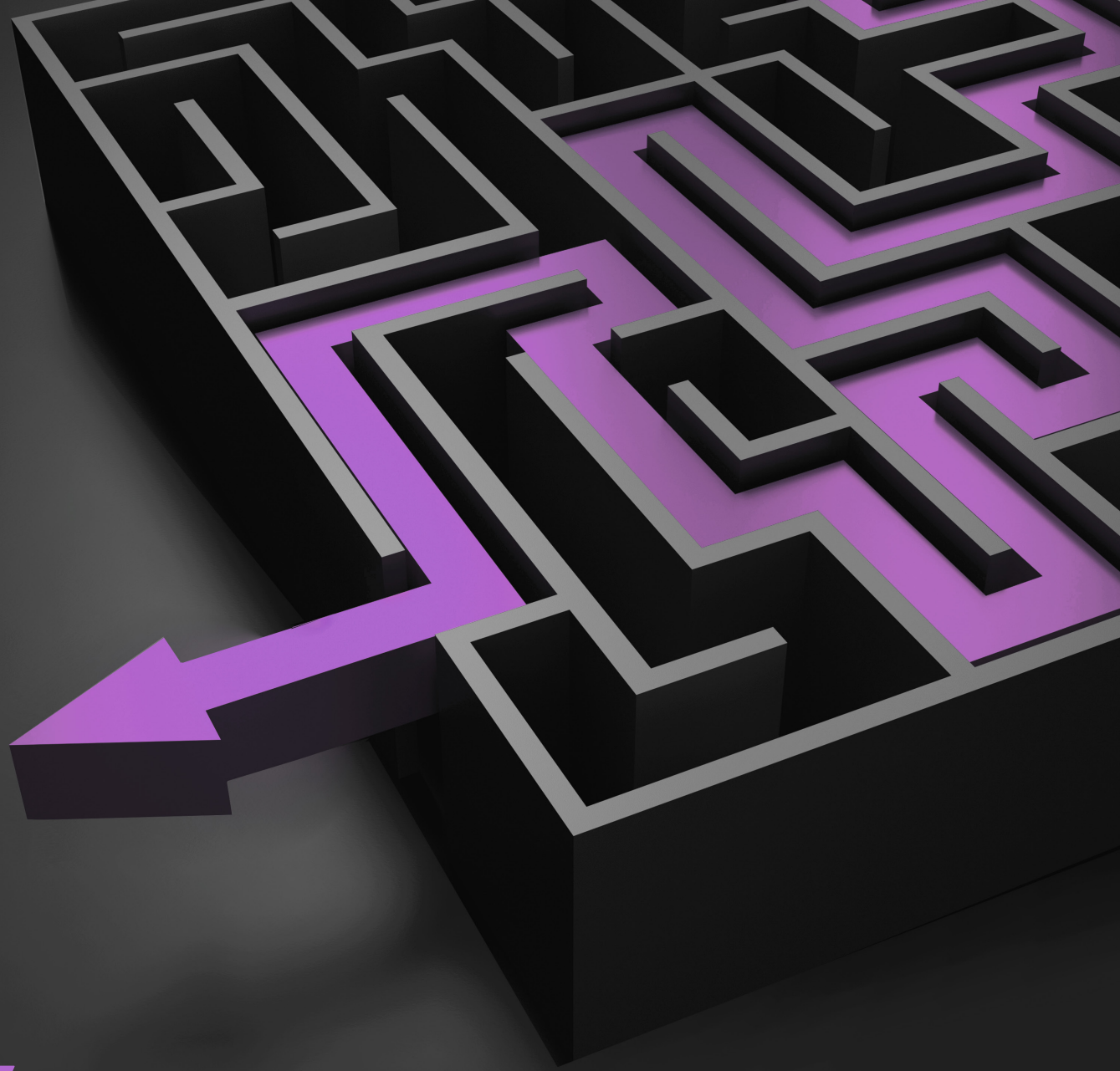


PENTERA

THE STATE OF PENTESTING 2024

SURVEY REPORT

Table of contents

Executive summary

Introduction 3

Methodology 3

Key findings 4

Survey report findings

Increasing complexity of cyber infrastructure 6

Threat actors are breaching the enterprise across all attack surfaces 7

Overwhelming alerts and noise 8

How are remediations prioritized? 9

The frequency gap between security testing and organizational change 10

What's driving modern pentesting practices? 11

Boards of directors are getting more involved in pentesting and security posture data 12

Barriers to pentesting 13

What is being pentested? 14

In-house security testing 15

What are enterprises spending on their security? 16

CISOs must do more with less: Budget outlook in 2024 17

A detailed look at the numbers behind this report 18

About Pentera 27

Introduction

With the introduction of the Continous Threat Exposure Management (CTEM) framework, organizations are placing more emphasis on identifying, validating, and mitigating risk within their digital environments. Pentera, the leader in Automated Security Validation, undertook our third annual State of Pentesting survey to understand the current state of security validation across organizations.

This report provides a snapshot of how security leaders in 2024 have adopted security validation strategies across their organizations. What are primary motivations and inhibitors to pentesting? How much are organizations investing in their security practices and their security validation? Is our security effective?

Methodology

To get more insight into the state of pentesting, we commissioned a survey of **450**, CISOs, CIOs, and IT security leaders across the Americas, EMEA, and APAC (150 respondents per region).

This year only organizations with pentesting practices in place were surveyed.

The average amount of time spent on the survey was 6 minutes and 48 seconds.

We screened for organizations with a minimum of **1,000** employees.

The survey was conducted by Global Surveyz, an independent survey company, and took place during December 2023. The respondents were recruited through a global B2B research panel, and invited via email to complete the survey.

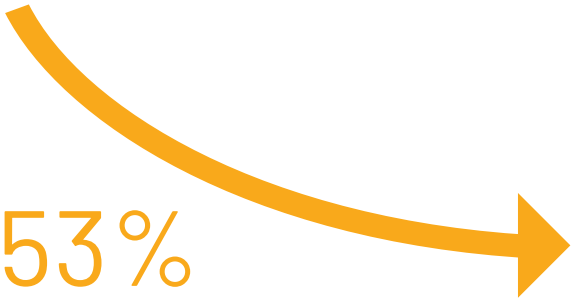
The answers to the majority of the non-numerical questions were randomized, to prevent order bias in the answers.

Executive summary

01

51% of enterprises reported a breach in the past 24 months

Threat actors are successfully breaching the entire attack surface (Cloud, Web-Facing, and On-Premises) across enterprise IT environments. CISOs are reporting unexpected downtime, data exposure, and financial damages with **only 7% reporting no significant damage as a result of a breach.**



53%

of enterprises report decreasing or stagnating IT Security budgets for 2024

02

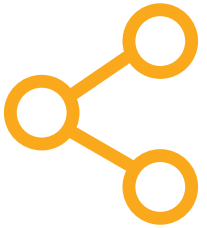
CISOs are being challenged to do more with less

53% of enterprises report decreasing or stagnating IT Security budgets for 2024. This is a major departure from the 2023 outlook where 92% of enterprises projected a rise to their IT Security budgets. When organizations cannot count on new resources, operational efficiency and getting more out of their existing security suite becomes paramount.

03

Boards are getting more involved in pentesting and security posture data

Over 50% of CISOs report that they share the results of pentest assessments with their leadership teams as well as their Boards of Directors (BoDs). With high-profile breaches in the news, management teams and BoDs are increasingly interested in understanding their organizational resilience, and the potential impact of cyberattacks to their operations and business.



Over

50%

of the respondents share the results of pentest assessments with BoDs

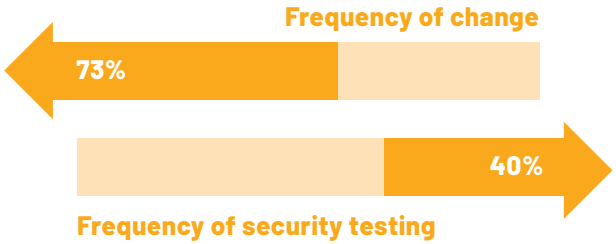
04

Manual pentesting is a major investment for intermittent security assessment

Globally enterprises are spending an average of $164,400 (12.9% of their total IT Security Budget) **on manual pentest assessments.** With 60% of enterprises pentesting twice a year at most, this is a large investment and a sizable portion of the budget for a security activity that provides a snap-shot assessment of the security posture.

$164K

Average annual pentesting budget



05

Security testing still outpaced by frequency of network change

73% of enterprises report changes to their IT environments at least quarterly, however only 40% report pentesting at the same frequency.
This underscores a serious frequency gap between the rate at which changes occur within the IT infrastructure and the rate of security validation testing, leaving organizations open to risk for extended periods of time.

06

Prioritization is KING for security teams

Over 60% of enterprises report a minimum of 500 security events for remediation per week. With a limit on how many remediations they can address, becoming "patch perfect" is an unfeasible, if not impossible, target for organizations. Security teams must concentrate their remediations on addressing the most critical security gaps before hackers have a chance to exploit them.

500

Security events for remediation per week

Increasing complexity of cyber infrastructure

As the complexity of IT environments continues to grow, organizations are integrating a greater number of cybersecurity solutions to manage their risk.

