data from 2023 serves as a stark reminder of the evolving challenge cybersecurity professionals face in protecting digital assets in an increasingly hostile and complex digital environment. Today’s organizations need robust, proactive cybersecurity strategies. By prioritizing vulnerability management, adopting comprehensive security frameworks, and leveraging advanced threat intelligence and automation tools, they can better stay ahead of emerging risks.



FOCUS GAP:

HALF OF ALL 2023 VULNERABILITIES
ARE HIGH OR CRITICAL SEVERITY.

The Race Against Time: 2023 Exploit Trends Tighten Remediation Timelines

The cybersecurity terrain of 2023 has been distinctly marked by an upsurge in vulnerability exploits and the sophistication of attack vectors, underscoring an accelerated and alarming trend in the digital threat landscape. A stark comparison with the previous year reveals a notable escalation in the potential for cyberattacks: 2023 has witnessed over 7,000 vulnerabilities accompanied by proof-of-concept exploit code, according to Qualys. Skybox's own research identified 2000 vulnerabilities with confirmed weaponized exploit code, signaling a rise in the discovery of vulnerabilities and a significant advancement in the readiness and capability of threat actors to weaponize these vulnerabilities.

Rapid exploitation timelines severely limit the window for remediation



The timeline for exploitation has also tightened considerably, with the mean time between the publication of a CVE and the emergence of its exploit standing at 44 days. More alarming is the revelation that 25% of CVEs were exploited the day they were published and 75% within 19 days.

At the same time, the timeline for identifying a breach remains lengthy. According to IBM, organizations take over 200 days to identify a breach.

This rapid exploitation timeline and the long delay in identifying malicious activity necessitate swift and effective response mechanisms from organizations. There is a very short window for remediation of new vulnerabilities, which leaves cybercriminals ample time to compromise your networks if not acted upon quickly.

THE RISE OF AI: How Artificial Intelligence Impacts Cybersecurity

The attack vectors that dominated the cybersecurity landscape in 2023 include a range of both traditional and novel techniques. Among the most prevalent have been phishing attacks, now increasingly powered by artificial intelligence (AI) to enhance their effectiveness. AI-assisted phishing has become more sophisticated, with attackers leveraging AI to customize phishing emails, making them more convincing and difficult for users to identify. This use of AI extends beyond phishing, encompassing other techniques such as automated vulnerability scanning and the development of AI-powered malware, which presents challenges in detection and mitigation due to its dynamic and adaptive nature.

“75% of security professionals witnessed an increase in attacks over the past 12 months, with 85% attributing this rise to bad actors using generative AI.”

– DEEP INSTINCT, SAPIO RESEARCH, JUNE 2023

The impact of these AI-assisted cyber threats is profound, offering cybercriminals the ability to automate and scale their operations efficiently. This represents a significant shift in the cybersecurity paradigm, where the automation and adaptability of AI-powered threats demand equally dynamic and intelligent defense mechanisms. Organizations are thus compelled to integrate advanced technologies, including AI and machine learning, into their cybersecurity frameworks.

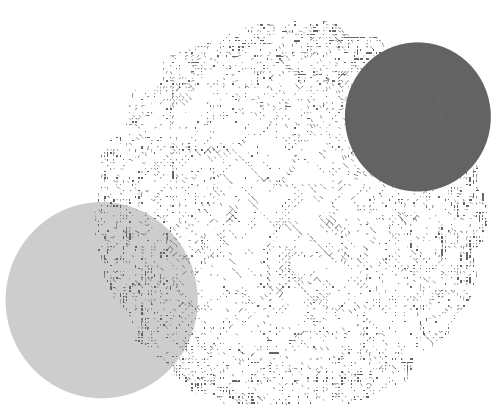
“44% of organizations reported success rates over 80% for their AI-powered cybersecurity tools.”

