PICUS

THE BLUE REPORT 2023

The State of Threat Exposure Management

https://t.me/learningnets

Table of Contents

https://t.me/learningnets

Key Findings

This report identifies four impossible trade-offs that organizations are making when it comes to managing their threat exposure.

As a result of these trade-offs, threat exposure management programs are often in poor shape. We found that on average security teams can only prevent just over half of all attacks (59%). Detection scores are even lower. Companies are only logging 1 in 3 successful attacks (37%) and creating alerts for less than 1 in 6 (16%).

1 The first trade-off is choosing between prevention efficacy and detection efficacy. We compared prevention and detection scores across regions and industries and found that performance varied between regions and industries. But, performance also varied within regions and industries. The stronger a region or industry is at prevention, the weaker they are at detection, and vice versa, especially across industries.

2 A second trade-off is between logging and alerting. Across all industries and all regions, there is a significant gap between log scores and alert scores, with alert scores being lower. Faced with a trade-off in time and resources, organizations are prioritizing logging over alerting.

3 The third trade-off is choosing which types of attacks to prevent. Prioritizing the prevention of one type of attack over another leaves gaps in organizations' defenses. For example, organizations have a dismal 18% prevention effectiveness rate against data exfiltration but 73% effectiveness rate against malware downloads. A similar trade-off exists when it comes to preventing attacker tactics outlined in the MITRE ATT&CK framework.

Unfortunately, attackers only need to find one gap in organizations' defenses to succeed. It is, therefore, not surprising then that the least prevented malware varieties all include multiple malicious actions across the kill chain. Similarly, cyber threat groups posing the most significant challenge are those whose attacks combine multiple techniques. These tend to be state-linked and financially motivated attack groups.

https://t.me/learningnets

4

The fourth trade-off is in the area of vulnerability management. A lot has been written about how security teams struggle to prioritize and patch common vulnerabilities and exposures (CVEs). With limited resources, vulnerability management teams must choose to remediate some CVEs over others – at their peril. This report identified a list of vulnerabilities – including high severity vulnerabilities and vulnerabilities over 3 years old – for which over 80% of organizations remain exposed.

What are security teams to do? Threat exposure management, sometimes referred to as continuous threat exposure management (CTEM), is one approach to cybersecurity that organizations can use to overcome these trade-offs. Organizations wanting to implement a CTEM program can look to Picus Security for a complete solution. Picus customers prevent twice as many attacks, within just three months of deployment.

https://t.me/learningnets

What Is Threat Exposure Management?

Threat exposure management, sometimes referred to as continuous threat exposure management (CTEM), is an approach to cybersecurity in which organizations effectively prioritize potential risks and corresponding remediation efforts, particularly in the face of a rapidly expanding attack surface. To obtain the insights they need, CTEM programs integrate attack surface discovery, vulnerability management and security validation.

Security validation typically involves the use of breach and attack simulations (BAS) to discover, verify, prioritize and mitigate real-world threats to an organization's networks and systems. BAS solutions allows organizations to proactively test their security posture and identify vulnerabilities before they are exploited by real attackers.

The success of a CTEM program can be measured by observing a substantial decrease in cyber risk, improved threat prevention and detection, and a shorter mean time to respond (MTTR). In addition, an effective CTEM program will show improved security control performance, better compliance with regulatory standards, and closer alignment with key business priorities.

https://t.me/learningnets

Methodology

The goal of this report is to provide insights into the state of threat exposure management so that security organizations can benchmark their performance against their peers and identify areas for improvement. The findings in this report are based on the results of simulated attack scenarios executed by Picus Security customers from January to June 2023. The data has been anonymized and aggregated from over 14 million simulations. Research and analysis was completed by Picus Labs, the research arm of Picus Security.

Definitions

Simulations were assessed in terms of organizations' prevention and detection effectiveness.

Prevention Effectiveness measures whether an organization's cybersecurity controls block possible cyber attacks. In the context of this report, prevention effectiveness is a measure of the number of prevented attacks as a percentage of all simulated attacks that were executed. For example, an effectiveness score of 80% indicates that 80 out of every 100 simulated attacks were successfully stopped. A high preventive effectiveness score implies that the security controls in place are adept at preventing attacks and lowering the likelihood of successful breaches. A poor prevention effectiveness score, on the other hand, indicates that there are gaps in an organizations' security controls, and that the organization would benefit from further investigating and improving the effectiveness of their security measures.

Detection Effectiveness measures whether an organization's security controls can detect possible cyber threats. In this report, we use two key indicators to evaluate the detection performance of cybersecurity controls: Log Score and Alert Score.

The **log score** measures the percentage of simulated attacks where attacker behavior was logged. The higher the log score, the greater the number of attacks that are being accurately logged by detection controls like a SIEM. A high log score typically indicates the existence of effective monitoring controls that are capturing large volumes of events and identifying threat indicators. The **alert score** provides the percentage of simulated attacks that generate alerts. Alerts are critical for triggering a response to a potential attack. A high alert score ensures that cybersecurity teams are promptly informed of any threats so they can take action to neutralize them.

Note that in this report some industries and regions do not have detection effectiveness scores due to small sample sizes. All industries and regions have prevention effectiveness scores.

https://t.me/learningnets

Scoring Legend

Results are color coded and grouped according to five levels of threat exposure management: inadequate, basic, moderate, managed and optimized (see table below).

Legend	Range	Description
Optimized	**90-100%**	Organizations with optimized security controls continuously monitor, refine, and update their controls to keep up with the evolving threat landscape and maintain their leading edge in exposure management.
Managed	**70-89%**	Managed security controls offer a high level of protection against a wide range of threats, significantly reducing the risk of successful attacks. Organizations at this level should maintain their strong security posture, regularly assess the effectiveness of their controls, and address identified gaps in exposure management.
Moderate	**40-69%**	Moderate security controls provide a reasonable level of protection against various threats. Organizations at this level should continue to refine their security controls and consider additional measures to further reduce their threat exposure.
Basic	**20-39%**	Basic security controls offer limited protection against a narrow range of threats. Organizations at this level should invest in enhancing and expanding their security controls to achieve a more effective threat exposure management program.
Inadequate	**0-19%**	Inadequate security controls provide minimal or almost no protection against threats, leaving the system highly vulnerable to attacks. At this level, only a few basic security measures are in place, and nearly all attacks are likely to succeed. Organizations with this level of exposure need to urgently review and improve their security posture.

