

Exposure Report 2023

Assessing Cyber Risks from the Outside In

HADRIAN

Executive summary

In the fast-paced world of cybersecurity, organizations have traditionally leaned heavily on defense-oriented strategies to safeguard their digital assets. This approach has delivered results but it often forces organizations into a reactive stance, prioritizing incident response over prevention. In many cases, offensive security measures have been implemented on an ad hoc basis, lacking a comprehensive and coordinated strategy.

However, in today's era of relentless cyber threats, Hadrian advocates for a shift towards a proactive and holistic offensive security approach. Instead of sporadic, point solutions, we propose the adoption of a continuous and integrated platform-based approach.

This report is a comprehensive compilation of key insights and noteworthy developments from the year 2023. It underscores the ever-increasing importance of offensive security measures and highlights the critical need for a cybersecurity strategy characterized by continuous monitoring and effective use of resources. Our goal is to shine a spotlight on the vital role that offensive cyber security plays in helping organizations stay one step ahead of emerging threats and fortify their digital defenses.

Through this report, we aim to raise awareness about the significance of offensive cybersecurity in a way that resonates with forward-thinking tech leaders. Our vision is to empower businesses to operate securely and thrive in the dynamic and challenging digital landscape of today, by advocating for a platform-driven, holistic approach to offensive security. Together, we can pave the way for a more proactive and effective cybersecurity strategy that benefits organizations and society as a whole.



Rogier Fischer

CEO, Hadrian



Table of content

4. Assessing from the Outside In
5. Shifting Left
6. The Kill Chain
7. Initial Access Vectors
8. Dangerous Weaknesses
9. Remote Code Execution
10. Insecure Direct Object References
11. IDOR Explained
12. Configuration Flaws
13. Exploited targets
14. What's new in CVSS 4.0
15. Timeline to exploitation
16. Inside DORA and NIS2
17. Supply chain risks
18. Timeline of MOVEit
19. Software Bill of Materials
20. The Secure Software Development
21. Offensive Security Testing
22. Simplifying Offensive Security
23. Under The Hood
24. About Hadrian
25. References



Assessing from the Outside In

To accurately assess security posture and validate defensive security controls a robust offensive security practice is required. It evaluates how real-world threats could compromise an organization’s environment.

Crucially, it addresses the early stages of the cyber kill chain by identifying unknown risks across the entire environment. As shown in Figures 1 and 2, many organizations are planning to expand their offensive security in response to the concerns about unknown risk and their security posture.

In this report we explore the latest cyber threat trends and cases to show how offensive security can uncover hidden vulnerabilities, reveal misconfigurations and prioritize risk remediation. The impact of this approach benefits DevSecOps, Security Operations Centers, and Red Teams.

Top threat exposure concerns

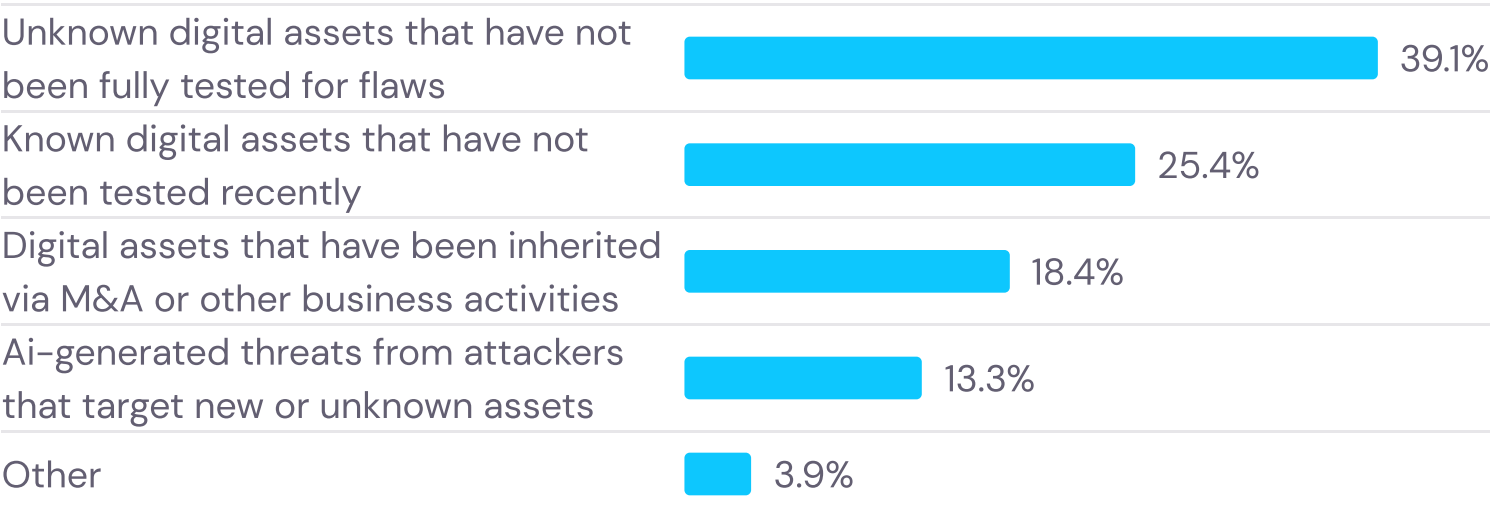


Figure 2. – Top threat exposure concerns¹

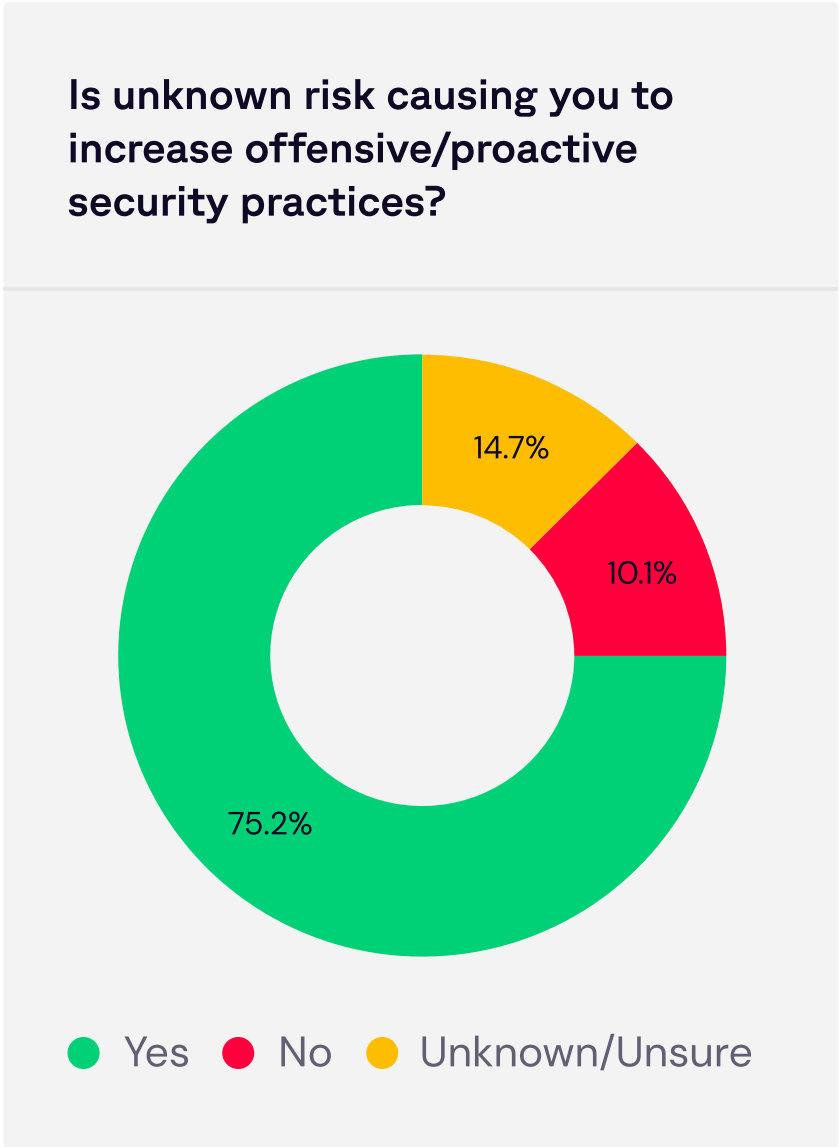


Figure 1. Influence of unknown risk on offensive security practices¹



Shifting Left

The volume and sophistication of cyber attacks are pushing security teams to their limits. Rather than reacting and remediating incidents, the concept of “Shifting left” suggests that organizations should take a proactive approach. Shifting left is the practice of testing and fixing issues earlier in a project lifecycle, the theory is that by shifting left the “cost” is minimized and fewer resources are required. By applying this to cybersecurity, it is possible to reduce risk with fewer resources.

