HADRIAN

The Ultimate Guide to

Exposure Management

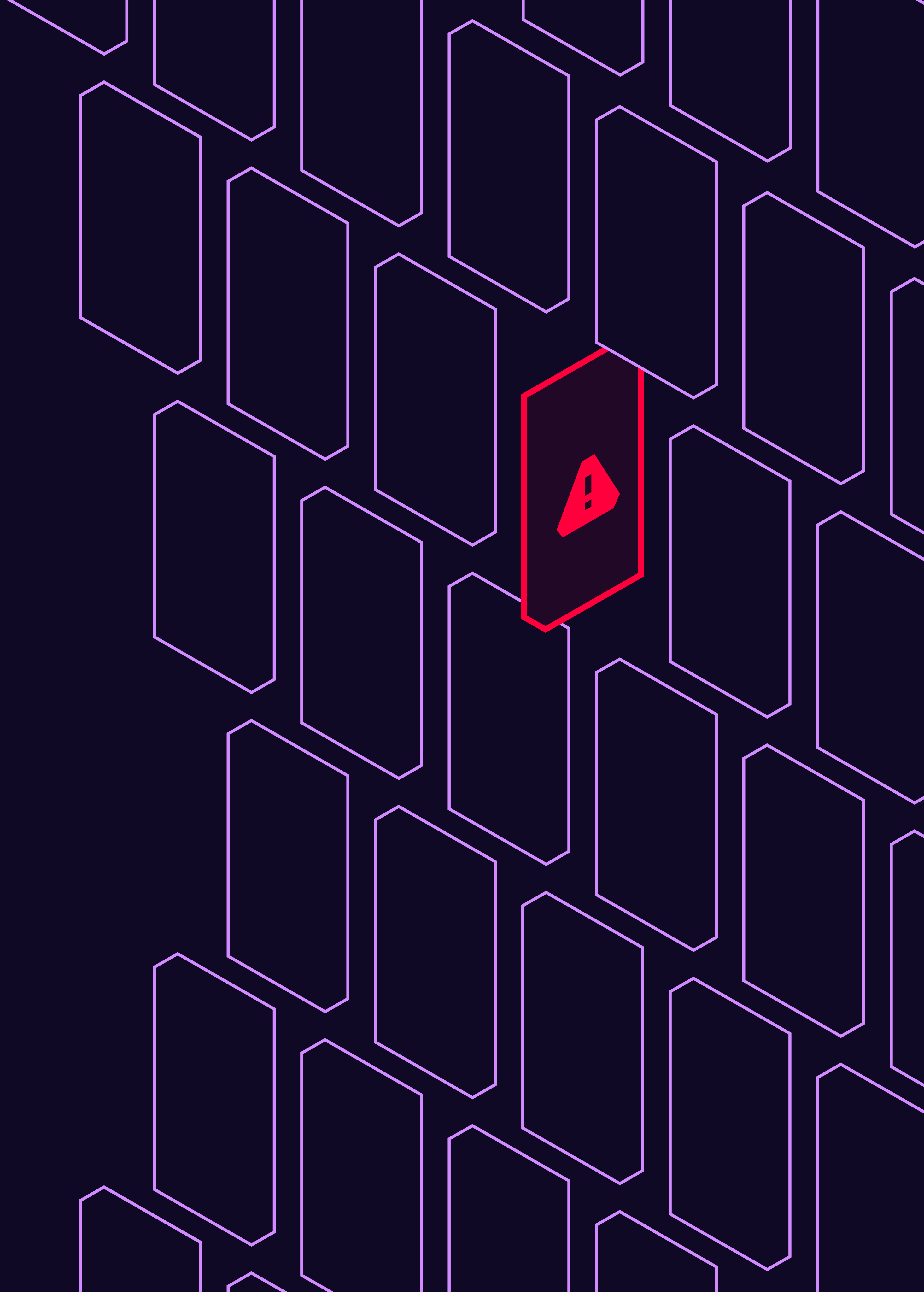


Table of contents

The Growing Need For Exposure Management

Today's cybersecurity attackers pivot fast, leaving organizations scrambling to automate controls and deploy security patches to keep up, but such tactics don't reduce future exposure. Gartner has outlined continuous threat exposure management (CTEM) as a program that surfaces and actively prioritizes whatever most threatens your business.