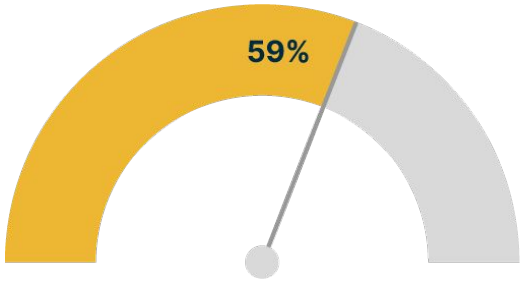
Threat exposure management scoring legend

https://t.me/learningnets

Overall Performance

This report finds that organizations do not consistently prevent or detect cyber attacks. The reason is likely less about the quality or capability of the security controls they have in place, but more about how effectively these organizations are utilizing these tools.

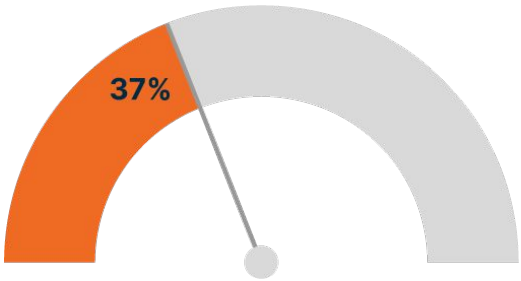
We found that security organizations only prevent just over half of attacks (59%) using their existing security controls, such as IPS, NGFW, or WAF solutions.



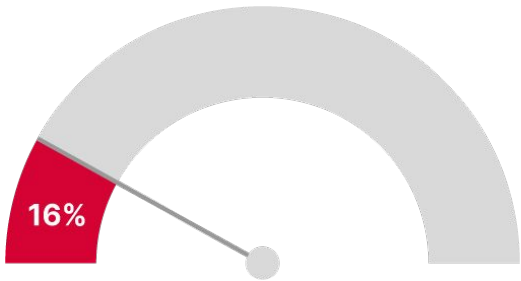
Only 59% of attacks were prevented

Security organizations fared even worse when it came to detecting successful attacks. To start, they are failing to effectively log and identify attacks.

A distressingly low percentage of attacks (37%) are successfully logged after infiltrating environments. Similarly, less than 1 in 6 (16%) of attacks trigger alerts, hampering security teams' ability to identify and respond promptly to potential threats.



Only 37% of attacks were logged



Only 16% of attacks triggered alerts

Based on our experience running breach and attack simulations, many organizations will be surprised by these results due to a false sense of security. They do not realize the degree to which their existing controls are insufficient for detecting attacks, especially sophisticated ones. To overcome these gaps, organizations may benefit from changing their perspective and taking an "assume breach" approach to cybersecurity.

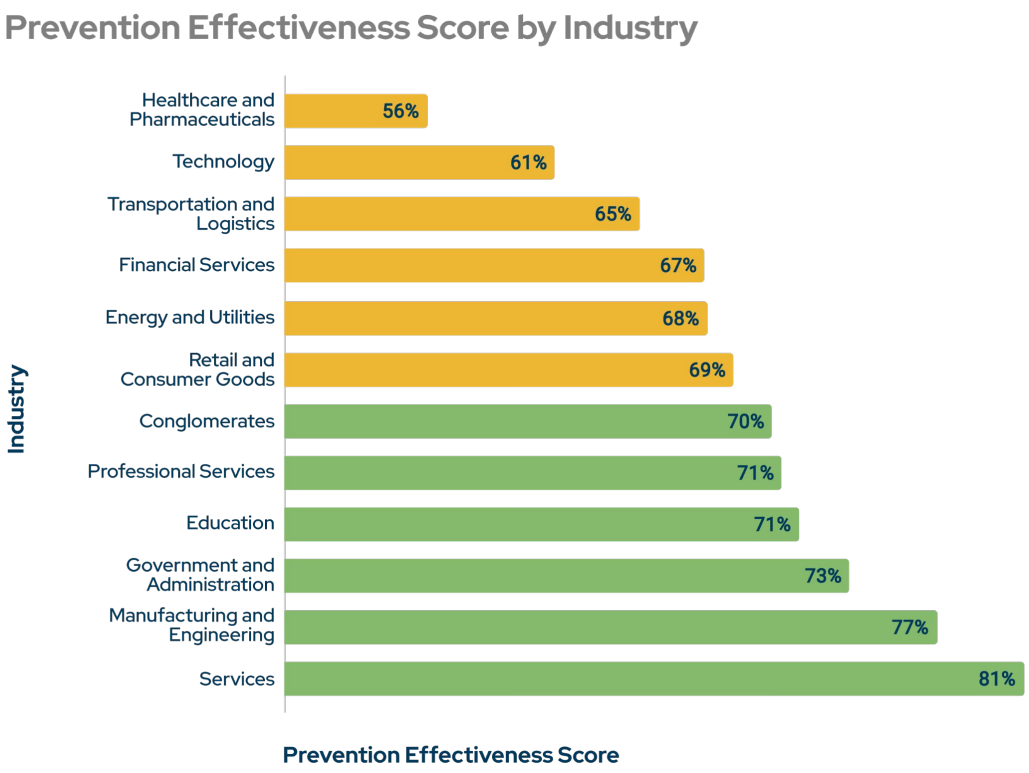
https://t.me/learningnets

Performance by Industry

Our findings suggest that organizations' cyberattack prevention and detection readiness vary considerably both between industries and within industries.