Chief Information Security Officers (CISOs) are pivotal in this shift, tasked with managing organizational risk within set boundaries. Their goal is to minimize the likelihood of a major incident and limit potential harm. While it's impossible to completely eliminate risk, it can be effectively managed through proactive processes and procedures that are “shifted to the left” of traditional security practices.



In cybersecurity, attackers have a structural advantage: they need to find only one exploitable weakness across an organization.

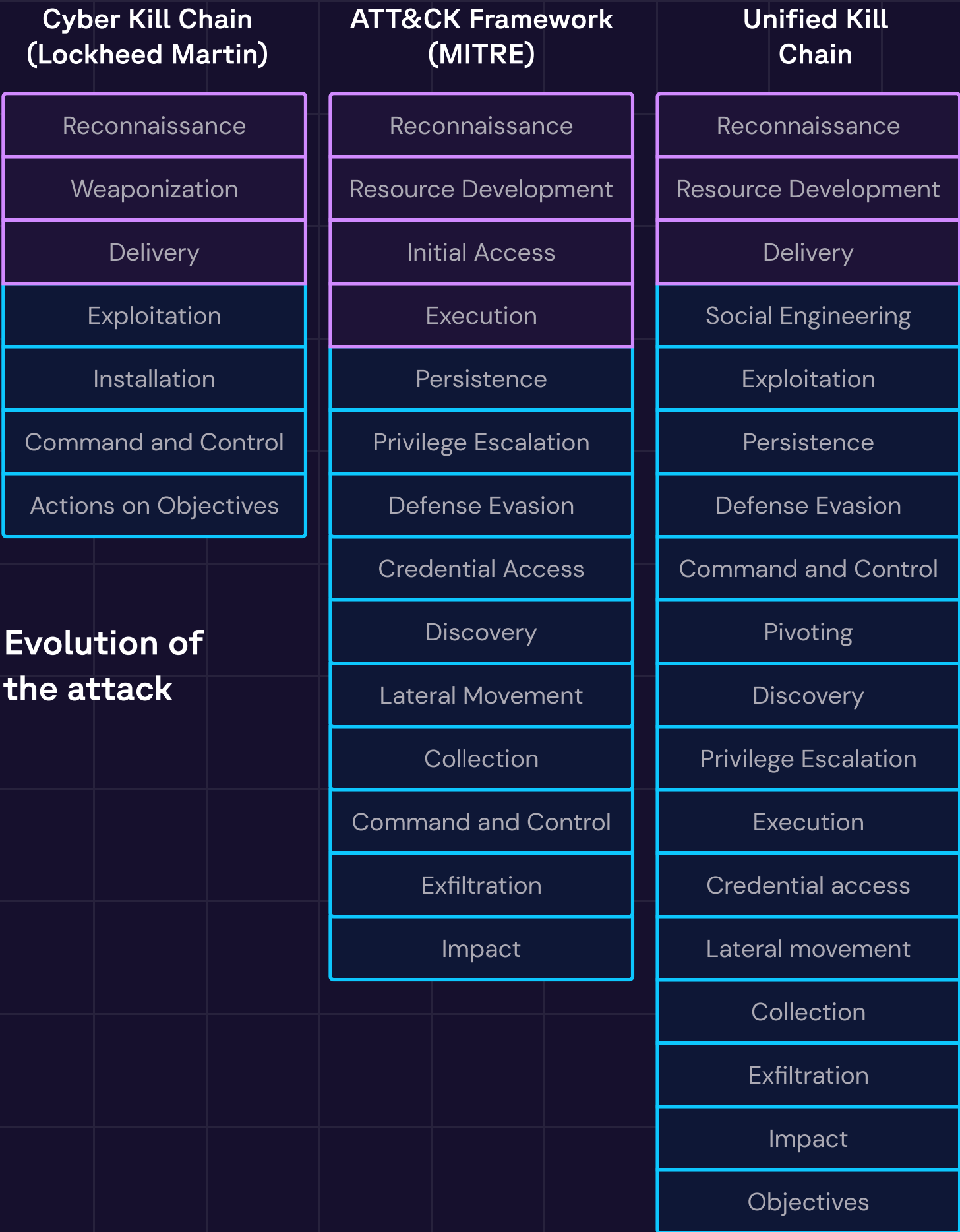
World Economic Forum

The Kill Chain

The cyber kill chain outlines the stages of a cyberattack, starting from early reconnaissance and often culminating in data exfiltration.

The kill chain has been through several iterations, shown on the right, becoming more adept at describing attack techniques. The concept is attributed to Lockheed Martin, however the most widely utilized version is the MITRE ATT&CK framework. There have been efforts to further improve the chain by including non-technical elements, such as social engineering, as with the Unified Kill Chain.

While most efforts in the kill chain focus after an attack is underway (shown in blue), understanding the early stages (purple) allows us to anticipate and prevent attacks before they happen.



Initial Access Vectors

Initial Access involves tactics that adversaries use to establish their initial presence within an ICS environment. This includes compromising operational technology assets, IT resources in the OT network, and external remote services. They may also target third-party entities and users with privileged access, often gaining access to devices and communication mechanisms with privileges in both the IT and OT environments.

This is leading to threat actors often targeting internet-facing applications and remote services due to their accessibility, as shown in Figure 3. Attacking such assets is usually low-risk, and automation streamlines various stages of reconnaissance and exploitation.

Initial access vector for techniques in first half of 2023

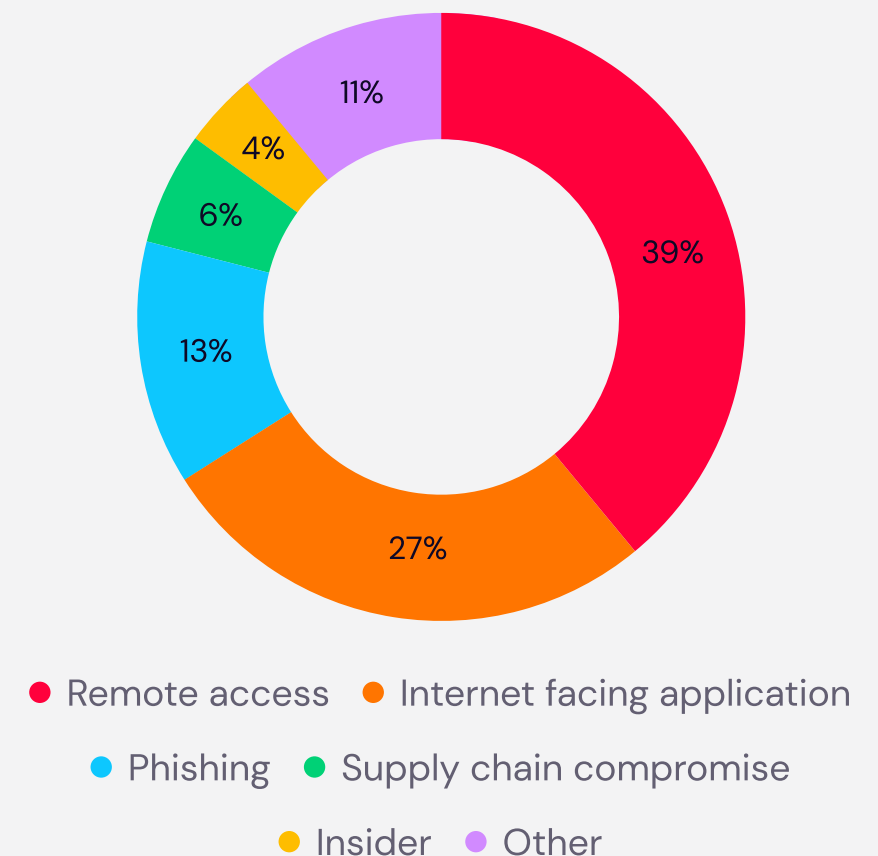


Figure 3. Initial access vectors used in the first half of 2023²

Dangerous Weaknesses

The tools and techniques used by threat actors are constantly developing which results in different software weaknesses being exploited. By understanding the preferred techniques used by threat actors, security controls can be validated. The Common Weakness Enumeration (CWE) in Figure 4 is ranked based on frequency and severity.

The Cybersecurity & Infrastructure Security Agency (CISA) recently released an analysis from their red and blue teaming assessment of the top software misconfigurations⁴. The analysis provides further evidence that there is systemic weakness and failure to implement secure design practices in many software applications.

