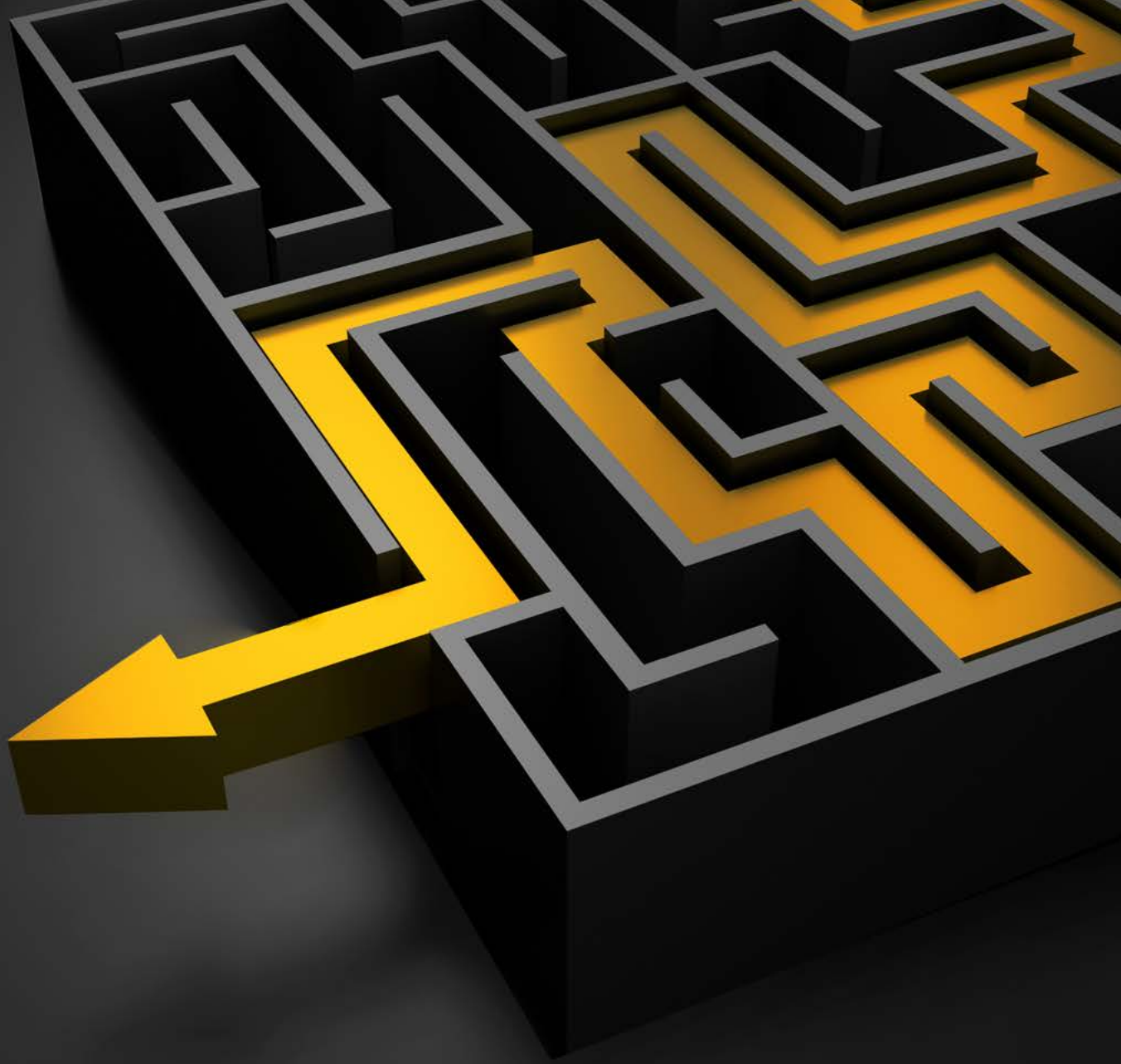


PENTERA

THE STATE OF PENTESTING 2023

SURVEY REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction 2

Methodology 2

Key Findings 3

SURVEY REPORT FINDINGS

Defense in Depth Is Not Sufficient Anymore 5

What's Driving Pentesting? 7

How are Pentest Reports Being Used? 8

Tested Aspects During Pentesting Assessment 9

Biggest Barriers to Pentesting: Percieved Risk to Business Continuity and a Talent Shortage 10

Current Economic Slowdown is Not Impacting Cybersecurity Budgets 11

Projected Annual IT Security and Pentesting Budgets 12

Pentesting is Standard, But There is Room for Improvement 13

The Validation vs. Change Rate – Frequency Gap 15

A Detailed Look at the Numbers Behind this Report 16

About Pentera 25

INTRODUCTION

Pentera, the leaders in Automated Security Validation, undertook this research to understand the current state of security validation in organizations of different sizes across Europe and the USA.
How are today's organizations approaching pentesting, compared to common practices a few years ago? What are the motivations driving pentesting? And how is the current economic situation impacting cybersecurity - both specifically for pentesting initiatives and for the wider IT security budget?

This report is a snapshot of how security leaders in 2023 perceive and choose to adopt security validation strategies, shining a light on budget, sentiment, drivers, and inhibitors for their current practices.

METHODOLOGY

We commissioned a survey of **300** security executives who hold VP or C-level positions

in companies with more than **1,000** employees.

Respondents were split between the U.S., the UK, and Western Europe. We screened for those who were aware of their pentesting activities, and how frequently they implemented manual pentests, if at all. This report was administered online by Global Surveyz Research, a global research firm.

The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during December 2022.

The average amount of time spent on the survey was 6 minutes and 44 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during December 2022.

01

DESPITE LARGE INVESTMENTS IN DEFENSE-IN-DEPTH STRATEGIES, 88% OF ORGANIZATIONS REPORT RECENT ATTACKS

On average, companies have almost 44 security solutions in place, indicating a defense-in-depth strategy, where multiple security solutions are layered to best protect critical assets. However, despite the large number of security solutions implemented, 88% of organizations admit to being compromised by a cyber incident over the past two years.

02

CYBERSECURITY BUDGETS AREN'T IMPACTED BY THE FINANCIAL SLOWDOWN

Despite the recent global economic slowdown, cybersecurity budgets are not expected to be impacted in 2023. 92% of organizations report a raise in their IT security budgets, and 85% report a raise in their pentesting budget specifically.

03

THE IMPORTANCE OF CYBER INSURANCE HAS SKYROCKETED FOR SECURITY EXECUTIVES

The global discussion around the evolution of cyber insurance requirements has taken center stage as the number of attacks increased throughout the Covid-19 pandemic. Cyber insurance assessment is becoming a critical driver for pentesting, with 36% of respondents naming it as their top reason for conducting pentesting compared to only 2% who listed it as a primary motivation in a similar survey that was conducted towards the beginning of the pandemic in 2020.

04

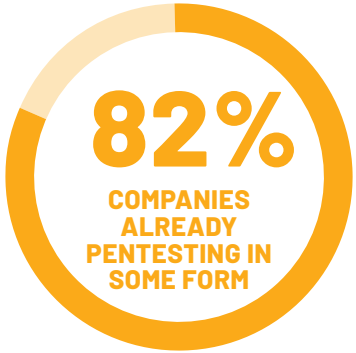
THE DRIVERS FOR PENTESTING HAVE EVOLVED BEYOND REGULATIONS

While the need for pentesting originated with regulatory requirements, the top-of-mind motivations for pentesting today are security validation, potential damage assessment, and cyber insurance. With only 22% of respondents citing compliance as their primary motivation for the practice, regulatory or executive mandates are still impactful, but not the primary rationale driving pentesting.

05

RISK TO BUSINESS CONTINUITY IS THE BIGGEST BARRIER TO PENTESTING

While the practice of pentesting is already ubiquitous, with 82% of companies today already pentesting in some form, the primary barrier for the practice is the fear for business continuity. Companies who are already pentesting, and those who do not pentest at all, cite the risk to business continuity as the largest concern when considering adopting a greater amount of pentests, with a lack of available pentesters as the second largest issue.