Prevention Effectiveness

There is a broad range in performance when it comes to attack prevention. It is striking that several of the least effective industries are critically sensitive industries, including healthcare, technology, transportation, financial services, and energy and utilities. More than 3 out of 10 attacks successfully bypassed these industries' security controls. Given how fundamental these industries are to society's well being, the sensitivity of data in these sectors and the attractiveness of these organizations to cybercriminals, there is an urgent need for them to enhance their efforts and their investments in cybersecurity defenses.

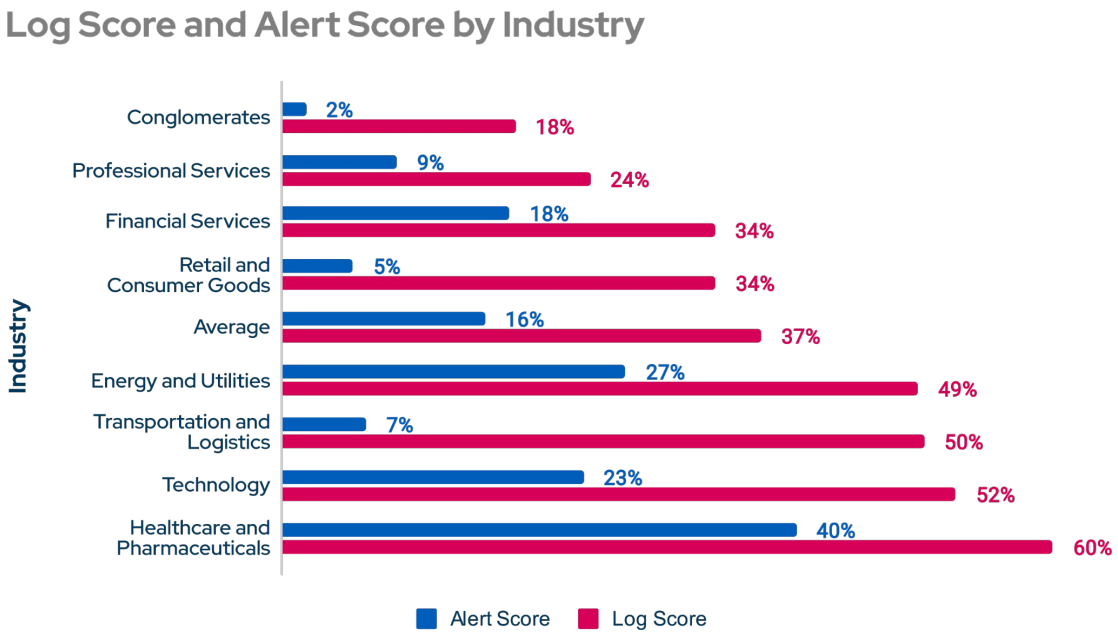


On the other hand, it's reassuring to note that some sectors fare better: the government and administration sector has a superior prevention effectiveness score of 73%, while manufacturing and engineering and the services sector have leading prevention effectiveness scores of 77% and 81% respectively. These industries may have practices other sectors can learn from.

https://t.me/learningnets

Detection Effectiveness

Detection effectiveness is measured in terms of organizations' ability to log and alert on attacks. As previously noted, the average security organization only logs 37% of attacks and alerts on 16% of attacks. However, there are significant variances between industries.



The healthcare and pharmaceuticals industry leads in detection effectiveness, with both the highest log and alert scores at 60% and 40% respectively. This superior performance could be due to the heightened regulatory oversight and sensitive nature of data in this industry during the pandemic, which likely necessitated stronger cybersecurity measures. The technology, and energy and utilities industries also show better than average results.

At the other end of the spectrum, conglomerates, and organizations in the professional services industry have the least success logging attacks. They also have low alert scores, along with organizations in the transportation and logistics, professional services and retail and consumer goods industries.

In addition to variances between industries, organizations within an industry also appear to be making a trade-off between their prevention and detection capabilities. Industries that are strong at detection are weak at prevention, and vice versa. For example, the industries with the top 6 detection scores also have the 6 lowest prevention scores.

https://t.me/learningnets

Organizations also appear to be making another trade-off between logging and alerting. Across all industries, there is a significant gap between log scores and alert scores. This discrepancy is concerning. Fewer than half of the number of attacks being logged and recorded by security systems are being alerted and flagged for action. This gap gives adversaries an opportunity to exploit these non-alerted security breaches, potentially leading to significant data loss or business disruption.

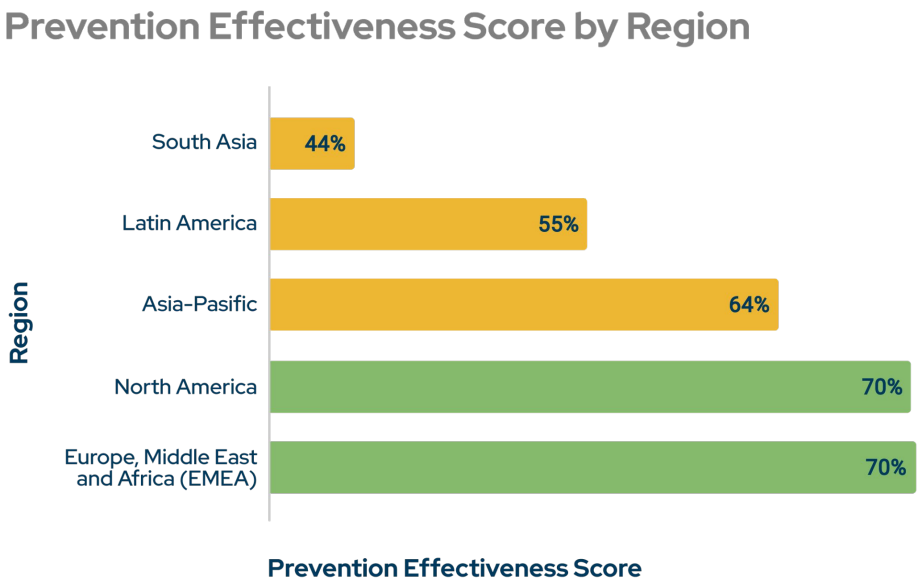
To address this gap, organizations need to enhance their alert mechanisms. Options for doing so could include: improving automated alerting systems, incorporating more sophisticated threat detection algorithms, or even retraining staff for more effective manual responses. The objective should be to ensure that every logged attack generates an appropriate alert and subsequent action, minimizing the opportunities that cybercriminals have to exploit unnoticed vulnerabilities.

https://t.me/learningnets

Performance by Region

Prevention Effectiveness

When it comes to regional disparities, there is a North-South divide in cybersecurity preparedness. The disparity may be rooted in various factors, like a region's economic development status, level of digital maturity, access to skilled cybersecurity professionals, and the degree to which governments focus on cybersecurity regulations.