Rank of most dangerous software weaknesses

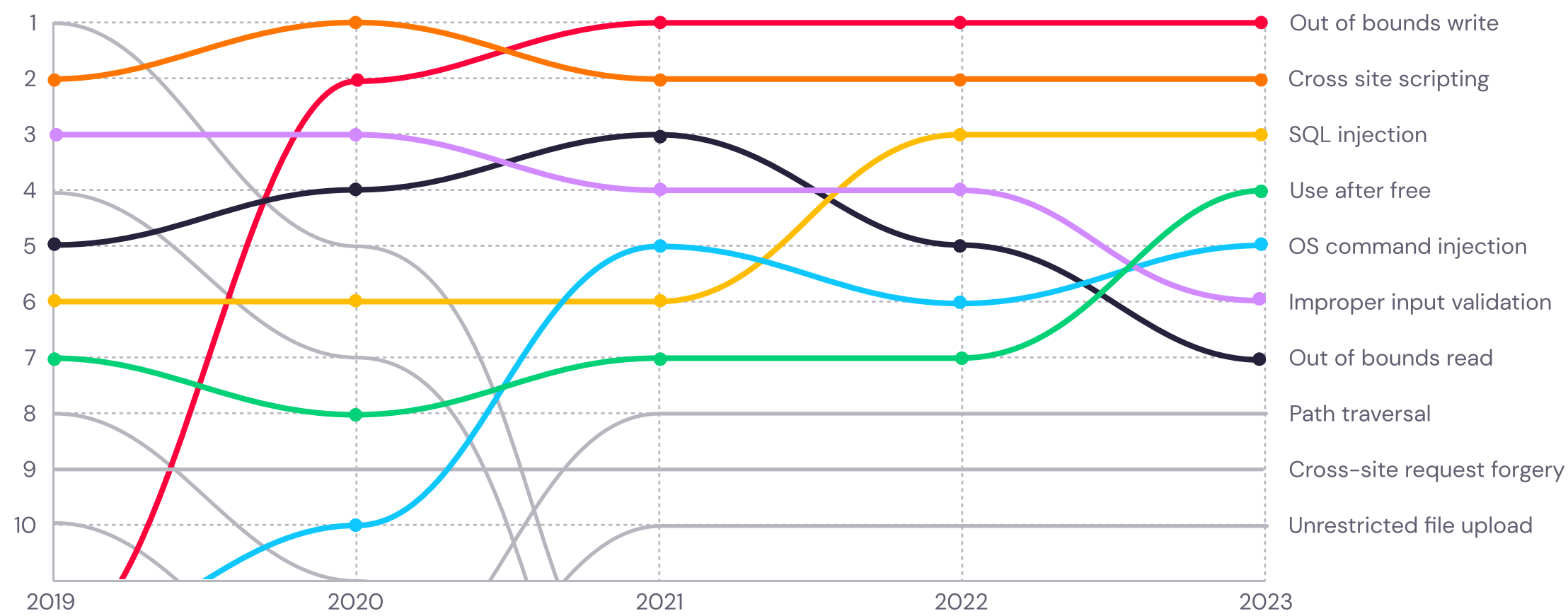


Figure 4. Rank of the Most Dangerous Software Weaknesses⁴

Remote Code Execution

Remote Code Execution (RCE) remains one of the most dangerous software weaknesses. RCE can take many forms including out-of-bounds write, SQL injection, use after free and cross-site request forgery attacks, which are ranked 1, 3, 4 and 9 respectively this year. In many cases, the main issue is the use of out-of-date software, and can be resolved by patching.



Notable RCE exploits discovered this year

CVE-2023-34362 (CVSS 9.8) is a MOVEit Transfer web application exploit that could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. The vulnerability was actively exploited by CIOp and resulted in over 2,500 organizations being breached, impacting 67 million individuals. Learn more in [our blog](#).

CVE-2023-27997 (CVSS score: 9.8), also called XORTigate, is a critical vulnerability impacting Fortinet FortiOS and FortiProxy SSL-VPN appliances that could allow a remote attacker to execute arbitrary code or commands via specifically crafted requests. The vulnerability is under active exploitation in the wild and when discovered impacted the majority of the 490,000 exposed Fortinet SSL-VPN interfaces.

Insecure Direct Object Reference

While not one of the top ten weaknesses shown in Figure 4, Insecure Direct Object Reference (IDOR), also known as Authorization Bypass Through User-Controlled Key, has been increasingly utilized in breaches.

Understanding the weakness and how to mitigate it could become critical for organizations in the future. Types of IDOR vulnerability:

- Horizontal – Occurs when users can access data that they should not be able to access at the same privilege level (e.g., other user's data).
- Vertical – Occurs when a user can access data that they should not be able to access because the data requires a higher privilege level.
- Object-level – Occurs when a user can modify or delete an object that they should not be able to modify or delete.
- Function-level – Occurs when a user can access a function or action that they should not be able to access.

Stalkerware Data Harvest

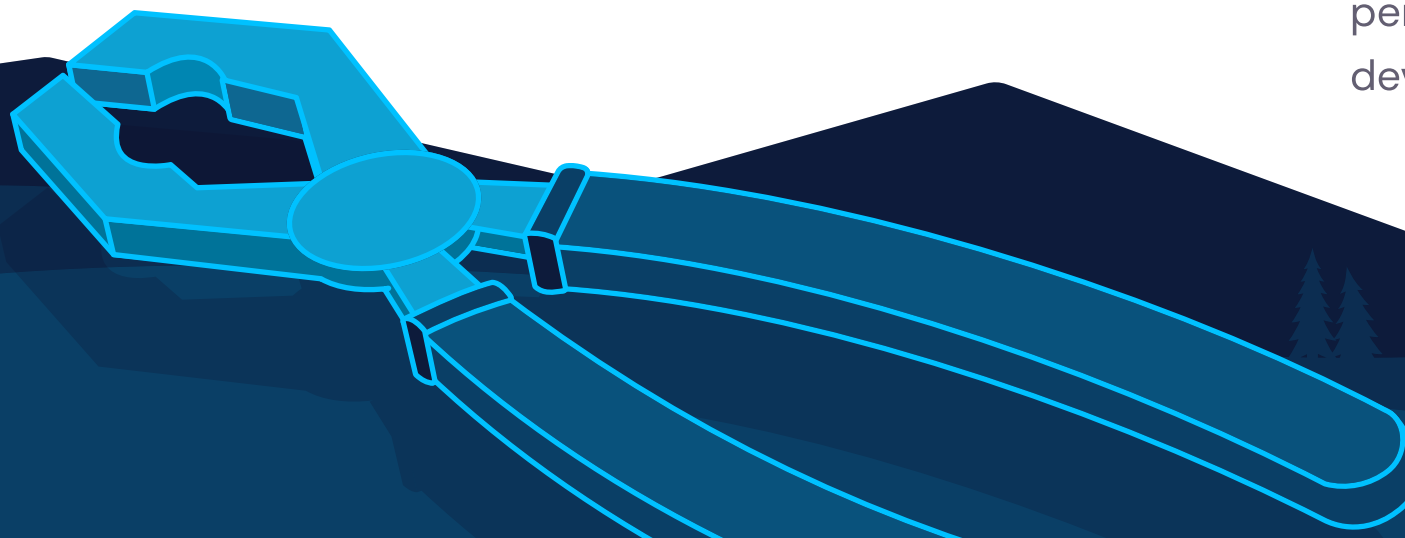
In October 2021 a [global incident](#) caused phone data, including text messages, call details, photos, and geolocation from hundreds of thousands of devices was leaked

Document Data Leak

A 2019 data breach [incident](#) exposed over 880 million personal financial records, including bank statements, bank account numbers, and mortgage payment documents

iPad Account Slurper

A [data breach](#) in 2012 resulted in a malicious cyber actor obtaining the personal data of +100,000 mobile device owners



IDOR Explained

IDOR refers to a type of access control vulnerability that occurs when an application allows users to manipulate identifiers, such as URLs or parameters, to access or modify objects they should not have access to. This vulnerability can lead to unauthorized access to sensitive data or actions.

One of the most common examples of an IDOR vulnerability can be seen within a simple website URL. In Figure 5, the URL of a banking website provides users with access to their account. Without any additional verification tools, a cyberattacker is able to simply modify the "ID" number and access information relating to other customers.