Our report found that on average, enterprises already have **53 security solutions** in use across their organization. **Only 12% of enterprises report utilizing less than 20 security solutions, while 21% report in excess of 76 solutions in their cyber stack.**

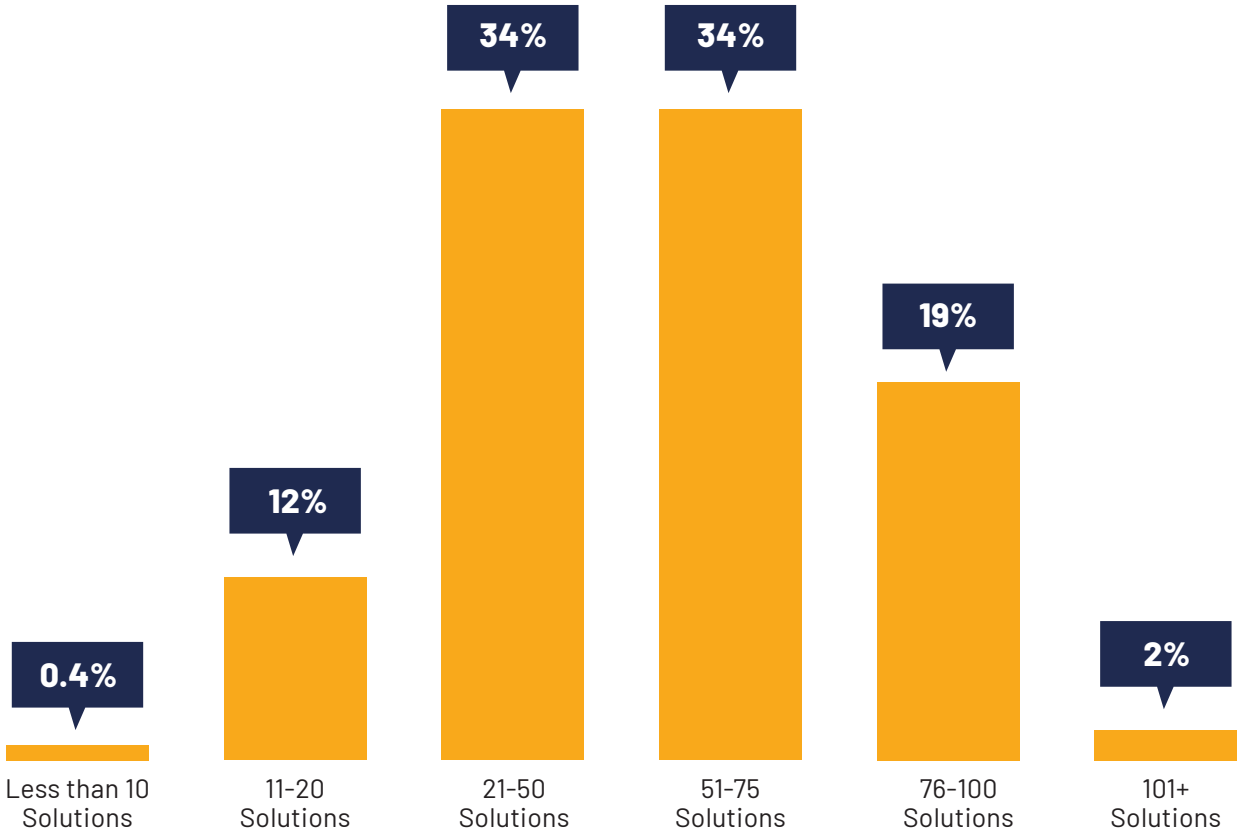
While there are benefits to layering security and creating a level of overlap within your security architecture, the noise created by such a large number of solutions can actually inhibit an organization's ability to detect and react to security threats.

Number of security solutions by organization size

52
1,000-4,999 Employees

53
5,000-9,999 Employees

58
10,000+ Employees

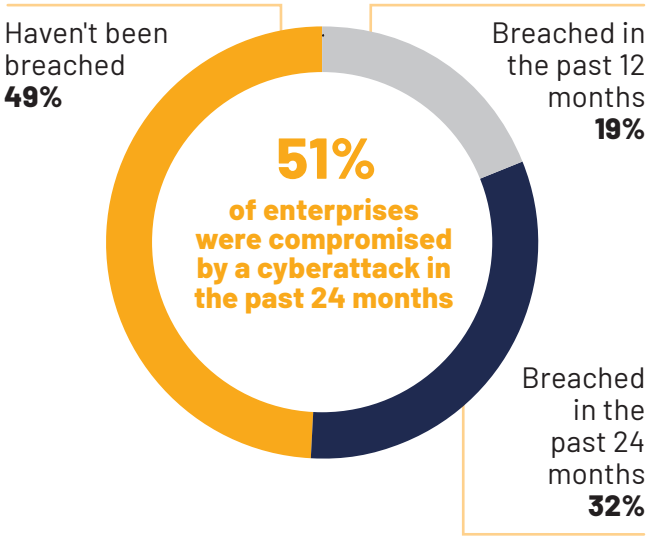


The number of security solutions does appear to be correlated with the size of the organization, however the difference is not massive with **the smallest enterprise group (1,000 - 4,999 employees) averaging 51 solutions and the largest (10,000+ employees) averaging 58.**

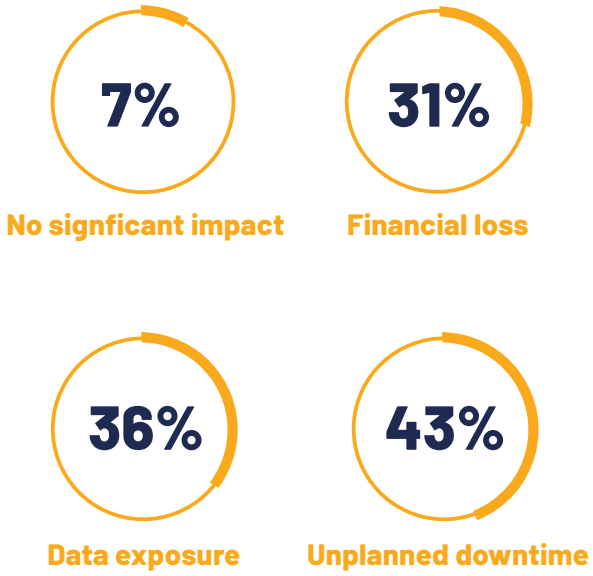
Threat actors are breaching the enterprise across all attack surfaces

Despite significant investment in security infrastructure, 51% of organizations surveyed reported that their organization was compromised by a cyberattack over the past 24 months.

93% of CISOs who reported a breach cited an impact on the confidentiality, integrity, and/or availability of their IT environment, while **only 7% reported no significant impact as a result of the breach.**



Impact of the breaches



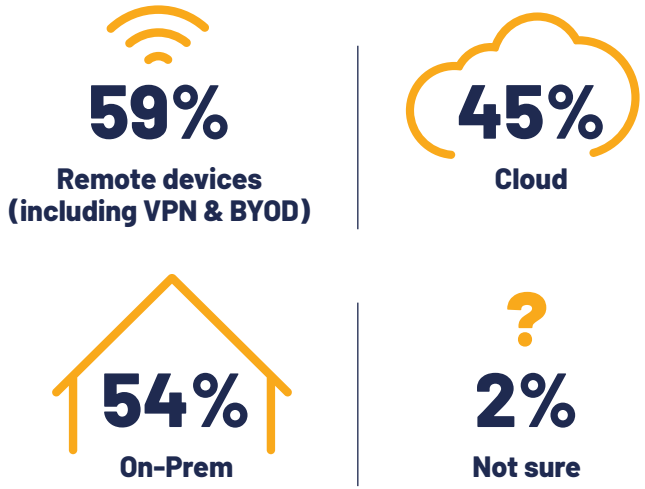
Close to a third of CISOs reported financial loss and a similar amount (just over 36%) reported data exposure. **However, the biggest risk was to business continuity with 43% reporting unplanned downtime as a result of the cyberattack**.

Threat actors do not appear to be limiting their activities to any specific attack vector or infrastructure environment. There was a fairly equal distribution across all environments.

Almost 60% of organizations that were compromised reported impact to their remote devices, while 54% cited their on-premise infrastructure as the target. Meanwhile, just under 50% reported a breach in their cloud infrastructure.

Crowdstrike's recent Global Threat Report 2024 reported a 75% increase in cloud intrusions YoY*. As more organizations continue their cloud migration journeys and move towards majority cloud or cloud-native deployments, we expect that this number will continue to rise.

Where were enterprises impacted?



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

*https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

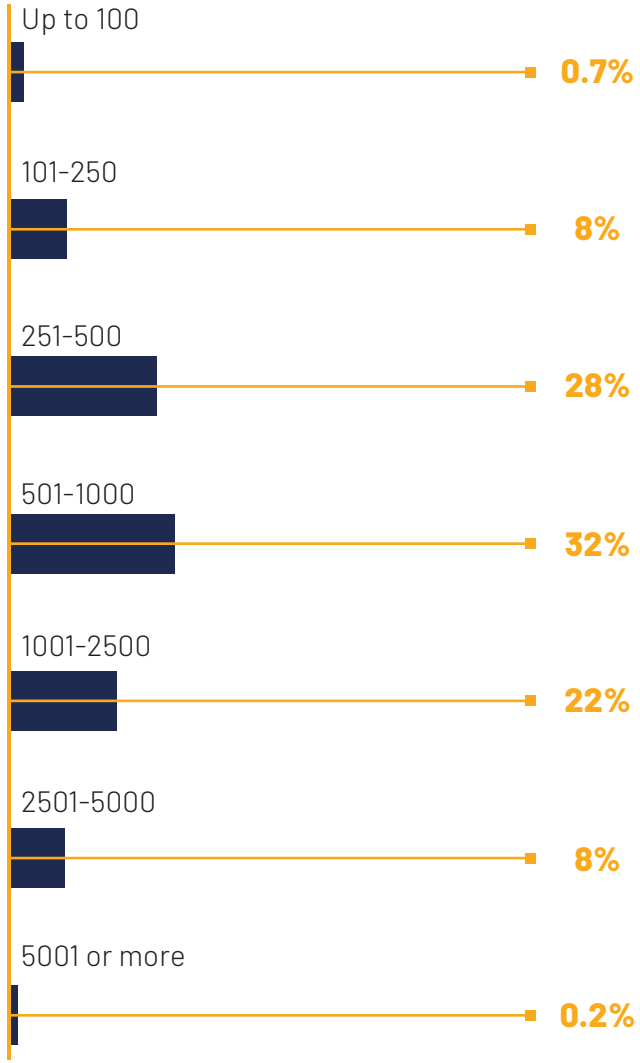
Overwhelming alerts and noise

In addition to remediation tasks, security professionals are grappling with an overwhelming number of demands across the enterprise. These can include (but are not limited to) activities such as preparation for compliance audits, incident response, policy management (GRC), Identity Management, and third party vendor management.

The median organization surveyed reported between 500-1,000 security events per week, **and over 60% of respondents reported a minimum of 500 security events per week.**

For the purpose of this survey an "event" was defined as an actionable security item - "a security matter that requires a remediation action, such as patching vulnerabilities, user password reset, or an endpoint quarantine."

Number of alerts for remediation per week



The large volume of alerts underscores the challenge that, while necessary, defense-in-depth security infrastructures also introduce a level of complexity and significant noise. This can make it difficult for security teams to effectively identify and prioritize the most dangerous security gaps that necessitate immediate remediation.