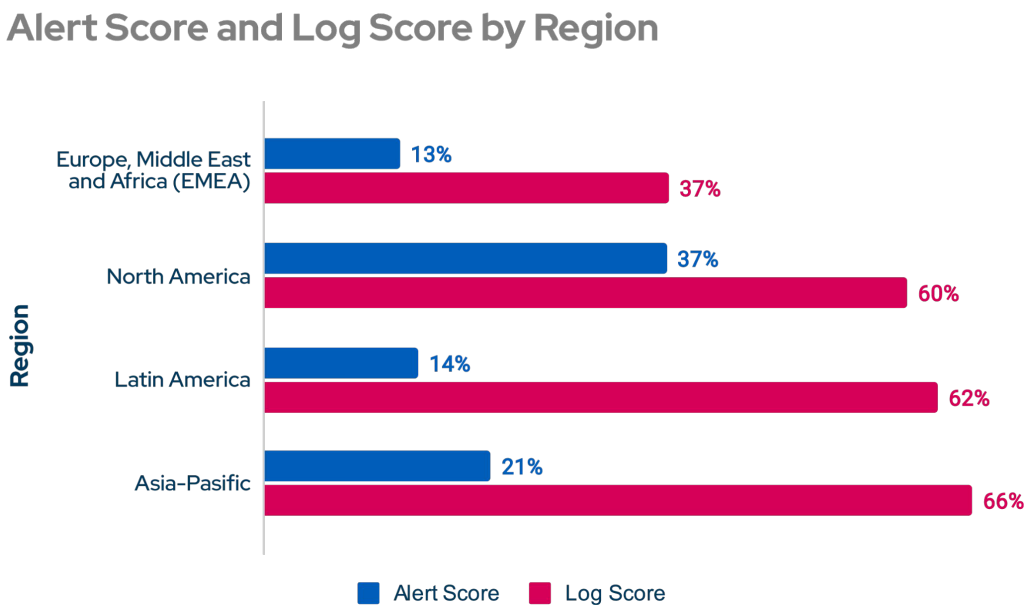
In general, organizations in South Asia, Latin America and Asia-Pacific regions exhibit more limited abilities to prevent attacks, with scores of 44%, 55% and 64%, respectively. As regions are experiencing strong digital growth, a robust expansion in cybersecurity measures could potentially prevent cyber threats from disrupting their digital booms.

In contrast, North America and Europe, Middle East and Africa (EMEA), with identical scores of 70%, exhibit a more robust level of threat protection. Organizations in these regions likely have the security measures in place to provide a reasonable level of protection against various threats. However, their scores also suggest the need for continued investment to enhance protections and stay ahead of the evolving threat landscape.

https://t.me/learningnets

Detection Effectiveness

The inverse correlation between prevent and detection we saw for industries breaks down somewhat when viewed by region. Latin America and Asia-Pacific face the same struggles with attack alerting that they do with prevention effectiveness. In contrast, they have the highest logging scores of all regions.



Organizations in EMEA face a clearer trade-off. They have commendable average prevention scores of 70%, but fall short in detection effectiveness, showing the lowest log and alert scores, 37% and 13% respectively. This discrepancy suggests that organizations in EMEA are investing heavily in preventive technologies and strategies but not allocating sufficient resources towards detection controls. This can leave them vulnerable to attacks that evade preventive measures, thereby undermining their overall security posture.

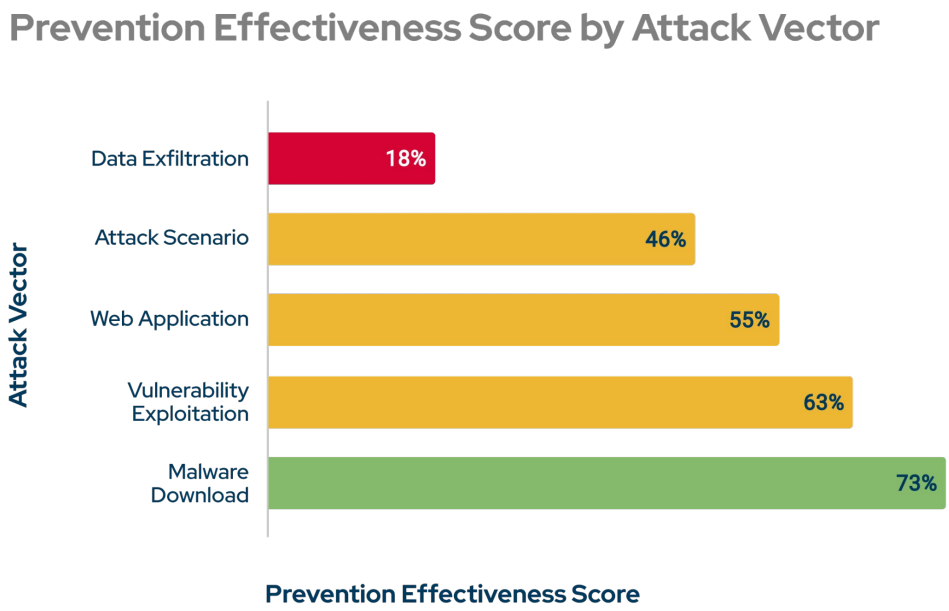
When it comes to attack detection, North America again ranks at the top, with high scores for attack logging and alerting. Combined with high prevention effectiveness, North America organizations demonstrate a relatively comprehensive and mature approach to cybersecurity. The lower detection scores, in particular a logging score of 37% suggests that there is still significant room for these organizations in this region to optimize their security controls.