[Read blog post](#)

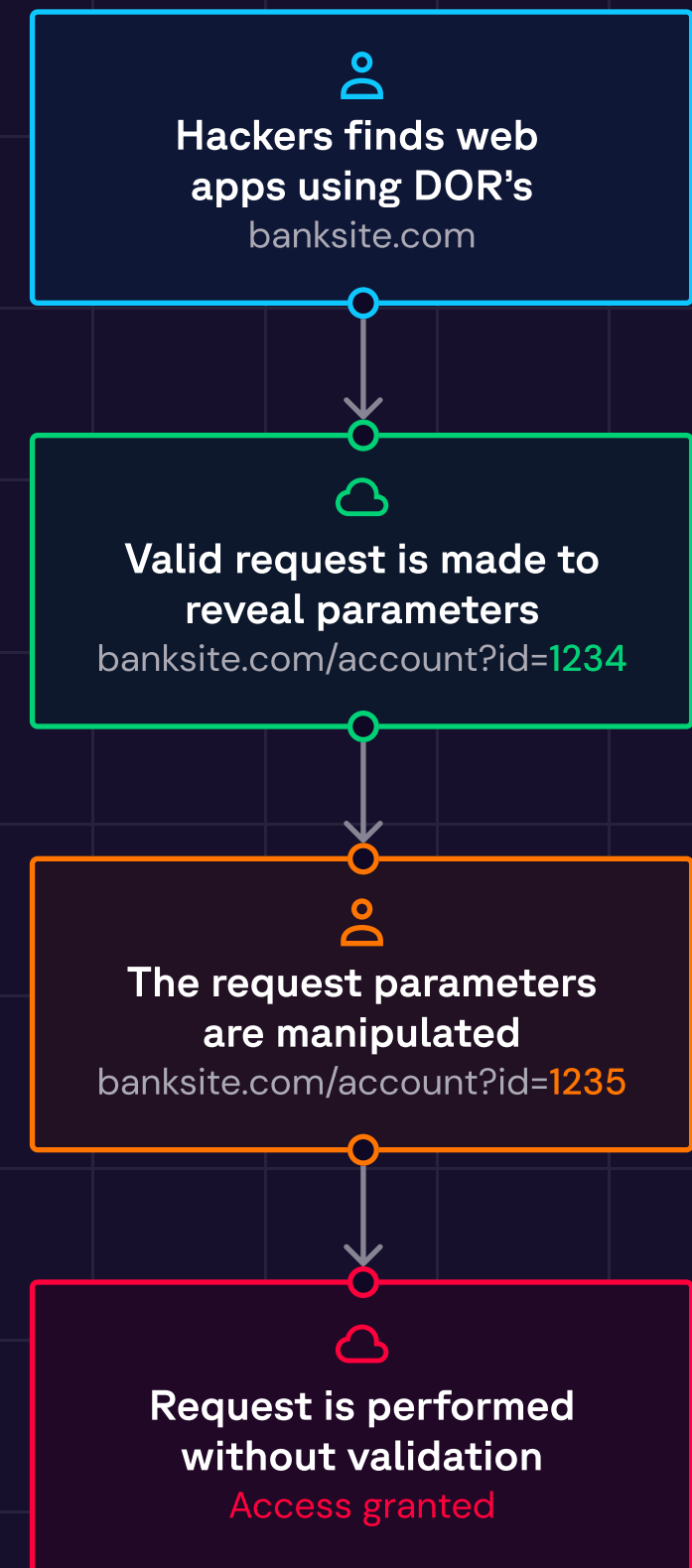
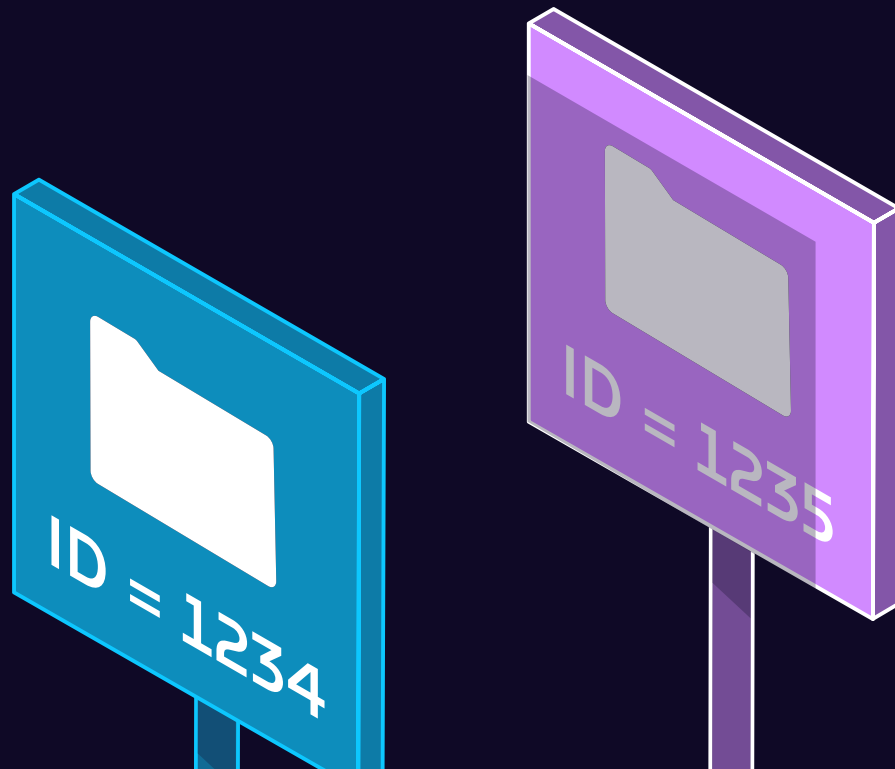


Figure 5. Flow diagram demonstrating Insecure Direct Object Reference exploitation

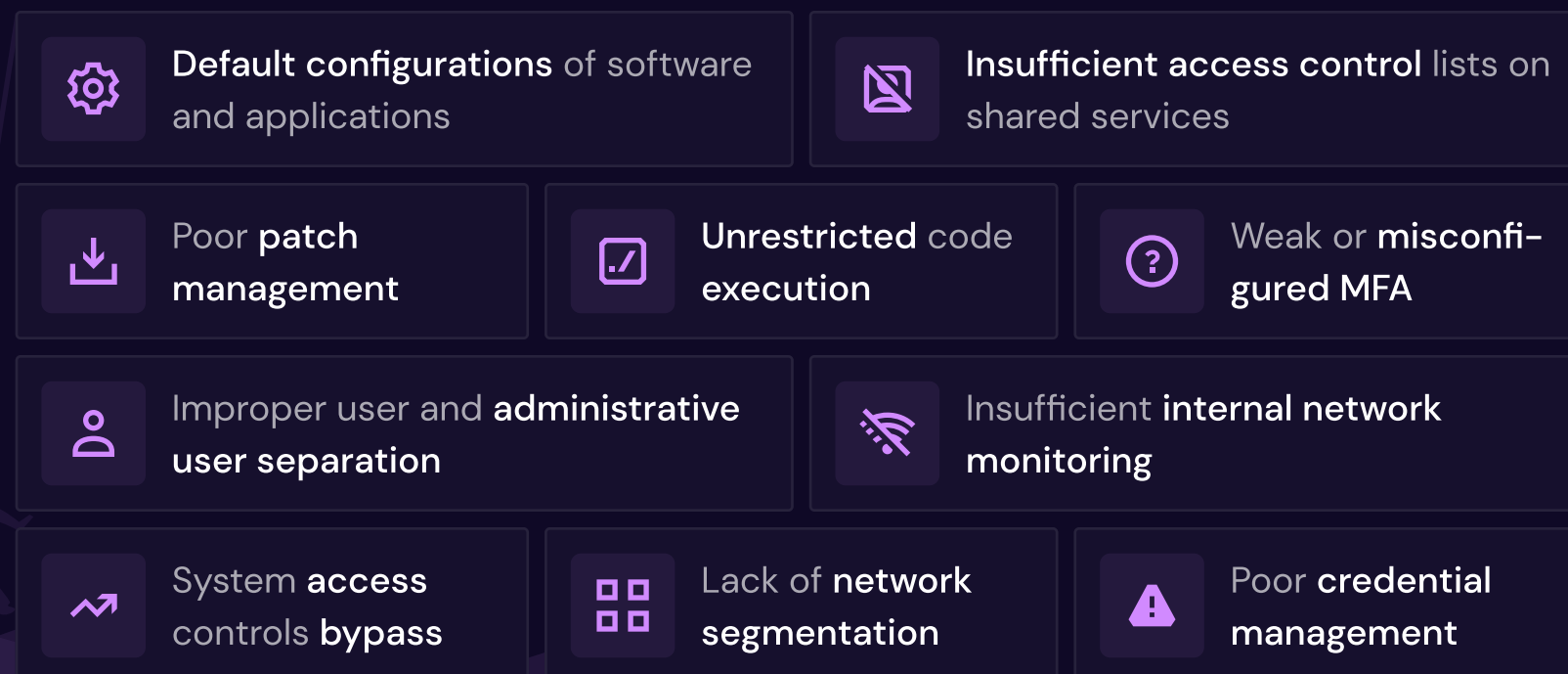
Configuration Flaws

During Hadrian's investigations we often discover public admin panels that utilize default credentials and sometimes the software has not been configured at all.