DEFENSE IN DEPTH IS NOT SUFFICIENT ANYMORE

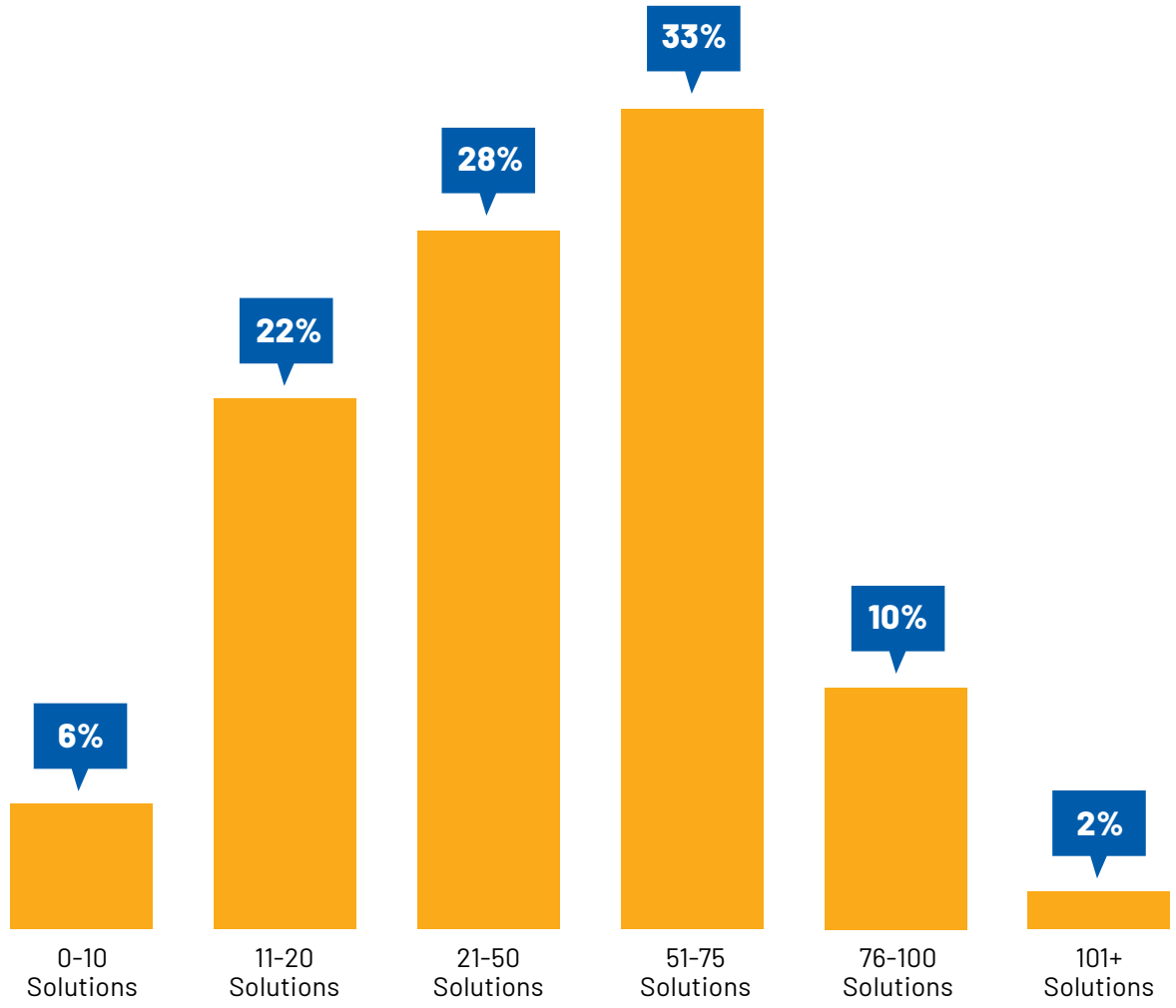
Defense-in-depth (DiD) is a security strategy where multiple security technologies are layered on top of one another, working with the assumption that no single tool can keep an organization fully secure. Instead, the DiD methodology states that layering security from multiple directions will best protect critical assets.

Research shows that 92% of organizations utilize a DiD strategy. Our data reiterates the focus on DiD, as respondents are currently investing in an average of 43.8 security solutions, and only 6% have less than ten tools in place.

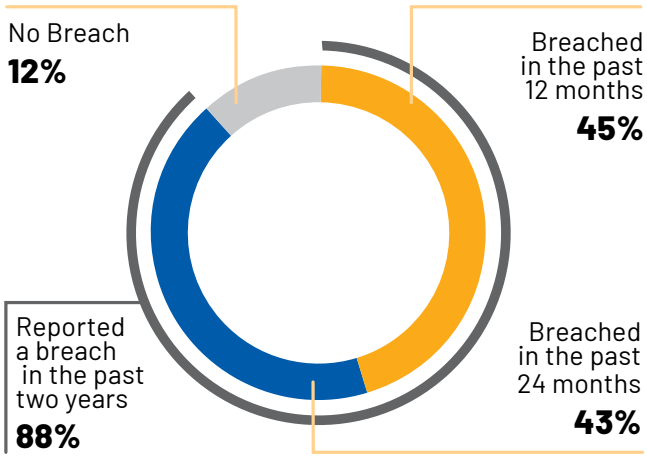
92%
ORGANIZATIONS UTILIZE A DID STRATEGY

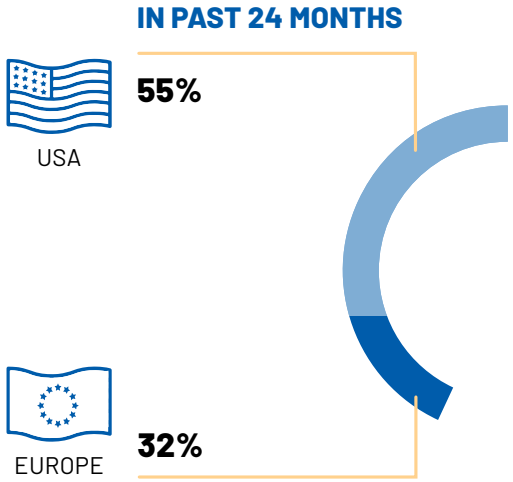
43.8
SECURITY SOLUTIONS

6%
LESS THAN TEN TOOLS IN PLACE



However, despite this strategy, **88% of respondents have admitted to being compromised by a cyber attack over the past two years**, with 45% reporting an attack in the past 12 months. Based on our findings, it's clear that the current DiD strategy is not sufficient towards preventing cyber breaches.

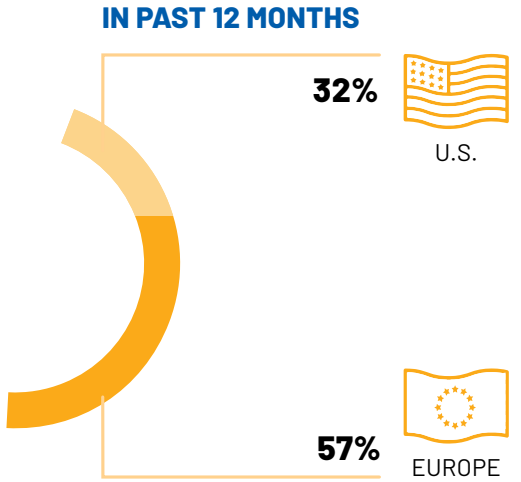




57%

EUROPEAN ORGANIZATION REPORTED A BREACH IN THE PAST YEAR

We can see that in 2021, cyber attacks were more common for U.S. organizations than those in Europe, (55% and 32% respectively). However, in 2022, the onslaught of attacks trended towards Europe, and 57% of European respondents reported a breach, compared to 32% in the U.S.



WHAT'S DRIVING PENTESTING?

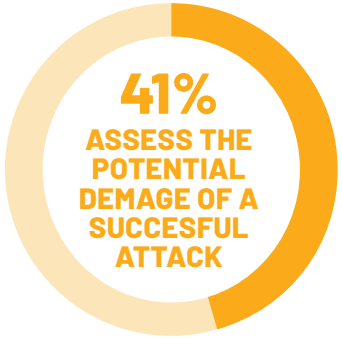
We asked security leaders why they conduct pentesting in their organization to find out what's driving the practice.

What we found is that while pentesting originated from regulations and compliance, security validation is now the primary driver for the practice.

The top reasons that companies perform pentesting for are to validate their cyber security controls, and to assess the potential damage of a successful attack, both named by 41% of respondents.

While this focus on control and validation has remained unchanged from our previous survey, The State of Penetration Testing 2020, other drivers show a marked shift over the past two years.

In 2020, the second most-common reason for pentesting was to satisfy regulatory compliance, which is the origin of pentesting as a security practice. As shown in the data, regulatory compliance has since fallen in priority to the least critical driver in todays' pentesting discussion with only 22% listing it as a top reason for the practice.



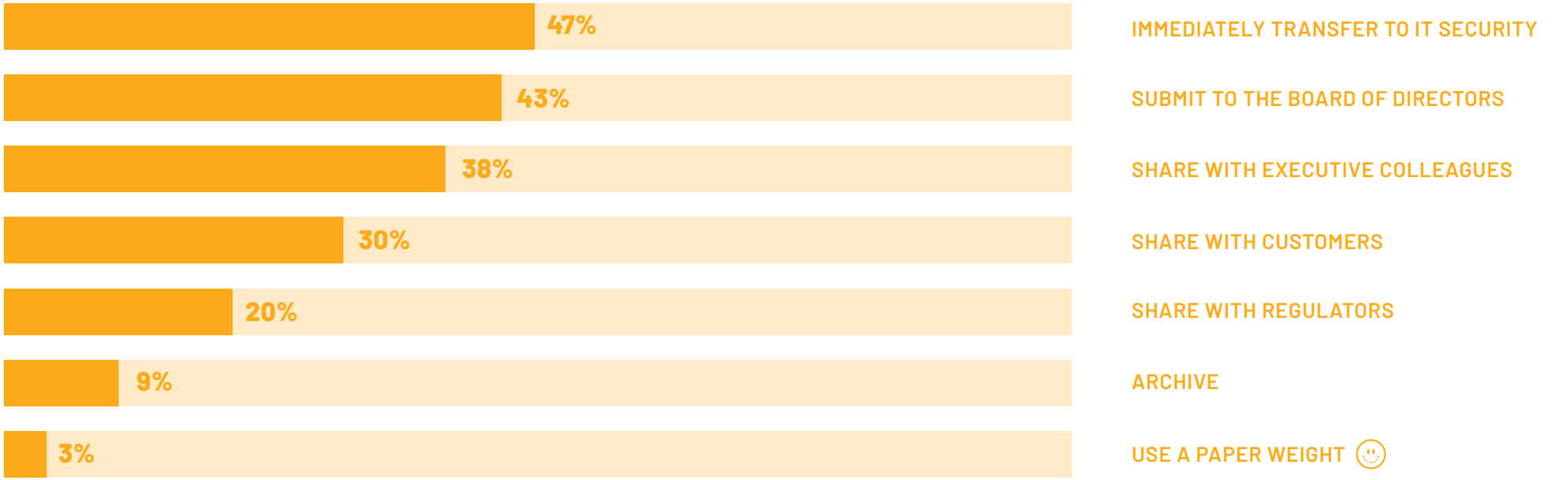
As regulatory compliance has moved down the list of priorities, cyber insurance has taken leaps in the opposite direction. In 2020, only 2% of respondents named cyber insurance as a reason to adopt pentesting, while today this is a top driver for 36% of respondents. Cyber insurance has become a major factor in security decision making.