With a limit on time and resources for remediation actions the volume of events makes the prospect of becoming "patch perfect" difficult or completely unfeasible. **The focus for security teams becomes prioritization; addressing the exploitable security gaps hidden amongst the thousands of vulnerabilities that are only theoretically dangerous.**

How are remediations prioritized?

CISOs were asked about how they prioritize remediation within their organizations. They were requested to grade the relative priority they assign each methodology for assessing the urgency and prioritization of remediations.

The options included the potential business impact, the CVSS score, relying on vendor risk scoring, or simple chronology (addressing the events in the order they entered the system).

While providing the most contextual and relevant view of how cyber risk threatens overall business continuity and operations, **only 34% of respondents place business impact as a top priority to guide their remediation strategy**.

Our informed hypothesis for the greater reliance on other prioritization strategies is because they are more readily available and easier to do. For instance, CVSS score rankings are typically built into visibility metrics of most Vulnerability Management solutions while the down-stream impact on business operations of a vulnerability would be out of reach for the majority of organizations.

✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

The frequency gap between security testing and organizational change

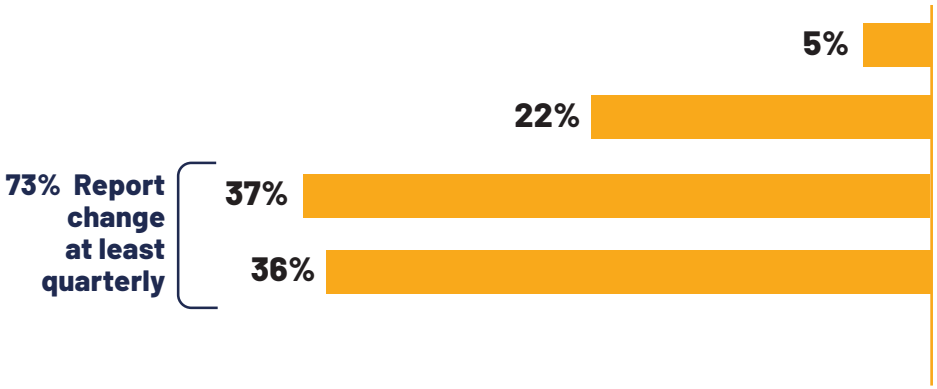
Changes to the IT infrastructure, in the form of new deployments, addition or subtraction of workstations, etc, all inevitably alter the organization's cyber posture. Each change introduces new potential gaps for threat actors to engage with and exploit.

Pentesting and Red-Teaming exercises, whether via third party services or in-house capabilities, are still the primary methods that organizations utilize to validate their security.

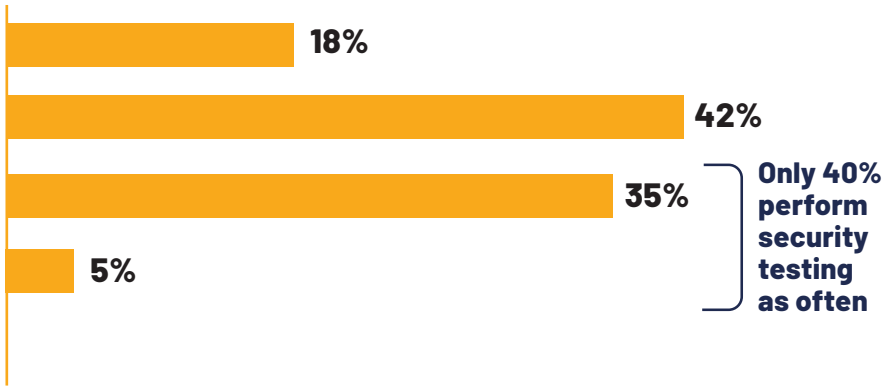
73% of enterprises report changes to their deployments at least quarterly, however only 40% report testing their security at the same frequency.

This underscores a serious frequency gap between the rate at which changes occur within the IT infrastructure and the rate of security validation testing, leaving organizations open to risk for extended periods.

How often are you adding/subtracting resources to/from your network?



How often does your organization conduct manual pentest assessments?



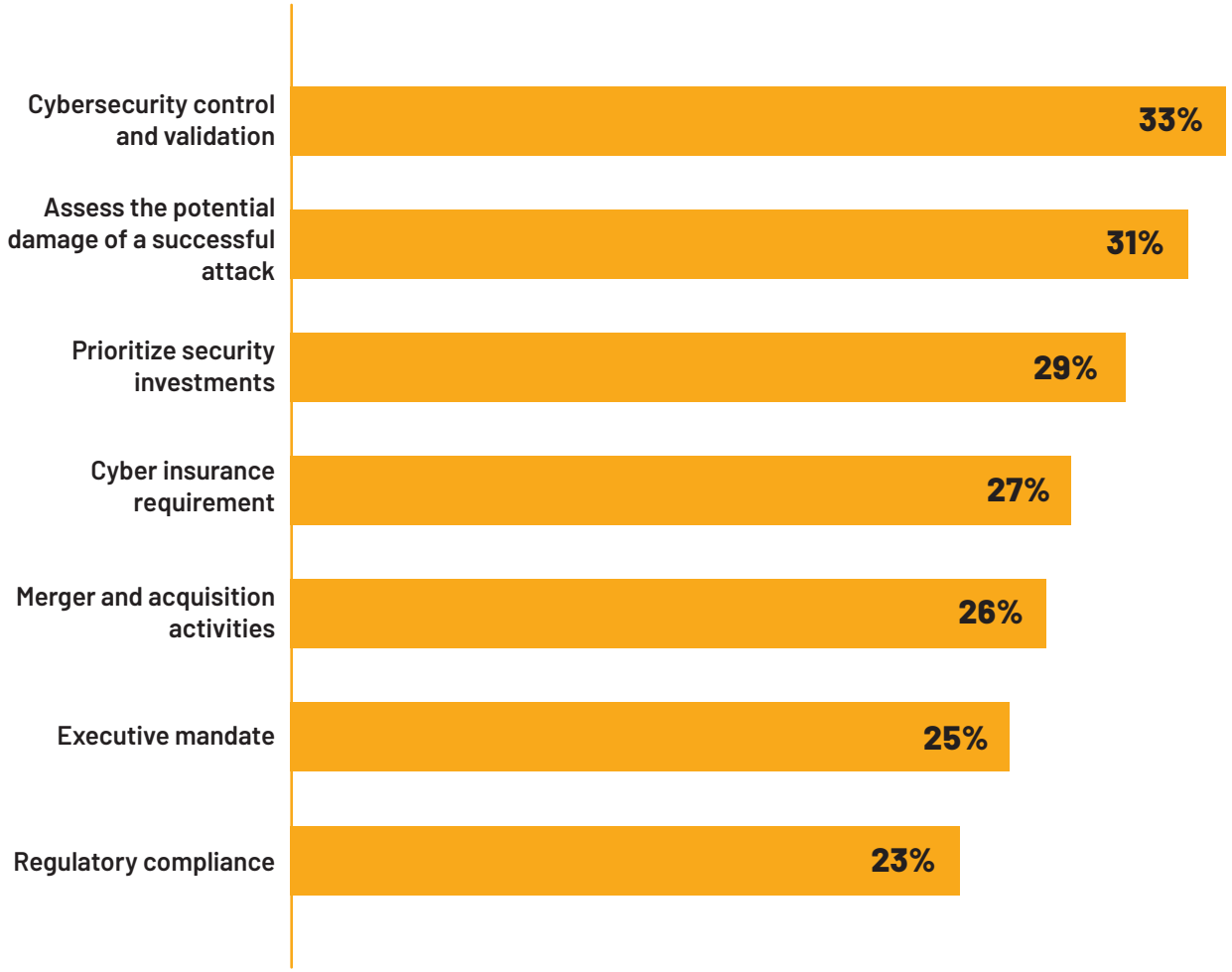
What's driving modern pentesting practices?

To discover what's driving the practice, security leaders were asked why they conduct pentesting in their organization.

Traditionally, pentesting originated as a compliance requirement within many industries. There's no question that these compliance requirements, whether imposed by regulatory bodies or cyber insurance providers, are still driving pentesting to some degree. However, the primary drivers for pentesting have evolved and today it is a security driven practice.

Cybersecurity control and validation and *Assess the potential damage of a successful attack* return as the top two motivations for pentesting. This indicates that many businesses today are no longer pentesting because they "have to" but because they "want to."

This year we introduced a new potential category and found that a substantial portion of CISOs and businesses are pentesting to facilitate potential M&A activities. Organizations are wary of third party risks, and are utilizing pentests to assess the potential risk profile when acquiring a company.



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

Boards of directors are getting more involved in pentesting and security posture data