"Continuous threat exposure management is a pragmatic and effective systemic approach to continuously refine priorities and walk the tightrope between two modern security realities. Organizations can't fix everything, nor can they be completely sure what vulnerability remediation they can safely postpone." [1]
Jeremy D'Hoinne, Gartner VP Analyst

Exposure management operates across a number of domains, enhancing multiple workflows to strengthen the cybersecurity posture of the organization.

Gartner

By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be 3x less likely to suffer from a breach. [1]

Challenges Faced By Security Teams

	Challenge	Statistics
Vulnerability Management	Effectively identifying, prioritizing, and managing vulnerabilities across a vast and diverse array of assets.	69% of organizations have experienced an attack targeting an unknown, unmanaged, or poorly managed external-facing asset. [2]
SOC Analyst	Swiftly and effectively responding to emerging security threats while dealing with alert overload and fatigue.	68% of all cyberattacks exploit vulnerabilities that have had a patch available for over a year. [3]
DevSecOps	Integrating real-time monitoring and feedback loops in development processes in a scalable way.	86% of codebases contain at least one vulnerability and 48% contain a high-risk vulnerability. [4]
Penetration Testing	Accurately and continuously testing as many assets as possible for the latest threats while minimizing false positives.	52% of organizations are considering changing to new assessment solutions to reduce the volume of false positive alerts. [5]
Threat Hunting	Identifying threats proactively while grappling with a lack of visibility, context, and data quality.	66% of security teams say that it is difficult to protect complex and dynamically changing attack surfaces. [6]

Exposure Management Explained

Continuous Threat Exposure Management (CTEM) is the ongoing monitoring and identifying of threats, vulnerabilities, and risks in real-time. It enables organizations to identify and respond to threats quickly, reducing the risk of a successful attack.

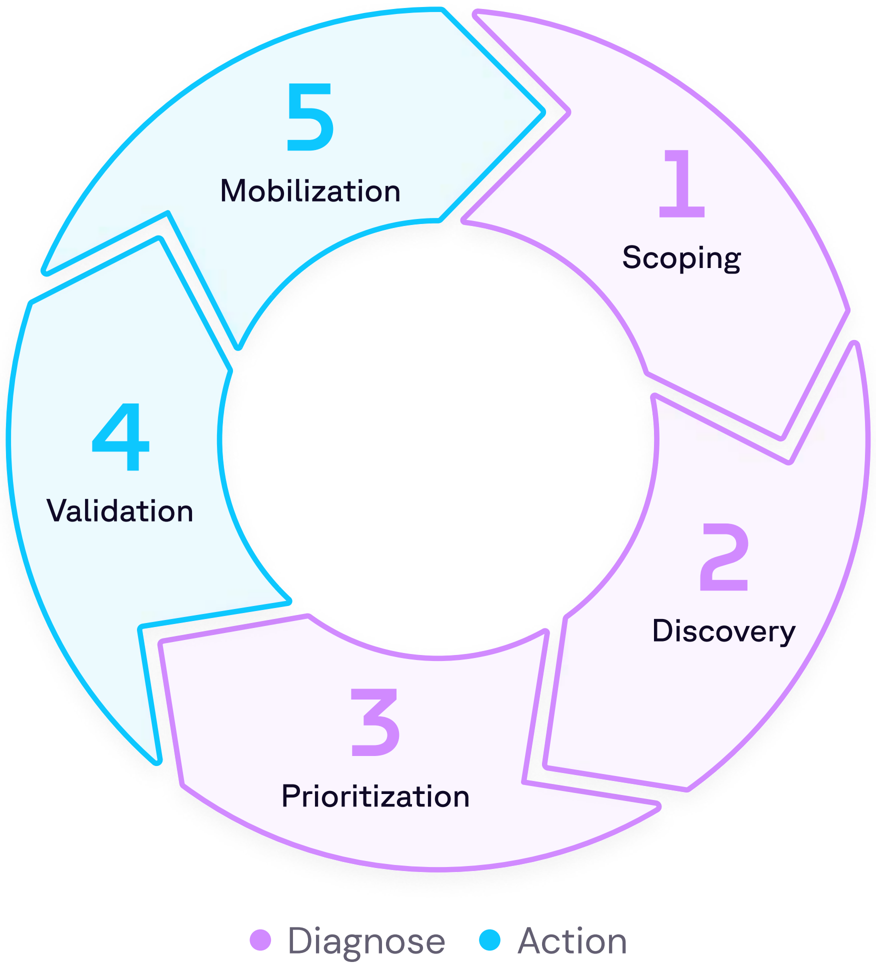
1 **Scoping** Comprehensively identify the organization's attack surface and create an inventory of assets.