Regardless of the region, alert scores are much lower than logging scores. The alert scores for all regions fall on the lower end of the scale, ranging from 13% to 37%. This suggests that detection security controls, such as SIEM systems, are not optimized to generate alerts for a significant number of attacks. This might be due to an overwhelming number of false positives, improper tuning of the alerting mechanisms, or an inability to effectively correlate and prioritize security events.

https://t.me/learningnets

Performance by Attack Vector

Organizations' ability to prevent attacks varies depending on the type of cyber attack being used. For example, organizations demonstrate a high level of preparedness for malware download attacks.



On the other hand, security teams significantly lag in their ability to prevent data exfiltration in the face of attacks on their network. Their 18% effectiveness rate against data exfiltration is alarmingly low and suggests that their cybersecurity controls are largely ineffective at preventing the unauthorized export of sensitive data. Given the significant financial, legal and reputational implications of data breaches, the prevention of data exfiltration attacks requires urgent attention and resources.

When it comes to attack scenarios – complex, multi-stage attacks – our findings indicate a prevention effectiveness score of only 46%. These types of attacks are increasingly common. Over a third of malware samples exhibit 20 or more attacker tactics, techniques and procedures (TTPs) according to analysis compiled in **The Red Report 2023.**

Web application attacks are another type of attack that security teams should pay attention to since an overwhelming majority of modern businesses use web platforms as a core part of their business. Unfortunately, organizations' prevention effectiveness against web application attacks stands at a moderate 55%, which could expose them to significant risk, especially given the rise of such attacks in recent years.

Overall, these figures suggest that organizations' cybersecurity postures, while robust against some types of threats, have significant gaps.

https://t.me/learningnets

Performance by MITRE ATT&CK Tactic

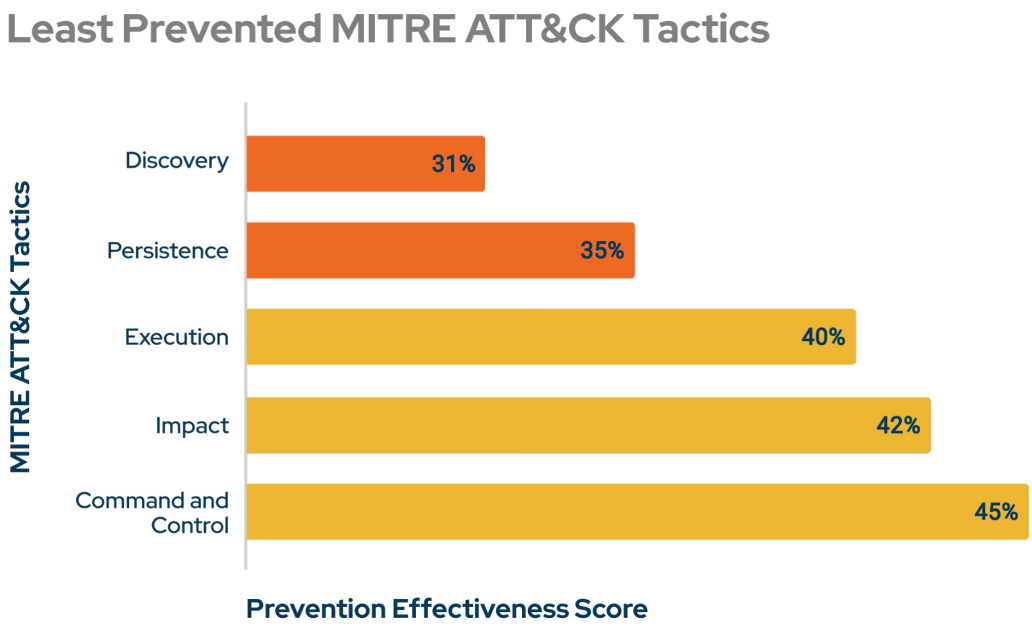
Many security organizations today use the MITRE ATT&CK framework to understand attack behavior and evaluate their own threat readiness. We analyzed organizations' ability to defend against the 14 attacker tactics in the **MITRE ATT&CK enterprise matrix.**

Organizations were least able to defend against the discovery tactic, preventing this tactic only 31% of the time. As a result, adversaries may be successful in gathering information about organizations' networks and systems to further their attack. For example, once inside a network attackers can identify critical systems, understand configuration details and learn about the privileges of compromised credentials. Organizations with a weak performance in this area should undertake an urgent review of their security controls, given that successful discovery is usually a key step for attackers to perpetuate a successful breach.

Organizations also had inadequate or basic efficacy defending against persistence (35%), execution (40%), impact (42%) and command and control (45%) tactics. Organizations can improve their defense against persistence techniques by improving their detection capabilities and thereby disrupt long-term intrusions. To better defend against the execution tactic, organizations should strengthen security controls that prevent malicious software write, modify, or execute processes in their systems.