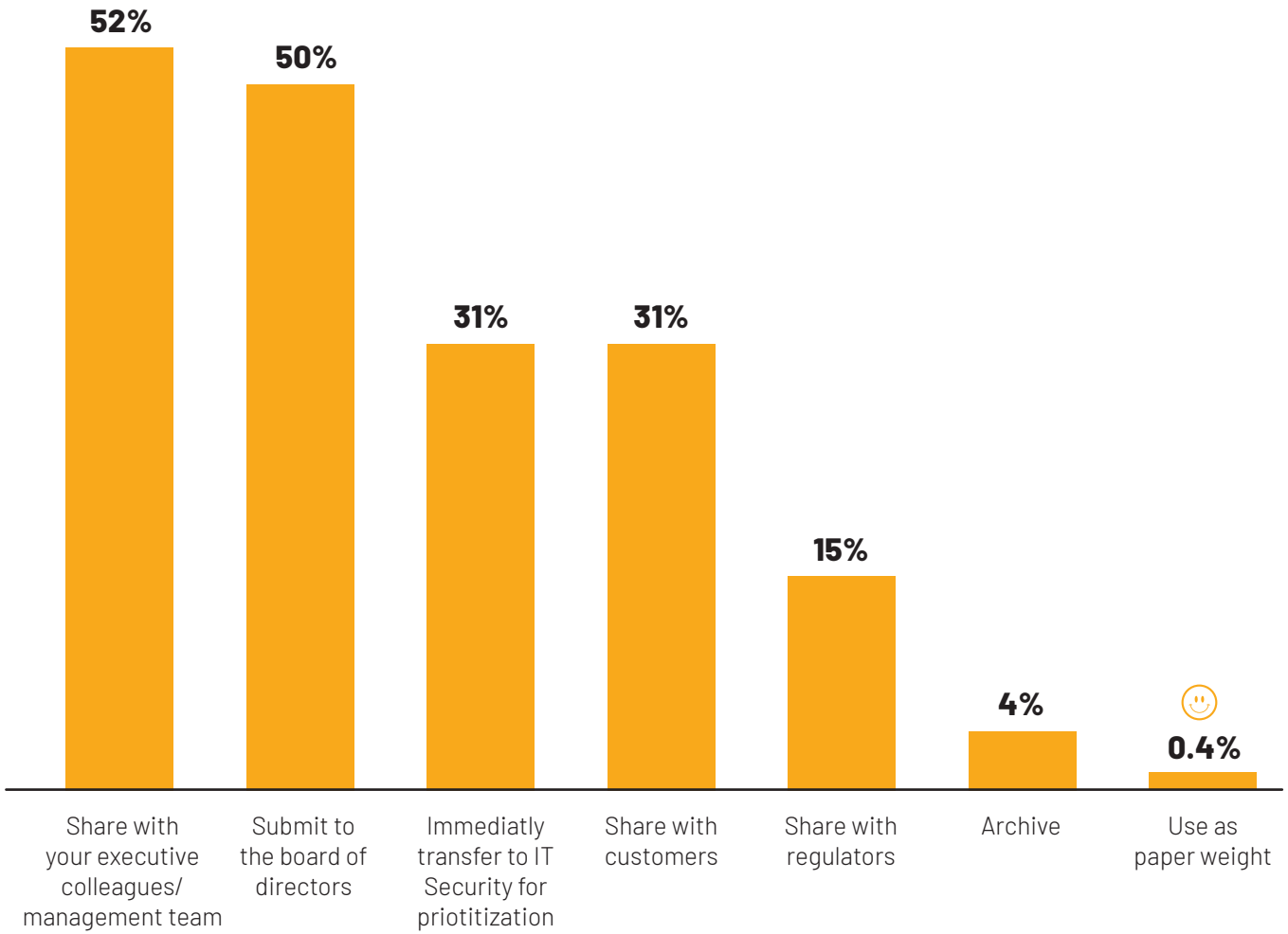
CISOs were surveyed about their use of pentesting reports, revealing that beyond security enhancement, these reports are increasingly utilized as a tool to communicate cybersecurity risk both internally and externally.

Over 50% of CISOs reported they share pentest results with the executive team and the Board of Directors (BoD). With the rise in high profile breaches, the BoD and management teams are becoming more cognizant of cybersecurity and the business risk it represents.

It also reflects the trend towards more expertise within BoDs. As cybersecurity expertise becomes more common among BoDs, it's likely that they will increasingly request reports such as pentesting results to benchmark security performance and posture over time.

The communication of pentesting results also expands beyond the organization. As the rise of third party and supply chain risks continues to grow, customers are becoming far more aware of their risk via their partners and vendors. **31% of CISOs report that they share the results of pentesting with their customers.**

What CISOs do with their pentesting report

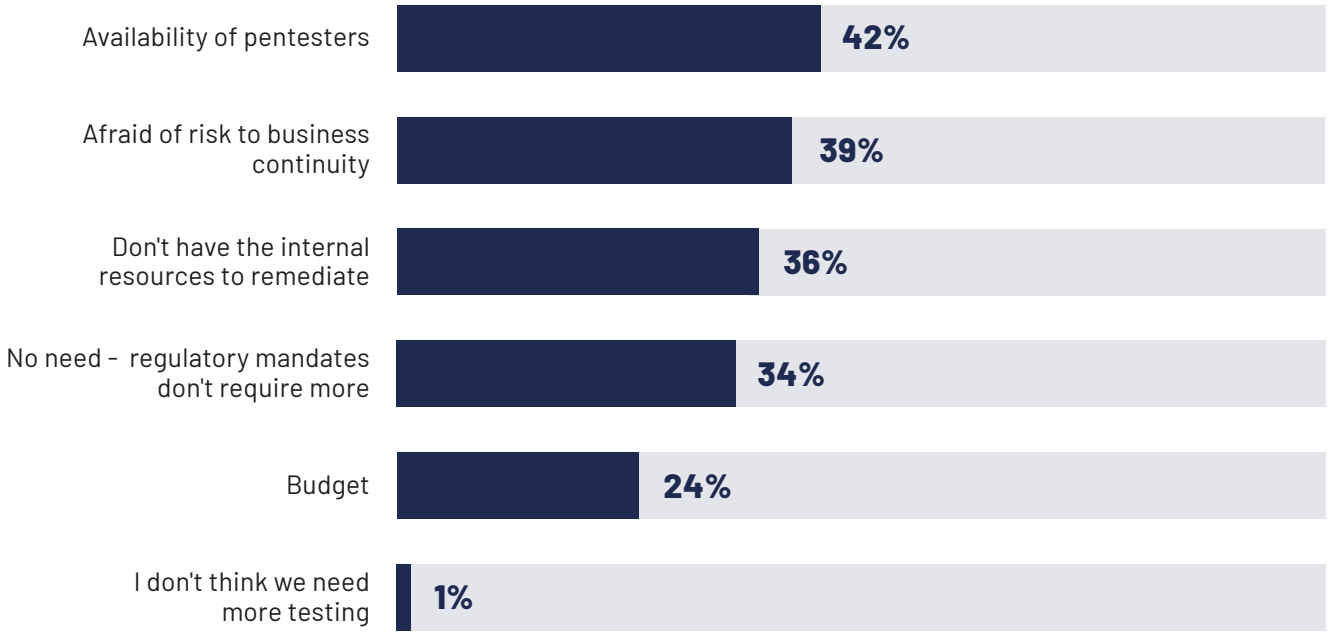


✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

Barriers to pentesting

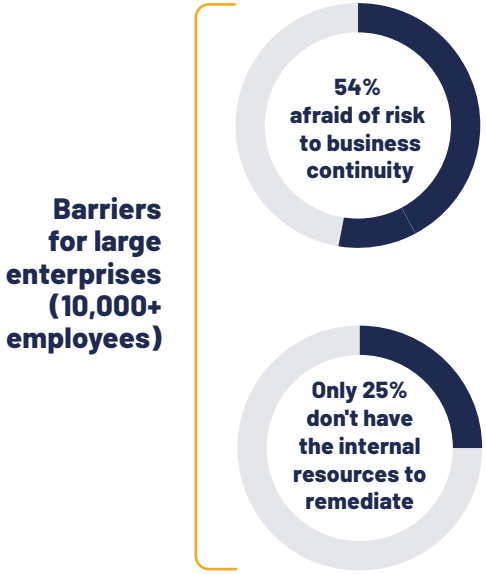
Similar to what was shown in the 2023 report, the top two barriers to pentesting remain the availability of pentesters, and the fear of risk to business continuity.

Above all, security teams are tasked with ensuring that IT environments are safe and that business operations are uninterrupted. Security leaders are cautious around pentesting as many have experienced network downtime due to pentesting in the past. CISOs want to work with the most experienced pentesters who provide the highest level of validation to their security, while also posing the least risk to operations.



✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

The largest change in comparison to the responses in 2023 is the rise in concern about internal remediations. **In 2023, only 21% reported a lack of internal resources for remediation as a barrier to pentesting, while this year the number has leapt to 36%.** This was rated a primary concern amongst smaller enterprises. Among CISOs at large enterprise organizations (10,000+ employees), only 25% cited a lack of internal remediation resources as a concern, while **54% listed risk to business continuity as a primary barrier.**



What is being pentested?

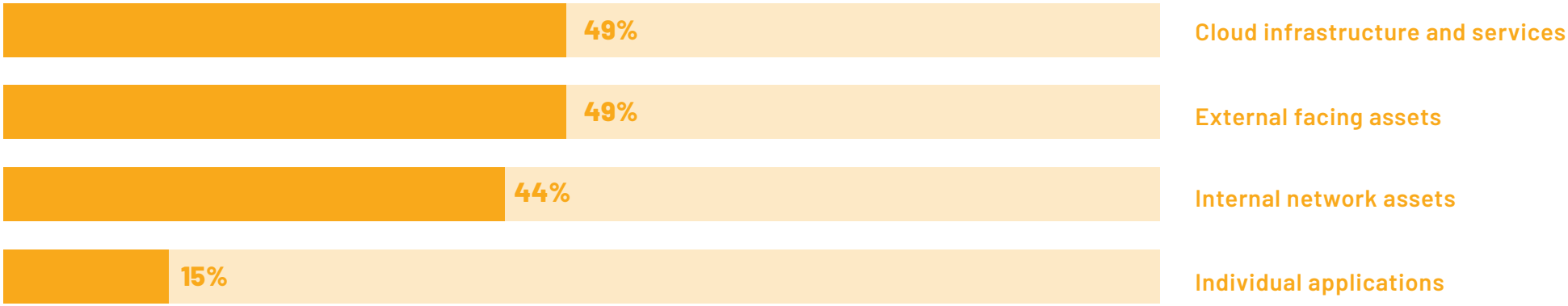
While pentesting the entire IT environment would be ideal, the associated costs and resource limitations of manual pentests, especially via third party service providers, make this unrealistic.

Instead, pentests are largely conducted on a biannual basis as a **sampling exercise** that spans across all aspects of the modern attack surface. With this limitation, CISOs are forced to choose the highest priority areas of their network, and typically test areas of the organization that they believe have the least visibility and most potential risk.

We see an even distribution across the three major attack surfaces: Cloud, External/Web-facing assets, and On-Prem.

An interesting note is that CISOs are not utilizing their pentests to validate the security of individual applications. Pentesting is an expensive endeavor, and CISOs are likely not able to justify an investment at this level to test an individual application.

Additionally, while most organizations are not primarily driven by compliance, it is still a major factor in pentesting practices. Many industries are compelled to test by existing regulations, and testing an individual application does not satisfy most compliance requirements. As such CISOs likely cannot justify a test that doesn't both satisfy their security as well as their compliance needs.



