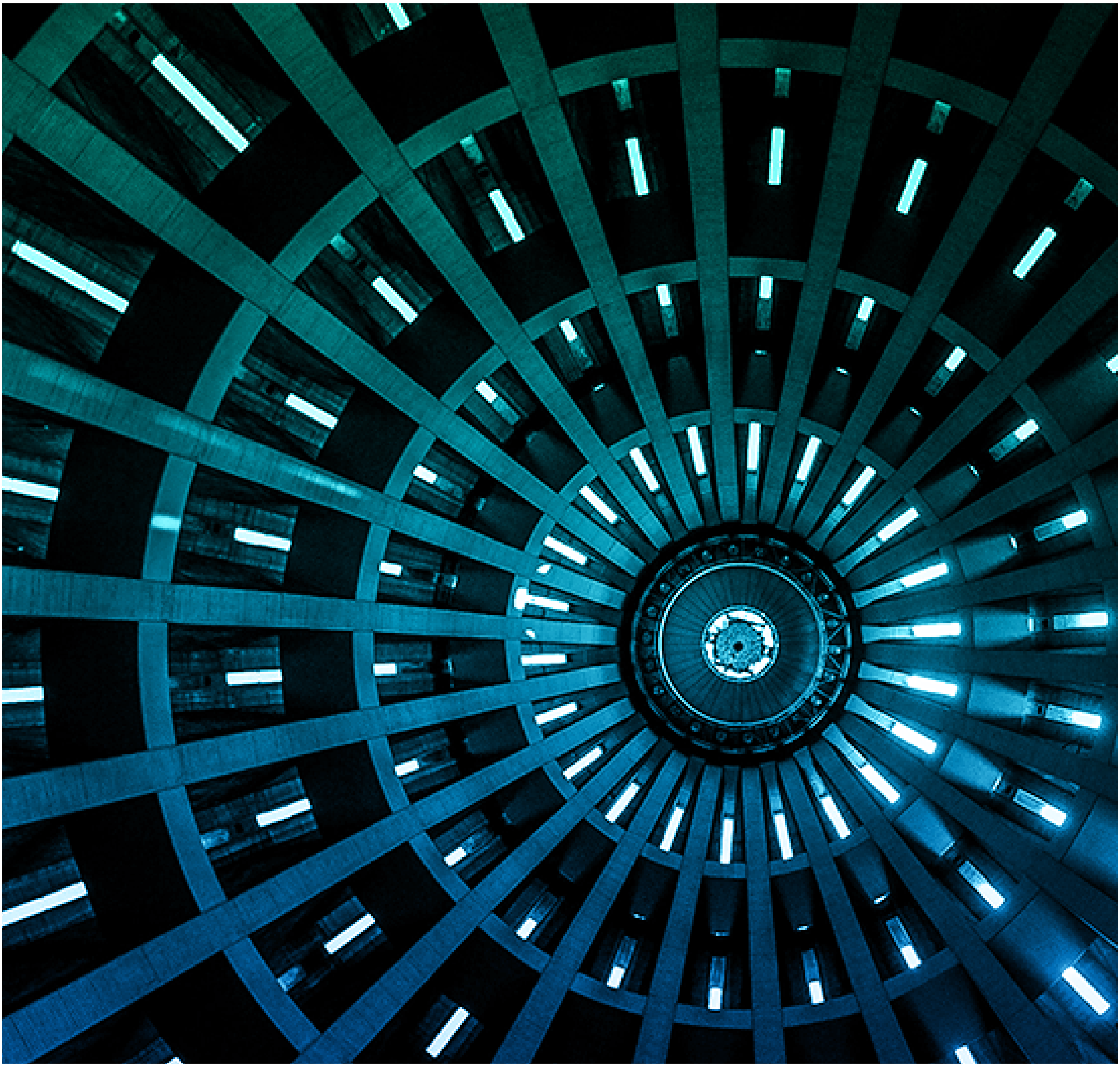
VULCAN. VOYAGER18

Cyber risk in 2022: A 360° view

Table of Contents

01 Introduction



Cyber risk today is a mutating, unpredictable beast

Threats are increasing and cyber risk data is sprawling. This puts IT security teams in the difficult position of having to fend off cyber attacks from multiple directions at once, all while trying to navigate an ever-changing threat environment. Threat actors aren't letting up, and breaches are causing more damage than ever before. Teams are stretched thin as they seek better ways to make sense of and prioritize their vulnerability risk data at massive scale, but fundamental blind spots stand in the way. **The next big attack could come from anywhere.**

18,378
new vulnerabilities were reported in 2021.[1]

The solution isn't just about identifying vulnerabilities or emerging threats, but recognizing the common threats and pitfalls that cause so much trouble for security teams again and again. Attackers are often lazy and are waiting to be presented with easy targets. Understanding individual threads within a cyber-risk tapestry is critical to a healthy security posture.

This research project is designed to help organizations **see the security forest through the vulnerability trees.** Designed to provide an actionable, high-level view of the overall threat landscape, it highlights the biggest developments and underlying narratives in cyber risk in 2022, and suggests ways to improve and maintain security posture as we enter 2023.

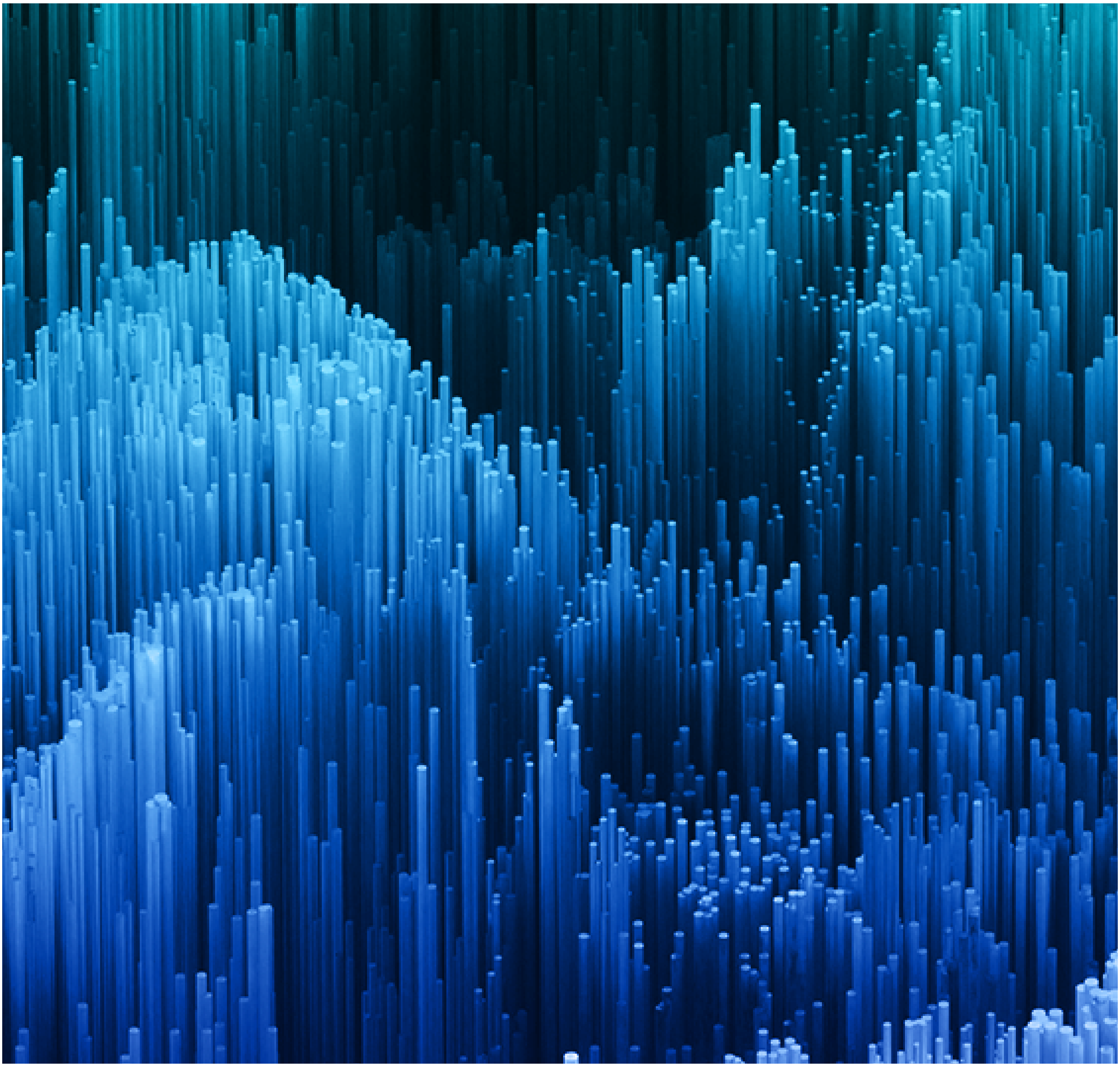
66%
of security leaders face a backlog of more than 100,000 vulnerabilities.[2]

Split into three parts, this report will first cover the world of **cyber risk as we know it** today, pointing to key trends and statistics affecting organizations globally. We then take a **deeper dive into cyber research**, exploring exactly how vulnerabilities are identified and how we can find connections to target overarching solutions rather than just solving individual problems. Finally, we take a look at **what 2023 holds** for cyber risk, including what trends we can expect and recommended actions we can take to stay secure as we head into the new year.

[1] Vulnerability management: Most orgs have a backlog of 100K vulnerabilities | VentureBeat

[2] Vulnerability management: Most orgs have a backlog of 100K vulnerabilities | VentureBeat

02 The cyber risk landscape



General trends

Cyber risk management remains a struggle for many organizations, particularly with the advent of remote work. Driven by the pandemic, organizations have modified their IT architectures and business operations to accommodate work-from-home initiatives.

Threat actors take advantage of these changes – including **cloud computing**, **remote access**, and other tools used to enable seamless operations – to find new attack vectors.

However, as the threat evolves, teams struggle to keep up with attacks.

Even worse, these cyber attacks are growing more sophisticated and common. For example, exploits of the Log4j vulnerability in late 2021 affected millions of companies, including tech giants like Amazon and Cisco.

The evolution of cyber risks has a substantial impact on cyber security trends. This makes it critical for organizations to adapt quickly so they can respond to the latest threats.

Some of the leading cyber risks and **cyber security trends in 2022** include the following:

$4.35m

the average cost of a data breach, rising by 2.6% from 2021.[3]

Malware on the rise

Malware attacks continue to plague businesses across industries.

According to McAfee[5], malware – including spyware and ransomware – represent the highest cost of damage for organizations, followed by data breaches.

$525m

malicious examples found in 13.7 billion collected samples, almost double the malware observed in 2020.[4]

Rise of ransomware attacks

Ransomware shows no signs of going away. In recent years, ransomware has grown into the most common and visible threat.

[3] Cost of a data breach 2022 | IBM

[4] 2022 Unit 42 Network Threat Trends Research Report | Palo Alto Networks

[5] The Hidden Costs of Cybercrime | McAfee

Ransomware encrypts the files on a system until the "ransom" is paid in cryptocurrency in exchange for a decryption key that is needed to restore access to those files. However, the key is not always delivered, or effective, even if the victim has paid the ransom.

Ransomware attacks are evolving rapidly, incorporating new methods of attack and new ways to extort money from victims. Today, threat actors often steal the data before encrypting it and then threaten to release the stolen data. In some cases, they will release part of the data on the dark web to show they have it. Bad actors also threaten to initiate distributed denial-of-service (DDoS) attacks to apply more pressure on victims to make them pay the ransom demand.