There are many publicly available wordlists of default passwords that threat actors can use to quickly compromise public admin panels with default configurations.

The NSA and CISA recently released a study⁵ on the most common cybersecurity misconfigurations and the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations. The top ten are summarized below:

Top software misconfigurations



Secure by default

The Secure Software Development Framework (SSDF), also known as the National Institute of Standards and Technology's (NIST's) SP 800-2184 outlines the requirements for Secure by design development.

CSA goes a step further by recommending that organizations build, purchase and use software that is Secure by default⁶.

Exploited Targets

Vendors that have products that are frequently exploited are not inherently insecure. In fact, it is often their widespread adoption that makes them attractive targets for hackers.

When prioritizing remediation organisations should also consider the impact of exploitation. For example, Citrix and Atlassian, which are not featured in Figure 6, are commonly targeted because of how impactful a compromise could be. A Citrix vulnerability could result in complete access to remote environments and Atlassian could enable threat actors access to source code.



A program is made up of a complex set of rules following a certain execution flow that ultimately tells the computer what to do. Exploiting a program is simply a clever way of getting the computer to do what you want it to do, even if the currently running program was designed to prevent that action.

Jon Erikson - Hacking the Art of Exploitation

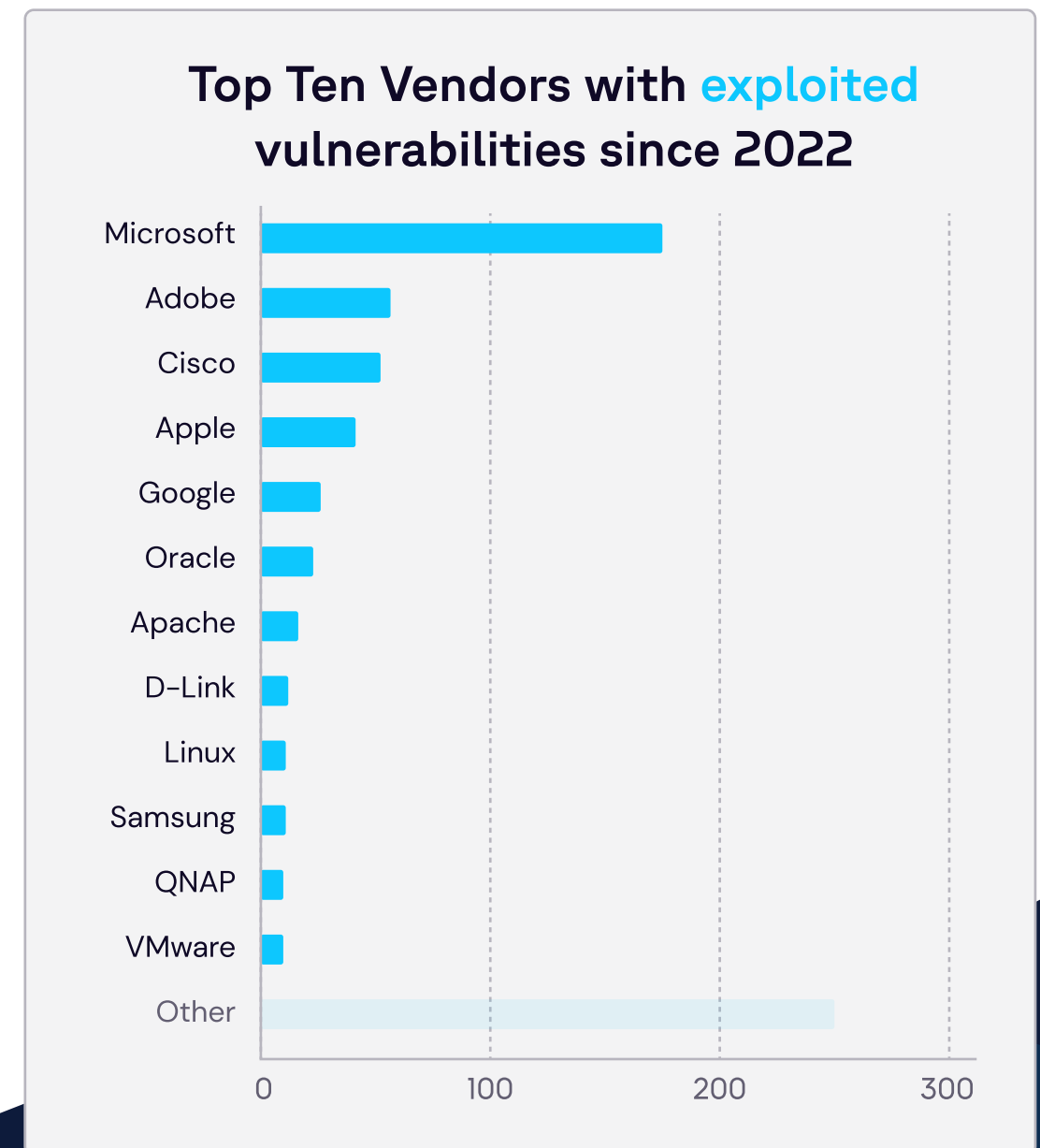


Figure 6. Top vendors with exploited vulnerabilities discovered since 2022⁷

What's New in CVSS 4.0

The Common Vulnerability Scoring System (CVSS) is widely used to gauge the severity of Common Vulnerabilities and Exposures (CVEs). It is also often misused to prioritise the remediation activity without considering any contextual factors. To address this Forum of Incident Response and Security Teams (FIRST) have introduced new nomenclature in CVSS 4.0.

The new standard provides a more detailed analysis of the Base Metrics for a better evaluation of vulnerabilities. CVSS 4.0 has also introduced new terminology to describe the mix of Base, Threat, and Environmental metrics. Moreover, it includes new Base metric values to describe how users interact with a system, distinguishing between Passive (no user action required) and Active (user action required) interactions.

FIRST have created a [free training course](#) to help teams use CVSS 4.0 that requires no prior knowledge

| New CVSS Nomenclature | CVSS Metrics Used |
|-----------------------|-------------------------------------|
| CVSS-B | Base metrics |
| CVSS-BE | Base and Environmental metrics |
| CVSS-BT | Base and Threat metrics |
| CVSS-BTE | Base, Threat, Environmental metrics |



Timeline to Exploitation

The timeline from discovery to exploitation has continued its downward trend, requiring increasingly faster remediation by security teams.

It is estimated that 50 – 70 % of all exploited vulnerabilities are zero days⁸. Interestingly, the time-to-exploitation (TTE) of n-day exploits has decreased dramatically over the last few years. In 2019, the TTE was approximated to be 63 days. In 2022, the TTE was observed to be only 32 days.

Gartner recommends

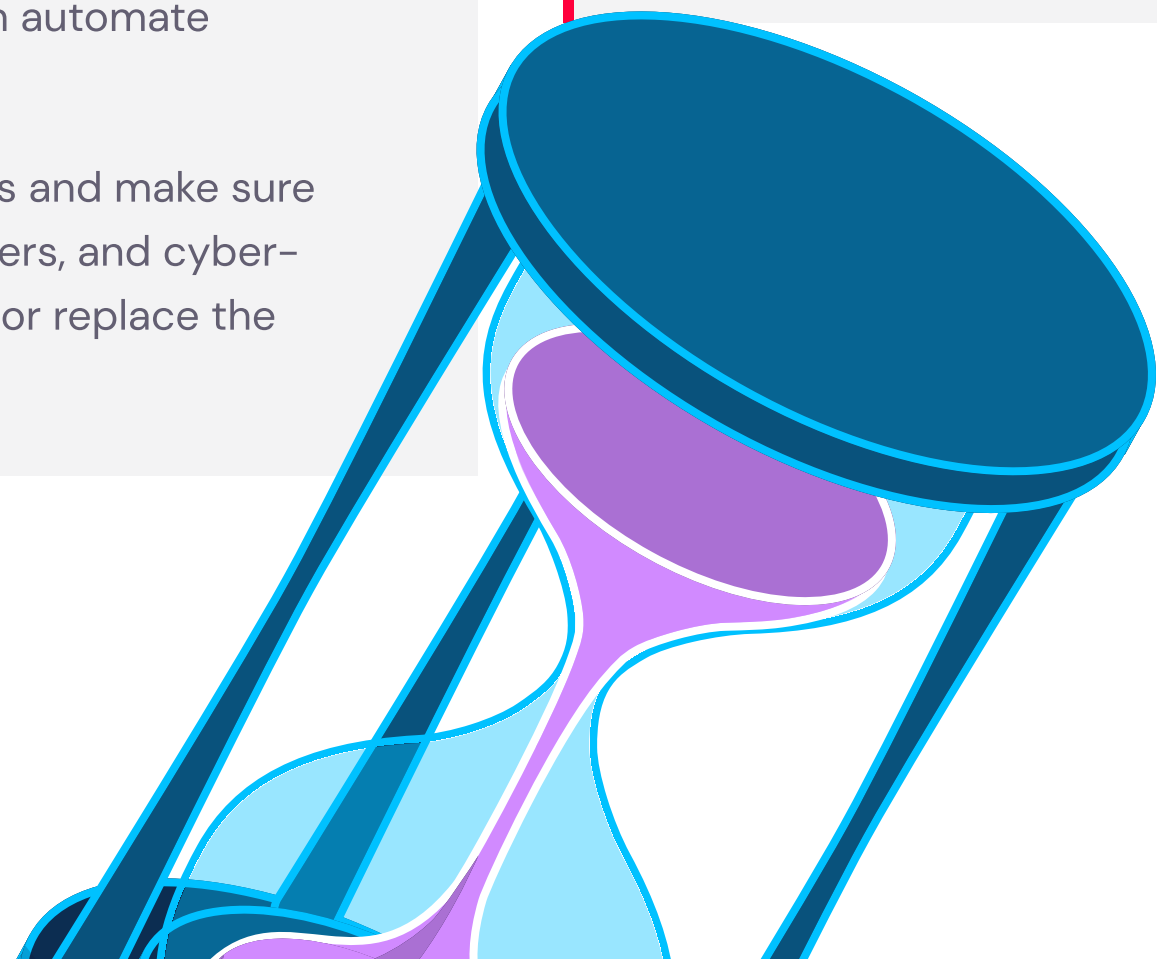
“Use technologies to automate vulnerability analysis. Improve remediation windows and efficiency by using technologies that can automate vulnerability analysis.