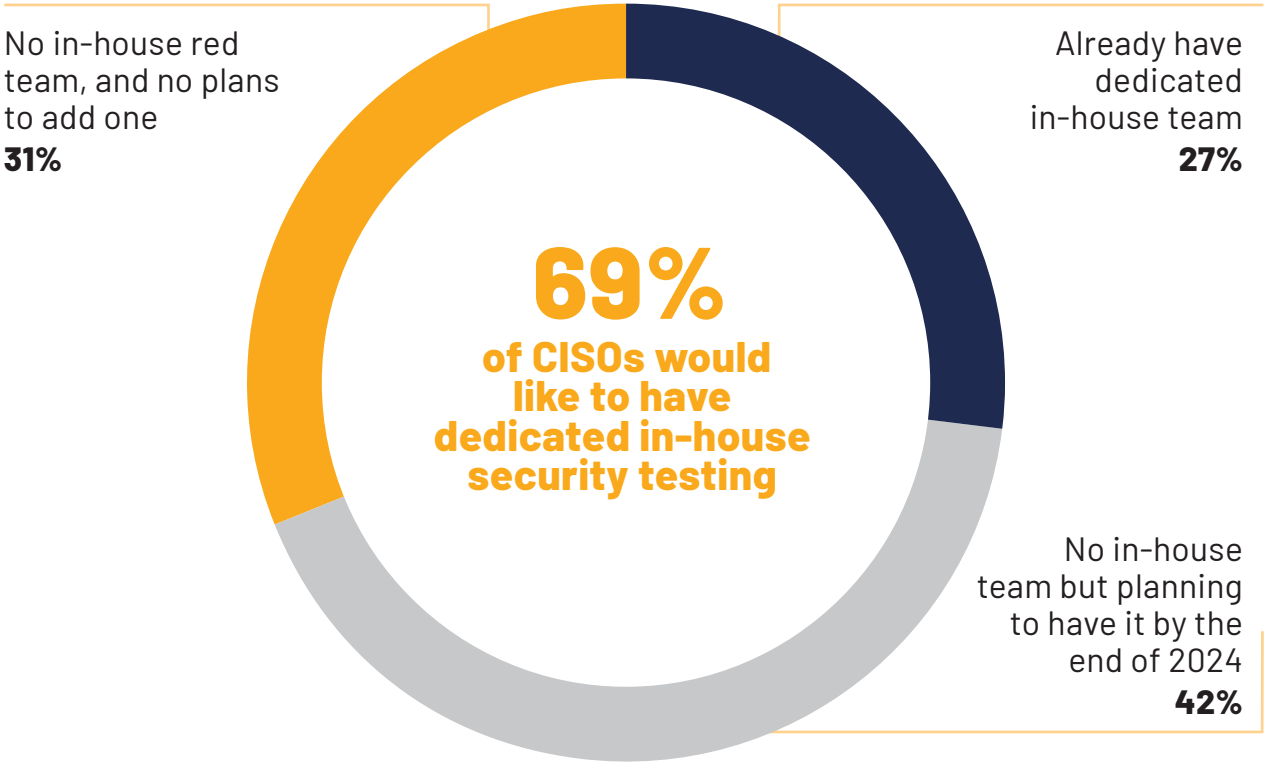
✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

In-house security testing

Last year when asked "Do you have an in-house Red Team or Pentesting team?" 67% of respondents reported that they did have an in-house team. While encouraging, that number appeared unexpectedly high, so this year the question was adjusted to add the word **dedicated**. Thus, *"Do you have a dedicated in-house Red Team or Pentesting team?"*

While small, this change was intended to understand the percentage of organizations that have committed teams for security validation. Of the organizations surveyed this year, **27% reported a dedicated pentesting or red-team in-house.**

Making sense of this difference is that around two thirds of enterprises have members of their security teams who pentest or perform red-teaming activities, however they are not wholly dedicated to these tasks. Therefore when limiting it to a **dedicated in-house** red-team or pentesters, that number drops to about a quarter of enterprises.



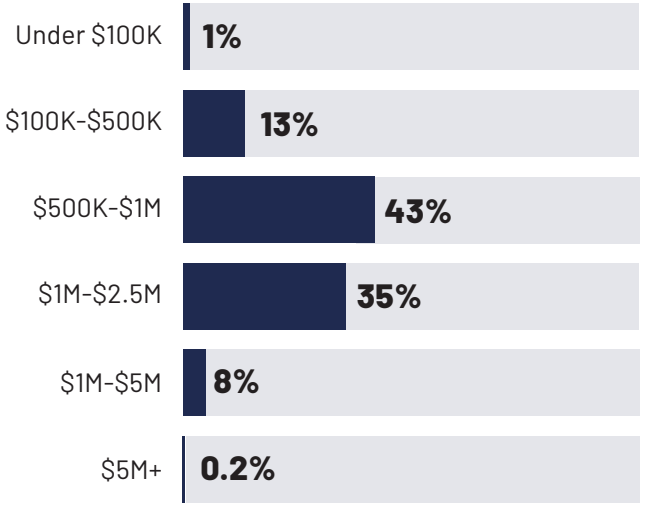
What are enterprises spending on their security?

When asked about how much they spend on their security in 2023, respondents reported an average budget of **$1.27M for IT Security.** Over 42% of enterprises reported a budget of over $1M while only 14% cited a budget under $500k.

The average spending on pentesting is $164,400, which represents 12.9% of the total average IT Security budget. Only 7% of enterprises reported spending less than $50k on their yearly pentesting budget.

$1.27M

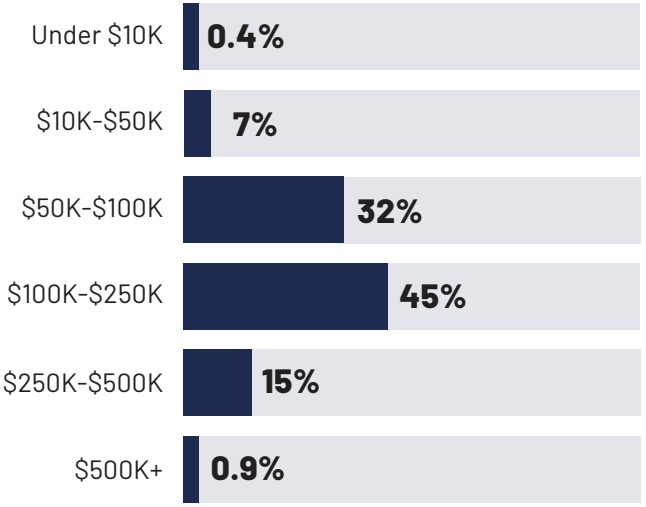
Average annual IT Security budget



Globally, pentesting averages 13% of the total IT Security budget

$164.4K

Average annual pentesting budget



CISOs must do more with less: Budget outlook in 2024

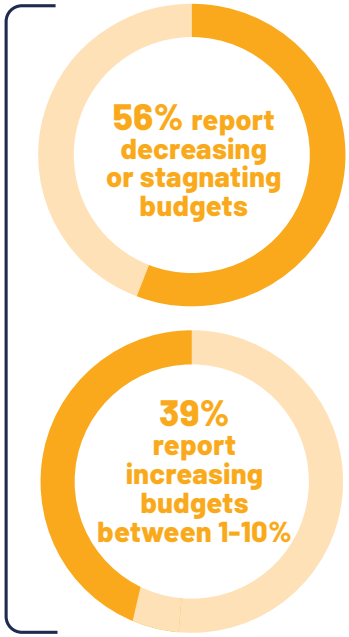
The budget landscape for IT Security and pentesting has undergone a significant transformation since last year's.

While the economic slowdown was already starting to impact organizations in late 2022, Pentera's State of Pentesting 2023 report showcased that it was not projected to impact cybersecurity budgets. 92% of respondents expected increases in their overall IT Security budgets, while 85% anticipated their pentesting budget to grow.

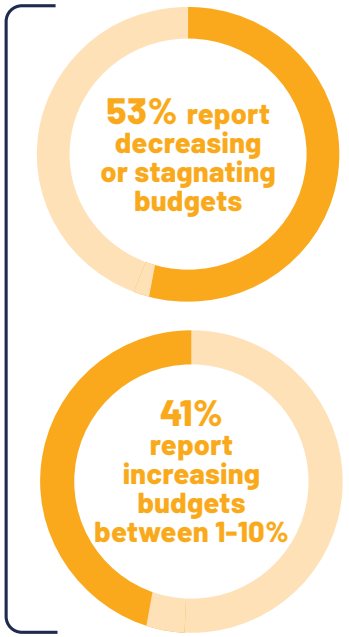
This year, CISOs are being challenged to do more with less. **53% of CISOs project their overall IT Security budgets will either stagnate or decrease in 2024, while 56% expect the same for their pentesting budgets.**

While that a significant number of organizations are still projecting increases to their overall IT security and their pentesting budgets, most increases are far more modest compared to 2023. **Only 5% of CISOs this year are projecting their IT security budgets to grow by more than 10% compared to 36% in 2023.**

Pentesting budget outlook



IT Security budget outlook



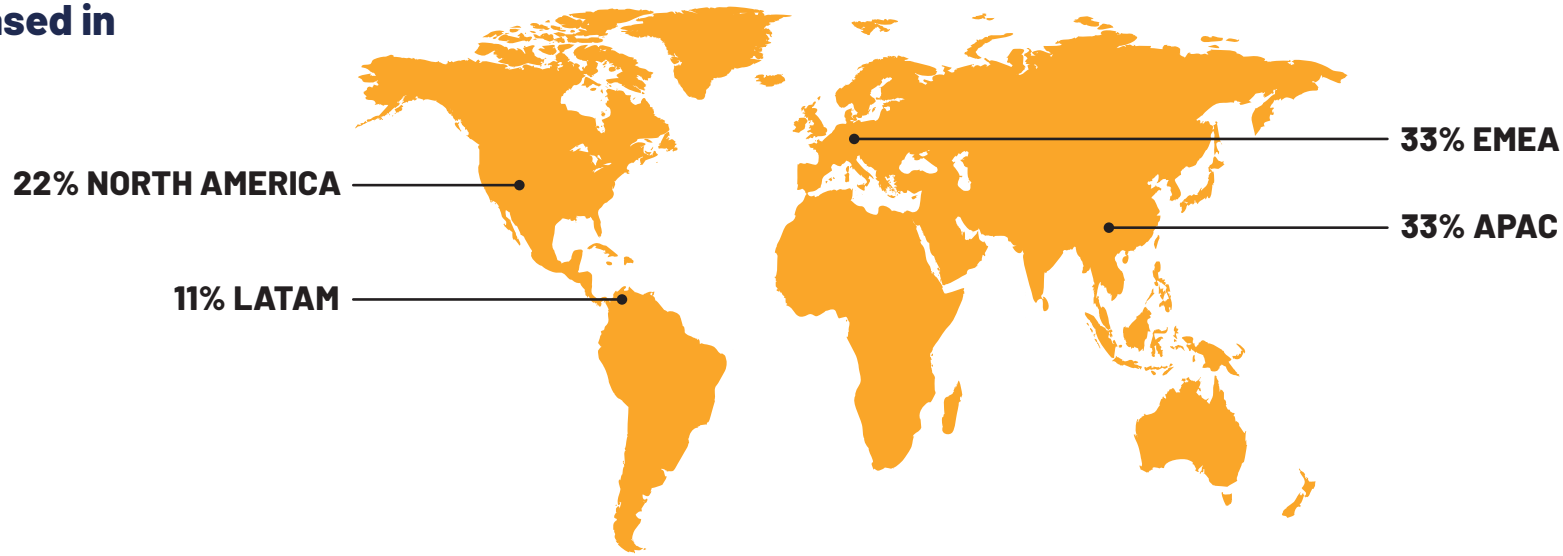
✱ Note - the survey responses were gathered in December 2023, when budgets for 2024 had been decided and approved.