2 **Discovery** Continuously diagnose the potential vulnerabilities and misconfigurations of assets in the scope.

3 **Prioritization** Rank the threats by their technical impact, business context, and asset value.

4 **Validation** Determine which threats are exploitable and should be resolved immediately or can be delayed.

5 **Mobilization** Coordinate and verify action remediation across the organization to resolve threats.



How you reduce risk is unique to your organization, however, CTEM provides the architecture to address the challenges you face:

Minimizing the number of security incidents that organizations currently face

Creating safe environments in constantly changing environments

Identifying the weak points in your security posture that an attack could utilize

Reducing the risk created by the technology that supports remote workers

Moving critical business functions to 3rd party services or platforms

Top Implementation Challenges

Attack surface | Threat landscape | AI-Powered Attacks

Large attack surfaces. This is caused by the large expanse a company covers, multiple brands owned by the holding company, or the number of marketing campaigns running with sites. Whatever the reason, this is a problem because it gives threat actors more places to attack. In the first half of 2023, 66% of initial access vectors were remote and internet-facing apps[7].

Multicloud environments. Organizations are increasingly supporting multicloud environments which creates visibility challenges for 42% [8]. Assets accessible from the internet are an easy target because sometimes a cyber team is unaware of them, or sometimes the assets haven't been tested recently enough.

Complex infrastructure. These can be due to technology migrations, frequent code deployments, and M&A activity that result in a disparate range of internet-facing apps. According to research organizations with complex infrastructure have a 45% increased security risk [8].

Rapid development cycles. The world is calling for more applications and feature updates daily. Developers are responding with speed, but that speed sometimes doesn't leave time for adequate cybersecurity. 60% of developers using DevOps say they are releasing code twice as quickly as they were before and nearly half of organizations consciously deploy vulnerable code because of time pressure [9].

Many factors have contributed to the urgency and complexity of implementing threat exposure management. They include:

Top Implementation Challenges (cont.)

Attack surface | Threat landscape | AI-Powered Attacks

Cybercrime is evolving toward more mass attacks. Threat actors used to conduct highly targeted attacks on a small number of organizations for potentially high returns. Now, with so much on the internet and many automated tools for hackers, they can conduct mass attacks. Many organizations have web applications or apps, and threat actors target these technologies to automate their attack processes. In fact, attackers typically start scanning for vulnerabilities within 15 minutes of a CVE being announced [10].

Software supply chain vulnerability. Software supply chains have gained prominence as a rapidly growing access vector for cyber threats. Software is built out of hundreds, and sometimes even thousands, of components. Vulnerability increases with each component added. The more components, the greater the risk. For example, threat actors can inject malicious code into the software build environment, or they can take advantage of a developer's overlooked error.