Security teams seemed to be getting better at defending against ransomware attacks. During the second and fourth quarters of 2021[6], ransomware attacks decreased from nearly **189 million cases to 133 million.** However, we have already surpassed that number in 2022.

$236.1m

ransomware attacks in first half of 2022 alone.[7]

Zero-day attacks

The first half of 2022 had a total of **18 zero-day exploits** (and counting). Half of these exploits were preventable flaws left unpatched. The good news is that this number is **significantly lower** than the 80 zero-day exploits[9] recorded in 2021, and almost **40%** of all zero-day exploits recorded over the last decade.

This suggests that security teams are getting better at managing cyber risk. However, it's best to avoid making connections between the decrease of zero-day threats and published vulnerabilities. The number of zero-days can vary wildly from year to year, as does the number of published vulnerabilities. However, this doesn't necessarily mean that every one of these vulnerabilities will be exploited.

50%

of zero-day vulnerabilities exploited during the first six months of 2022 were simply variants of previously patched bugs.[10]

[6] Number of ransomware attacks per year 2022 | Statista

[7] Number of ransomware attacks per year 2022 | Statista

[8] 18 Zero-Days Exploited So Far in 2022 | Dark Reading

[9] 40% of Zero Days Exploits From the Last Decade Happened in 2021 | Security Intelligence

[10] 18 Zero-Days Exploited So Far in 2022 | Dark Reading

Remote code execution

As the name suggests, remote code execution attacks allow threat actors to execute malicious code on a device remotely. These attacks can lead to malware execution that provides the attacker with complete control over the compromised machine.

The rise of cryptocurrencies also drives remote code execution attacks. In 2021, as many as **90%**[12] of such attacks, were related to cryptomining.

>262m

network exploit attempts observed, with most of these targeting high-severity vulnerabilities.[11]

Attack surface expansion

With hybrid working models on the rise, the attack surface is increasing daily. It is, therefore, no surprise that remote attacks have grown more prevalent and severe.

Digital supply-chain risks

It is predicted that **as many as 45%**[13] of organizations worldwide will experience attacks on their software supply-chains by 2025. That number represents a **three-fold increase** from 2021. Going forward, it is important for security teams and risk management leaders to strategize and prioritize digital supply-chain risk. This approach will help drive software partners across the supply chain to demonstrate security best practices.

Cyber security mesh

Cyber security mesh architecture[14] is growing increasingly popular, as it offers a standard integrated security structure and posture to protect all digital assets in the cloud or on-premises. This trend will be driven by security product consolidation, essentially accelerating the integration of security architecture components. As cyber risks evolve, cyber security mesh architecture will help CISOs respond better to future security and cyber risk management challenges.

[11] Google Details the Biggest Zero-Day Vulnerabilities Found So Far This Year | PCMag

[12] 2022 Cyber Security Statistics | PurpleSec

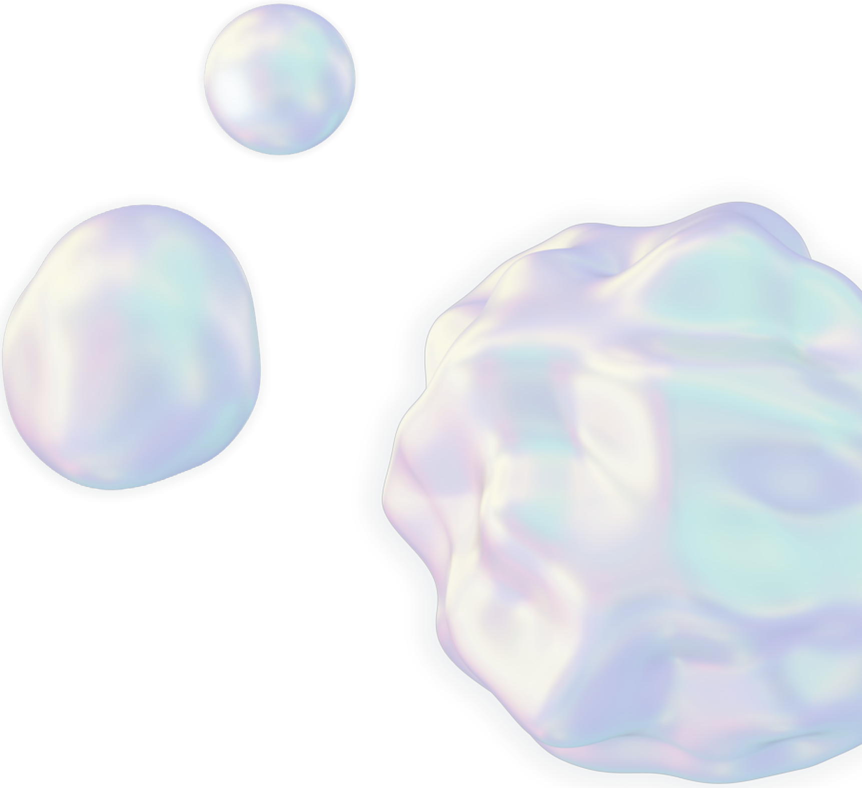
[13] Gartner Identifies Top Security and Risk Management Trends for 2022 | Gartner

[14] Cybersecurity Mesh Architecture (CSMA)? | Check Point Software

Zero trust

Zero trust — the approach of eliminating implicit trust within an organization and continually validating user security — is also a strong approach to mitigating risk in the new **hybrid workforce** reality. However, security teams must keep up with the latest cyber security trends and regularly update and patch their systems. It is imperative to maintain an up-to-date security posture that forces threat actors to start from scratch before trying to initiate an attack.

The increase in hybrid work models, brought about by the COVID-19 pandemic, mean employees are no longer subject to in-house security measures. As people lean more on their own work environments — either at home or in public spaces — security teams must implement zero trust measures to ensure the organization's workforce does not become an attack surface of its own.



Cyber risk in numbers

How effective are organizations in managing their cyber risk?

The general trajectory of cyber risk is one of increased threat to organizations' sensitive data. It should follow that IT security teams also get better at protecting their assets — or, at least, identifying where they're most vulnerable.

Through original research in partnership with Gartner Peer Insights, we surveyed practitioners in our industry to understand exactly how organizations were getting their vulnerability data, and how they were leveraging it to stay secure. Below are just some of the highlights from the two surveys we conducted this year:

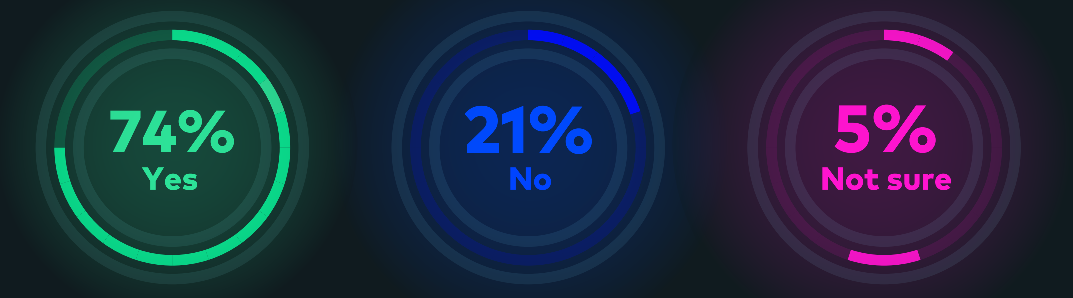
75% of respondents were impacted by an IT security vulnerability.

79% agree that vulnerabilities are misprioritized when taking their specific business environments into account.

65% confirmed that many vulnerabilities prioritized as low should be much higher for their organizations.

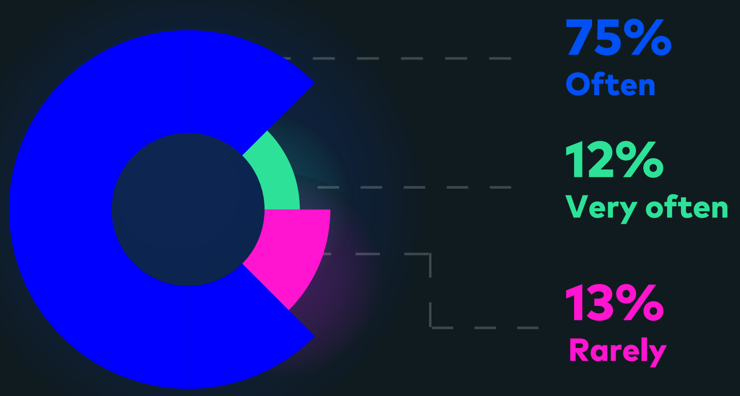
Diving deeper, we were especially interested to see increased dependence on threat intelligence by organizations for their cyber risk management efforts:

Do you have a team dedicated specifically to threat intelligence in place?



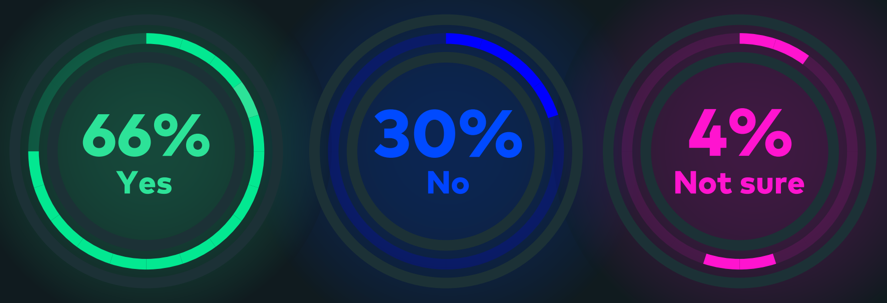
Nearly 75% of respondents' organizations have a dedicated threat intelligence team to assist with prioritization.

How often does your organization rely on threat intelligence for vulnerability prioritization?



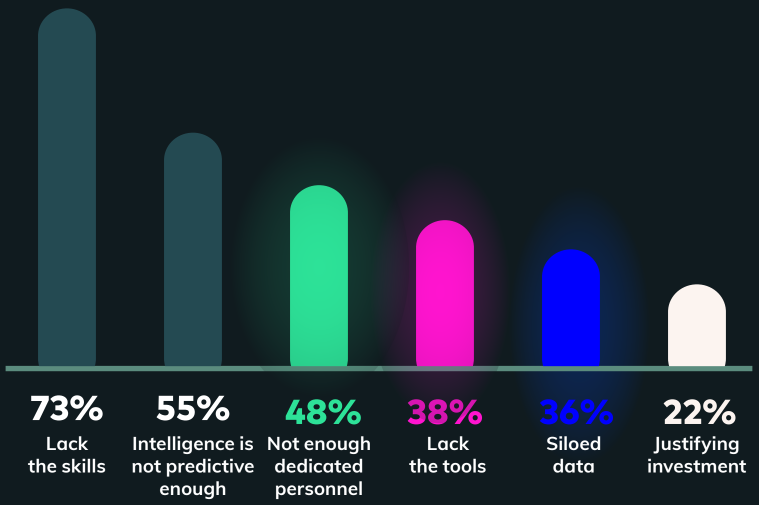
87% of respondents depend on threat intelligence for their prioritization.

Do you have budget allocated specifically for threat intelligence?



But only 66% have dedicated budgets for threat intelligence.