Organizations inability to defend themselves against the impact and command and control tactics means that organizations could be vulnerable to detrimental impacts of a cyber attack. Essentially, these weaknesses could allow cybercriminals to cause significant disruption, including but not limited to data destruction, encryption, and manipulation, system downtime, financial loss, and tarnished reputation. To mitigate against this threat, organizations should both improve their ability to prevent initial system intrusion as well as tighten controls that prevent an intruder from executing actions that could directly impact their business. Organizations need to preclude malicious actors from communicating with compromised systems to extract data, command malicious software, or control system functions.

https://t.me/learningnets



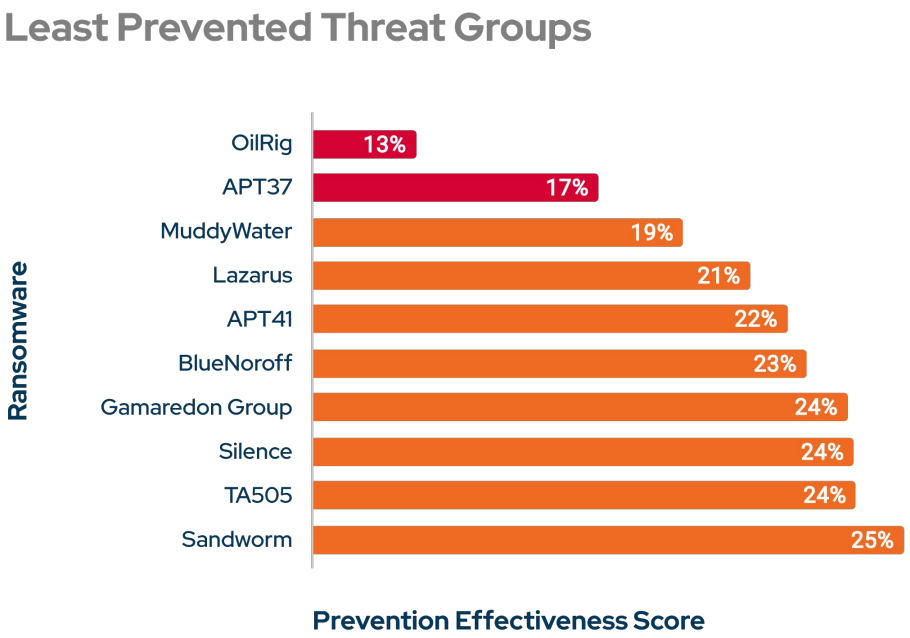
Overall, organizations' performance against attacker tactics as defined in the MITRE ATT&CK framework differs by tactic. This finding is similar to the varying performance we found organizations have when it comes to preventing different attack vectors. As they invest in one area, they appear to be trading-off investing in others, creating gaps in their security.

https://t.me/learningnets

Performance by Ransomware Group

In 2023, ransomware groups are using a diverse range of TTPs. Given this report's earlier finding that organizations' ability to prevent attacks varies depending on the type of attack being used, it is no surprise then that organizations' ability to defend against different ransomware groups also varies.

Cyber threat groups posing the most significant challenge tend to be state-linked and financially motivated. The majority of these groups use sophisticated TTPs including defense evasion techniques, vulnerability exploitation, spear-phishing, and living-off-the-land binaries (LOLBins) to bypass defensive measures. As these groups evolve and refine their TTPs, organizations must continually validate and strengthen their security controls.



In our analysis, we found that organizations are least successful (13%) at preventing attacks by OilRig (a.k.a. APT34), which has suspected links to the Iranian government. This group has made headlines for its high-tech cyber-espionage campaigns primarily targeting Middle Eastern and other entities linked to the finance, energy, telecommunications, and chemical industries.

Organizations don't do much better (17%) against APT37, also known as Reaper, a group backed by North Korea. APT37 primarily targets South Korean public and private entities, but has expanded the scope of its attacks to include Japan, Vietnam, and the Middle East. With a keen interest in industries like chemicals, electronics, manufacturing, aerospace, automotive, and healthcare, the group has undertaken campaigns involving espionage, data theft, and even sabotage.

https://t.me/learningnets

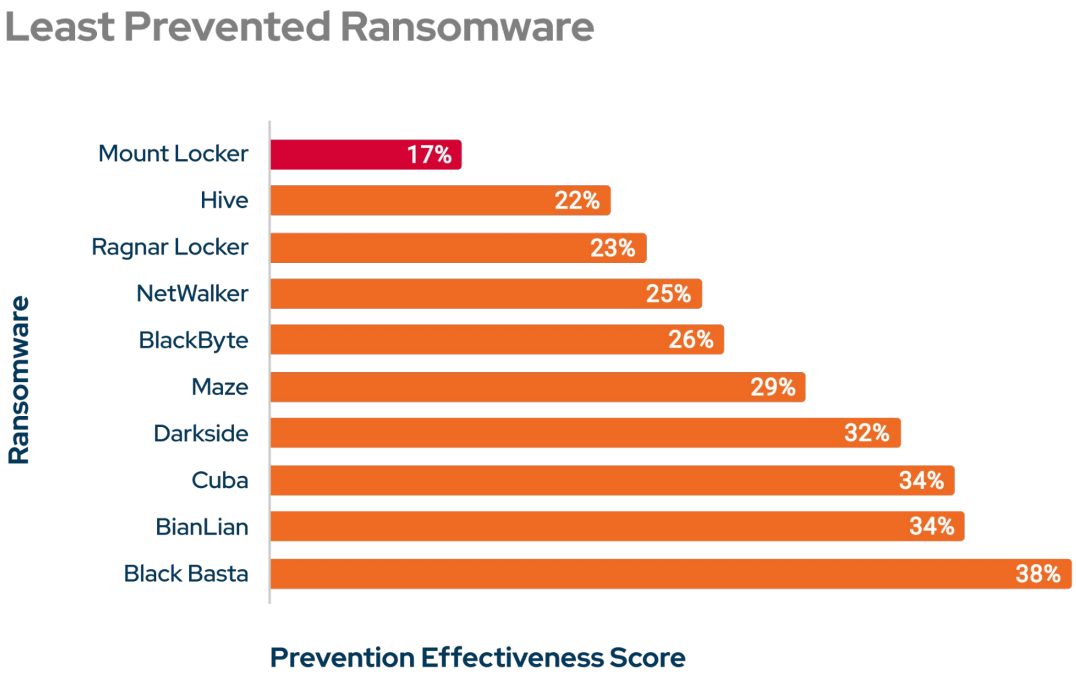
Organizations also struggle to prevent attacks (21%) against the Lazarus Group, another North Korea-backed group, known for the infamous Sony Pictures hack and WannaCry ransomware attack. Their victims span the finance, manufacturing, media, aerospace, and critical infrastructure industries in nations worldwide.