Geopolitical tensions and the increase in zero days. Geopolitical tensions have led to an increase in the number of zero-day attacks from nation-state threat actors. In 2023, there were 56 zero days spotted in the wild--the second-highest number ever seen. A lot of the zero days being detected in the wild are actually permutations and variations of previously discovered vulnerabilities. Patching only fixes the symptom and one particular attack path. Threat actors are able to find other methods to exploit that vulnerability to establish themselves within an organization and conduct their attack.

Top Implementation Challenges (cont.)

Attack surface

Threat landscape

AI-Powered Attacks

Exploit generation. AI algorithms have shown the ability to uncover previously unidentified exploits, vastly accelerating a once manual and time-intensive process. For example, AI systems can scrutinize databases housing known CVEs and craft original code to exploit these weaknesses. This method not only expedites the process but also uncovers potential exploitation avenues that might not be obvious to human researchers.

Attack permutation. Many defensive security tools operate by identifying specific indicators of compromise or attack. Utilizing artificial intelligence, cyber attacks can be adapted dynamically, to circumvent intrusion detection systems. Malicious actors can use machine learning to discern patterns within these systems, thereby adjusting their strategies to evade detection.

AI accelerated Phishing. AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails, CNBC says. Recently, there's been a 1,265% increase in malicious phishing emails, and a 967% rise in credential phishing, according to a new report by SlashNext.

With all of this to face on a daily basis, it's easy to see why reactive, traditional security is just not cutting it anymore. Hackers are using AI, you need to be, too. There are more ways than ever before for threat actors to access your network, and more motivation to go with it. Without a doubt, offensive security is rapidly becoming imperative.

Evaluating Exposure Posture

Offensive cybersecurity is a strategy that looks at cybersecurity through the eyes of a real threat actor. Instead of focusing on merely defending the perimeter in a reactive way, it focuses on the realistic current ways hackers attack and defend against these attacks before they happen. Offensive security can identify gaps in cybersecurity and evaluate exposure posture.

The hacker's perspective helps to find the most significant risks that need to be remediated. The hacker's perspective contextualizes assets to understand how an adversary would conduct an attack, probes for weaknesses, and prioritizes risks.

Accuracy + completeness scanning

Detecting Various Risks: Scanning should cover all risks, not just CVEs, to catch misconfigurations and insecure app designs that could lead to breaches.

Reducing False Positives: Validating results helps remove false positives, ensuring resources are focused on genuine security risks.

Rapid Response to Zero-Day Attacks: Quick adaptation of scanning tools allows for the identification and mitigation of emerging threats, like zero-day attacks.

Frequency + scope of scanning

Comprehensive Assessment: It's vital to scan everything that could be targeted, not just known assets, to discover vulnerabilities across the entire infrastructure.

Dynamic Security Scanning: As attack surfaces change daily, scans should occur whenever changes are made to ensure new cyber risks haven't been introduced.

Regression Testing: Checks to verify security posture are necessary post-resolution to confirm issues are fully addressed and no new risks are present.

Flexibility + cost of ownership

Ease of Use: The solution must be user-friendly for easy access and quick incident response. Complexity hinders adoption and effectiveness.

Cost Management: Low implementation, management, and maintenance costs are crucial for optimal ROI. Unexpected expenses erode value.

Future-Proofing and Compatibility: The solution should be adaptable and compatible with other systems to reduce costly replacements and ensure long-term effectiveness.

Legacy Tool Gap Analysis

All of the cybersecurity testing methods listed below are valuable in their own right, but they are not complete and can create a false sense of security when it comes to threat exposure management. Here are some of the cons to solely relying on them, especially in light of the top three most important variables: frequency, accuracy, and cost.

	Accuracy and completeness of scanning	Frequency and scope of scanning	Business flexibility and cost of ownership
Penetration testing	5	2	2
Penetration testing as a service	4	3	3
Bug bounty	3	4	2
Vulnerability scanners	2	5	3
Static application security testing	2	3	3
Dynamic Application Security Testing	2	3	3
Security rating services	1	4	4

Legacy Tool Gap Analysis (cont.)