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

HOW ARE PENTEST REPORTS BEING USED?

We asked CISOs how they utilize the reports they receive at the end of pentesting assessments. While the top response is to immediately transfer the information to IT so that they can remediate issues (47%), pentesting reports are also being used for communication, both internally and externally.

CISOs are utilizing pentesting reports as a more concrete way to communicate risk to the board of directors or to other executives within the organization who may not be as security-saavy. They also share pentesting reports with customers and regulators, providing assurances to these stakeholders that the security posture of the organization is robust.

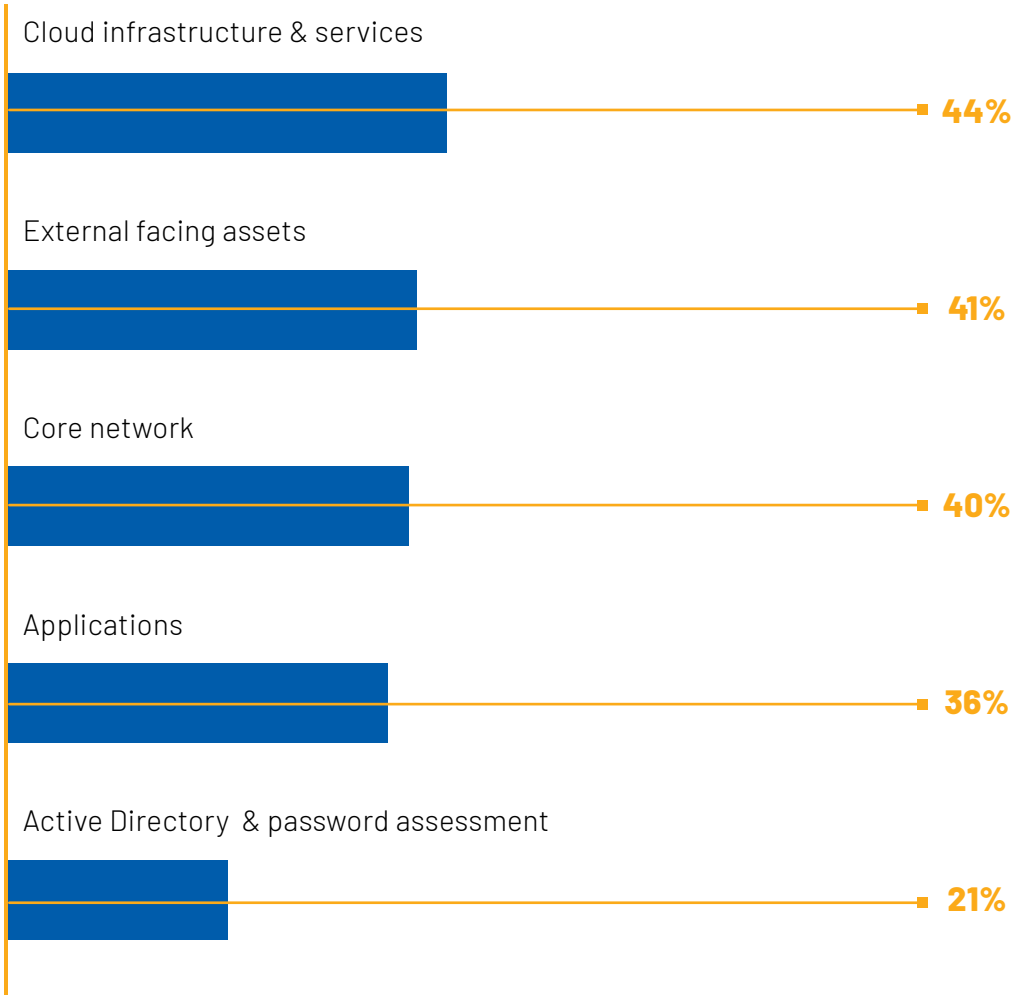


✱ Question allowed more than one answer and as a result, percentages will add up to more than 100%

TESTED ASPECTS DURING PENTESTING ASSESSMENT

Penetration testing spans all aspects of the modern attack surface as a sampling exercise. Interestingly, the top tested aspects during pentesting assessments include cloud infrastructure & services (44%), external facing assets (41%), and core network (40%).

Check Point Research has reported a dramatic spike in cloud network attacks during 2022. They uncovered a 48% increase in the number of attacks per organization. Our informed assumption is that the cloud environment is where many CISOs feel they have the least visibility and maturity, and therefore, this is where they choose to place their pentesting focus .



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

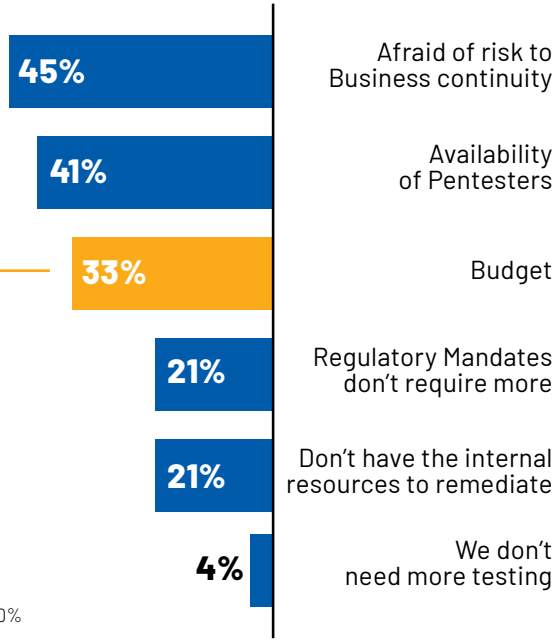
BIGGEST BARRIERS TO PENTESTING: PERCIEVED RISK TO BUSINESS CONTINUITY AND A TALENT SHORTAGE

When we asked respondents to name the main inhibitors for implementing pentesting or increasing their use of pentesting, the perceived risk to business continuity stood out as a core concern.

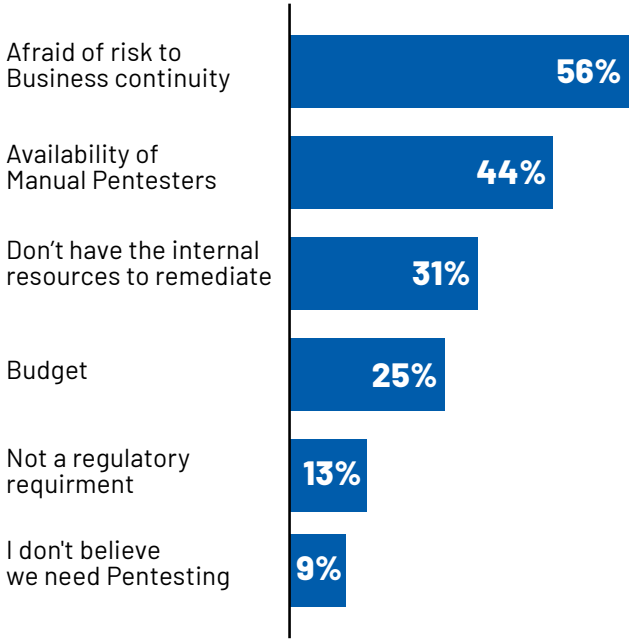
45% of those who already conduct pentesting, whether manual or automated, say that the risk to business applications or network availability prevents them from increasing the pentesting frequency, and this number increases to 56% when we look at those who don't conduct pentesting assessments at all. Availability of pentesters is the second largest concern for both groups. It's likely that many, if not most, organizations who engage in pentesting have suffered an network disruption as a result at some point, and the institutional memory of such incidents is strong. Businesses want to feel that they are working with the most experienced pentestersusing the highest quality pentesters who are least likely to impact business continuity. This will reduce the risk of business disruption or downtime, their number one fear.

Interestingly, budget does not appear to be a top-of-mind concern. Only 33% of the CISOs name budget as a reason not to increase the frequency of pentesting, and only 25% of those who don't pentest at all cite budget as a factor. While not the main concern for organizations, it is interesting to note that regionally, US respondents are more concerned with budget compared to their European counterparts.

INHIBITORS FOR DOING MORE FREQUENT MANUAL PENTESTING ASSESSMENTS



REASONS FOR NOT CONDUCTING PENTESTING ASSESSMENTS



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

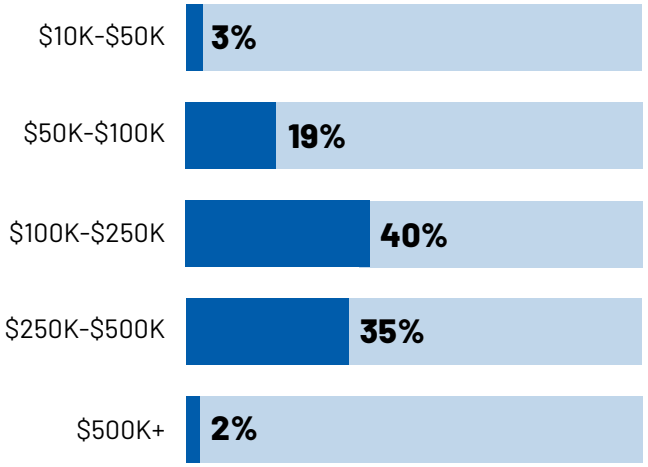
CURRENT ECONOMIC SLOWDOWN IS NOT IMPACTING CYBERSECURITY BUDGETS

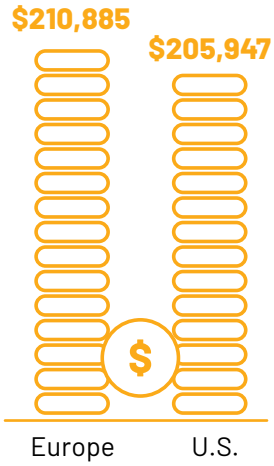
The average annual pentesting budget in 2022 was $208,224, with 77% of security leaders reporting a pentesting budget of more than $100,000. This is a dramatic increase from 2020, where our previous survey revealed that 49% of enterprises had a pentesting budget of less than $100k.