Review your existing vulnerability assessment solutions and make sure they support newer types of assets like cloud, containers, and cyber-physical systems in your environment. If not, augment or replace the solution.”¹⁰



Given the organization's scale and the potential for significant exploit risks, the Time to Exploitation (TTE) may compress to a matter of hours.

Olivier Beg - Head of Hacking, Hadrian



Inside DORA and NIS2

To increase cyber resilience, the European Union has introduced a number of new regulations. The Network and Information Security (NIS2) and Digital Operational Resilience Act (DORA) were both established in early 2023 and will come into force in late 2024 early 2025 respectively.



DORA

DORA's primary objective is to streamline and elevate Information Communication Technology (ICT) risk standards across the European Union's financial sector. ICT breaches that occur in the financial sector can “potentially trigger adverse consequences for the stability of the Union’s financial system,” EU says. The act extends the scope of financial regulators, granting them the authority to supervise and enforce requirements on relationships between financial services and their third-party ICT providers. The five pillars of DORA are:

- Digital Operational Resilience Testing
- ICT Risk Management
- ICT Third-Party Risk
- Information Sharing
- ICT-Related Incident Reporting

[Read blog post](#)

NIS2

NIS2 will expand upon the original directives scope beyond essential services and relevant digital service providers to include transportation, banking, financial assets, health sector, digital infrastructure, drinking water and energy. Organizations

- Article 21 requires that organizations take appropriate and proportionate technical, operational and organizational measures to manage the risks to the security of network and information systems
- Preamble 51 recommends the use of innovative technology, including artificial intelligence, to improve the detection and prevention of cyberattacks
- Preamble 58 states that exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk.

[Read blog post](#)

Supply Chain Risks

Fueled by the success of attacks, attacks on organizations supply chain have grown dramatically over the past few years.

A prime example of why software supply chain must be carefully monitored and protected is the MOVEit exploit (CVE-2023-34362) that was discovered this year. With over 2,500 organizations breached as a result of the exploit and its variants¹⁰.

Surveys indicate that 12% of all breaches target the software supply chain and 15% to business partners¹¹. The industry-wide damage that supply chain attacks can cause has lead to a high rate of awareness among cyber and business leaders, as shown in Figure 8.

Business leaders



Cyber leaders



- Far more resilient
- Slightly more resilient
- Equally as resilient
- Slightly less resilient
- Far less resilient

Figure 8. Perceived cyber resilience of third-party organizations in comparison to their own²

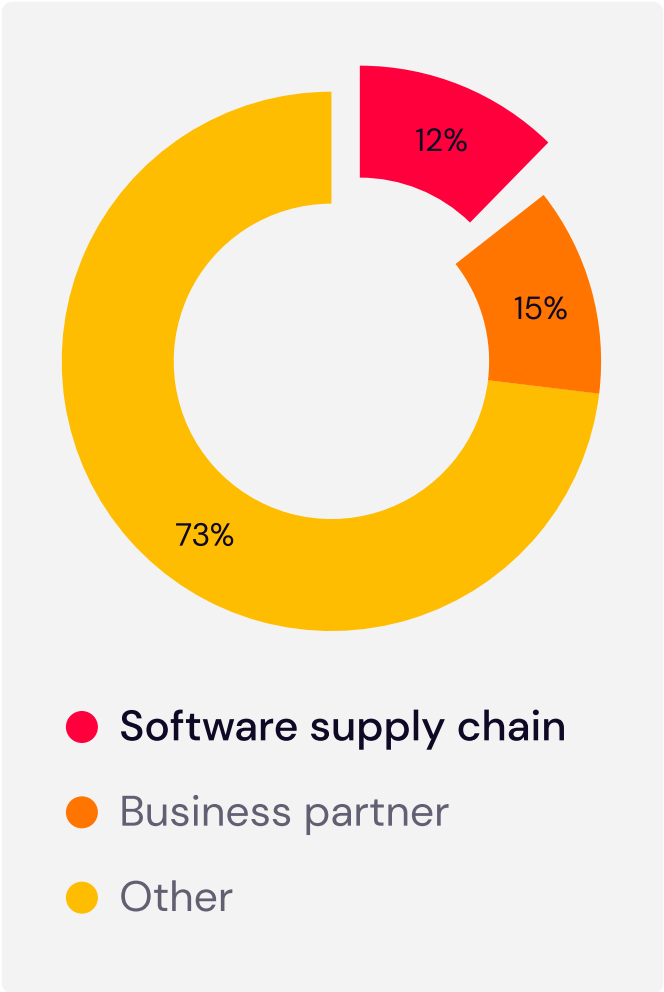


Figure 7. Target of malicious cyber attacks¹¹

Timeline of MOVEit

May 28: Progress software was alerted by a customer who reported unusual activity in their MOVEit environment

May 31: Progress discloses a zero-day vulnerability in MOVEit

June 1: Multiple threat intelligence firms share evidence of active exploitation

June 2: The zero-day is assigned CVE-2023-34362 and a severity of 9.8

June 4: The series of attacks is attributed to Clop

June 6: Clop ransomware group claims responsibility for exploiting MOVEit

June 7: CISA and the FBI released a joint advisory

June 9: An updated advisory is released introducing a patch for a second vulnerability (CVE-2023-35036)

June 15: Progress uncovers a fresh vulnerability, CVE-2023-35708, and issues an advisory

July 6: Progress reveals three more vulnerabilities (CVE-2023-36934, CVE-2023-36932, CVE-2023-36933) for MOVEit Transfer

[Read blog post](#)



File-transfer tools, including MOVEit, have become attractive targets for cybercriminals. Similar attacks have been observed, such as the exploitation of GoAnywhere MFT, emphasizing the prevalence of these types of threats.

Olivier Beg - Head of Hacking, Hadrian

Software Bill of Materials

Organizations should also be aware of vulnerabilities in open-source software that they have purchased, developed, and used. It is extremely common for developers to use open-source libraries and unknowingly introduce flaws into their software. The infamous example is the Log4j vulnerability (CVE-2021-44228) which prompted widespread remediation because the software was deployed across an estimated 3 billion devices.

[Read blog post](#)

Best practices state that organizations should maintain a formal record containing the details and supply chain relationships of various components used in their software. These so-called Software Bill of Materials (SBoM) enable organizations to continuously assess the IT landscape for potentially vulnerable software components.

Top 0.003%

Log4j 2.x is in the top 0.003% percentile in popularity by downloads out of a total population of 7.1 million¹²



The Secure Software Development Framework

The National Institute of Standards and Technology (NIST) standard for introducing the Secure Software Development Framework (SSDF) to address security issues through the software development life cycle (SDLC). Many organizations have built DevSecOps teams to own the SDLC, greatly reducing the likelihood and impact of breaches, as shown in Figure 9.