– GITNEX MARKETDATA REPORT 2024

These technologies not only aid in the early detection and response to threats but also in understanding and anticipating attacker behaviors and strategies. As the digital threat landscape continues to evolve, the emphasis on adaptive and proactive security measures becomes increasingly critical in safeguarding against the sophisticated and rapidly evolving threats of the modern era.

Sector Spotlight: Financial Services, Manufacturing, and Utilities Under Siege

In 2023, the cyber threat landscape witnessed significant escalations in the severity of attacks and the financial implications of data breaches. According to IBM, the average cost of a data breach soared to an unprecedented high of USD 4.45 million globally, with the United States facing even steeper costs at USD 9.48 million per incident. The per-record cost of compromised data stood at \$165, emphasizing the profound impact of cybersecurity breaches on organizations.



Cost of a data breach soared to
\$9.48M **...in the United States.**
- COST OF A DATA BREACH REPORT 2023, IBM

Industries across the spectrum faced heightened risks, but certain sectors were particularly vulnerable due to the nature of their operations and the sensitivity of the data they handle. Financial services, manufacturing, and utilities emerged as some of the most affected industries:

- + The financial sector, with its wealth of personal and financial data, remained a prime target for cybercriminals aiming for monetary gain.
- + Manufacturing, with its integral role in global supply chains and reliance on industrial control systems, experienced a notable increase in cyber threats, driven by the sector's technological advancements and digital integration.
- + Utilities faced unique challenges due to the critical infrastructure they manage and the potential for widespread disruption resulting from targeted cyberattacks.

Operational Technology (OT) environments, crucial across various industries, including utilities and manufacturing, have been under increasing threat. Frequently, vulnerability scanners don't cover OT networks or require the use of more than one scanner vendor, leaving you with an incomplete picture of your attack surface—referred to as the “visibility gap.” Notably, 47% of high-risk vulnerabilities affected network infrastructure and operating systems. This underscores the urgent need for a comprehensive vulnerability management strategy encompassing both IT and OT assets.



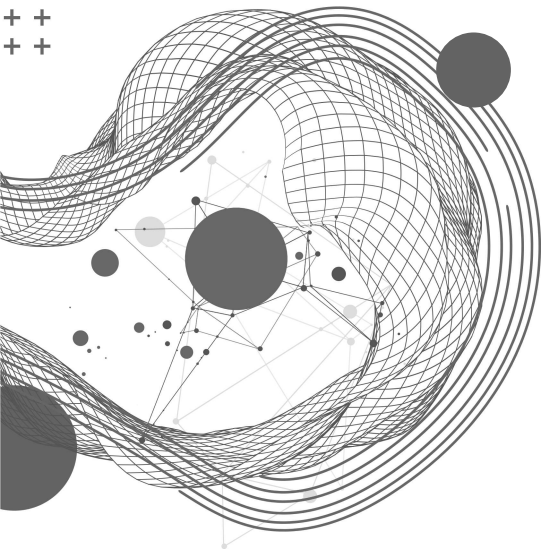
“47% of high-risk vulnerabilities affected network infrastructure and operating systems”

- QUALYS

Network anomalies and attacks dominated the threat landscape for OT and IoT environments in the latter half of 2023. Furthermore, critical manufacturing sectors witnessed a staggering 230% increase in vulnerabilities, spotlighting the escalating risks to industrial control systems.

75% of surveyed entities detected malicious cyber activity within their OT environments, with 24% being forced to shut down operations due to successful attacks, highlighting the tangible impact of these threats on operational continuity.