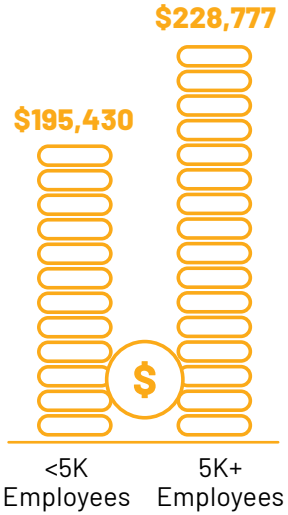
When broken down by region, the average annual pentesting budget in Europe ($210,885) is slightly higher than in the U.S. ($205,947). The breakdown by company size shows that the average annual budget of companies with under 5K employees is $196,430, compared to the $228,777 of companies with more than 5K employees. What we see is that neither region nor company size appears to significantly impact the size of pentesting budgets.

$208K

AVERAGE ANNUAL PENTESTING BUDGET







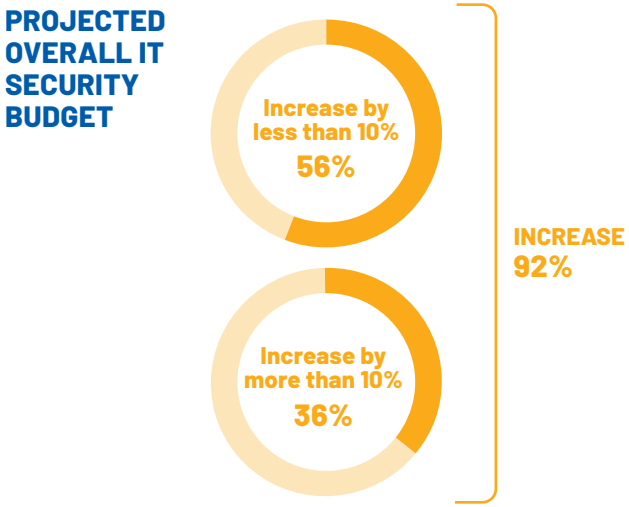
PROJECTED ANNUAL IT SECURITY AND PENTESTING BUDGETS

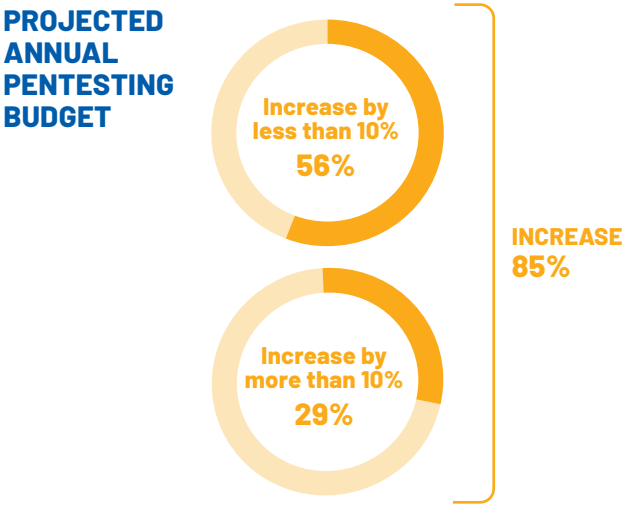
Both pentesting budgets and overall IT security budgets increased significantly for 2023. **92% of CISOs report an increase in their IT security budget in 2023**, and 85% of respondents say that their annual pentesting budget has increased as well.

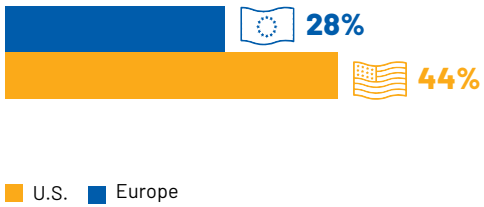
** Note - the survey responses were gathered in December 2022, when budgets for 2023 had been decided and approved.

According to a Gartner® Press Release, "Spending on information security and risk management products and services is forecast to grow 11.3% to reach more than $188.3 billion in 2023." *

There are regional differences to be aware of. While almost every company is reporting budget increases, European respondents report larger projected budgetary growth over the next year compared to the U.S. 42% of respondents from Europe say that their pentesting budget will increase by more than 10% in 2023, compared with just 17% of security leaders from the U.S. The same dynamic appears when we look at the budget for overall IT security, with 44% of European companies increasing their budget by more than 10%, against just 28% of those from the U.S.



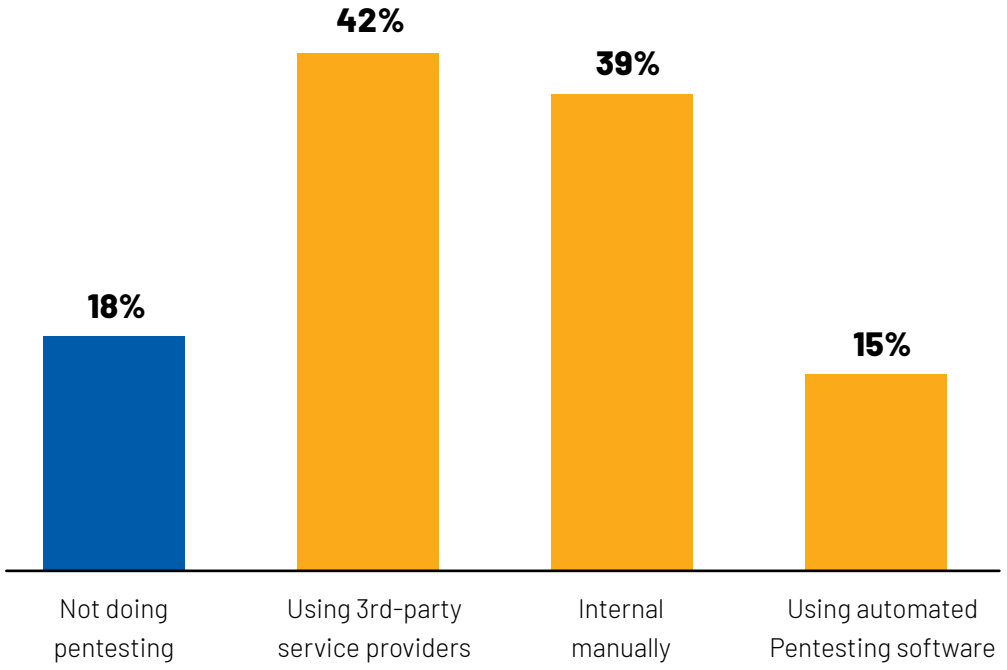




PENTESTING IS STANDARD, BUT THERE IS ROOM FOR IMPROVEMENT

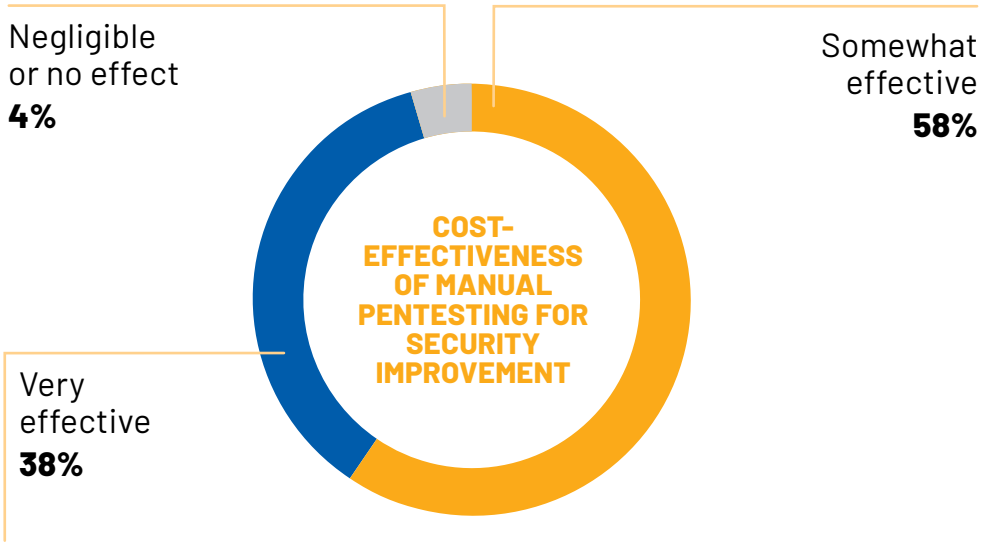
Pentesting is already a standard practice, but 62% of respondents recognize that there is room for improvement in their pentesting processes and the market is building towards in-house capabilities.