Breakdown

Penetration testing is costly and not frequent enough. Third-party traditional penetration tests are expensive and are conducted periodically, leaving time for cybercriminals to attack. The reports are often lengthy and vary in quality, making the findings difficult to action. Organizations complain of being unable to address all of the findings and find it hard to verify the impact of any fixes they make.

Bug bounty can be unreliable. Crowdsourcing ethical hackers to find your vulnerabilities might seem like a good idea because it brings together all types of hackers with all types of skills to work on your behalf. But this leaves questions as to whether the search will be done on time or with the level of quality and accuracy desired. It also can’t be done frequently enough to provide offensive security in the bigger picture.

Penetration Testing as a Service (PTaaS) provides partial visibility. This method provides incomplete coverage of an organization's entire attack surface, particularly in complex or distributed environments. It is also constrained by the skills and expertise of the penetration testers conducting the assessments, leading to gaps in vulnerability identification. Additionally, PTaaS does not provide continuous monitoring or real-time insights into evolving threats.

Vulnerability scanners lack accuracy. They are unable to validate their findings and cannot discover all types of risks. Many cyber teams report they are dissatisfied with the insights from their existing vulnerability scanners and security rating services. The information this tooling provides is not actionable.

Breakdown (cont.)

Static application security testing (SAST) can only identify superficial weaknesses. This testing is limited to using automated white box testing to analyze code during the early stages of the software development lifecycle. They are unable to identify issues that only manifest during runtime and may struggle with dynamic languages and third-party libraries. SAST tools sometimes come up with false positives, requiring manual verification.

Security Rating Service findings are not validated. Third-party security rating services use historical outside data to rate an organization's cybersecurity. This information can be old, outdated, or simply wrong. Reports provided by these services are geared toward executives rather than security teams. These tools lack fidelity of risks to help with security testing. Some comprehensive tools do exist, but they can be difficult to configure and use.

Dynamic Application Security Testing (DAST) is time-consuming to scale. This black box testing—or testing from the outside in—on an application's exposed interfaces is hard to automate. It may generate false positives due to its reliance on simulated attacks, and it can be challenging to maintain coverage for complex applications with dynamic content.

AI-Driven Exposure Management

Ideally, exposure management should be:

- **AI-driven** – Capable of deploying the same complex techniques and analyzing the results as a human penetration tester at any time.
- **Scalable** – Able to conduct assessments across the entire external attack surface and continuously monitor for changes that may require additional testing.
- **Flexible** – Should be cloud-based so that it can deployed quickly, integrate with any 3rd party tool, and enable fast remediation.

Out of the box Hadrian performs continuous attack surface discovery, performs automated penetration testing against that surface, and categorizes findings into true positives and potential exposures. The platform automatically enriches the findings with threat intelligence and asset context to prioritize the highest risks, to trigger orchestration and remediation, improving the posture in real-time.

Common use cases:

1. Attack surface discovery
2. Automated penetration testing
3. Risk-based vulnerability management
4. Threat exposure management
5. Compliance reporting
6. Cloud misconfigurations

About Hadrian

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.

Book a demo

Trusted by market leaders

ABN·AMRO	SHV ENERGY	macmillan education	CTC GLOBAL
WeatherTech	LEROY MERLIN	LOTTOMatica	CA
RITUALS...	BIOLANDES	nedap	Van Oord

Sources

[1] - Gartner, How to Manage Cybersecurity Threats Not Episodes (2023)

[2] - ESG, Security Hygiene and Posture Management (2022)

[3] - Abdalslam, Patch Management Statistics, Trends And Facts (2023)

[4] - Synopsys, Open Source Security and Risk Analysis Report (2023)

[5] - Netwrix, Vulnerability Assessment Analytical Note (2022)

[6] - Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)

[7] - RAPID9, Mid-Year Threat Review (2023)

[8] - NetApp, Cloud Complexity Report (2023)

[9] - GitLab, Annual Global DevSecOps Survey (2020)

[10] - Palo Alto, Attack Surface Threat Report (2021)