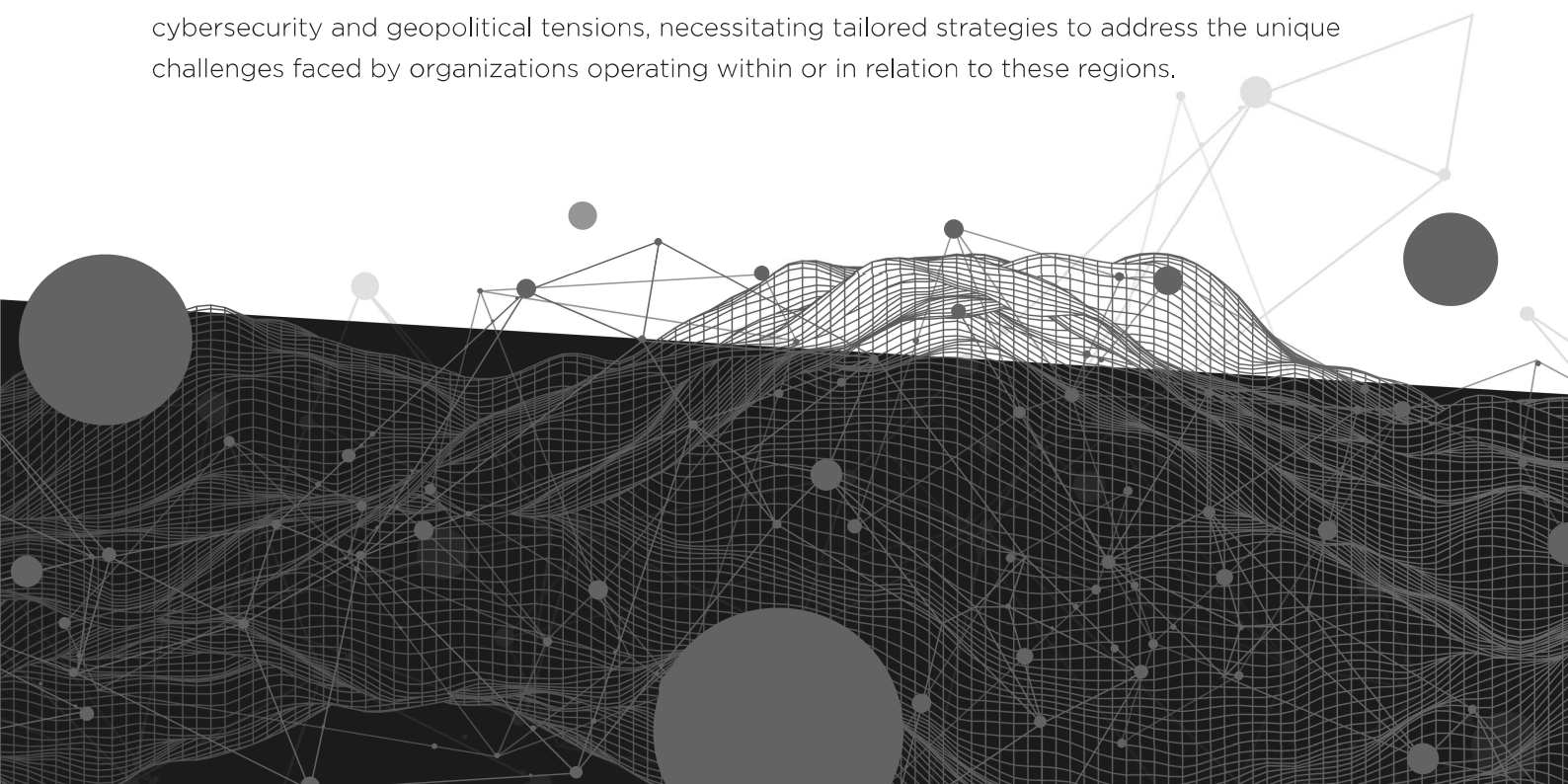
++
++
++



**“75% of teams detected
malicious cyber activity
within their OT environments,
24% were forced to shut
down operations”**

- PALO ALTO NETWORKS (PANW)

Geographic variations in vulnerability exposure and cyberattack patterns also emerged, with conflict zones like Ukraine, Israel, and regions involving China experiencing heightened cyber threats. These areas faced conventional cybercriminal activities and state-sponsored cyber operations aiming to exploit vulnerabilities for strategic advantages, disrupt critical infrastructure, or gather intelligence. This geographic differentiation in cyber threats underscores the complex interplay between cybersecurity and geopolitical tensions, necessitating tailored strategies to address the unique challenges faced by organizations operating within or in relation to these regions.