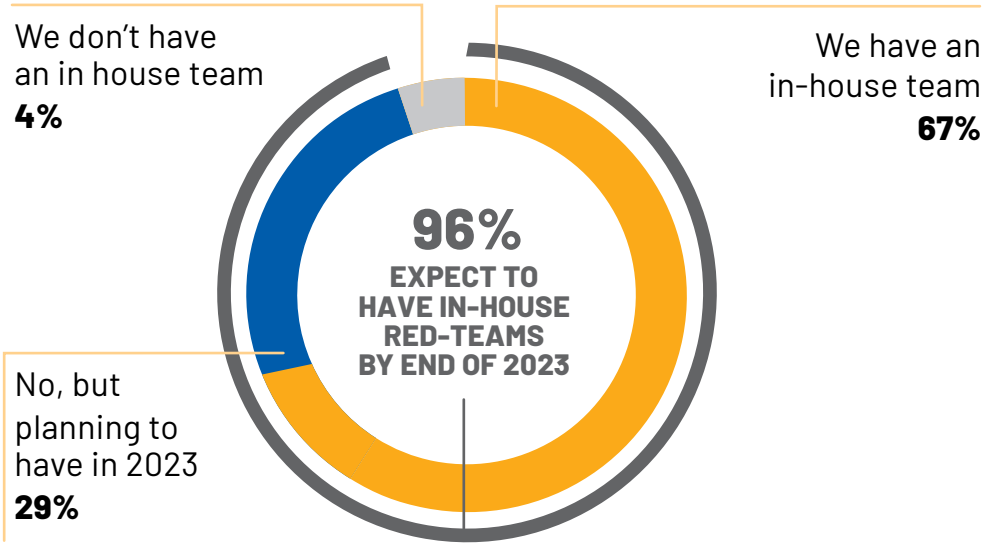
At the end of 2022, 82% of CISOs reported that they are conducting pentesting as part of their overall security strategy, however, only 42% report using an external party. 39% have in-house pentesting capabilities, for independence, efficiency and greater validation frequency. Still there is room for growth as only 15% are on the advanced end of the security validation maturity scale and are also using automation tools to conduct pentesting.



Our 2020 report reveals that 51% of CISOs reported in-house red-teams, and that number has grown to 67% today. More impressive than the growth, however, is that 96% of security executives reported that by the end of 2023 they will already have, or plan to have, an in-house red team for this critical task.

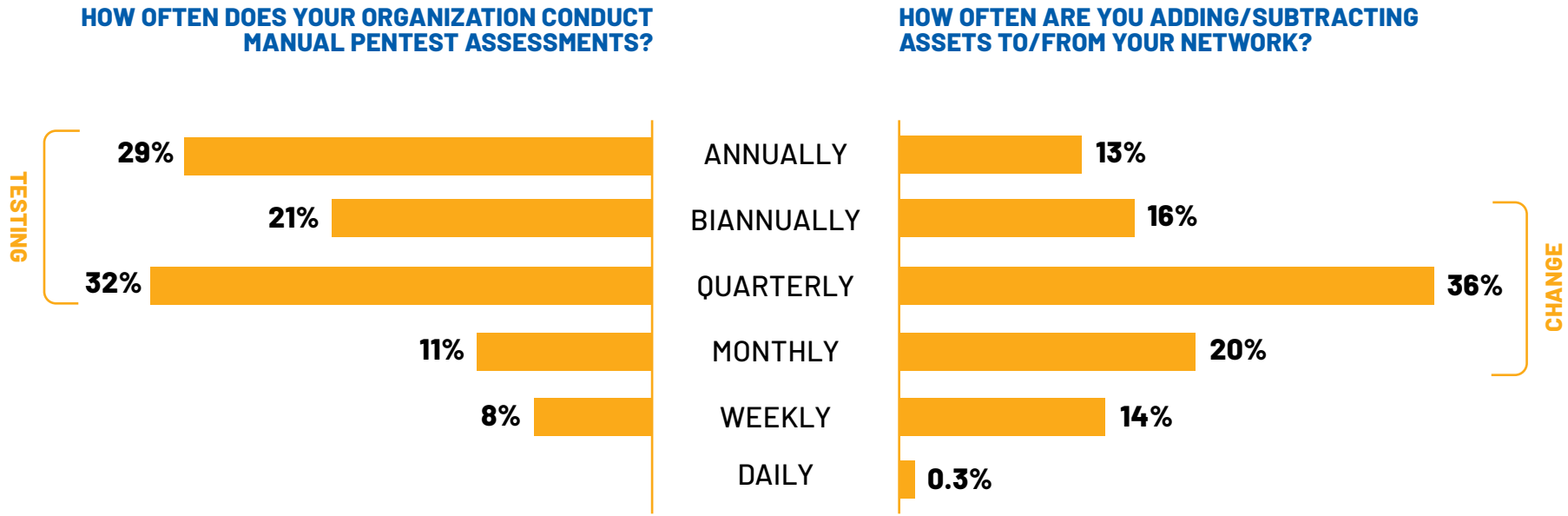
96% HAVE OR WILL HAVE IN-HOUSE RED-TEAM





THE VALIDATION VS. CHANGE RATE – FREQUENCY GAP

The push towards in-house capabilities likely stems from the need to validate the security of IT environments that are evolving faster than the current testing cadence and attack surfaces that are being assessed. 70% of the CISOs report that their IT environment is being updated with assets being added or removed on a quarterly, monthly or weekly basis. However, 82% of the CISOs reported that they test their network on a quarterly to annually basis. It is clear that there is a frequency gap between the change rate and the validation rate, leaving IT infrastructure untested for long periods of time or untested completely.