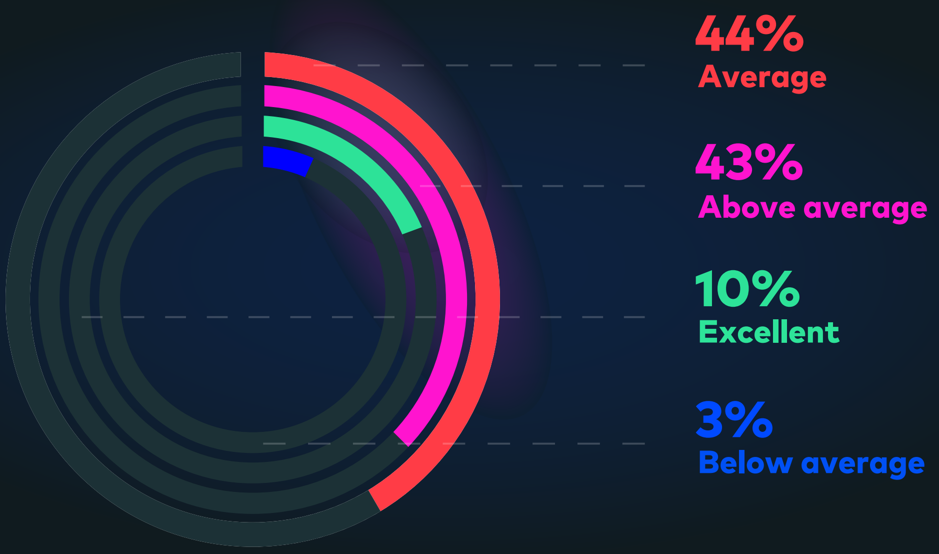
What are your biggest threat intelligence challenges?



Predictably, with budget limitations, 73% claim a skills shortage as one of the biggest challenges they face.

Please rate your organization's ability to take action based on threat intelligence.

While most respondents believe they have an at least average ability to take action on threat intelligence findings, the rise in data breaches and attacks over the past year tells a different story.

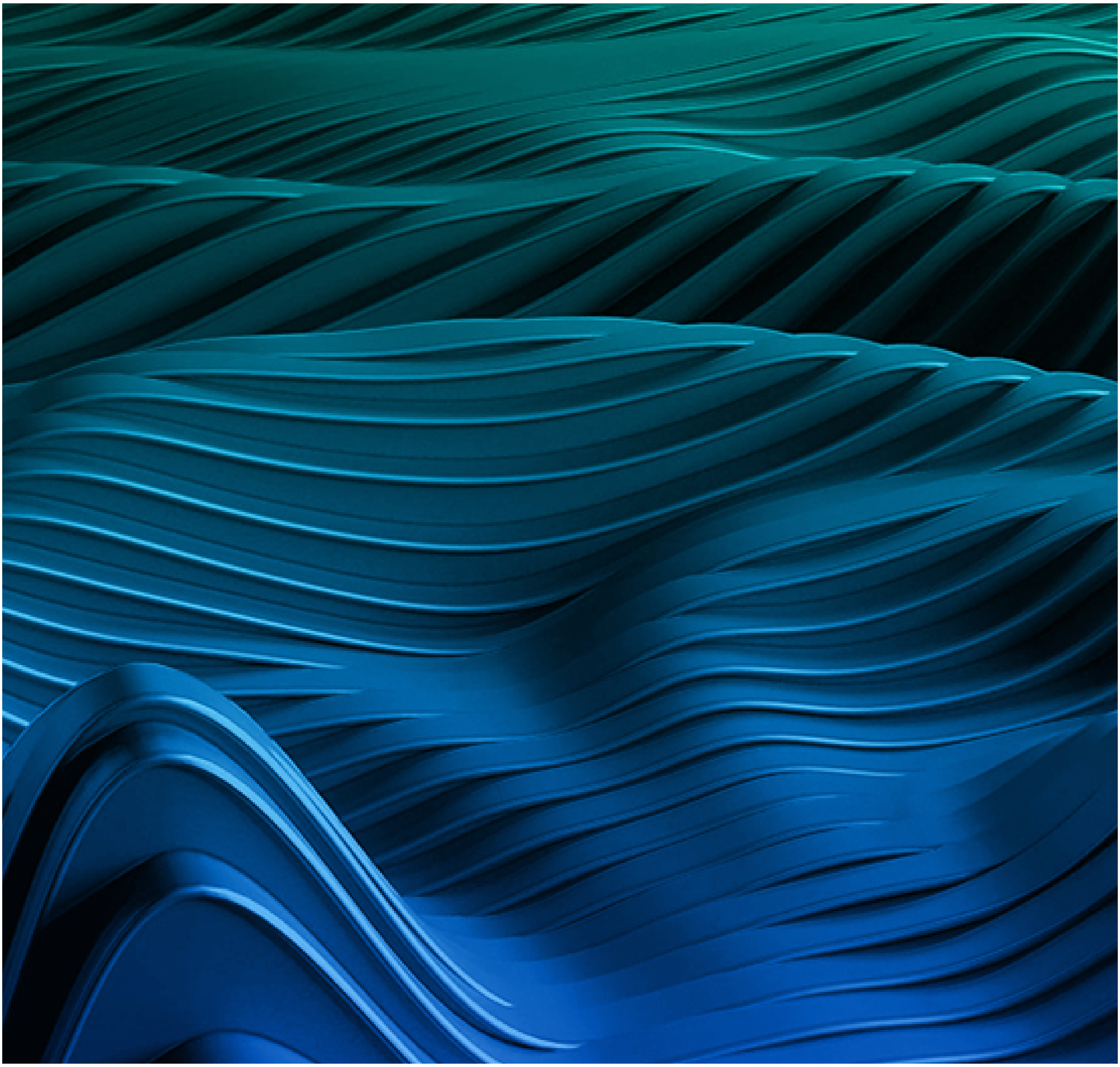


Practitioners will have different feelings about the efficacy of their vulnerability management or threat intelligence programs. Depending on their organizations and industry, some will be more confident than others about their ability to stay secure. But the fact remains that cyber risk is growing in general, and while the work of IT security teams is vital, processes must become more efficient to blunt the attacks coming from the unending flow of new vulnerabilities.

Part of this is gaining a clearer understanding of vulnerabilities: how they happen and how their potential impact is decided. Most importantly, we must recognize the common features that tie multiple vulnerabilities together, and implement strategies to target them as groups.

The next chapter will explore the nature of vulnerabilities, some of the most impactful in 2022, and how we can do better at recognizing repeat threats or common problems that can be easily fixed.

03 Inside cyber research



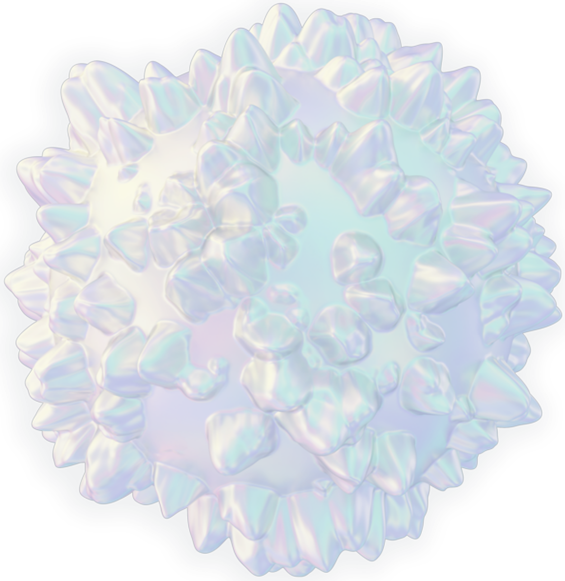
Introduction

With a greater frequency of threats – coupled with more serious consequences – and the greater attention teams are placing on threat intelligence and data, it makes sense that we ask the questions:

- How does **cyber research** work?
- What goes into identifying vulnerabilities and their **impact**?
- What can we learn about **common threats** and their solutions?

At Vulcan Cyber, our Voyager18 research team is dedicated to uncovering all the patterns, threats, and mitigation actions before theoretical breaches become very real problems. Leveraging the existing data and enriching it with further analysis, the Voyager18 team is uniquely positioned to identify and explore vulnerability trends as — not before — they emerge.

This chapter will cover the basics of exploit maturity and some of the most widely seen **vulnerabilities of 2022** as examples. We will also share the team's efforts to **map the MITRE ATT&CK** framework to common vulnerabilities. Finally, we'll present solutions to the common threats we have seen in the last year.



The evolution of exploit maturity

Vulnerability scanning across multiple attack surfaces of a product can often yield hundreds of vulnerabilities. Of course, it's impossible to resolve all of these vulnerabilities at once, as teams lack the capacity and/or resources to do so. At the same time, organizations are under constant pressure to update and improve their network, application, and cloud environments.

Exploit maturity data enables filtering of the vulnerabilities to identify mature ones with a record of exploitation, those vulnerabilities for which there is only proof that they could be exploited, and vulnerabilities with no recorded exploitation data.

Ultimately, the realistic goal is not to fix all the vulnerabilities, but rather to fix those that could negatively impact the business. Accordingly, first ascertaining the level of maturity of the vulnerability is an essential exercise when faced with multiple potentially serious threats.

Vulnerability maturity level

A vulnerability can be classified into one of three categories based on the exploitation records and cause:

- **Unknown:** A vulnerability has been identified and a warning has been issued by the developer or the maintainer of a third-party library, database, or operating system. There is no evidence of exploitation in the wild, and no published proof of concept is known.

- **Proof of concept:** No exploitation has been recorded, but there is a proof of concept that exploits the vulnerability. The exploit may be difficult to implement, impractical, or simply hasn't been used in the wild.

- **Exploited:** There are real cases in which attackers have exploited the system, or the vulnerability has been verified by an author in an authoritative exploit database.

Criteria for maturity levels

A vulnerability that is being actively exploited usually requires immediate attention, but there are several criteria to consider so that security operations teams can identify those with the highest priority.

1. Effort needed to exploit the vulnerability

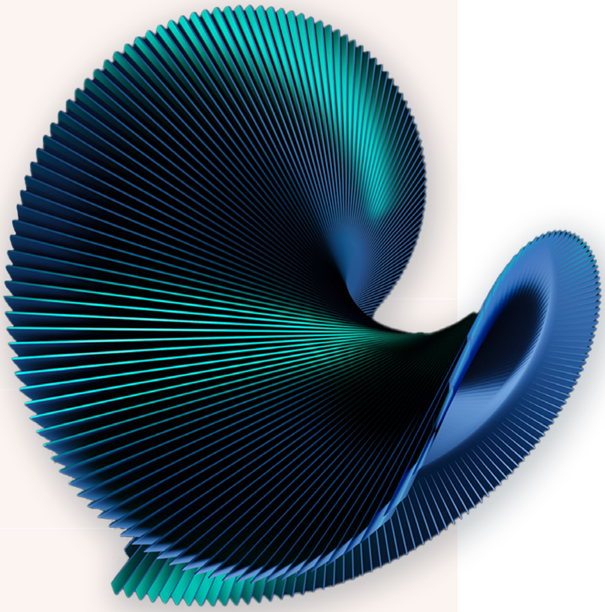
With attackers generally being opportunists seeking quick wins and open goals, they're likely to ignore exploits that require considerable effort to leverage:

- **Amount of work:** The more steps needed to exploit the vulnerability, the less appealing it is to threat actors, which will lower the risk.

- **Ease of exploitation:** How much expertise do threat actors need to exploit this vulnerability? A complex exploitation process will mean that threat actors are more likely to use other, easier, exploits which means the vulnerability is less likely to pose an immediate threat.