Advance Beyond Quarterly Scans: Continuous Vulnerability Management

In the evolving cybersecurity landscape, the significance of timely patch management and the overarching challenges in vulnerability remediation cannot be overstated. As the threat landscape intensifies, organizations face mounting pressures to mitigate vulnerabilities swiftly to avert potential breaches. However, this endeavor is fraught with complexities, notably due to the protracted Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR).

The MTTD, a critical metric in cybersecurity, is often prolonged significantly, partly because **regulatory frameworks like the Payment Card Industry Data Security Standard (PCI DSS) mandate only quarterly scans**. While monthly scans are deemed “ideal,” they still fall short of the agility required to counteract swiftly exploited vulnerabilities. This temporal “awareness gap” is further exacerbated by the MTTR, which in 2023 averages 65 days, according to Edgescan. Consequently, organizations face a daunting window of 95-155 days from the CVE publication to remediation. This timeline starkly contrasts with the mere 19 days it takes for 75% of vulnerabilities to have known exploits, leaving a critical vulnerability management gap – not to mention a wide-open door for many cybercriminals.

It takes just
19 days for 75%
of vulnerabilities to
be **exploited**

vs

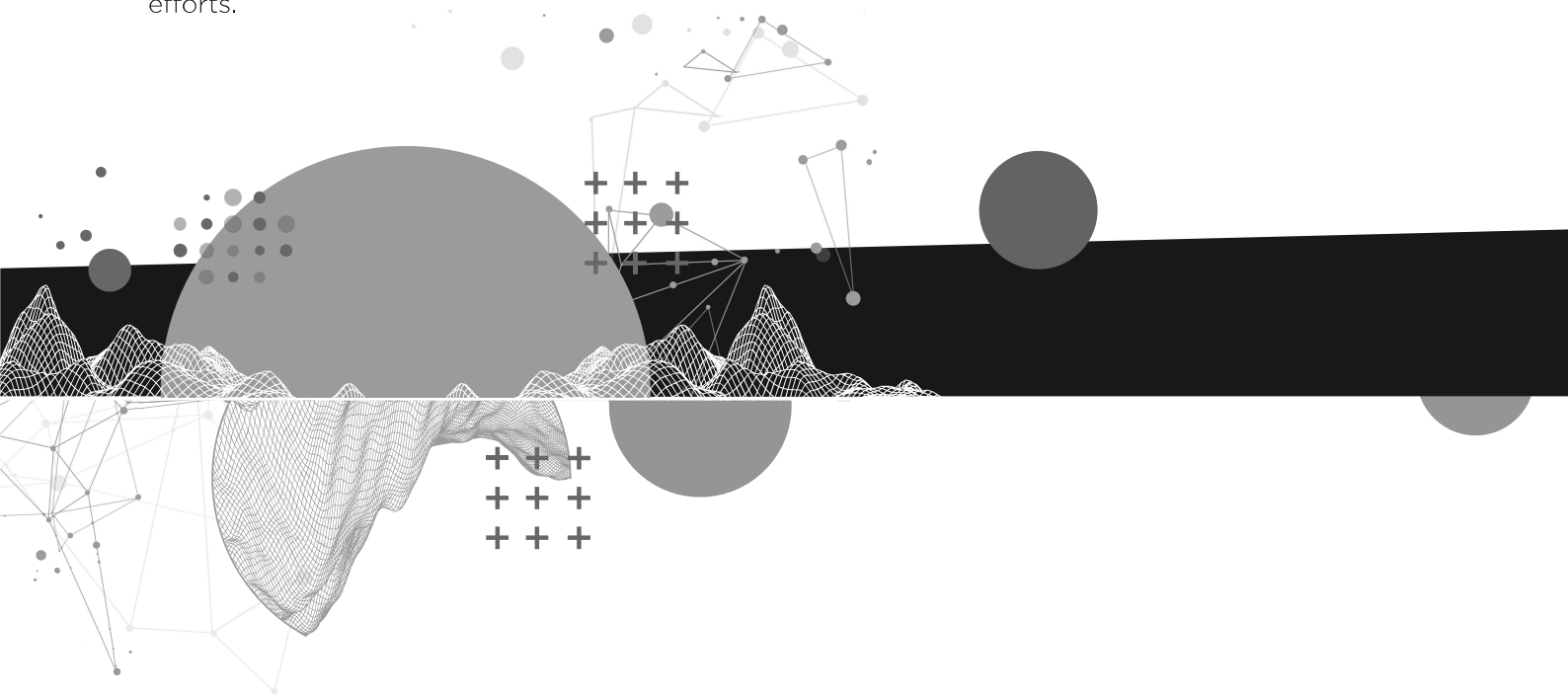
95 - 155 days
vulnerabilities take
to be **remediated**