A detailed look at the numbers behind this report

Industries of respondents

- 11% Industrial
- 8% Professional Services
- 8% Health & Pharma
- 8% Financial Services
- 8% Banking
- 7% Energy & Utilities
- 6% Insurance
- 5% Transport & Logistics
- 5% Telecom
- 5% Retail & eCommerce
- 4% Software Development
- 4% Media
- 4% Government
- 3% Education
- 3% Information Technology
- 3% Non Profit
- 2% Food
- 2% Agriculture & Mining
- 2% Public Services
- 1% Technology

Respondents are based in



Size of organizations

59%

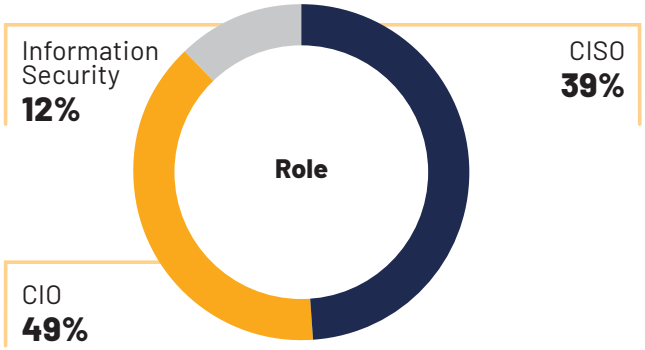
MID-SIZED
1K-5K Employees

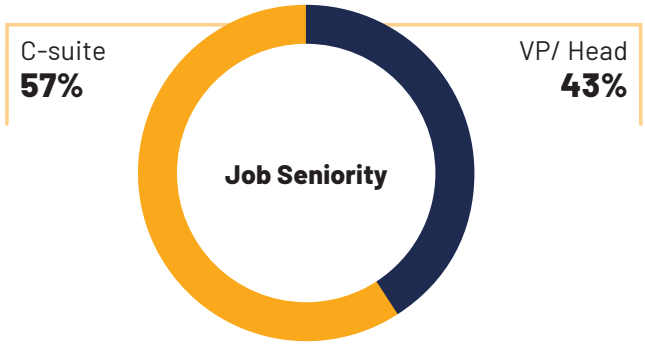
31%

LARGE
5K-10K Employees

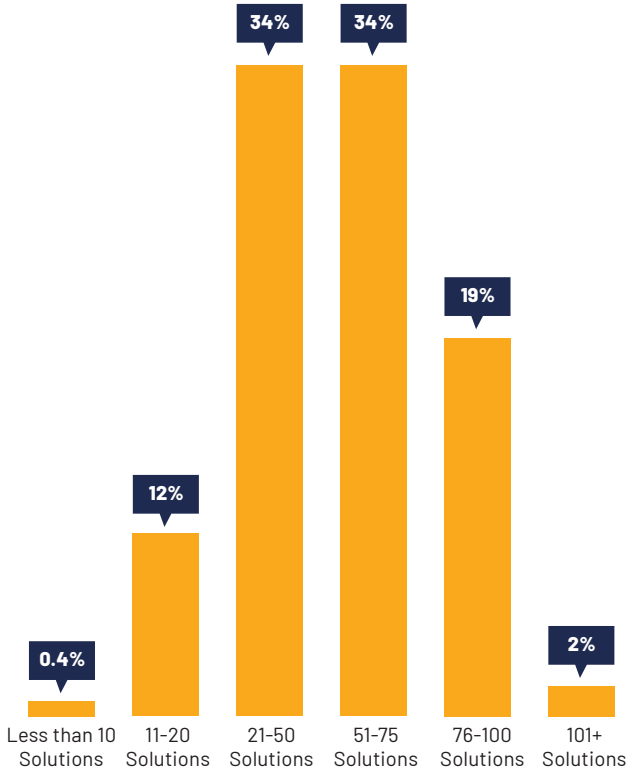
10%

X-LARGE
10k+ Employees

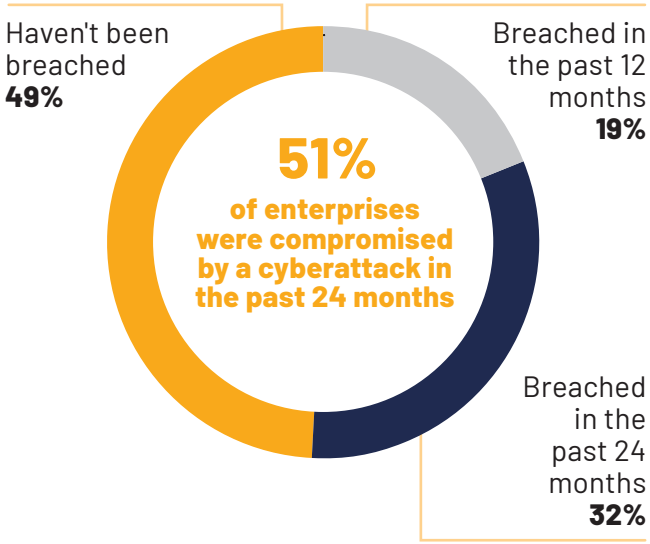




How many security solutions do you currently use across your organization?

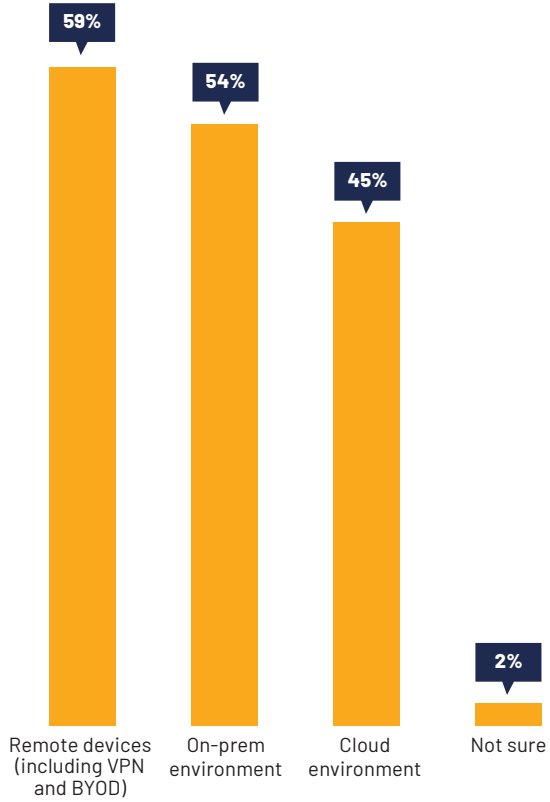


Has your organization been compromised by a cyberattack over the past 24 months?

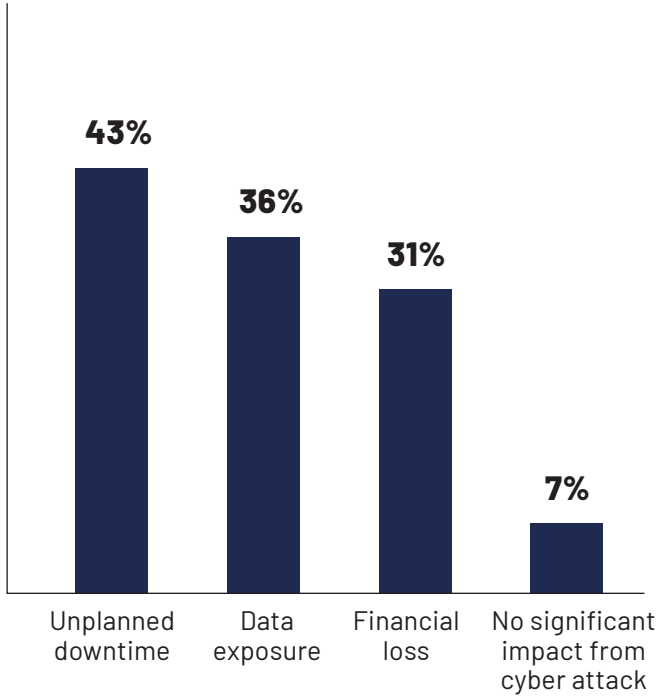


Which aspect of your organization's infrastructure was compromised as a result of the attack/s?