INDUSTRIES OF RESPONDENTS

16% Goverment

11% Energy & Utillites

9% Retail & eCommerce

8% Banking

7% Education

6% Financial Services

6% Health & Pharma

6% Transport & Logistics

5% Food

4% Travel & Hospitality

4% Information Technology

4% Media

3% Professional Services

3% Telecom

2% Technology

2% Industrial

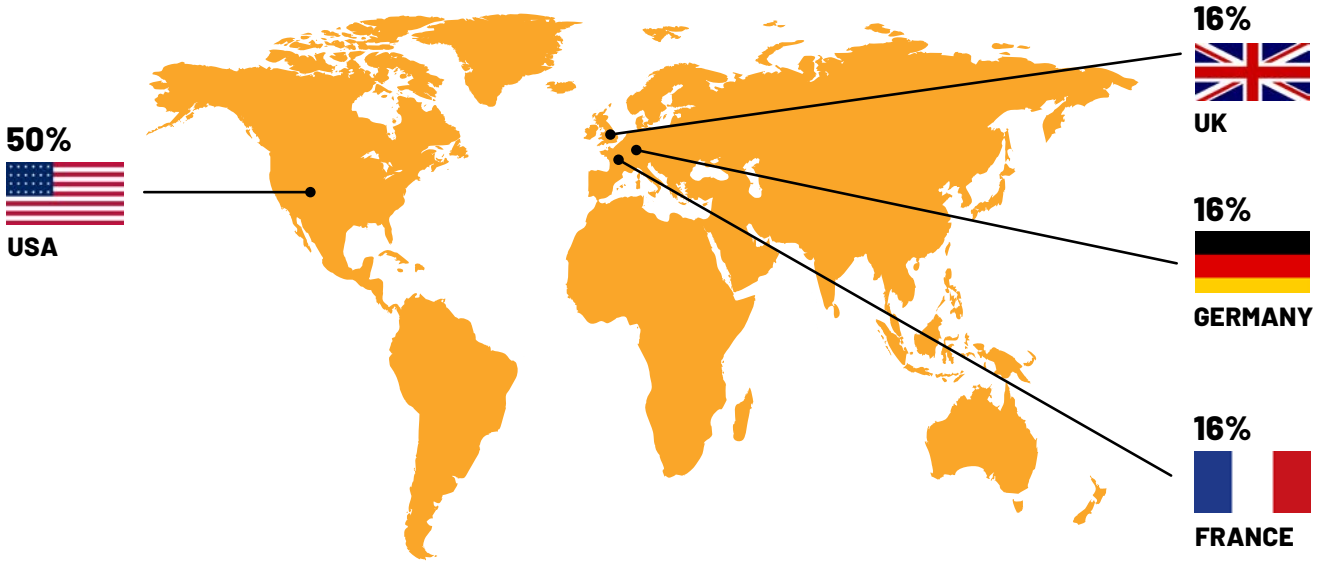
2% Insurance

1% Software Development

1% Agriculture & Mining

1% Public Services

RESPONDENTS ARE BASED IN

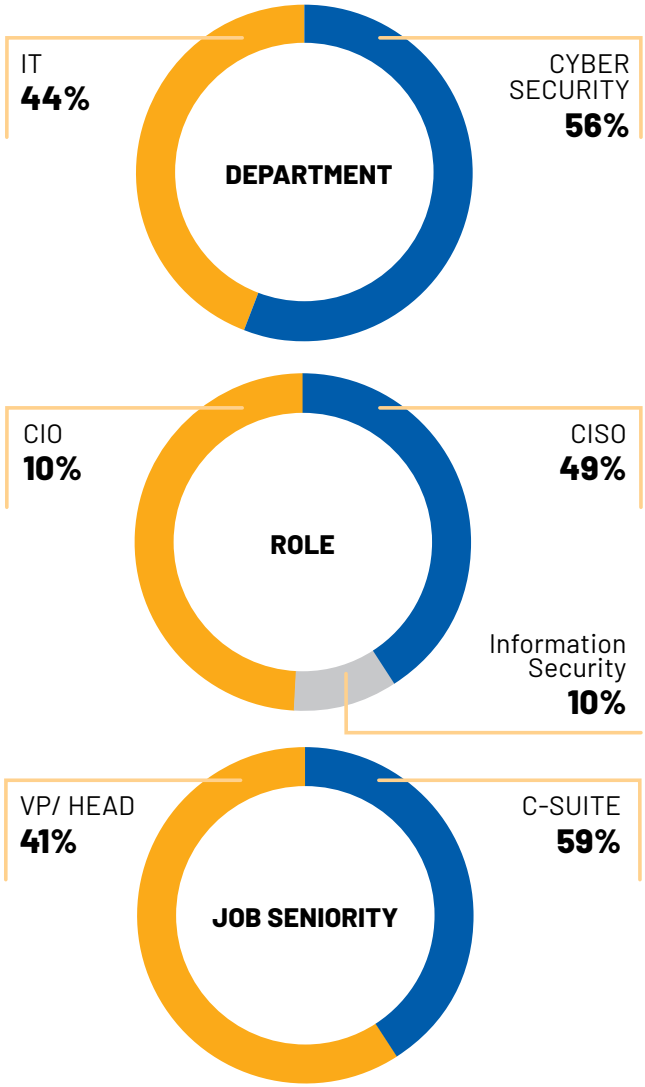


SIZE OF ORGANIZATIONS

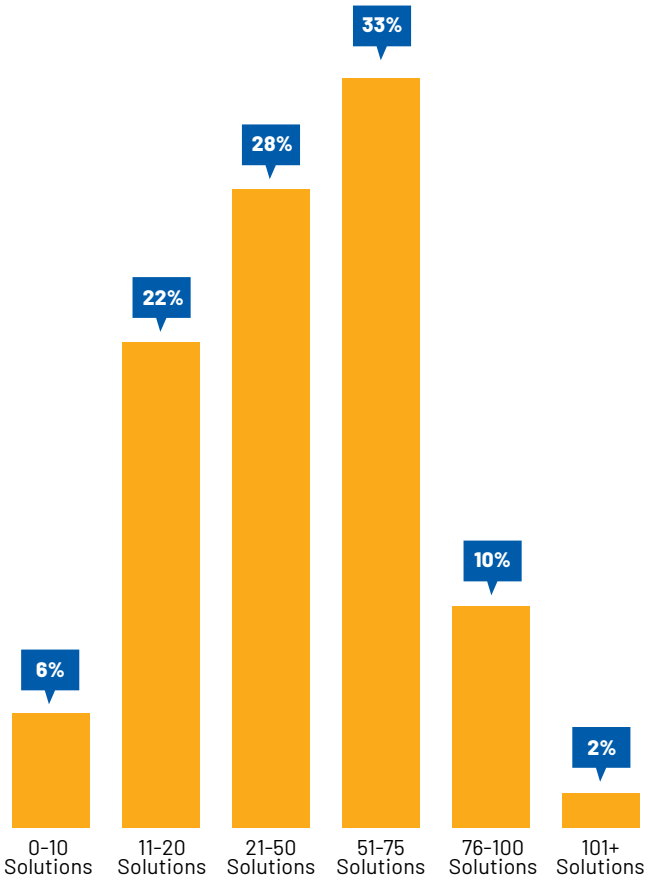
51%
MID-SIZED
1K-5K Employees

42%
LARGE
5K-10K Employees

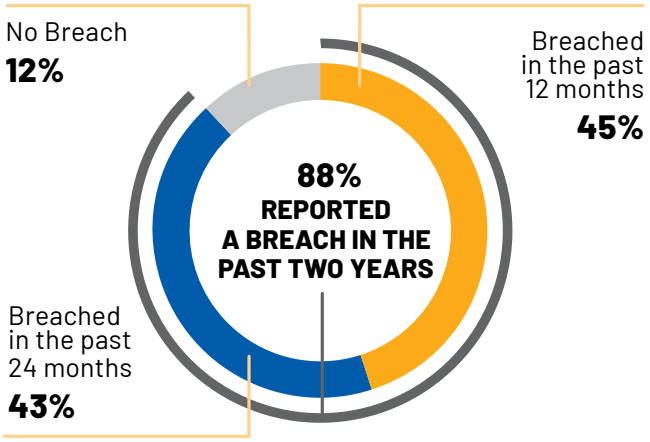
7%
X-LARGE
10k+ Employees

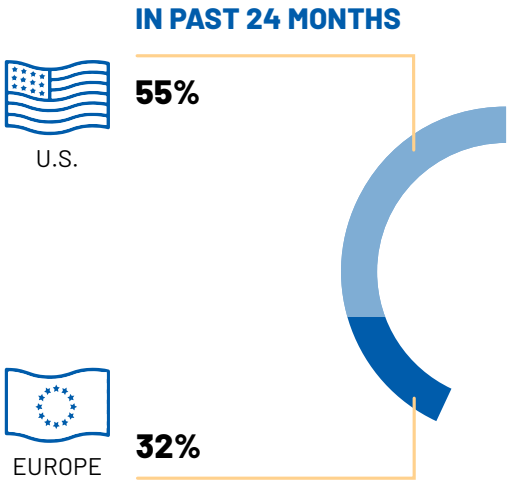


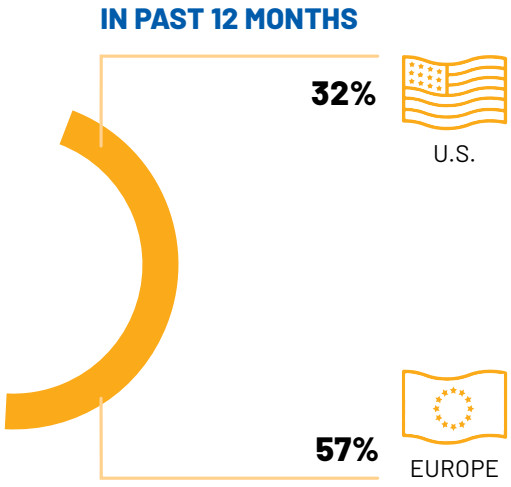
HOW MANY SECURITY SOLUTIONS DO YOU CURRENTLY USE ACROSS YOUR ORGANIZATION?



HAS YOUR ORGANIZATION BEEN COMPROMISED BY A CYBERATTACK OVER THE PAST 24 MONTHS?

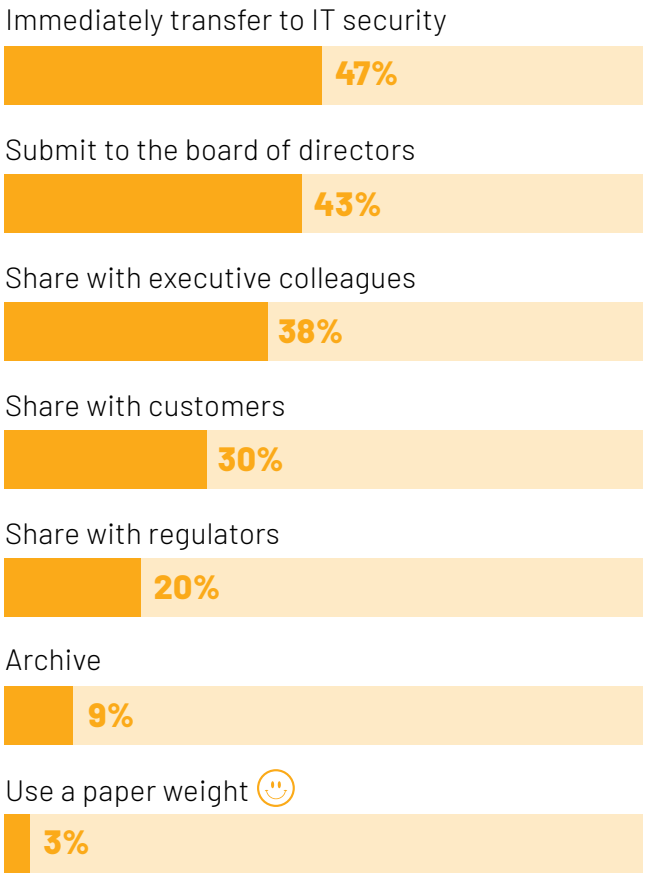




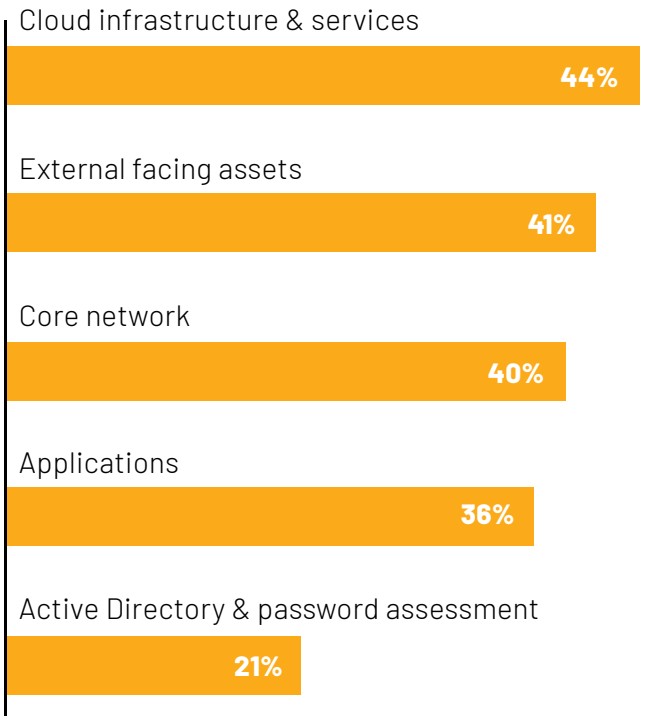


WHAT ARE THE MAIN REASONS YOUR ORGANIZATION CONDUCTS PENTESTING?