In this precarious interval, dubbed the “exposure gap” (or “patch lag”), organizations must employ strategic mitigation strategies and compensating controls. Case studies of successful mitigation often highlight the utilization of intrusion detection systems (IDS), rigorous network segmentation, and the deployment of web application firewalls (WAF) as interim safeguards until patches can be applied. These measures can significantly reduce the risk surface by limiting potential exploit paths and isolating critical systems from compromised network segments.

A notable example of effective vulnerability management comes from a large financial institution that implemented a layered defense strategy. While awaiting patches for critical vulnerabilities, the institution leveraged advanced threat intelligence to monitor for potential exploit activity related to the known CVEs. Concurrently, they enhanced their endpoint detection and response (EDR) capabilities to identify and isolate affected systems rapidly, thereby minimizing potential impact. This proactive approach, coupled with a robust incident response plan, enabled the institution to navigate the patch lag-related exposure gap without suffering significant breaches.

Moreover, organizations that prioritize vulnerability scanning with greater frequency than the minimum standards set by PCI DSS often achieve shorter MTTRs. By employing continuous monitoring and automated scanning technologies, these entities can detect vulnerabilities closer to real-time, thereby narrowing the window of exposure.

Ultimately, the case for enhancing vulnerability management practices is compelling, underscoring the need for organizations to adopt a more dynamic and proactive stance in their cybersecurity efforts.