Many steps may need to be executed in order to make an exploitation work, such as:

- Registering a new account in the customer portal
- Successfully purchasing the product
- Registering the purchased product kit with the current account
- Calling an API that has a vulnerability



2. Exploit availability

Where we might find the exploit is also important when it comes to assessing the risk of the vulnerability. If the exploit appears in the exploit database, it means an exploit is confirmed to exist, and the vulnerability should be remediated right away.

3. Exploit impact

For every exploited vulnerability found in the wild, its impact on the company, product, and reputation can differ. Confidentiality, integrity, and availability are all potentially affected in the case of a data breach. Understanding where you stand to be most impacted is key to determining what to focus on first.

4. Exploit scope

An exploit affecting a single system is a wholly different situation than one that targets an organization's entire environment. Security teams must identify the potential scope of an exploit in order to assess how much of a priority it is compared to others. Note that even exploits compromising a single host will often lead to the entire system being affected, so the scope must be considered in this context.

Exploring how vulnerabilities turn into exploits gives us visibility into the lifecycle of a potential system compromise — and helps us better strategize how to avoid one. But equally valuable is taking a look at some of the most critical exploited vulnerabilities of the past year and identifying what caused them and how they can be fixed. Moreover, as we close out 2022, many of these remain active concerns for organizations and so demand the attention of security teams.

Impact in context

In 2016[15], attackers exploited a security vulnerability in a major banking system to inject malware to delete database records of illegal transfers, resulting in fraudulent withdrawals equivalent to around $1 billion.

Scope in context

In 2017[16], The Google Project Zero team found that Cloudflare's servers were allowing sensitive date to be cached by search engines. The caching mecahnism was triggered 1,242,071 times, and, in Cloudflare's case the scope affected multipe web applications from around the world.

[15] How the New York Fed fumbled over the Bangladesh Bank cyber-heist | Reuters

[16] Incident report on memory leak caused by Cloudflare parser bug | Cloudflare

Notable vulnerabilities in 2022

Supply-chain, SaaS, cloud, IoT — the second new technologies emerge, new security vulnerabilities that use these technologies against us also seem to emerge, turning them into points of weakness and portals through which to attack our businesses.

So far, it's clear that 2022 is no exception, with attacks by entities small and large scanning for every possible weakness.

That's why it's essential to stay ahead of vulnerabilities as they emerge and, in particular, to understand whether or not they affect your business.

Our Voyager18 team took a look at 10 common vulnerabilities from 2022 and the corresponding mitigation actions.

CVE-2021-4034 / PwnKit
CVE-2022-0847 / Dirty Pipe
CVE-2022-22965 / Spring4Shell / Spring Framework RCE
CTX Package Vulnerability
CVE-2022-30190 / Follina Microsoft Support Diagnostic Tool
CVE-2022-26138 / Atlassian Questions for Confluence Vulnerability
CVE-2022-26136 / CVE-2022-26137 Atlassian Servlet Filter Dispatches
CVE-2022-22620 / Use-After-Free in Safari Zero-Day
CVE-2022-1096 / Type Confusion in V8
Cyber risk in SaaS products

For each of these vulnerabilities, we have provided some basic information about the vulnerability, how widespread it is, and what systems are affected. We've also included the remediation deadline determined by the U.S. Cyber and Infrastructure Security Agent (CISA), as updated in CISA's catalog.

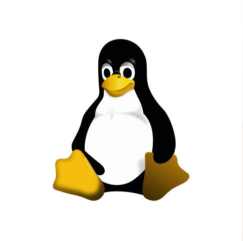
These deadlines were introduced in 2021, and although only mandatory for federal agencies, they are increasingly being adopted as the gold standard within the private sector as well.

CVE-2021-4034 / PwnKit

CISA deadline:	July 18, 2022
Type:	Local Privilege Escalation
Impact:	Non Privileged users and processes can gain root access
Wild exploit:	Yes
Affects:	Polkit's pkexec utility
Platforms:	Most major Linux distributions (Ubuntu, Debian, Fedora, CentOS, and others)
Workaround:	Remove the set setuid (SUID) bit from the pkexec binary, however this could potentially interfere with functionality
Remediation actions:	Read more

While PwnKit was first identified in January 2022, it was not actively being exploited in the wild at the time. In June 2022, however, CISA added PwnKit[17] to its list of vulnerabilities being actively exploited in the wild. That means that five months after the vulnerability became known and OS updates started becoming available to correct the problem, attackers were just beginning to use it as an attack vector. This highlights the importance of reducing time to remediation. Older vulnerabilities like PwnKit may pose some of the biggest risks, because they are so well known and with widely available proofs of concept.

CVE-2022-0847 / Dirty Pipe



CISA deadline:	May 16, 2022
Type:	Arbitrary File Manipulation
Impact:	Overwrite read-only or immutable data, local privilege escalation
Wild exploit:	Yes
Affects:	Linux and Android kernel (pipe buffer structure)
Platforms:	Linux kernel versions 5.8 and later, as well as Android kernel
Workaround:	None
Remediation actions:	Read more

Linux users have historically felt as though they were exempt from the waves of vulnerabilities and malware sweeping the industry, but that is no longer the case. With Linux bearing the brunt of a large number of mission-critical application servers for businesses and governments around the world, the number of Linux-targeted attacks is likely to rise over the next few years. This particular vulnerability came hot on the heels of PwnKit, and CISA confirmed just a few weeks after its discovery that it was being actively exploited in the wild.

[17] CISA warns of hackers exploiting PwnKit Linux vulnerability | Bleeping Computer

CVE-2022-22965 / Spring4Shell / Spring Framework RCE

CISA deadline:	April 25, 2022
Type:	Remote Code Execution
Impact:	Loss of system control
Wild exploit:	Yes
Affects:	Spring MVC or Spring WebFlux applications using data binding on JDK 9+ (unless application is deployed as a Spring Boot executable jar) — application must be deployed as a web application resource (WAR) on the Apache Tomcat server (Tomcat is one of today's most popular web server and Java Servlet Containers)
Platforms:	Spring Framework
Workaround:	None
Remediation actions:	Read more

The Spring Framework has become increasingly important in enterprise-level Java development since it is lightweight and ideal for creating today's loosely coupled applications, driven by dependency injection. Like many development tools today, it is open source and backed by a strong community. However, the fact that so many developers are using the Spring Framework means that when a vulnerability exists in the framework itself, it can be rapidly exploited in many places at once. While Spring4Shell is harder to exploit than the earlier Log4Shell vulnerability, this is yet another reminder of the security risks of today's fast-paced software development.

CTX Package Vulnerability

CISA deadline:	N/A
Type:	Repository Compromise
Impact:	Sends confidential and sensitive data to an attacker
Wild exploit:	Yes
Affects:	CTX, a library that provides Python developers with simpler ways to call common dictionary functions using dot notation; note that since CTX has been removed from PyPI, existing programs may not function as intended until they are updated
Platforms:	All Python applications
Workaround:	None
Remediation actions:	Read more

This CTX Package vulnerability is an outlier because it is not a conventional application vulnerability, but rather a problem with an independently produced update to the CTX package in Python. CTX is a library that remained relatively stable in Python for a long time (8 years), but the library's code in the centralized Python code repository (known as the Python Package Index, or PyPI) was compromised earlier this year, leading to a supply-chain attack. Because users often install all available updates directly from PyPI, many developers installed the compromised CTX package without realizing it.

CVE-2022-30190 / Follina Microsoft Support Diagnostic Tool (MSDT)

CISA deadline:	July 5, 2022
Type:	Remote Code Execution
Impact:	Arbitrary code execution to install programs, view, change, or delete data, or create new accounts
Wild exploit:	Yes
Affects:	Microsoft Support Diagnostic Tool (MSDT)
Platforms:	Windows 8.1, Windows Server 2012 R2, Windows Server 2012. Windows 7, Windows Server 2008 R2, and Windows Server 2008 SP2
Workaround:	Disable the MSDT protocol within the registry, following Microsoft guidance here
Remediation actions:	Read more

With MSDT being part of every single Windows installation, security researchers discovered that this ubiquitous vulnerability was being exploited in the wild within days of its being publicized. Attackers make use of this vulnerability to install payloads including information stealers like Qbot (also known as Pinkslipbot or Qakbot) and AsyncRAT, a variety of remote access trojan (RAT) that lets attackers take control. Alarmingly, while Follina was first discovered back in May 2022, and possibly exploited as long as a month earlier, Microsoft did not release a patch until late June.

CVE-2022-26138 / Atlassian Questions for Confluence Vulnerability

CISA deadline:	August 19, 2022
Type:	Hard-coded credential vulnerability
Impact:	Log into servers, view and edit non-restricted pages in Confluence
Wild exploit:	Yes
Affects:	Versions 2.7.34, 2.7.35, and 3.0.2 of Questions for Confluence
Platforms:	Confluence Server and Data Center
Workaround:	Disable or delete the disabledsystemuser account
Remediation actions:	Read more

This vulnerability is due to the use of a hard-coded username (disabledsystemuser) and password in the Questions for Confluence knowledge-sharing application. When the password was leaked on Twitter, it gave attackers a carte blanche to access and modify content. Hard-coded credentials (officially categorized by MITRE as CWE-798) is a common security weakness almost always caused by poor or deprecated coding practices. While the fix is not difficult, this series of vulnerabilities has managed to shake users' confidence in a wide range of vendor products.

CVE-2022-26136 / CVE-2022-26137 Atlassian Servlet Filter Dispatcher

CISA deadline:	N/A
Type:	Cross-site scripting (XSS) / Cross-origin resource sharing (CORS) bypass
Impact:	Authentication bypass, cross-site scripting
Wild exploit:	Yes
Affects:	See this site for all affected versions of the following platforms and products
Platforms:	Bamboo Server and Data Center, Bitbucket Server and Data Center, Confluence Server and Data Center, Crowd Server and Data Center, Fisheye and Crucible, Jira Server and Data Center, and Jira Service Management Server and Data Center; no Atlassian cloud instances are affected
Workaround:	Some may recommend that changing proxy settings is a viable workaround, but Atlassian recommends against this step, saying block lists are prone to bypass.
Remediation actions:	Read more

Servlet filters handle preprocessing of HTTP requests between a client and a backend, including providing a layer of security through auditing, authentication, authorization, and logging. Filters on systems affected by this vulnerability take advantage of cross-origin resource sharing (CORS), a shortcut method whereby web developers can embed resources from another domain, like images, stylesheets, scripts, iframes, and videos. Atlassian has claimed[18] that the flood of problems with its products is simply due to its having a large presence in the market. This further underscores the need for comprehensive protection, staying up to date to be aware of all vulnerabilities the minute they are released.

A rise in browser vulnerabilities

As the number of web-based attacks continues to grow, so does concern over web browser security vulnerabilities. Despite best efforts, there are a limited number of ways to secure browsing sessions and protect against these threats. In response, some browsers have implemented features such as built-in malware protection and anti-phishing measures. However, these tools are not foolproof and can sometimes give users a false sense of security.