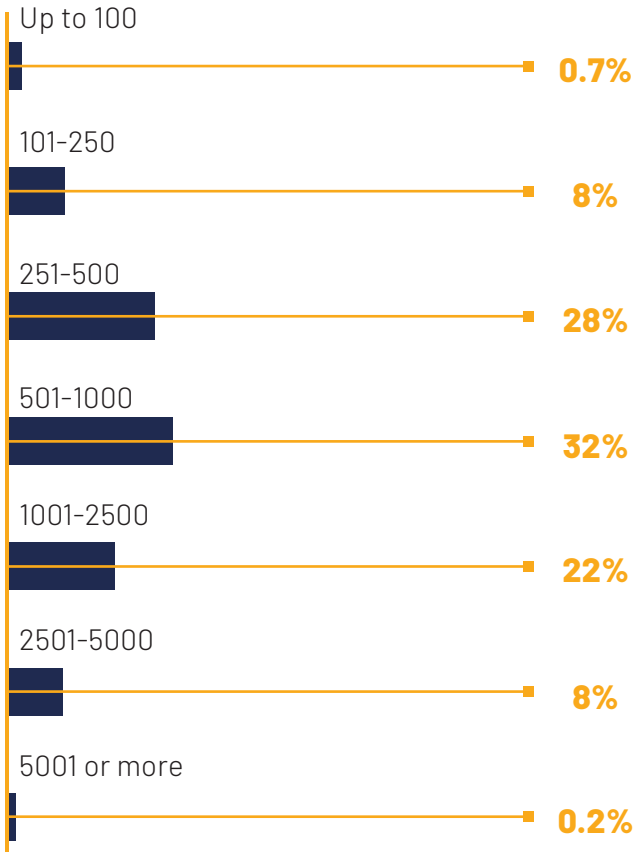
(Select all that apply)



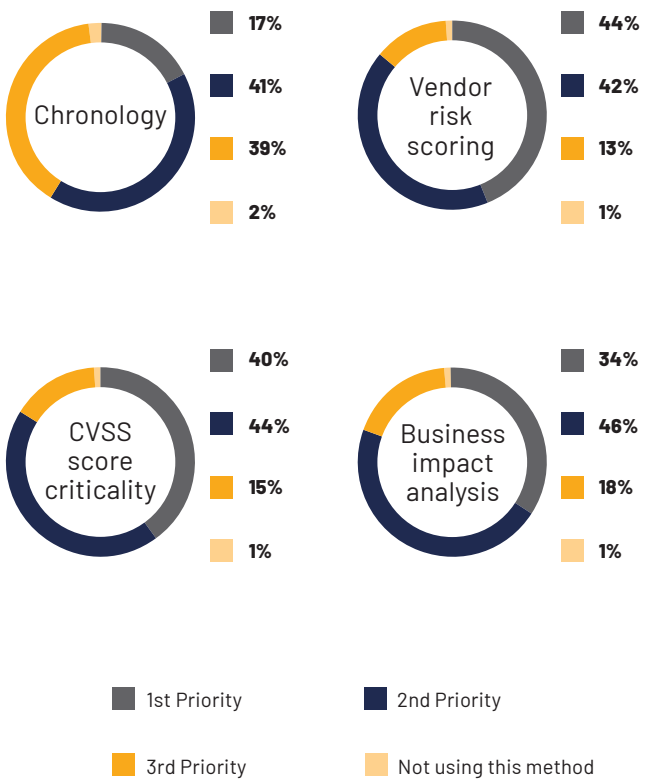
What kind of disruption or impact have your organization experienced as a result of the cyberattack, if at all?
(Select all that apply)



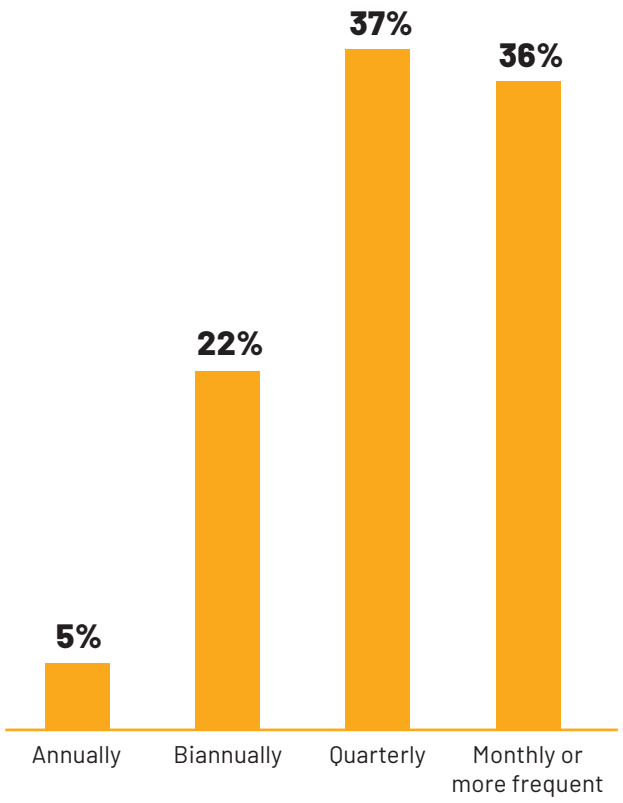
How many security "events" does your organization receive per week? ("Event" is defined as a security matter that requires a remediation action. Examples include, Vulnerability to be patched, User Password Reset, Endpoint Isolation/Quarantine)



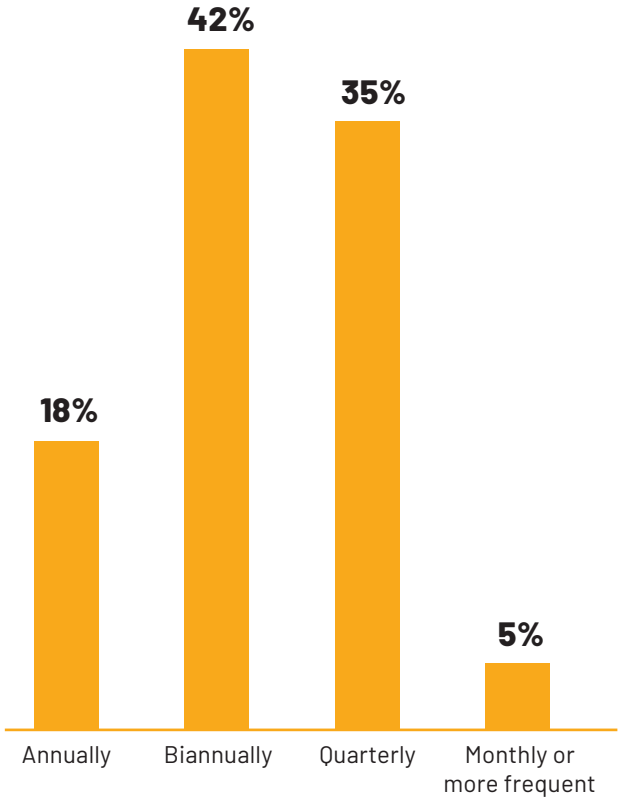
Rank what level of priority your organization assigns each of the following methods when deciding which security events to remediate: Business Impact Analysis, Vendor Risk Scoring, CVSS score criticality, Chronology (The order they entered your system)



How often are you adding and/or decommissioning (subtracting) resources from your network?

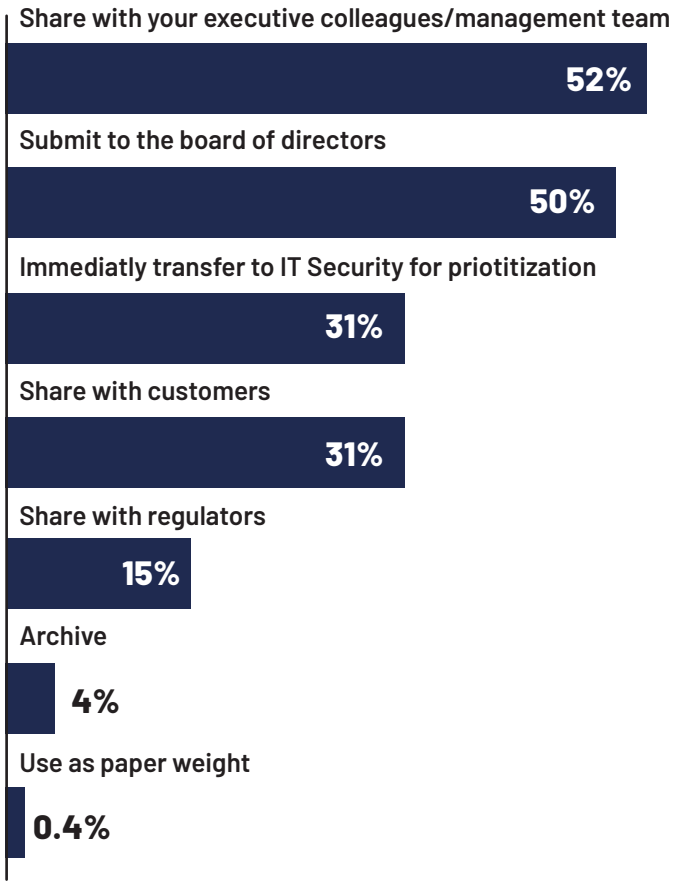


How often does your organization conduct MANUAL pentest assessments?



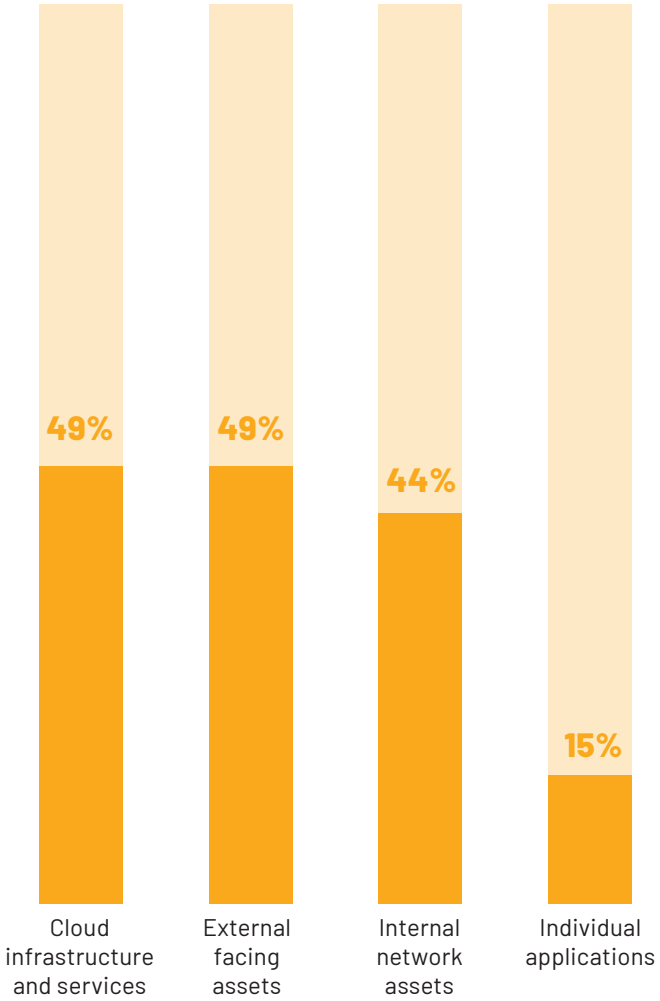
What are the MAIN reasons your organization conducts pentesting?