Other groups whose attacks organizations are least successful at preventing include MuddyWater (associated with Iran), APT41 (China-backed and known for both cyber-espionage and cybercrime operations), BlueNoroff (part of the Lazarus Group, focused on financial gain), the Russian-aligned Gamaredon group, the financially motivated TA505 group, Silence and Sandworm (a group linked to the Russian government and known for its destructive attacks against Ukrainian infrastructure).

https://t.me/learningnets

Spotlight on Ransomware Attacks

Ransomware poses an increasingly prevalent and severe threat to organizations across industries, and around the world. The disruptive impact, adaptability, and constant evolution of ransomware makes it a significant challenge for organizations to protect themselves. Even well-equipped organizations are not impervious, underlining the need for all organizations to take a proactive defensive posture.



In our analysis, we identified the 10 ransomware attacks that organizations were least able to prevent. All of the least prevented malware varieties include multiple malicious actions across the kill chain.

Mount Locker and Hive top the list. These malware varieties have proven to be extremely successful due to their rapid evolution and their advanced capabilities. Ragnar Locker, known for its sophisticated encryption techniques and the sizable ransom demands of its users, was also rarely prevented: less than one out of four times.

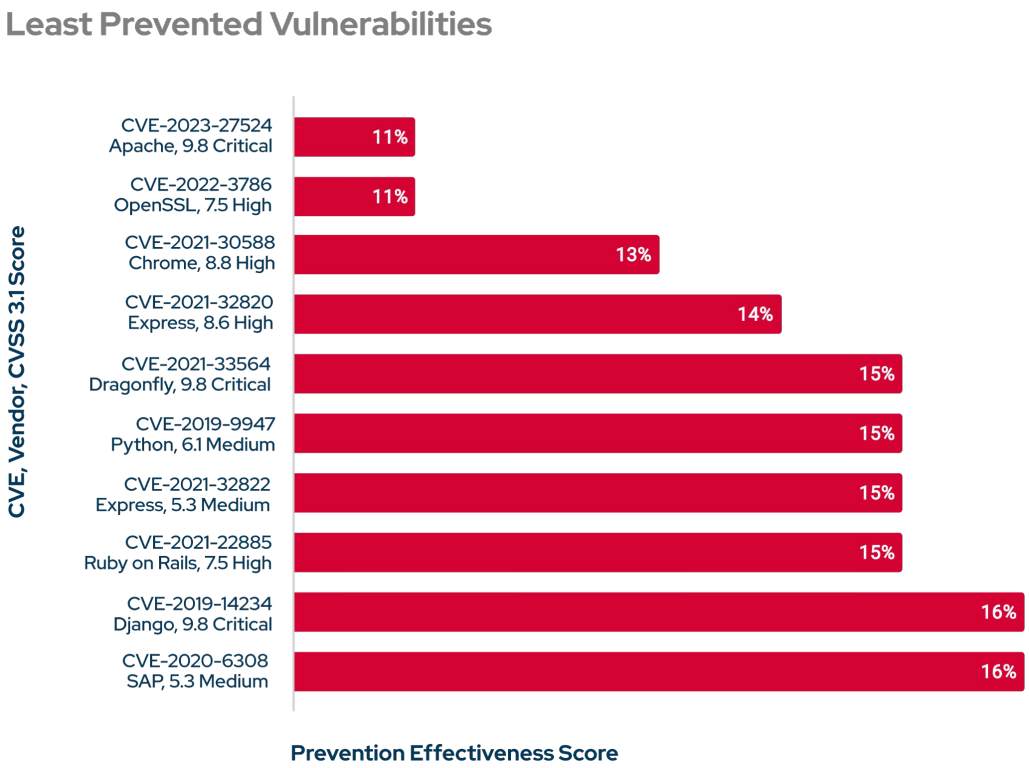
Other ransomware like the notorious NetWalker, Maze, and Darkside varieties, are infamous for their high-profile attacks. Despite the international attention they've drawn, organizations' relatively low prevention efficiency scores indicate that most of them remain exposed to these malware varieties. The same can be said for other malware strains like BlackByte, Cuba, BianLian, and Black Basta which, despite being less prominent in media headlines, pose equally severe threats.

Organizations should continuously improve their cyber resilience in the face of these highly adaptable and destructive threats. It's equally crucial for them to stay up to date in the face of the evolving ransomware landscape.

https://t.me/learningnets

Spotlight on Vulnerabilities

Software vulnerabilities, often referred to as common vulnerabilities and exposures (CVEs), are frequently targeted by attackers. And for good reason. For example, we identified the ten least prevented vulnerability exploits as part of the analysis of attack simulations done for this report. Organizations are only able to prevent them 11-16% of the time. Moreover, organizations are clearly not very effective at prioritizing vulnerability patching. Many of these vulnerabilities are either high severity or remain exposed despite having been known for years.



Several of the vulnerabilities in this list have drawn substantial media attention due to their high severity and widespread impact, including CVE-2021-30588 (affecting Chrome's JavaScript Engine), CVE-2021-33564 (affecting Linux distributions), and CVE-2021-22885 (impacting Ruby on Rails). Their continued exploitability underscores the ongoing need for vulnerability managers to prioritize patching them.

The presence of CVE-2019-9947 and CVE-2019-14234, both now 4 years old, highlights the fact that vulnerabilities can pose long-term security risks. Timely identification and remediation of vulnerabilities is essential, even in older systems.

Another finding is that these vulnerabilities affect a broad array of systems – from web browsers to operating systems. Organizations' vulnerability management programs should span their entire IT ecosystem, but they are clearly having to make trade-offs about what to protect. With that in mind, organizations may need to go beyond vulnerability management to reduce their threat exposure.

https://t.me/learningnets

The Need for Threat Exposure Management

The findings in this report underscore that many organizations continue to struggle to prevent and detect cyber attacks. Their struggle results from having to make four impossible trade-offs. Fortunately, their performance could be improved by taking a different approach.