Beyond Patching Alone: Enhance Remediation with Mitigating Security Controls

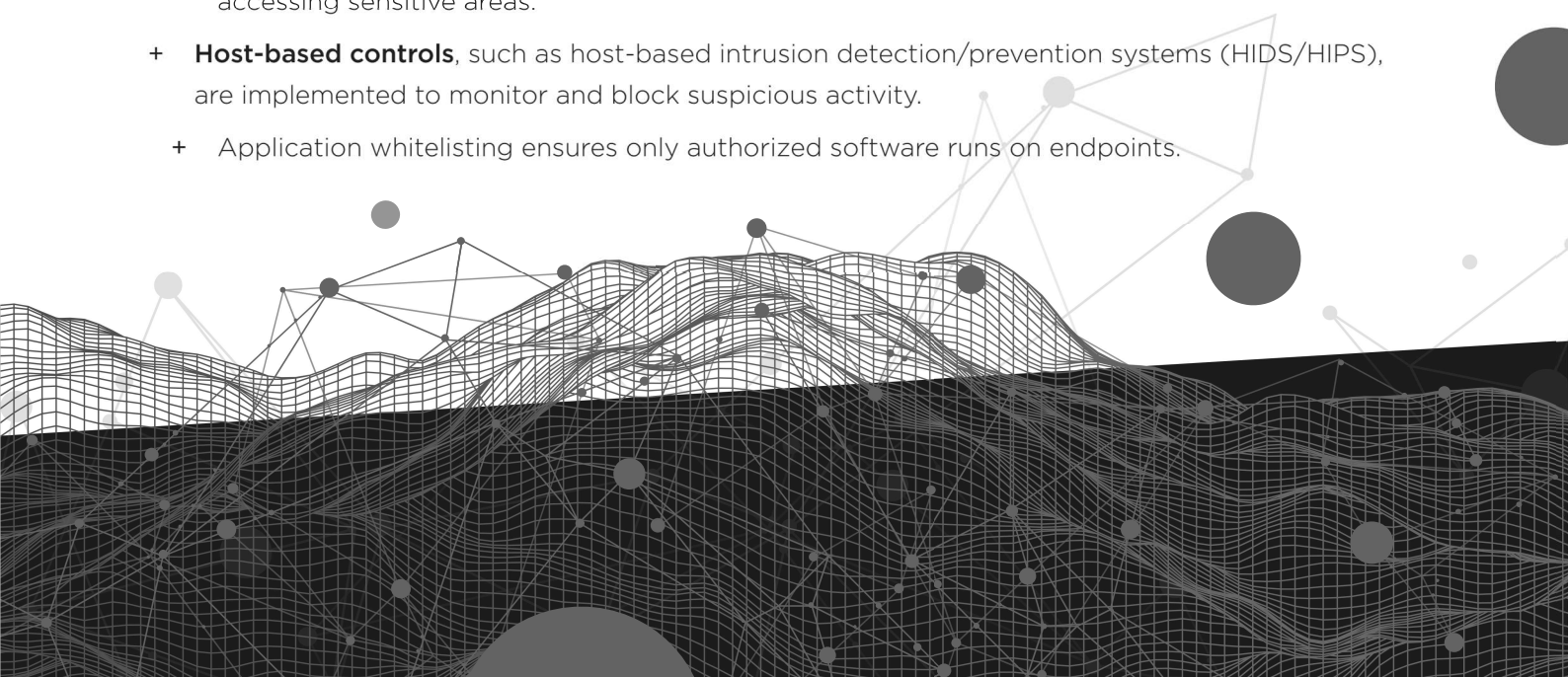
Organizations can better safeguard against the ever-present and evolving cyber threats by recognizing the criticality of reducing both MTTR and MTTR through advanced technologies and strategic compensating controls. One way to do this is to look at some of the current remediation techniques and see where or what may need to be updated.

For many organizations, patching remains the cornerstone of remediation efforts. However, relying solely on patching has its limitations, especially given the average patch cycle's time-consuming nature. Patching challenges include:

- + **Time-Consuming Process:** The patch lifecycle involves multiple stages—discovery, testing, deployment, and validation. This process can take weeks or even months.
- + **Downtime and Disruption:** Applying patches often requires system reboots or service interruptions, impacting business continuity.
- + **Zero-Day Vulnerabilities:** Some vulnerabilities have no official patches when discovered, leaving systems exposed until vendors release fixes.

These challenges make augmenting a patching strategy with additional security controls essential to reduce risk. Mitigating controls provide **immediate protection** while waiting for patches. Examples of compensating security controls include:

- + **Intrusion Prevention Systems (IPS)** signatures detect and block known attack patterns. They act as a virtual shield, preventing exploitation even before patches are applied.
 - + For example, if a critical vulnerability affects a web server, an IPS can block malicious requests targeting that vulnerability.
- + **Firewalls** filter network traffic based on predefined rules. Configuring firewall rules to strategically:
 - + **Block Known Exploits:** Deny traffic attempting to exploit known vulnerabilities.
 - + **Segmentation:** Isolate vulnerable systems from critical assets.
 - + **Whitelist/Blacklist:** Control communication to and from specific IP addresses or ports.
- + **Segmentation** divides the network into segments (e.g., DMZ, internal, external) to limit lateral movement.
 - + Even if a vulnerability exists, proper segmentation prevents attackers from easily accessing sensitive areas.
- + **Host-based controls**, such as host-based intrusion detection/prevention systems (HIDS/HIPS), are implemented to monitor and block suspicious activity.
 - + Application whitelisting ensures only authorized software runs on endpoints.