Secure Software Development Framework Practices:

- Ensure the organization's people, processes, and technology are able to secure software development.
- Protect all components of the software from tampering and unauthorized access.
- Produce secure software that has minimal security vulnerabilities in its releases.
- Identify and respond to vulnerabilities in software releases and prevent similar vulnerabilities in the future.

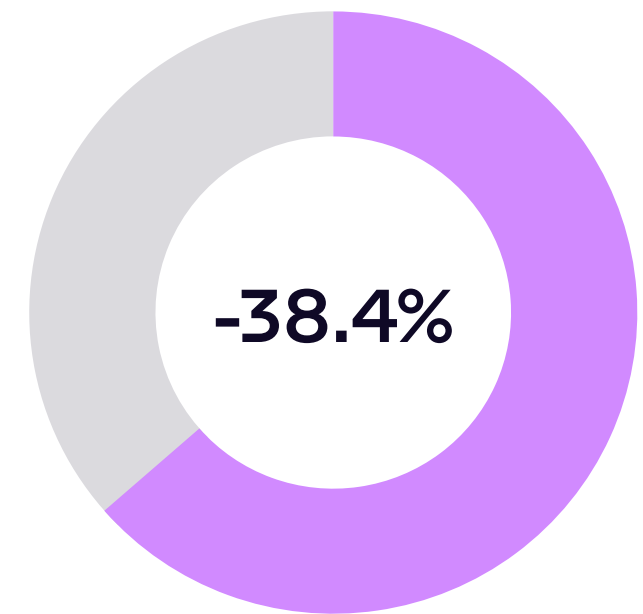
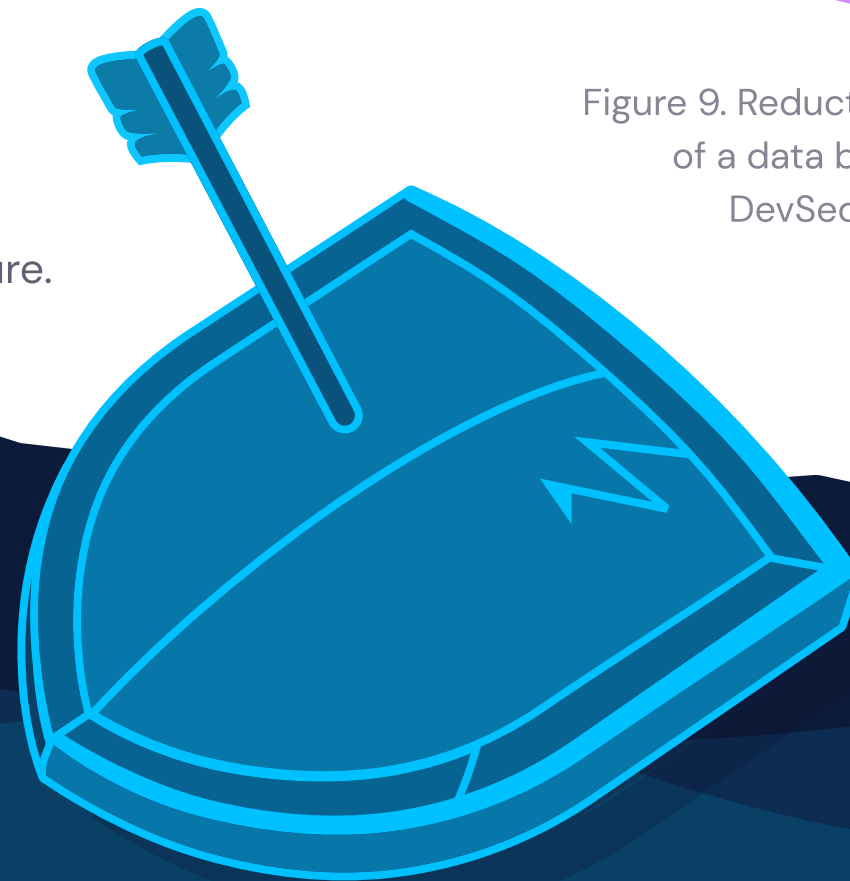


Figure 9. Reduction in the average cost of a data breach due to high DevSecOps maturity¹¹



Offensive Security Testing

DevSecOps teams must also monitor and manage the security of software that is in production. To do so they are increasingly relying on offensive security practices to identify flaws, as shown in Figure 10. Offensive security investment is quickly rising as one of the methods to prevent future breaches.

Offensive security also benefits Security Operation Center (SOC) teams, enabling them to validate threats and build robust risk-based vulnerability management programs. It also assists Red Teams by identifying areas of weakness that require further investigation.

Most common investment types among those increasing security investment following a breach

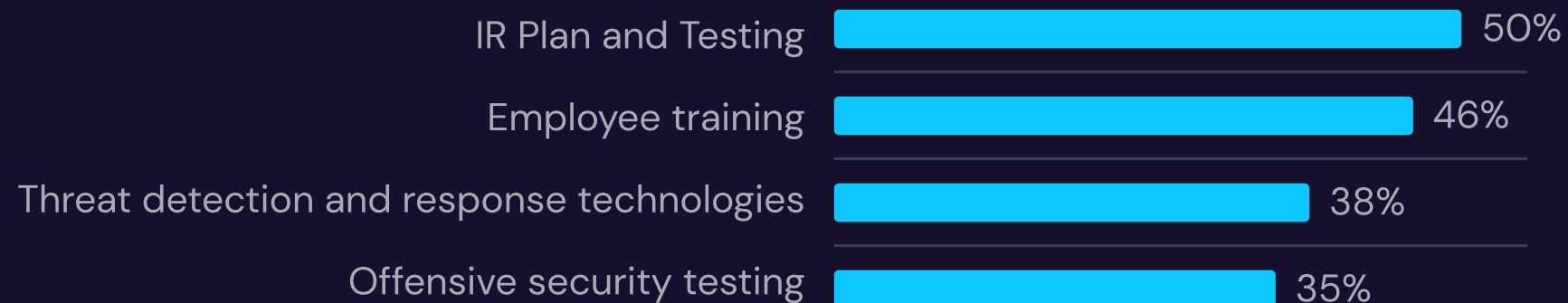


Figure 10. Most common investment types following a breach¹¹

Hadrian Simplifies Offensive Security

Shifting left is easy with Hadrian. The platform proactively identifies software weaknesses, exposed risks and defensive controls to be validated with automated offensive security. Stay secure with validated and prioritized findings and remediate risks with less effort.

[Book a demo](#)

Autonomous

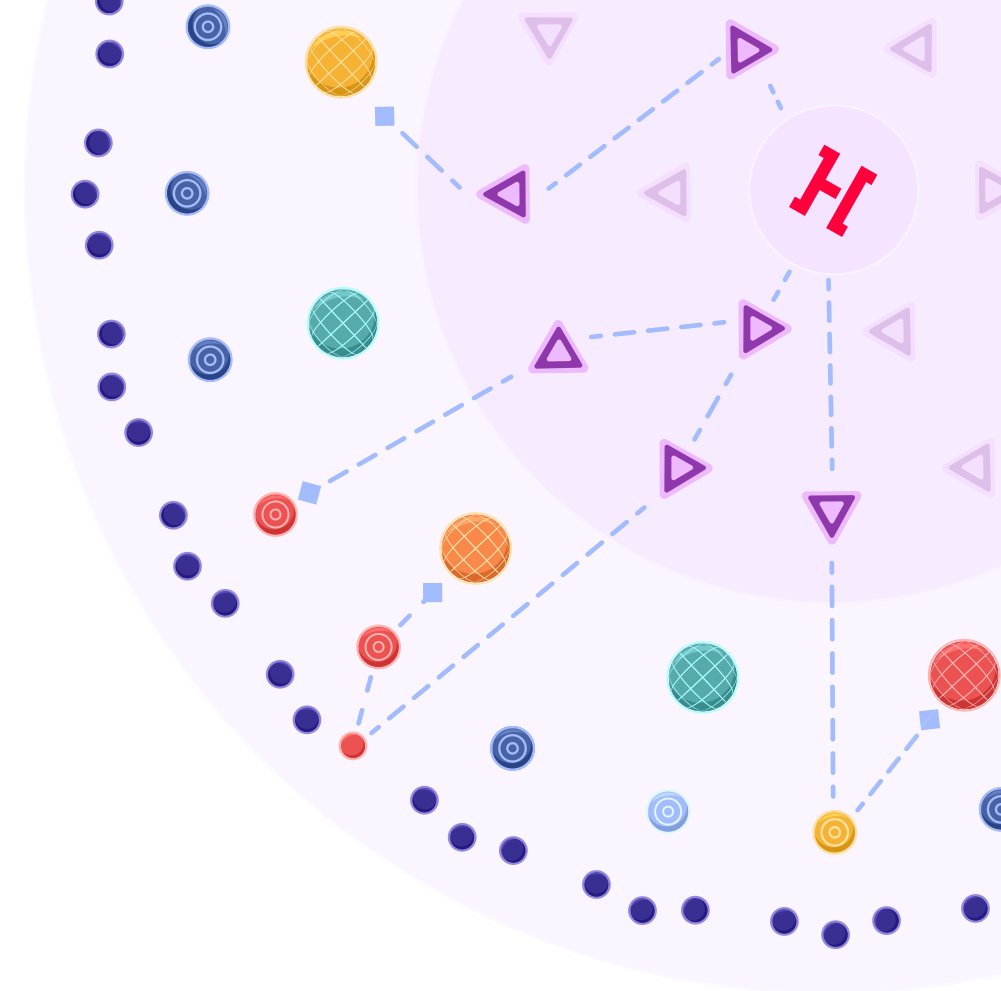
Hadrian validates risks across your entire organization using the same techniques as a penetration tester. The zero-touch design simulates a security expert with no configuration, no scheduling, and no manual intervention required. Results are automatically triaged for accuracy and reliability.