One major problem is that many users do not update their browsers regularly, which leaves them vulnerable to known exploits. Additionally, new vulnerabilities are constantly being discovered, meaning that even up-to-date versions of popular browsers may still be at risk. Another issue is that most browsers rely on third-party plugins in order to provide certain functionality. These plugins often introduce their own set of vulnerabilities

Following are **two examples of significant browser vulnerabilities** we've seen in the past year:

[18] Atlassian Confluence zero day triggers IT security ire | TechTarget

CVE 2022-22620 / Use-After-Free in Safari Zero-Day

CISA deadline:	February 25, 2022
Type:	Memory Safety Vulnerability
Impact:	Execution of arbitrary code
Wild exploit:	Yes
Affects:	Apple iOS browsers for mobile devices
Platforms:	All browsers for iOS, iPadOS and MacOS: Safari, Chrome, FireFox and others
Workaround:	None
Remediation actions:	Read more

This vulnerability may have come from a lack of memory safety mitigations, which can then lead to arbitrary code execution when processing maliciously crafted web content. It is particularly fascinating because the Google Project Zero team considers it to be a "zombie" vulnerability, meaning one which was previously considered fully fixed as far back as 2013, came back from the dead in 2016, and is back again in 2022. In fact, according to Google, fully 25% of all zero-day attacks in 2020 were based on "zombies[19]," variants of previously disclosed vulnerabilities, and in 2022, we're seeing similar numbers.

CVE-2022-1096 / Type Confusion in V8

CISA deadline:	April 18, 2022
Type:	Memory Safety Vulnerability
Impact:	Remote code execution following out-of-bounds memory access
Wild exploit:	Yes
Affects:	V8 JavaScript and Web Assembly engine within Chrome
Platforms:	Chromium Open Source Software (OSS) and all browsers using it, including Google Chrome, Microsoft Edge, Amazon Silk, Brave, Opera, and many others
Workaround:	None
Remediation actions:	Read more

Even if you're not using Chrome, don't start thinking you're safe from this vulnerability, since the Chromium V8 JavaScript and Web Assembly engine is used by a wide range of other browsers like Amazon Silk, Brave, Microsoft Edge, and Opera. Unless you've upgraded to the latest versions of every single browser on your systems, you're probably not safe. This vulnerability is a sobering reminder of the importance of software supply-chain security given developers' increasing reliance on open-source code. You don't have to be using a particular vendor's product directly to find your resources vulnerable in surprising — and sometimes horrifying — new ways.

[19] An Autopsy on a Zombie In-the-Wild 0-day | Project Zero

Cyber risk in SaaS products

As more and more businesses move to SaaS solutions for their critical data and applications, the risk of third-party SaaS breaches is growing. In the past year, there have been a number of high-profile breaches of popular SaaS platforms. In each of these cases, the attackers were able to gain access to a large amount of sensitive customer data, including names, email addresses, and in some cases, credit card information.

Because SaaS platforms typically contain a large amount of sensitive data, a successful breach can result in significant data loss, having serious impact on business operations.

To protect against third-party SaaS breaches, businesses need to carefully vet the security of any SaaS solution they are considering using and to implement strong security controls such as two-factor authentication and data encryption to protect their data.

Some examples of breaches from 2022 include:

HubSpot

In March, malicious actors gained access to the contact data of several accounts through an email address used by an employee for customer service. Disabling the "Hubspot employee access control" option in the HubSpot account settings can counter this threat. This is a common feature in many SaaS products, but should only be switched on when customers require assistance.

okta

Gaining remote access to the computer of an employee at Sitel — a company providing Okta with customer service functions — the malicious Lapsus$ group was able to compromise Okta's[20] systems. While the scope of the attack was not as wide as first thought, this was an alarming breach given Okta's status as an access management provider for a number of well-known reputable organizations, with millions of users of their own.

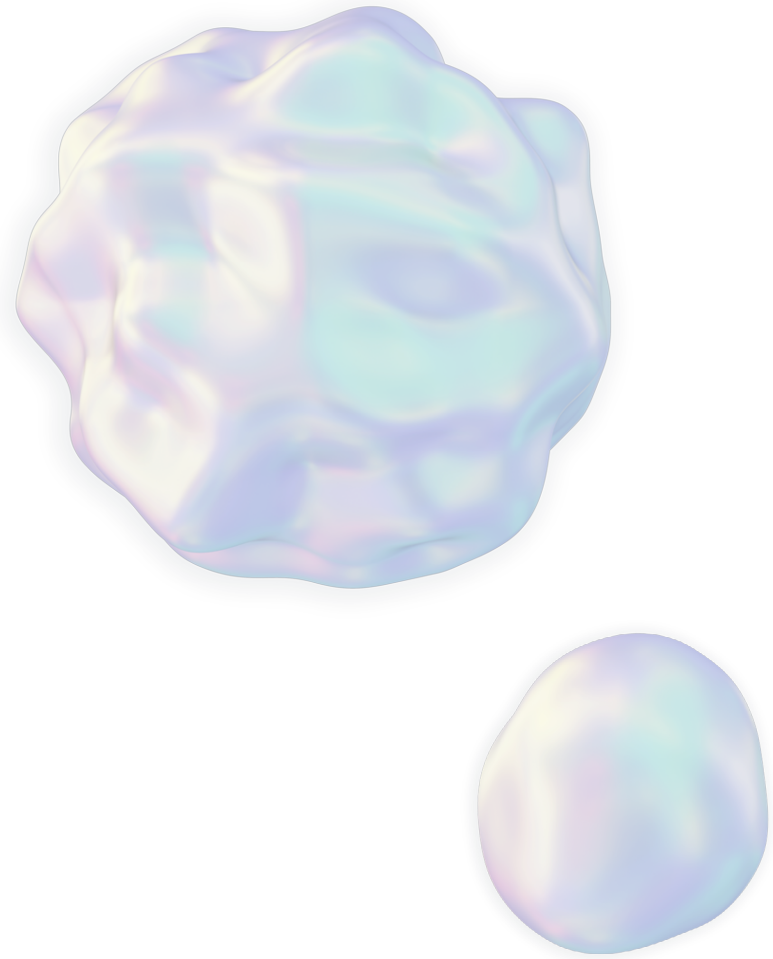
[20] Okta ends Lapsus$ hack investigation, says breach lasted just 25 minutes | The Verge

Looking beyond CVEs

This list covers just some of the biggest vulnerabilities we saw in 2022. Note that it is by no means exhaustive; there were — and will likely continue to be — other serious vulnerabilities before the close of 2022.

And while CVEs are important, they are not the only security metric that we should be looking at. In fact, CWEs (Common Weakness Enumeration) provide a more comprehensive view of security issues and can help us better understand and prioritize vulnerabilities. As CWEs group together similar problems, we are able to better understand the root cause of vulnerabilities and identify areas that need additional attention.

In the next section, we'll explore some examples of the **top CWEs in 2022**, according to MITRE, and what we can learn from them.



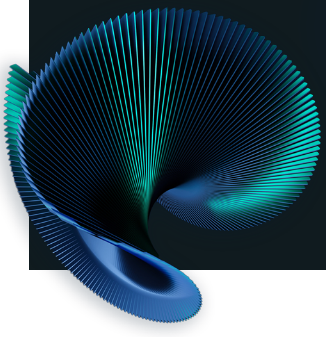
MITRE's top CWEs – and what they mean

Every year, MITRE releases its list of the top 25 CWEs. The list charts the most dangerous weaknesses in hardware and software, determined based on their commonality and impact.

Clarity on these weaknesses is vitally important to organizations constantly updating and releasing new products. The CWE Top 25 provides key insights into some of the most pressing concerns relating to application security and cyber risk.

To quote MITRE:

MITRE



> "Many professionals who deal with software will find the CWE Top 25 a practical and convenient resource to help mitigate risk. This may include software architects, designers, developers, testers, users, project managers, security researchers, educators, and contributors to standards developing organizations (SDOs)."

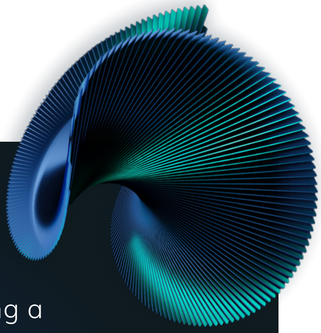
In short, the CWE Top 25 serves as an invaluable resource as companies scale their application security efforts.

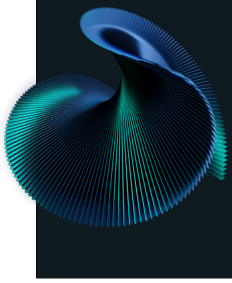
MITRE’s methodology

The list was developed through looking at public vulnerability data from the National Vulnerability Database (NVD). Once the data was obtained, MITRE used a scoring formula to rank the CWEs according to frequency and CVSS severity score.

MITRE details its full methodology for identifying the top CWEs here.

The CWE Top 25 leverages NVD data with CVE IDs from the last two years, downloaded four different times. The Top 25 team analyzes a subset of CVE records and performs remappings that either change or agree with the existing CWE mappings found within NVD, using the lowest-level CWEs available.





> “The NVD obtains vulnerability data from CVE and then supplements it with additional analysis and information including a mapping to one or more weaknesses, and a CVSS score, which is a numerical score representing the potential severity of a vulnerability based upon a standardized set of characteristics about the vulnerability.”

Top 10 CWEs

Rank	ID	Name	score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0

New additions

The Common Weakness Enumeration list evolves as threat actors change their tools and tactics, with some techniques falling out of favor and others becoming more prevalent. Below, we have noted the techniques that moved into the most recent top 25 list. While this is largely for academic interest, it does provide insight into how exploits are evolving over time.

Rank	ID	Name	score	KEV Count (CVEs)	Rank Change vs. 2021
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

Notable CWEs

CWE-787

For the second year in a row, CWE-787 ("Out-of-bounds Write") has ranked first place on the list. So if teams weren't watching it before, they certainly should be now.

CWE-787 is a security vulnerability that allows an attacker to inject arbitrary code into a program, which is then executed in that context. This can be used to take control of the program, and potentially the entire system.

CWE-77

Moving up eight places into the 17th position, CWE-77 is a security issue that enables an attacker to inject code into a web application. This can allow the attacker to take control of the web application and possibly the server that it is running on. CWE-77 can be mitigated by validating all user input.

CWE-362

A code sequence that can run concurrently with other code exists in the program, and although it needs temporary, exclusive access to a shared resource, there is a timing window in which the shared resource can be changed by another code sequence that is running concurrently.

CWE-400

A security weakness where, because the program does not effectively manage the allocation and upkeep of a finite resource, an actor is able to affect how much is used, eventually causing the finite resource to run out.

CWE-94

A classification for Improper Control of Generated Code ("Injection") weaknesses. Injection flaws occur when untrusted input is used to dynamically generate content that is later executed by the application. This can allow an attacker to execute malicious code within the application context, potentially leading to a compromise of the application or data. The best way to fix this issue is to update the software or library that is vulnerable. If updating is not possible, then you should use input validation to ensure that all user input is valid and within expectations.

The list of the top 25 CWEs represents the application vulnerabilities most exploited in attacks and deserving of attention from security teams. Compared to last year, **CWE-200, CWE-522** and **CWE-732** have been replaced by **CWE-362**, **CWE-400**, and **CWE-94** respectively.