Implementing a continuous threat exposure management (CTEM) program is one approach to cybersecurity that empowers organizations to effectively prioritize potential risks and corresponding remediation efforts.

As discussed at the outset of the report, organizations with effective CTEM programs use attack simulations to identify and mitigate real-world threats to their networks and systems. Simulations allow them to test their security posture and identify vulnerabilities before they are exploited by real attackers.

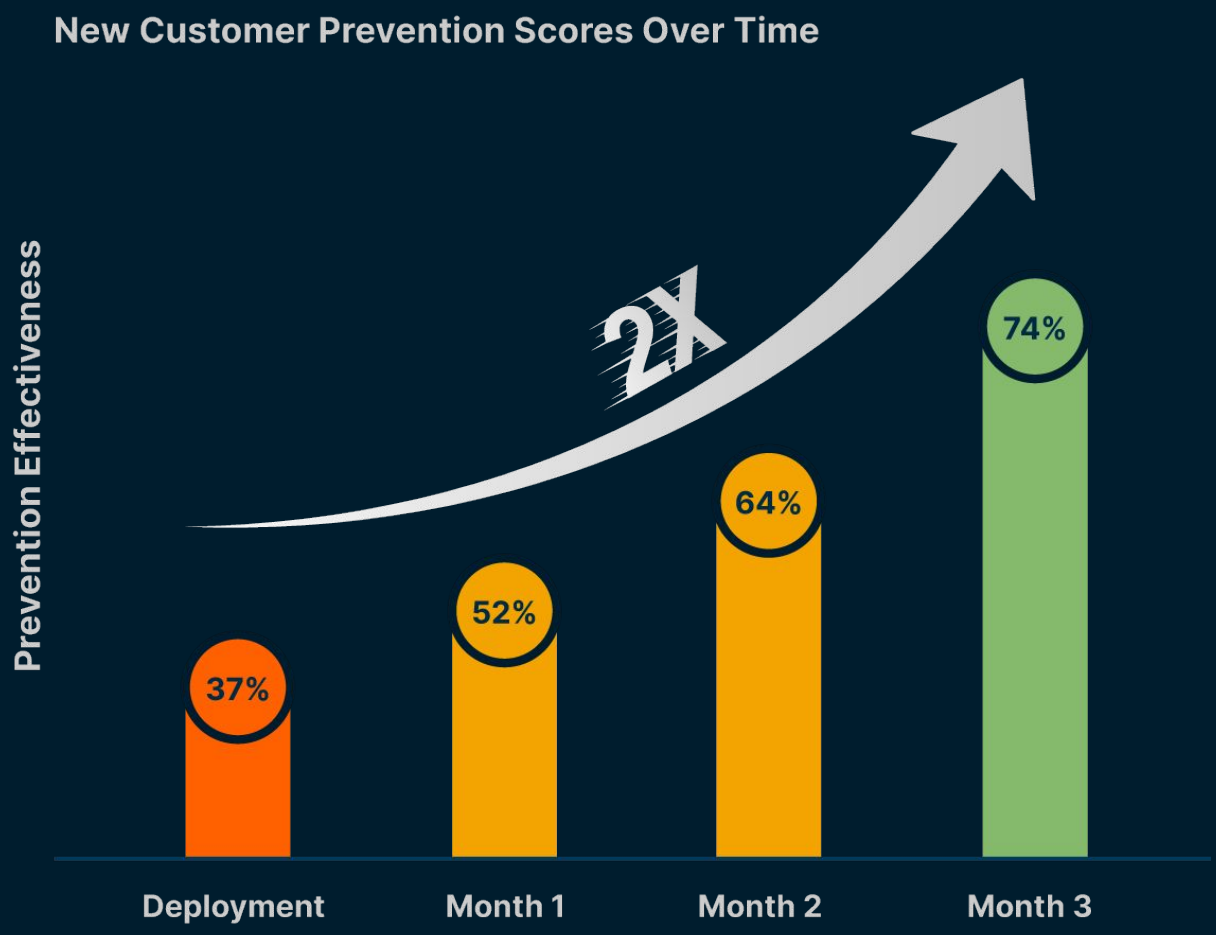
Moreover, attack simulations can allow organizations to better balance attack prevention and detection, and logging and alerting. By simultaneously evaluating the ability of their security controls to prevent attacks, log potential threats, and generate appropriate alerts, organizations can identify the gaps in their cyber defense posture that matter the most. Organizations can then allocate resources efficiently and effectively to address the most critical areas of concern, rather than making trade-offs between them.

By proactively validating their security controls, organizations continually improve their defenses and are empowered to stay one step ahead of their adversaries. They can take a data-driven approach to identify shortcomings in security controls and strengthen their overall cybersecurity posture before issues become a problem.

As a result, they should also observe a substantial decrease in cyber risk, improved threat detection abilities, and a shorter mean time to respond (MTTR).

https://t.me/learningnets

Picus Security Customers Prevent Twice As Many Attacks



Picus Security provides a CTEM solution, powered by our pioneering breach and attack simulations, to help organizations of all sizes to continuously validate and enhance their cyber resilience. Security teams can evaluate the effectiveness of their security controls, discover at-risk assets and identify high-risk attack paths that attackers could use to access critical systems and users.

On average, our customers prevent twice as many attacks, within just three months (see chart above). With Picus, security leaders can quickly mature their security posture and move beyond basic vulnerability management. Instead of spending their days making impossible trade-offs that may leave gaps in their defenses, they can consistently and successfully defend against sophisticated multi-pronged attacks.

https://t.me/learningnets

About PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Complete Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, our people and technology empower customers worldwide to be threat-centric and proactive.

For more information, visit **www.picussecurity.com**

https://t.me/learningnets

THE BLUE REPORT 2023

picussecurity

www.picussecurity.com

PICUS

© 2023 Picus Security. All Rights Reserved.

Both MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.

https://t.me/learningnets