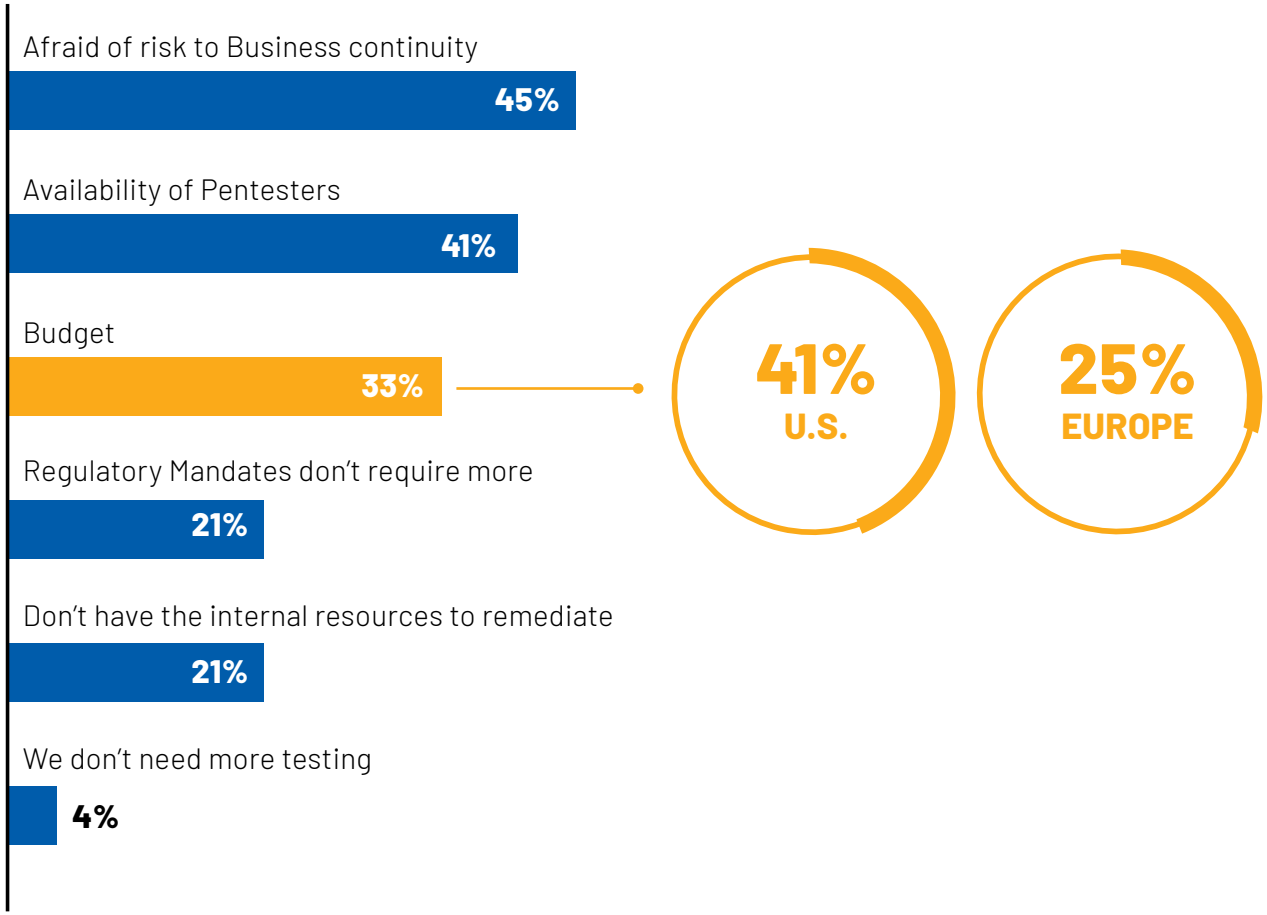
WHAT DO YOU DO WITH YOUR PENTEST REPORT?



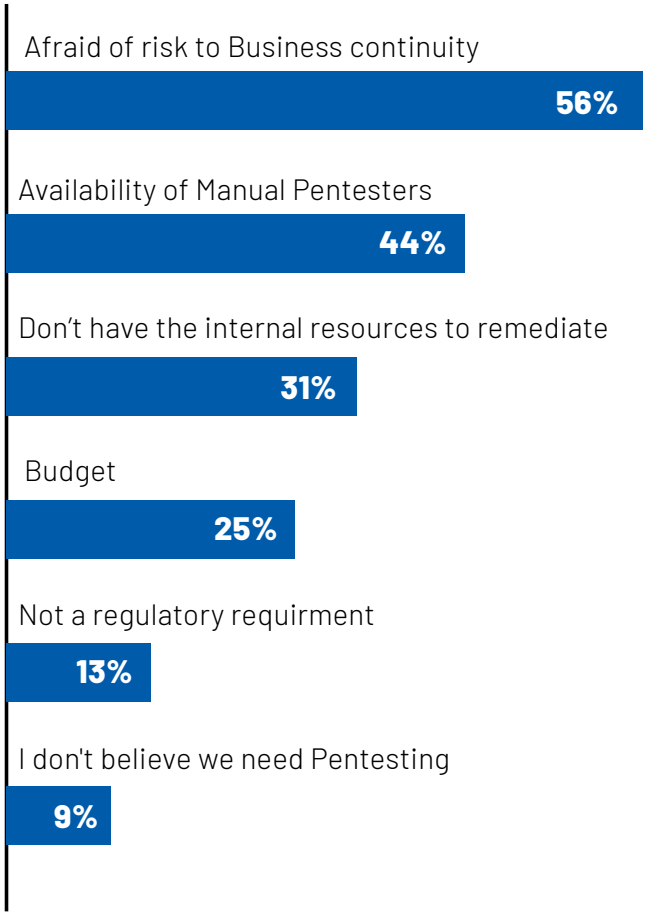
WHAT ASPECTS OF YOUR ORGANIZATION ARE YOU TESTING DURING A PENTESTING ASSESSMENT?



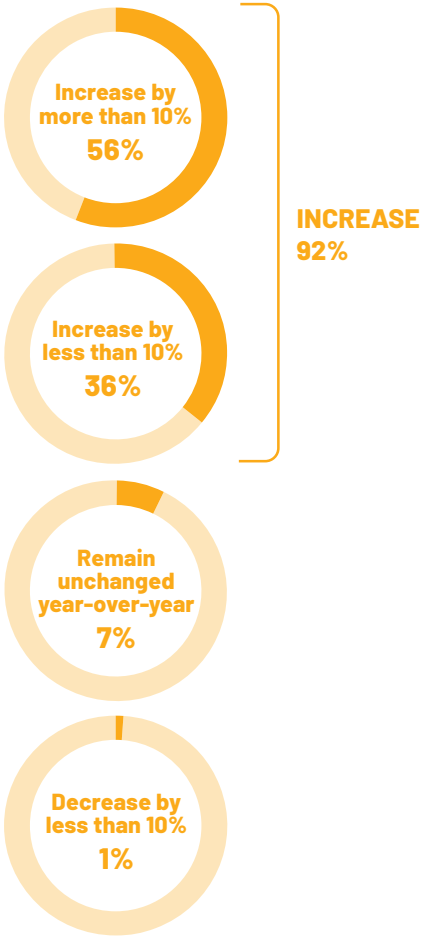
WHY ARE YOU NOT CONDUCTING MANUAL PENTESTING ASSESSMENTS MORE OFTEN?



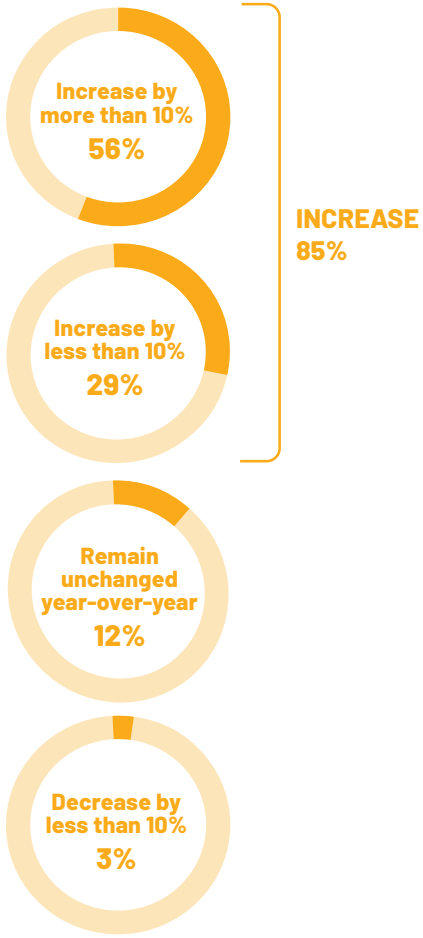
REASONS FOR NOT CONDUCTING PENTESTING ASSESSMENTS



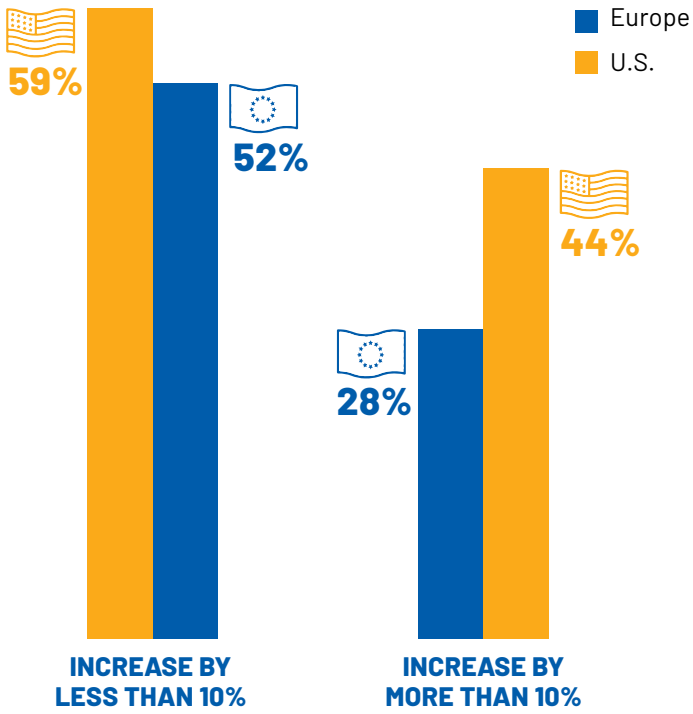
YOUR ANNUAL *OVERALL* IT SECURITY BUDGET FOR 2023 IS DUE TO?