Continuous

Hadrian provides real-time visibility of threat exposure to your environment. The event-based architecture monitors your attack surface 24x7x365 for changes a threat actor could exploit. Investigative scans are triggered the moment a potential threat is detected, keeping you fully aware at all times.

Comprehensive

Hadrian tests in breadth and depth to uncover and validate exploits. The platform's Orchestrator AI is trained and updated by our in-house hackers to emulate real-world attacks and discover threats that other tools can't. The automated penetration testing capabilities rival that of human operators.



Under the hood

At the heart of Hadrian's platform is Orchestrator AI, an event-based threat exposure engine, that replicates real-world hackers to autonomously identify risks before they are exploited.

Step 1: Discovery

Orchestrator AI's discovers all of your external-facing assets, building a complete picture of your potential attack vectors, using its neural network graph of the internet.

Step 2: Contextualization

Hadrian identifies potential software weaknesses and exploitable targets by fingerprinting OS information, modules, libraries, input fields, authentication methods and much more.

Step 3: Validation

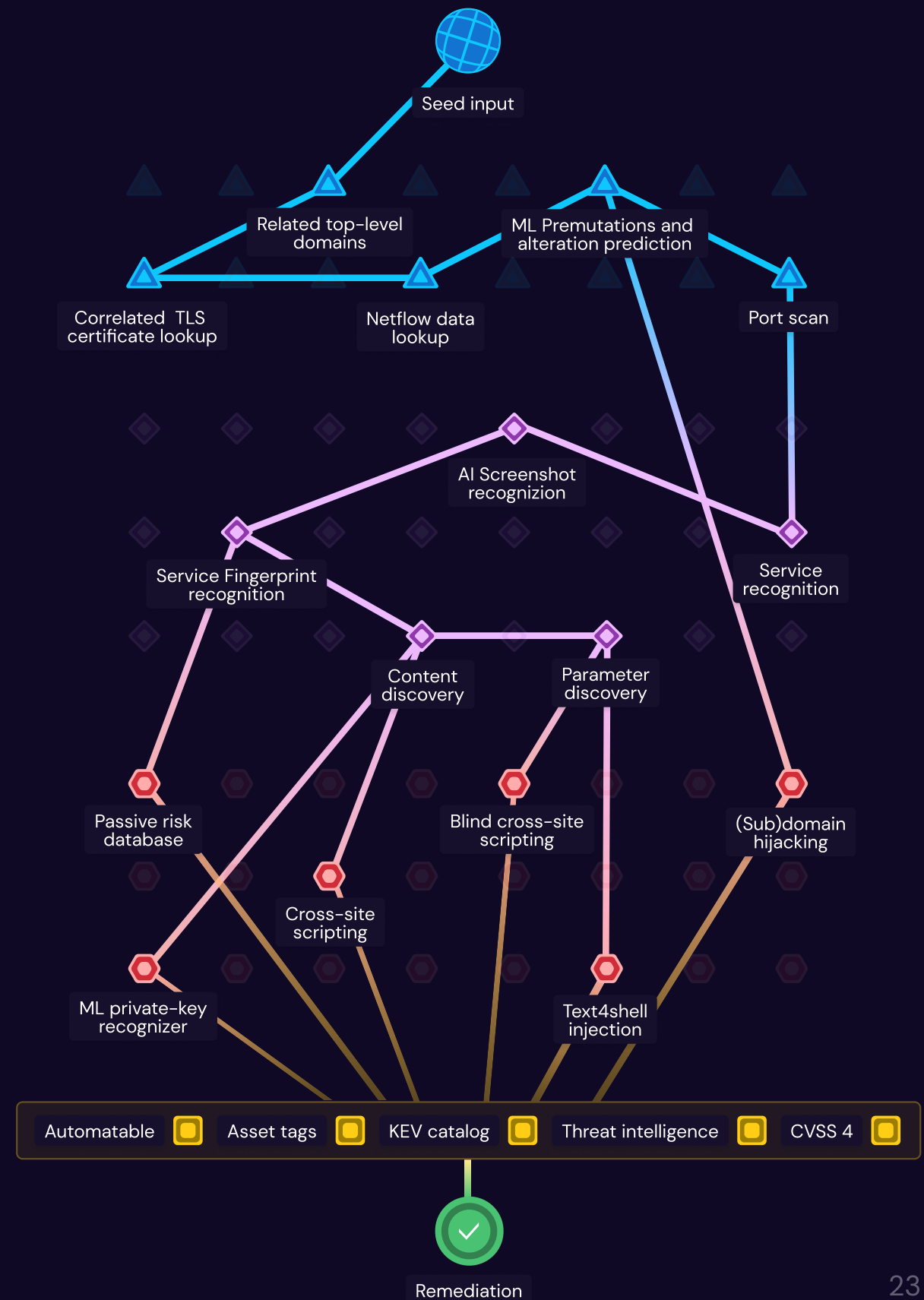
Orchestrator AI removes false positives by chained together "hacker modules" to simulate complex multidimensional attacks. OWASP Top Ten risks, known and zero-day vulnerabilities, and exposed and misconfigured services are confirmed.

Step 4: Prioritization

Hadrian goes beyond CVSS with proprietary scoring algorithms prioritize validated risks based on technical factors, the likelihood of exploitation, and potential business impact.

Step 5: Remediation

Orchestrator AI streamlines remediation by providing relevant business units with actionable step-by-step resolution instructions for DevSecOps to action.



About Hadrian













Defensive security should be validated by offensive security. Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian’s continuous and comprehensive testing discovers and validates risks completely autonomously. Hadrian’s platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian’s in-house hacker team.



‘What’s exciting about what Hadrian is doing is they solved a seemingly impossible puzzle: finding weaknesses in a complex network with human-like detail, at scale, from the outside and continuously. What usually takes a dedicated team of security engineers a few weeks to figure out for one system, they can do in minutes for thousands of systems.’

Tiago Teles - Security Lead, ABN AMRO

Trusted by

| | | | |
|---|--|---|---|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

References



- 1 – SANS (2023) 'Building a Resilient Offensive Security Strategy'
- 2 – World Economic Forum (2023) 'Global Cybersecurity Outlook 2023'
- 3 – RAPID7 (2023) '2023 Mid-Year Threat Review'
- 4 – MITRE (2023) '2023 CWE Top 25 Key Insights' Available at: https://cwe.mitre.org/top25/archive/2023/2023_key_insights.html (Accessed: 8 November 2023)
- 5 – Cybersecurity and Infrastructure Security Agency (2023) 'NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations' Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a> (Accessed: 8 November 2023)
- 6 – Cybersecurity and Infrastructure Security Agency (2023) 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software'
- 7 – Cybersecurity and Infrastructure Security Agency (2023) 'Known Exploited Vulnerabilities Catalog' Available at: https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv (Accessed: 8 November)
- 8 – Mandiant (2023) 'Analysis of Time-to-Exploit Trends: 2021-2022' Available at: <https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022> (Accessed: 8 November)
- 9 – Gartner (2023) 'How to Set Practical Time Frames to Remedy Security Vulnerabilities' Available at: <https://www.gartner.com/smarterwithgartner/how-to-set-practical-time-frames-to-remedy-security-vulnerabilities> (Accessed: 8 November)
- 10 – Emsisoft (2023) 'Unpacking the MOVEit Breach: Statistics and Analysis' Available at: <https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/> (Accessed: 8 November)
- 11 – IBM Security (2023) 'Cost of a Data Breach Report 2023'
- 12 – Sonatype (2021) 'Log4shell by the numbers- Why did CVE-2021-44228 set the Internet on Fire?' Available at: <https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire> (Accessed: 8 November)