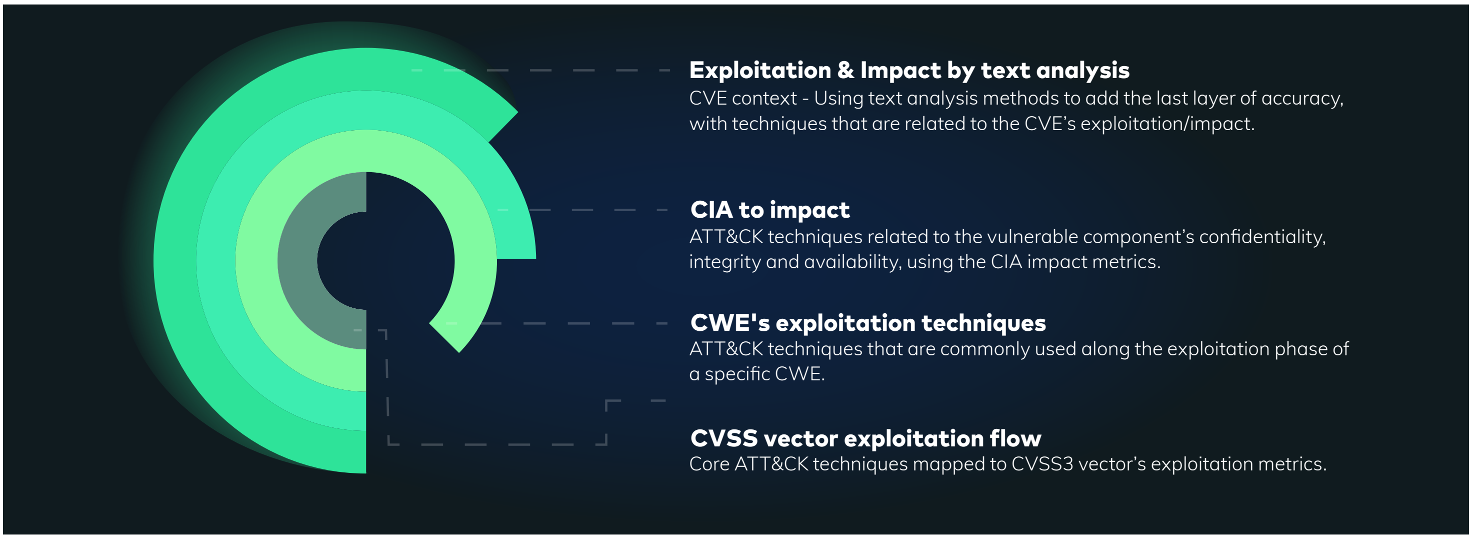
Nonetheless, MITRE recommends also addressing vulnerabilities ranking 26-40, as all weaknesses could become exploitable under the right circumstances.

Mapping the MITRE ATT&CK framework

The MITRE ATT&CK framework is an encyclopedia that centralizes techniques used by threat actors along with cyber attacks. It is broken down into “milestones” for attackers to reach before arriving at their end goal. Mapping offensive techniques to CVEs allows defenders to follow the “flow” of an attack, breaking down the steps and actions taken during its exploitation, and identifying what can be achieved (Impact) following successful exploitation.

While many have tried to map ATT&CK techniques to CVEs, these efforts have largely proven ineffective. MITRE also released its own community-driven methodology for mapping, but – while promising – it has not been updated recently and so is of limited use.

The Voyager18 approach relies on the MITRE methodology as a basis for its own project. Using CVE descriptions, CWE data, and CVSS vector information – alongside text analysis and machine learning processes – this ongoing project maps relevant techniques to each CVE:



Exploitation & Impact by text analysis
CVE context - Using text analysis methods to add the last layer of accuracy, with techniques that are related to the CVE’s exploitation/impact.

CIA to impact
ATT&CK techniques related to the vulnerable component’s confidentiality, integrity and availability, using the CIA impact metrics.

CWE's exploitation techniques
ATT&CK techniques that are commonly used along the exploitation phase of a specific CWE.

CVSS vector exploitation flow
Core ATT&CK techniques mapped to CVSS3 vector’s exploitation metrics.

CVSS3 Vector

The CVSS value of a vulnerability gives us an overview of the requirements and behavior of its exploitation flow. For instance, we can infer whether the exploitation requires a phishing campaign against the victim or whether the attacker has to be granted privileges prior to the exploitation.

CWE

The CWE of a vulnerability reveals the weaknesses under the hood. By knowing the weakness or vulnerability type of a CVE, we can, in some cases, automatically map relevant techniques to the CVE.

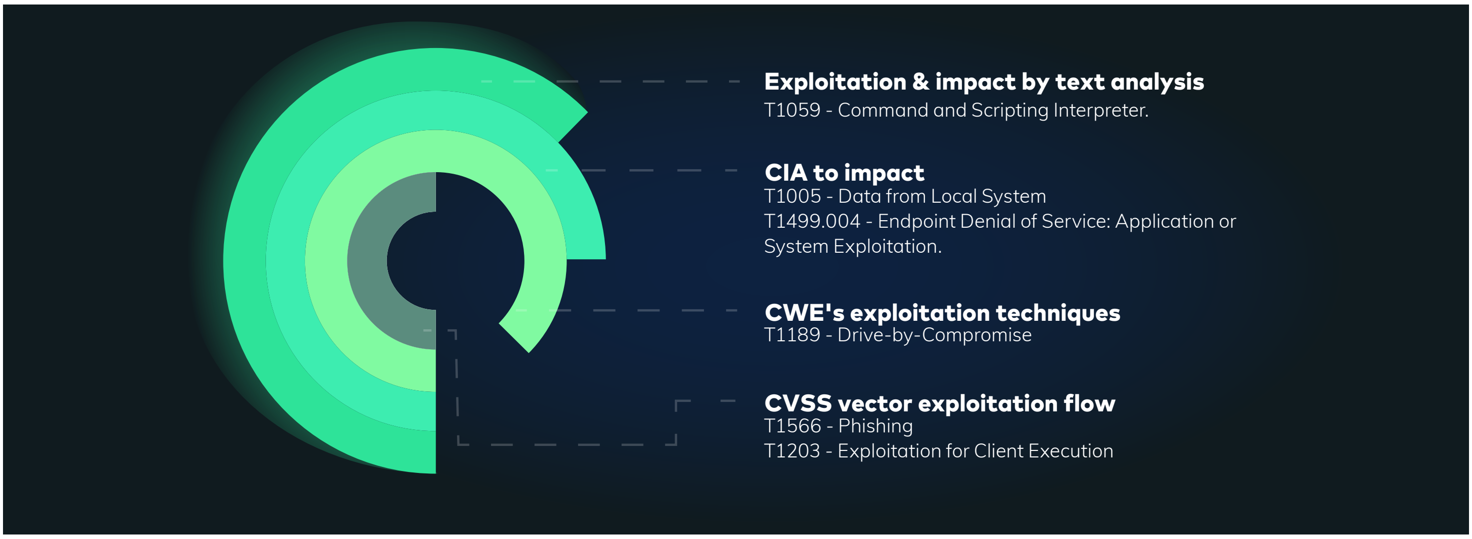
CIA

The confidentiality, integrity, and availability of a CVE can help us infer a vulnerability's impact, such as reading local data, destruction of data, or loss of availability.

Text analysis

Finally, though we initially avoided textual analysis, we found it difficult to map ATT&CK techniques to CVEs using patterns of CWEs and CVSS3 vectors alone. In order to overcome these difficulties, we added text analysis methods to the mapping process. First, we extracted phrases from CVE descriptions using the Rapid Automatic Keyword Extraction (RAKE) algorithm. Next, we manually selected meaningful phrases for each CWE and categorized them into groups with similar semantic meanings that characterize the CWE.

Each phase of the mapping process comes together to form a powerful tool for identifying patterns in the MITRE ATT&CK framework:



Exploitation & impact by text analysis
T1059 - Command and Scripting Interpreter.

CIA to impact
T1005 - Data from Local System
T1499.004 - Endpoint Denial of Service: Application or System Exploitation.

CWE's exploitation techniques
T1189 - Drive-by-Compromise

CVSS vector exploitation flow
T1566 - Phishing
T1203 - Exploitation for Client Execution

Our project to map the MITRE ATT&CK framework to common CVEs is part of a wider mission to identify causes and mitigation actions for vulnerabilities and threats that we see all too often. Attackers know that they can successfully obtain sensitive information through tried and tested attack methods that simply haven't yet been shut down by organizations.

Next, we'll explore some of the **more common types** of vulnerabilities and protection methods.

Common CVE types (and how to fix them)

Most of the vulnerabilities with CVE entries are never exploited in the wild. The problem is those that are exploited. While the raw number is far lower than the total number of vulnerabilities, the impact can be dramatically higher.

Fortunately, not every exploitable vulnerability turns into events like those that followed the Log4J or Microsoft Exchange Server issues.

One of the challenges security operations teams face is prioritizing the constant stream of CVEs and coordinating with their counterparts in IT. These IT teams are usually the ones tasked with deploying the patches once the vendor makes them available; or, at minimum, with altering the configuration, turning off unused features, or applying whatever other mitigations are available and don't go to the SecOps team.

Each vulnerability is either a new issue or a new take on an old one, with no single all-in-one solution capable of covering every new problem that arises. Nonetheless there are still some actions we can take to help with broad categories of CVEs. These are best practices we should be following in the first place. Nonetheless they warrant repeating, as far too many breaches occur due to the organization's failure to abide by industry best practices or vendor configuration recommendations.

Configuration issues

A fair number of CVE entries cover vulnerabilities that are only relevant for applications or systems using a specific — often unusual — configuration. In some cases, this non-standard configuration may be required to meet a specific business need. If that is the case, these must be reviewed regularly, which — again — is a standard best practice.

The bottom line is that if a vendor has a recommended, hardened, or otherwise secure configuration, it is best to follow it unless there are business-specific requirements that dictate otherwise.

Example

CVEs based on configuration issues

CVE-2022-20695

CVE-2022-24774

Access control

This is another common thread that shows up in many CVE entries that either provide privilege escalation, or local exploits that require some kind of existing access. In either case, restricting access to potentially vulnerable systems is a step toward preventing any attack that relies on access to execute. How that access is limited obviously depends on the system. With servers, the first step is limiting access to only include people who truly require it. While it may be tempting to grant access to everyone who asks, the reality is that the fewer people who can get into the system, the fewer opportunities there are for someone to exploit it.

Many operating systems — including Linux, Windows, and MacOS — offer a range of tools to help lock the system down. There is no reason not to use these tools, aside from minimal administrative overhead and some added complexity. The benefits usually outweigh the costs.

Servers aren't the only targets of access exploitation, since workstations can be used to launch attacks against servers and can be inviting targets in their own right. Implementing multi-factor authentication wherever it is practical across the environment can help restrict access on both workstations and servers.

While users may find MFA cumbersome, the benefits of that second step far outweigh the minor inconvenience. Numerous breaches over the years have originated with compromised credentials, and multi-factor authentication can reduce the risk of an intrusion even if credentials are somehow revealed. Keeping attackers out not only protects an organization's IP and valuable data, it gives threat actors fewer opportunities to deploy exploits.

Example

CVEs based on access control

CVE-2022-28759

CVE-2022-20923

Perimeter controls

There is a common theme in cyber security that the perimeter is effectively dead, and with the shift to remote work as a result of the COVID-19 pandemic, it's easy to see why. Most of the workforce is outside the perimeter working from home. While that started to change back to in-office in early 2022, chances are people will remain outside the office as long as they can. Though to be fair, COVID didn't change things for the applications that still live on-premises in the data center. The wholesale shift to cloud computing, however, has had an effect.

Example

CVEs based on perimeter controls

CVE-2022-39956

CVE-2022-24706

But the perimeter isn't dead, and the servers and systems that remain in the enterprise environment are still the subject of a large number of CVEs. Even with many applications in the cloud, some of them are the subject of CVEs as well. Thus, the perimeter is still a useful layer of protection for both systems and applications.