What do you do with your pentest report?

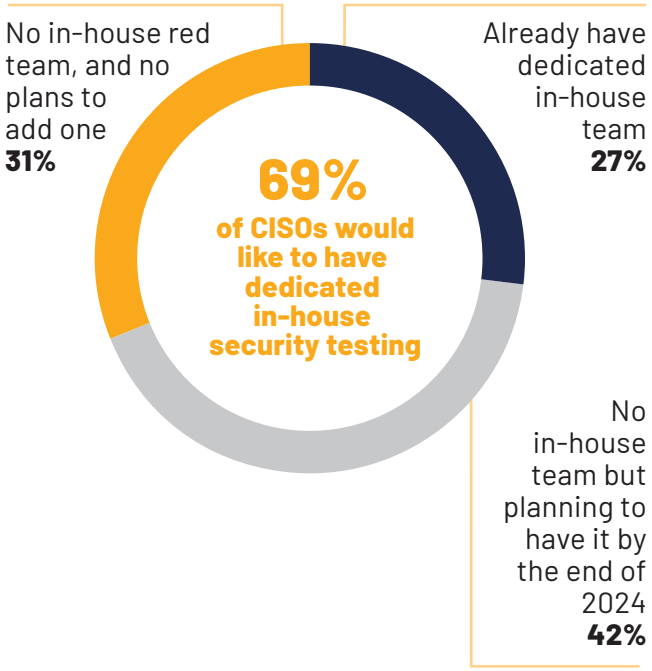


Why are you NOT conducting manual pentesting assessments more often?

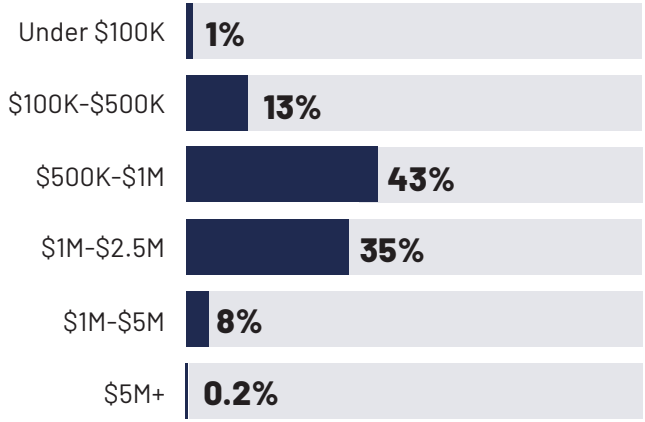
During a penetration test, you direct the pentesters to target/test my organization's:



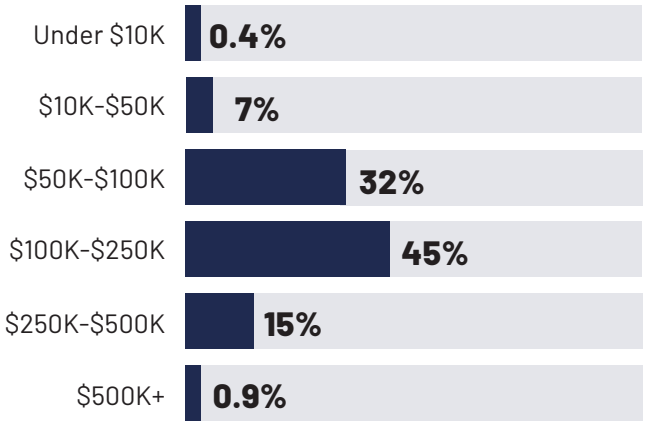
Do you have a dedicated in-house Red Team or Pentesting team?



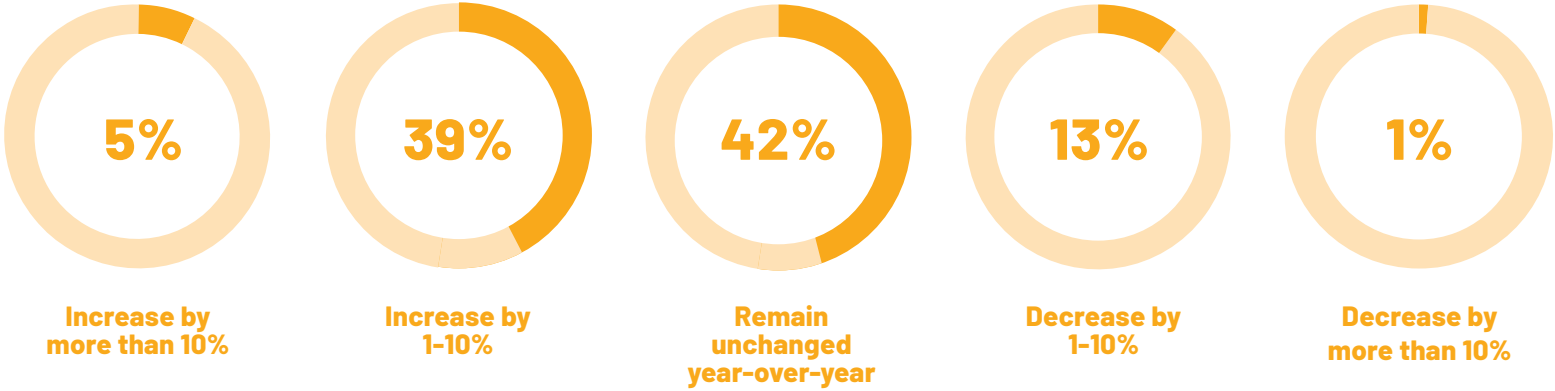
What is your current annual budget for your OVERALL IT Security (2023)?



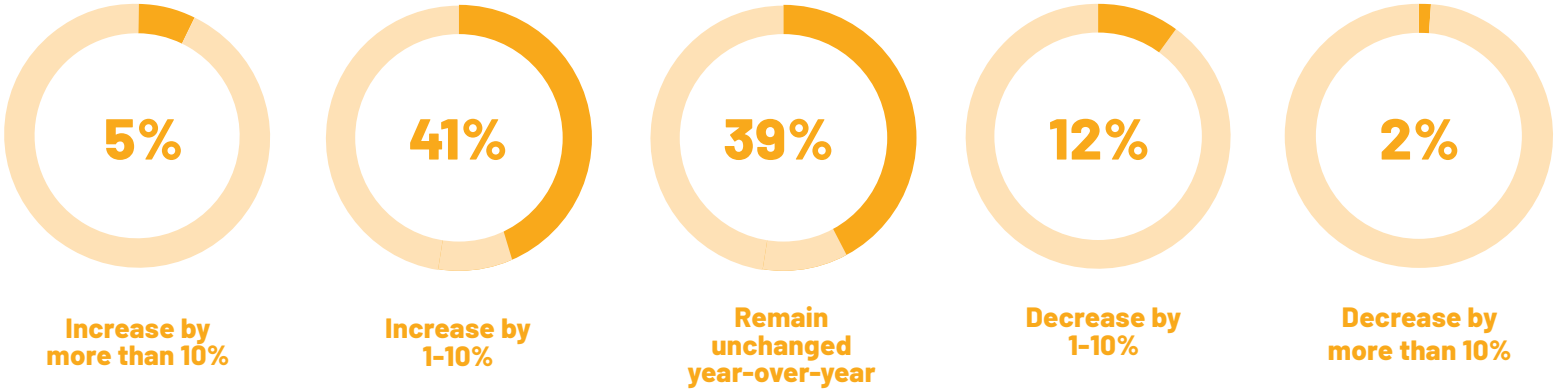
What is your current annual budget for PENTESTING (2023)?

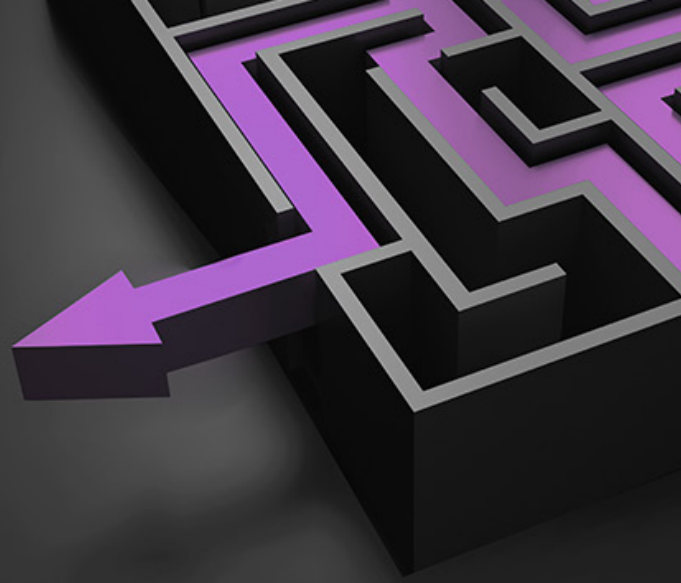


Your annual PENTESTING budget for 2024 is due to:



Your annual OVERALL IT Security budget for 2024 is due to:





Pentera's Automated Security Validation Platform

The Pentera Platform automatically uncovers real exposures in the organization's IT environment. Pentera uses an adaptive, rule-based, algorithm to scan and challenge the entire attack surface - Internal, External, and Cloud, providing real-time security validation at scale. Pentera safely performs the actions a malicious adversary would — reconnaissance, sniffing, spoofing, cracking, (harmless) malware injection, file-less exploitation, post-exploitation, lateral movement, and privilege escalation — all the way to data exfiltration. Requiring no agents or pre-installations, the platform gives security teams a complete attack operation view that provides a true assessment of their resiliency against real attacks, prioritizing remediation efforts with a threat-facing perspective. Pentera applies the latest hacking techniques, including ransomware strains and leaked credentials, enabling organizations to focus their resources on the remediation of the vulnerabilities that take part in a damaging "kill chain". With Pentera, organizations continuously reduce cyber exposure and maintain the highest resilience posture by performing validation tests as frequently as needed - daily, weekly, or monthly. This gives companies a better grasp not only of their security gaps but also allows them to test the efficiency of the security stack and maintain consistency across the organization.

About Pentera

Pentera is the market leader for Automated Security Validation, empowering organizations to easily test the integrity of all cybersecurity layers across the complete attack surface. With continuous validation, Pentera identifies true security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world trust Pentera to guide remediation and close security gaps before they are exploited. **For more info, visit: pentera.io**