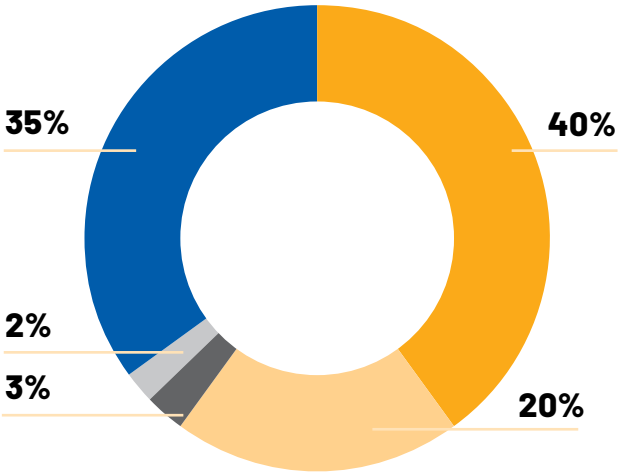
YOUR ANNUAL *PENTESTING* BUDGET FOR 2023 IS DUE TO?



ANNUAL OVERALL IT BUDGET DUE TO? SPLIT BY REGION



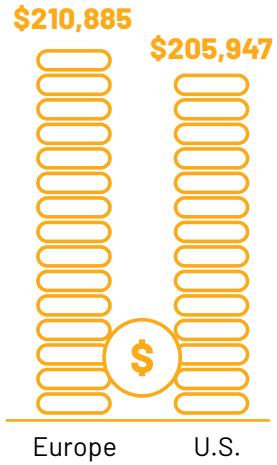
WHAT IS YOUR CURRENT ANNUAL BUDGET FOR *PENTESTING*?



- **40%** $100K-$250K
- **35%** $250K-$500K
- **20%** $50K-$100K
- **3%** $10K-$50K
- **2%** $500K+

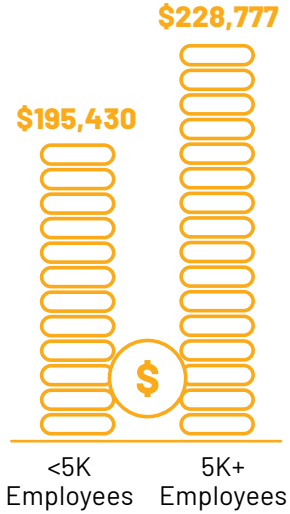
WHAT IS YOUR CURRENT ANNUAL BUDGET FOR *PENTESTING*?

SPLIT BY REGION

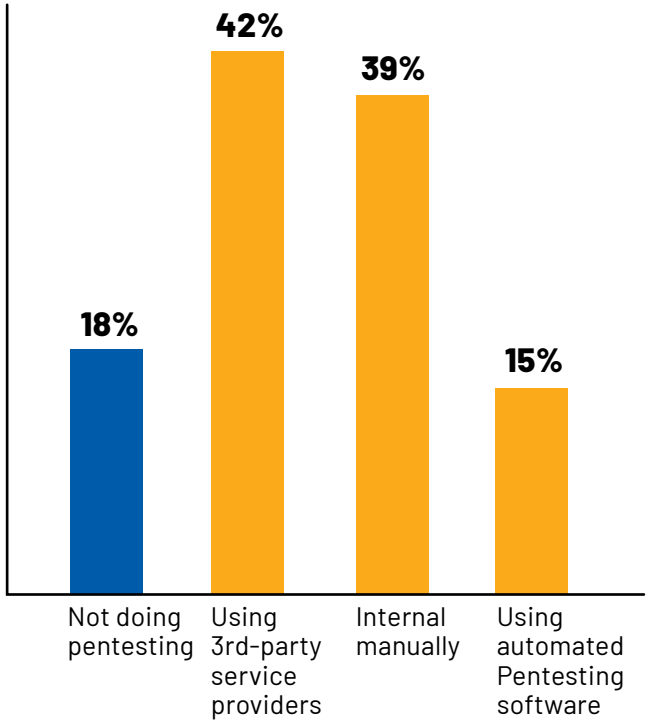


WHAT IS YOUR CURRENT ANNUAL BUDGET FOR *PENTESTING*?

SPLIT BY ORGANIZATION SIZE

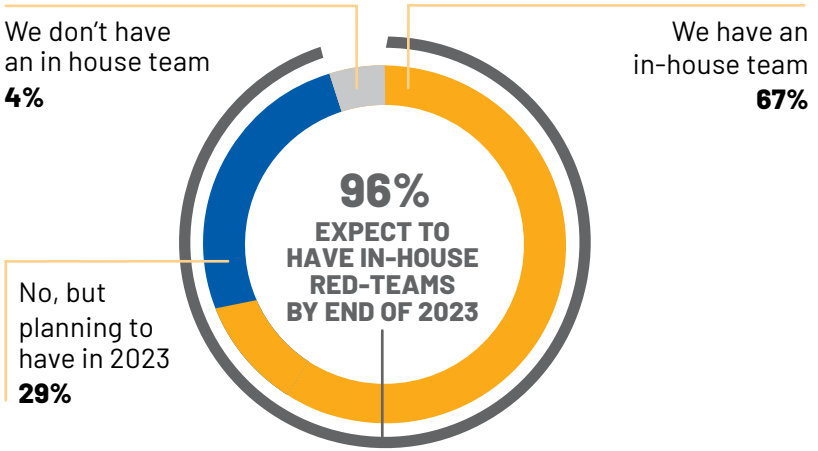


ARE YOU DOING PENTESTING TODAY?

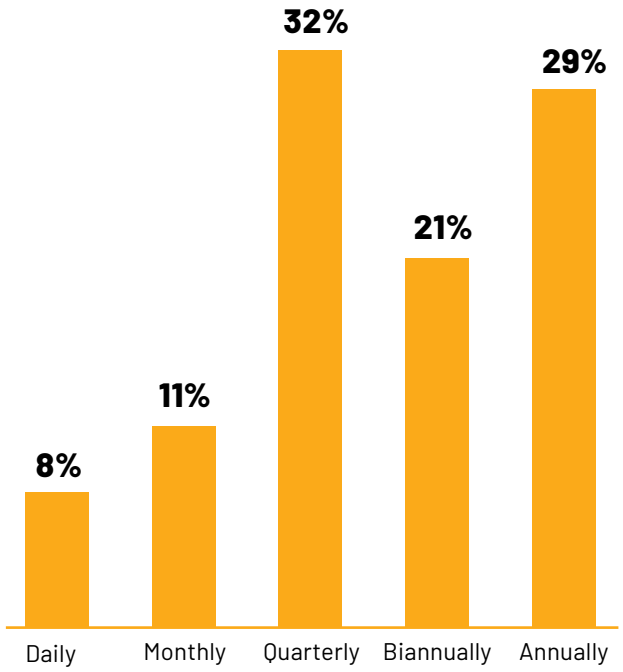


OVERALL, HOW COST-EFFECTIVE ARE YOUR MANUAL PENTESTING EFFORTS TOWARDS IMPROVING YOUR SECURITY OVER TIME?

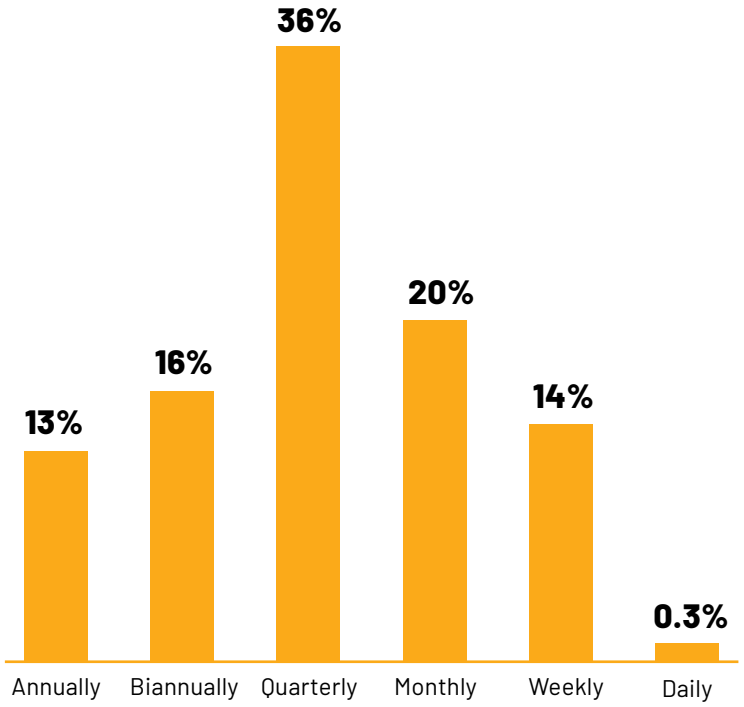
DO YOU HAVE AN IN-HOUSE RED TEAM OR PENTESTING TEAM?



HOW OFTEN DOES YOUR ORGANIZATION CONDUCT MANUAL PENTEST ASSESSMENTS?



HOW OFTEN ARE YOU ADDING/ SUBTRACTING ASSETS TO/FROM YOUR NETWORK?



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 and External), 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 category leader for Automated Security Validation, allowing every organization to test with ease the integrity of all cybersecurity layers, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited. **For more info, visit: pentera.io**