Firewalls, web firewalls, web gateways, and the like are still important. While it is impossible to predict what specific vulnerabilities will come up next and become CVE entries, configuring the perimeter to allow only the minimum necessary access can help keep attackers from reaching vulnerable systems. Likewise, sanitizing entries in web applications and providing the workforce with secure gateways can prevent application compromise in either direction.

No silver bullet for common CVEs

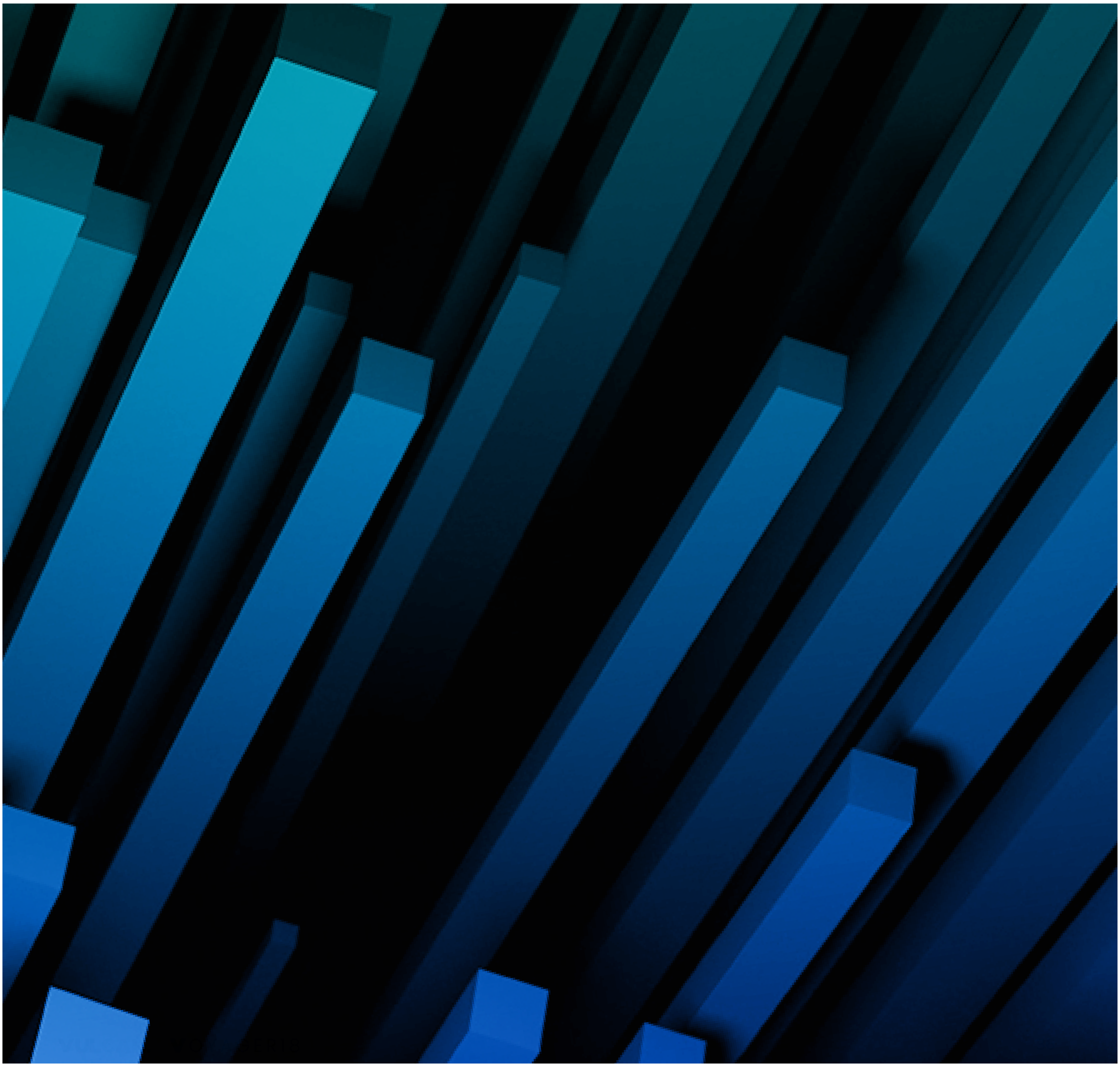
There is no "one size fits all" solution to address every possible new CVE. There is no silver bullet. But there are the basic best practices all organizations should be following to keep their environments safe. So when the latest CVE drops, we may have some breathing room while we analyze the risk and decide how to prioritize the patches.

Cyber risk is something all organizations need to face. Siloed teams, muddy data, and slow, inefficient processes represent a golden opportunity for threat actors. Communication and collaboration between teams are vital, as is full visibility of vulnerability data — all in one place.

Understanding the common types of CVEs that organizations are faced with is a small part of a much bigger picture, and the mounting threats across attack surfaces can cause cyber risk to spiral out of control and out of sight. However, while we can't predict everything that will happen in our industry, there are some **growing trends** that we can reasonably expect to increase in importance through 2023 and beyond.

The final chapter of this report focuses on the future that is already taking shape, and the mitigation actions we recommend that can keep our organizations secure.

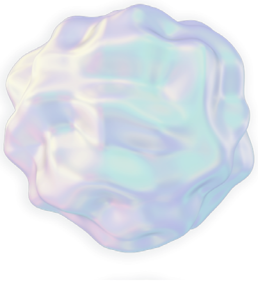
04 Looking ahead to 2023

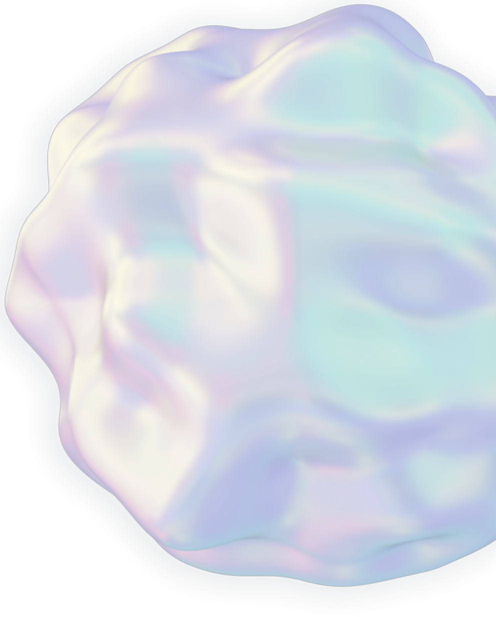


Introduction

The cyber risk landscape is one of constant change. With 2022 drawing to a close, organizations are left considering the results and consequences of weaknesses addressed and threats missed, and what the future might hold. The simple reality is that nobody knows the answer to this last question, but we can glean the general direction of cyber security from what we've seen in our industry, from our customers' experiences, and from our own internal efforts as we work to turn cyber risk management into step-by-step processes for all.

This final section explores the most notable **future trends of cyber risk** as we see them, and the mitigating actions that we at Vulcan Cyber recommend organizations take in order to stay protected. Finally, we propose a new way of approaching the growing concern of duplicated cyber risk data, empowering IT security teams to see their cyber risk clearly and take the necessary steps to reduce it.





Trends for 2023: what to expect

Charting the future trajectory of cyber security is a tall order. The rapid proliferation of new attack surfaces means more opportunities for threat actors than ever before, and this will only continue as new technologies are introduced. Still, there are some things we can confidently predict for 2023, given that they are trends that have already been gathering pace this year. Below are just a few of the topics we expect to be of greater relevance to organizations over the next few months.

More attacks in the cloud

The year 2022 saw the ongoing rapid adoption of cloud environments by organizations looking to take advantage of the many obvious benefits of cloud technology. And 2023 will be no different, but security in the cloud remains immature, with default cloud services often providing inadequate essential security functions. Threat actors are keenly aware of this, and security teams must keep up with their organizations' appetite for cloud adoption.

We expect greater focus on **predictive security** and **multi-factor authentication** for the cloud, and a continued interest in threat intelligence for threats targeting the cloud.

92%

of organizations are storing at least some data in the cloud.[21]

27%

of organizations were impacted by a security incident in their public cloud infrastructure over the past 12 months.[22]

Threats on the go – the mobile attack surface

With around two thirds of the world's population using smart devices as of 2021, it is no surprise that mobile is fast emerging as a major target for threat actors. People manage almost all aspects of their digital lives on their phones, and most aren't experts in securing their assets. Attackers leverage easy opportunities in ecommerce, banking, and online booking applications. And, with mobile devices not going anywhere soon, this attack surface will only continue to grow.

45%

of surveyed companies experienced a mobile security incident in the past 12 months.[23]

[21] Up to Date Cybersecurity Statistics for 2022 | NinjaOne

[22] The Biggest Cloud Security Challenges in 2022 | Check Point Software

[23] Cybersecurity in 2022? Remote working and mobile are changing everything... | Thales Group

Threat actors turn to IoT

As internet of things (IoT) devices continue to grow in popularity, they will become an increasingly attractive target for threat actors. The interconnected nature of IoT devices makes them especially vulnerable to attack, as a successful breach of one device can often provide access to an entire network. In the future, we can expect to see more **sophisticated and targeted attacks** on IoT devices, as well as a greater range of malicious actors targeting this technology in their attacks.

>25.4b

active IoT devices by 2030.[24]

5,200

IoT attacks per month on average.[25]

The healthcare sector at risk

With the healthcare sector representing particularly high liability to organizations and individuals alike when affected by a cyber attack, it is no surprise that the healthcare security industry is predicted to be worth **$125 billion** by 2025. Ransomware attacks **increased by 94%** from 2021 to 2022[26], and with more and more patient data being stored online and in the cloud — together with the residual impact on healthcare services of the COVID-19 pandemic — the sector is increasingly vulnerable.

>50%

of connected devices in a hospital contain critical cyber risks.[27]

AI in security efforts

A welcome development for 2023 will be the increased implementation of advanced machine learning and other artificial intelligence techniques in identifying and responding to threats. Today, IT security teams have huge datasets to work with, coming from multiple threat intelligence feeds and scan data. AI would help parse this data and efficiently identify underlying patterns and future threats, giving organizations the best possible chance of staying secure. This is already a widely accepted reality in the industry, with **talent and skills shortages** driving practitioners to adopt AI and automation into their cyber risk management programs.

93%

of organizations using or considering use of AI in managing their cyber risk.[28]

[24] Internet of Things statistics for 2022 - Taking Things Apart | DataProt

[25] 166 Cybersecurity Statistics and Trends [updated 2022] | Varonis

[26] 'Lives are at stake': hacking of US hospitals highlights deadly risk of ransomware | The Guardian

[27] The State of Healthcare IoT Device Security 2022 | Cynerio

[28] AI and automation for cybersecurity | IBM

Users as an attack surface

An organization's user base will remain a primary target, with threat actors leveraging phishing, social engineering, and other techniques to try to compromise the organization's employees and their customers.

Many breaches start with an email, SMS message, or other contact with an unsuspecting user — and that will almost certainly continue into 2023. While user education programs, tools, and security processes continue to improve, the users are likely to remain **part of the threat surface** rather than part of the security stack for the foreseeable future.

11m

the approximate number of files employees have access to.[29]

40%

of breaches in 2021 were phishing attacks.[30]

Diversified cyber risk requires a better solution

With the avenues of attack growing in number, IT security teams cannot rely on outdated methods to stay secure. The final section of this report explores the ways in which organizations can meet the increased demands of the cyber risk landscape.