Vulnerability Prioritization: A Crucial Cybersecurity Strategy

Cybersecurity experts unanimously agree that vulnerability prioritization is a critical strategy due to the sheer quantity of threats in most organizations' operational landscape. Prioritization enables organizations to allocate resources effectively, address the most critical security gaps, and reduce exposure risk. A common strategy among security teams is to concentrate on industry standards such as CVSS score and known exploits (EPSS). However, this approach has major limitations.

Common Vulnerability Scoring System (CVSS) provides a numerical score to assess the severity of vulnerabilities. However, it is a one-size-fits-all model that treats all assets equally, ignoring contextual factors. It also only focuses on technical details; emphasizing technical aspects and overlooking other critical factors, such as business impact. **Exploit Prediction Scoring System (EPSS)** predicts exploit likelihood, but it lacks granularity and doesn't consider company or asset-specific factors.

This is why examining risk metrics specific to your business is important to prioritize risk in your environment better. Let's look deeper at the criticality of customer-specific context:

- + **Business Context Matters:** Not all vulnerabilities pose equal risks. Prioritization must align with business goals and asset importance.
- + **Network Exposure and Accessibility:** Consider how accessible a vulnerable asset is within your network. High-risk assets directly exposed to the internet demand immediate attention.
- + **Asset Criticality:** Prioritize based on asset criticality (e.g., critical infrastructure, customer data servers). Losing these assets could have severe consequences.
- + **Attack Surface Analysis:** Assess the attack surface to identify entry points for attackers. Prioritize vulnerabilities affecting critical entry points.
- + **Threat Intelligence:** Leverage threat intelligence to identify active exploits and emerging threats.
- + **Tailored Approach:** Organizations should customize their prioritization based on their unique environment, business processes, and risk appetite.
- + **Risk-Based Decision-Making:** Consider the impact of a successful attack on customer trust, financial losses, and regulatory compliance.
- + **Collaboration:** Involve stakeholders (IT, security, business units) to align priorities with organizational goals.

The Legal Lens on CISOs: A 2023 Trend of Growing Accountability

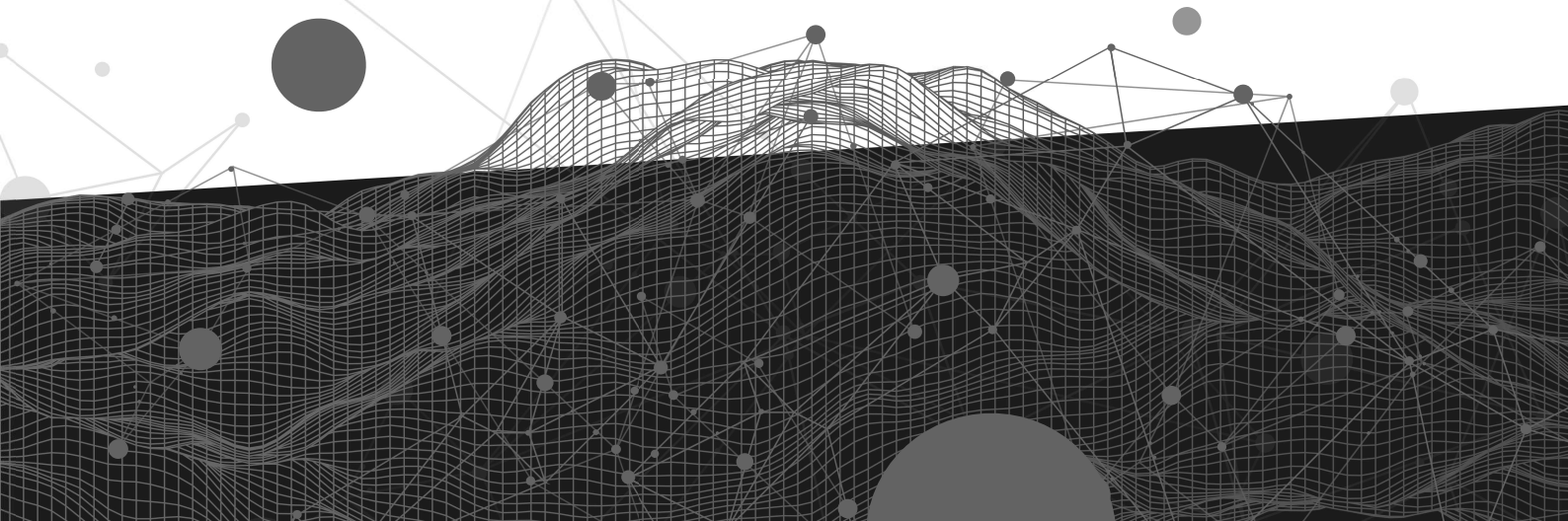
In 2023, the cybersecurity landscape underwent a seismic shift, with a notable increase in the accountability of Chief Information Security Officers (CISOs). This trend was starkly highlighted by recent actions from the U.S. Securities and Exchange Commission (SEC), which sent shockwaves through the security ranks. In a landmark case, **the SEC charged SolarWinds and its CISO with fraud and internal control failures**, emphasizing a willingness to hold CISOs legally liable for security shortcomings. This move underscores a broader trend where not just corporate entities but individual executives face scrutiny and potential legal consequences for cybersecurity failings.

“SEC charged SolarWinds and its CISO with fraud and internal control failures”

- U.S. SECURITIES AND EXCHANGE COMMISSION ON OCTOBER 30, 2023

The SEC's actions against SolarWinds and its CISO for fraudulently misleading investors about cybersecurity practices and known risks have underscored the importance of transparency and diligence in cybersecurity management. The charges highlight the growing expectation for CISOs to ensure the effectiveness of their cybersecurity programs and the accuracy and completeness of their disclosures to investors and the public. This situation is a stark reminder that the SEC will more strictly enforce its disclosure requirements, setting a precedent that could reshape how companies and their security leaders approach cybersecurity risk and compliance.

Adding to the narrative of heightened accountability, the cybersecurity community has closely followed the case of Uber's CISO, who was sentenced to probation for his role in covering up a 2016 cyberattack. This case further illustrates the serious legal risks facing security executives who fail to appropriately manage and disclose cybersecurity incidents. The judge's stern warning—that even someone with an exemplary character could face prison time for similar offenses in the future—highlights the increasing seriousness with which cybersecurity governance and ethical conduct are being treated.



These developments mark a pivotal moment in cybersecurity governance, where legal accountability is becoming a key part of the conversation. CISOs and other security leaders are now operating under a microscope, with their actions and decisions subject to not just internal scrutiny but also regulatory and legal consequences. This trend will likely prompt a reevaluation of security strategies and governance models, emphasizing transparency, compliance, and ethical responsibility.

“If I have a similar case tomorrow, even if the defendant had the character of Pope Francis, they would be going to prison”

- WILLIAM ORRICK, FEDERAL JUDGE,
NORTHERN DISTRICT OF CALIFORNIA

But CISOs don't have to go it alone. By leveraging the right tools and partnering with the right security partners, CISOs will be better prepared for this scrutiny while finding better ways to secure their organizations.

Conclusion

The year 2023 has undeniably marked a turning point in the cybersecurity landscape, characterized by a record surge in vulnerabilities, escalating severity of cyber threats, and heightened legal accountability for security leaders. These developments underscore the imperative for organizations to adopt a more dynamic, transparent, and proactive approach to cybersecurity. By leveraging continuous exposure management, prioritizing vulnerabilities based on risk, and adhering to ethical and legal standards in cybersecurity management, organizations can navigate the complexities of the modern digital environment, safeguarding against the sophisticated and rapidly evolving threats of our time.

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo 

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.