[29] Data Risk Report: Financial Services | Varonis

[30] DBIR Master's Guide | Verizon

The importance of managing cyber risk data

Much has changed in cyber security, even in the last few years. In the past, managing cyber risk data was a more straightforward challenge to overcome, but today's landscape presents entirely new dimensions of difficulty. Today, most security practitioners we work with are managing cyber risk across **multiple attack surfaces** on **multiple platforms**, and must contend with the proliferation of duplicate and confusing data impeding their progress.

The rise of duplicated data

Recently, there has been a tendency for organizations to onboard more and more scanning tools to identify vulnerabilities. The issue with this is that many of these tools are effectively scanning for the same information, resulting in a mass of **duplicated data** that quickly overwhelms security teams.

3-5

scanners used by organizations to scan their public cloud environments.[31]

Last year's Log4j vulnerability serves as a case in point. We heard from many customers that the vulnerability was picked up by multiple scanners, but the subsequent triage process was almost unmanageable, especially during the holiday season.

The proliferation of threats across SaaS, public cloud, and IoT environments (among others) — on top of the traditional attack vectors — means that security teams are scanning for vulnerabilities in more areas than they can handle. Moreover, alongside the increase in CVEs over the past few years, we are also seeing non-CVE indicators becoming more relevant to organizations.

[31] How to Achieve Complete Cyber Risk Management | BrightTalk

In the table below, we show the evolution of the threat landscape and resulting growth of platforms and duplicated risk data:

Attack surface	2015	2022
Network	Qualys. RAPID7 tenable	Qualys. RAPID7 tenable
Applications	VERACODE WhiteHat SECURITY SYNOPSYS	Acunetix hackerone WhiteSource
SaaS		OBSIDIAN AppOmni ADAPTIVE SHIELD
PaaS		Laminar eureka
IaaS and Public Cloud		paloalto NETWORKS aqua WIZ orca security
IoT		CLAROTY ARMIS.
Data		Laminar eureka
Code	BLACKDUCK VERACODE	BLACKDUCK VERACODE GitHub snyk

x10.5
Known / reported CVEs

The result:
More risk data =more security posture challenges

The bottom line is that security teams are working in far more directions than they are used to when it comes to staying secure, but are doing so with essentially the same resources they had when they were only thinking about a handful of attack surfaces. **This results in security operations that cannot scale up to meet the increasing cyber risk.**

Some of the challenges teams face:

Noise

The enormous **volume of scan data** from myriad scanners and threat intelligence feeds often generates duplicate or spurious data, leading to a poor signal (valid risks) to noise (spurious data) ratio. With an unmanageable stream of noisy data, teams often lack control as they try to turn raw information into useful intelligence.

Accuracy

Different data sources may present the same data in different forms and deliver different risk measures for the same vulnerability. This can make it difficult to determine what the real threat is to the environment and can lead to **miscalculating the actual risk**.

Depth

The ideal situation would be to synchronize data across all attack surfaces. Without this, teams **lack context** and often fail to prioritize vulnerabilities correctly for their organizations.

Data is crucial to successful cyber risk posture management. But when the data creates more questions than answers, organizations are left to contend with information overload as they remain open to attack.

The need for vulnerability correlation

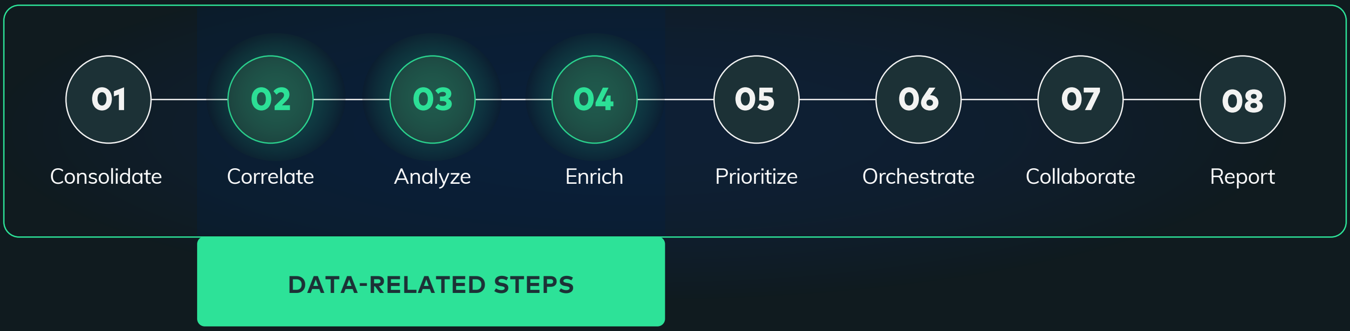
As we've seen throughout this report, it is essential to view vulnerabilities not simply as individual issues, but as groups of common weaknesses that can be fixed with the same strategies or mitigating actions. Correlating our data allows us to take action on unified entities, rather than disparate and often overlapping cyber risk concerns.

Effective deduplication methods can be based on:

- **Asset attributes**: Identify unique assets across scanners and attack surfaces.
- **Affected software**: Dramatically reduce vulnerability clusters by focusing on the affected software and all findings associated with them.
- **CVEs**: Monitor CVEs from multiple scanners regardless of detection methods.

Still, correlation is only a piece of the puzzle. Organizations should incorporate a wider and more holistic approach to managing cyber risk data, from the very beginning of the **cyber risk management lifecycle**.

Introducing a new approach to managing cyber risk data



The three highlighted stages above represent the steps in the cyber risk management lifecycle that are centered around **collecting, understanding, and deduplicating** the data before any prioritization or remediation actions take place. Fundamentally, this data should be viewed within one context, presenting a reliable source of truth for security practitioners to work with.

The key objective of data deduplication in cyber security data is to ensure that those involved in any stage of the vulnerability management process, including those who aren't security personnel with expert knowledge, are able to take action fast on the critical vulnerabilities **posing real risk** to their organizations.

General recommendations

The fast development of new technologies and attack surfaces can make the future of cyber risk seem overwhelming. Threat actors find new ways to satisfy voracious appetites for exploiting weaknesses in systems and accessing critical data, as IT security teams continue to grapple with a backlog of existing threats.

While the fight may be unbalanced, there are steps teams and organizations can take to make themselves less attractive to attackers seeking easy wins. Ultimately, a permanently watertight digital environment is unrealistic, but a vigilant and smart approach to securing critical assets makes an attack on your systems a much less worthwhile endeavor for threat actors.

Below are some basic but essential recommendations to help organizations give themselves the best possible chance of staying secure — in 2023 and beyond.

Make employees part of your defense

Organizations are only as strong as their weakest link. IT security teams may be well versed in protecting company data, but the vast majority of employees in an organization are not — and cannot be expected to be — cyber security experts. While turning every employee into a CISO is unrealistic, security teams should push for a baseline of understanding that ensures workers don't fall into any obvious traps.

Updating company laptops when prompted, recognizing phishing emails, and use of a password manager should all form the basis of a company-wide educational program in cyber risk. Going a step further, security teams must be responsible for articulating the message that cyber risk represents **real business risk** and that a breach can mean significant **loss of revenue and reputation**.

Keep patches up to date

This is nothing new. IT security teams will be aware that many data breaches **stem from unpatched software**, but — in spite of this — struggle to apply the necessary fixes. The volume of patches — increasing rapidly as attack surfaces expand — challenges teams' ability to make any real progress in mitigating their cyber risk.

Moreover, logistical issues within organizations can mean scheduled patches are pushed back, or the infrastructure simply doesn't support widespread patching. Improvements in this area must be led by the IT security team, but responsibility cannot rest solely with them. A DevSecOps culture within the organization would go a long way to curbing the growing number of unpatched software, as would better collaboration to get teams looking at the same cyber risk picture.

Restrict unnecessary access

In a large organization, the average employee has access to millions of files[32], many of which contain **sensitive company data**. At the enterprise level, it is easy to lose track of which shared folders contain what, and what data workers actually need to access. However, with threat actors viewing employees as the likeliest entry point into an organization's systems, it is important to restrict all unnecessary access and minimize the exposure when employees are the victims of an attack.

Implement multi-factor authentication

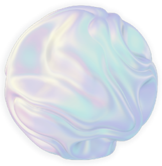
Finally, organizations should implement multi-factor authentication for all employees to access all company accounts and devices. Ultimately, persistent attackers will find ways to breach company data, but creating an **infrastructure of security obstacles** at all levels of an organization makes the prospect of targeting it significantly more daunting. Multi-factor authentication is a basic but powerful measure that organizations can take to stay secure.

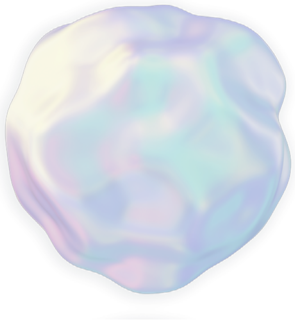
[32] Data Risk Report: Financial Services | Varonis

Follow industry best practices

As cyber security practitioners, we all have a shared enemy. The malicious actors looking to exploit any weaknesses in our systems provide us with common ground as we all work to avoid data breaches. Our shared efforts mean that our industry has an established and constantly updated set of best practices and recommendations for staying secure. In the United States, **CISA and MITRE** lead the way in keeping the industry aware of all developing trends and vulnerabilities, while the steady publication of reports, studies, and research projects mean that we have a wealth of information available to us.

Of course, as we have already seen throughout this report, information without application is limited in its value. Practitioners must take action on the well-publicized industry best practices and stay up to date with any changes or new developments.





05 About Vulcan Cyber

Vulnerability description		Severity	
Log4j, CVE-2021-44227	Weaponized RCE Remote Unauthenticated Exploitable	98	Jun19,2022
Mysql Workbench Critical Patch Update	Weaponi cated	83	Jun19,2022
nginx < 1.17.7 In formation Disclosure	Remote	80	Jun19,2022
SSL Version 2 and 3 Protocol Detection	RCE CIS	79	Jun19,2022
CentOS Security Update for Unbound	RCE	65	Jun19,2022

Risk Breakdown ⓘ

Critical	7,760 assets
High	3,600 assets
Medium	1,300 assets
No Risk	5,000 assets

VULCAN.

Start owning your risk

Vulcan Cyber breaks down organizational cyber risk into measurable, manageable processes to help security teams go beyond their scan data and actually reduce risk. With powerful prioritization, orchestration, and mitigation capabilities, the Vulcan Cyber risk management SaaS platform provides clear solutions to help manage risk effectively.

Vulcan Cyber enhances teams' existing cyber environments by connecting with all the tools they already use, supporting every stage of the cyber security lifecycle across cloud, network, and application attack surfaces.

Trusted by leading global customers worldwide, we help security professionals own their cyber risk, at scale.

TRY VULCAN CYBER NOW

GET A DEMO

READ OUR BLOG

06 About Voyager18

VOYAGER18

Stay up to date with the latest research trends

The Vulcan Cyber research team, also known as Voyager18, is a team of cyber experts working to leverage machine learning and cyber research to ensure Vulcan Cyber remains a cyber security leader. The team's main objective is to research the latest cyber risk trends, including new attack types and remediations. The team is also responsible for bringing innovation to the Vulcan Cyber platform so that our customers get improved and customized cyber risk management capabilities.

This includes research of more specific and accurate risk calculations that can truly help our customers own their risk. Most recently, the team mapped out the MITRE ATT&CK framework to relevant CVEs, providing granular insights into the most critical vulnerabilities. The full research is available here.

GET MORE RESEARCH