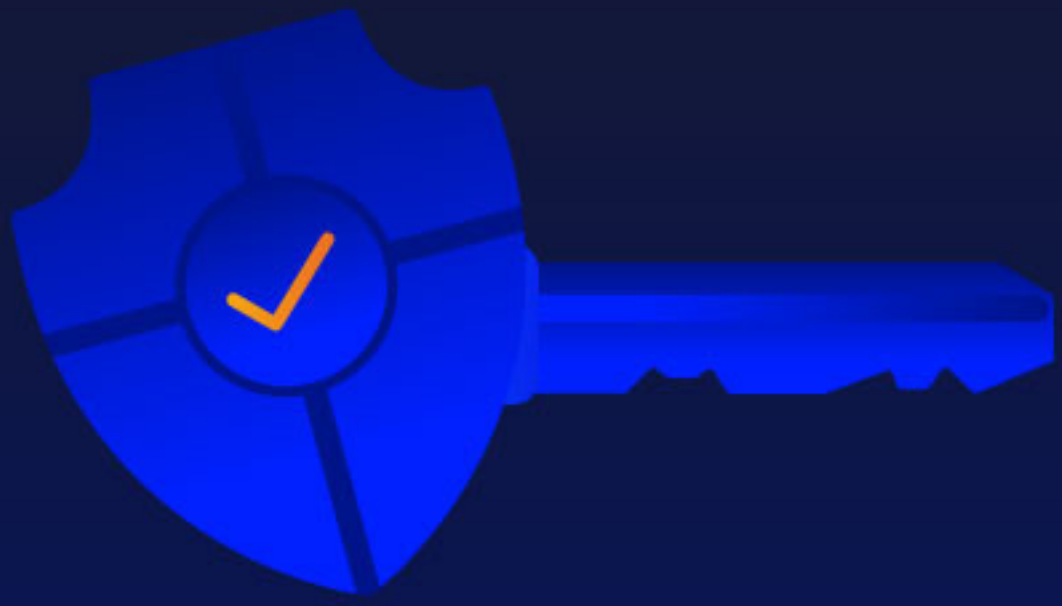
PENTERA

THE STATE OF PENETRATION TESTING

Global Research 2020



Survey Methodology & Respondent Demographics

In today's cyber threatscape, it's becoming increasingly clear that security validation of the network controls and processes must take center stage in the organizational cyber security strategy.

With penetration testing being the most common practice for validation, Cyber Security Hub and Pentera recently decided to field a survey to capture enterprise pentesting practices from cybersecurity project influencers and decision makers. Data has been collected from 55 enterprises that currently conduct penetration testing. The findings below are brought to you in their raw format for you to draw your own conclusions.

Executive Summary

Penetration testing is a common practice in various aspects of cyber security defenses.

It is mostly performed by 3rd parties or internal red teams and has evolved very slowly in the past decade. This survey clearly indicates the practice shortcomings and the need to scale and automate these tests while maintaining control of the activity's cost.

Forward Looking

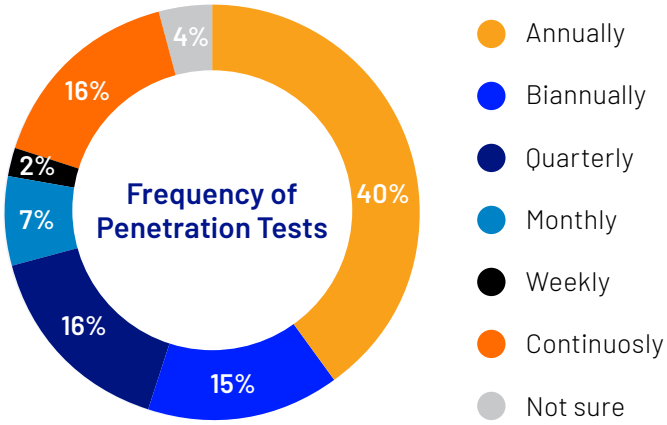
The technology-based solutions within the realm of vulnerability management and attack emulation that have been introduced in the past five years have reached a point of maturity. We've added an interview with Pentera Executive, Aviv Cohen, to provide an expert opinion of this trend along with pragmatic recommendations on how to advance the adoption of these technologies.

The "New Normal" Challenge

The current state of access and the inability of penetration testing teams to travel due to COVID19 related limitations raise the question of how organizations are going to continue to fulfill the need to test their infrastructure, whether for compliance requirements or as part of their ongoing risk management protocols. Remote penetration testing, without increasing exposure, is now essential.

Q1 How often does your organization conduct penetration tests?

55% of respondents run penetration tests only once or twice a year

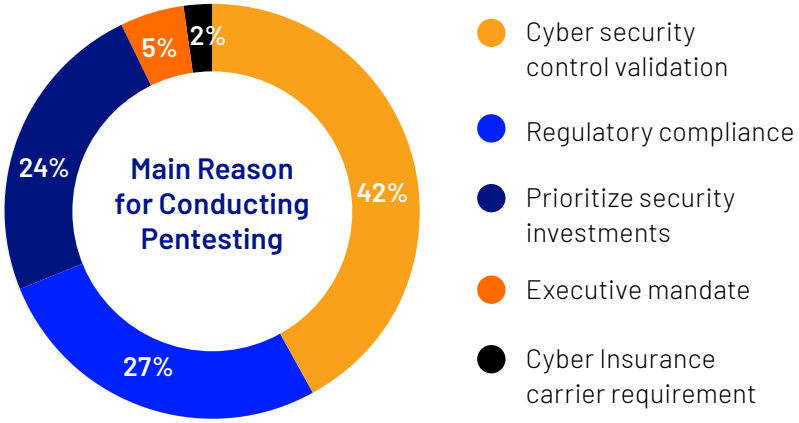


Insights

With penetration testing being the most common practice for validation, Cyber Security Hub and Pentera recently decided to field a survey to capture enterprise pentesting practices from cybersecurity project influencers and decision makers. Data has been collected from 55 enterprises that currently conduct penetration testing. The findings below are brought to you in their raw format for you to draw your own conclusions.

Q2 What is the main reason your organization conducts pentesting?

42% run penetration tests for security validation reasons



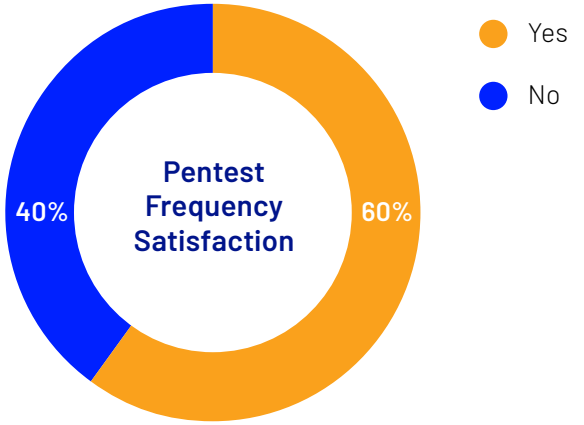
Insights

The results align with and highlight the market need to apply the attacker's perspective in security testing to validate that the controls in place are effective. Still, a fair part of the penetration testing investment is driven mainly by compliance.

What is uniquely interesting to see is the connection between penetration testing and its influence over security technology investment prioritization, shedding light on flawed architecture or missing controls.

Q3 Do you feel that your current pentesting frequency is sufficient?

40% of respondents feel their penetration testing frequency isn't enough



Insights

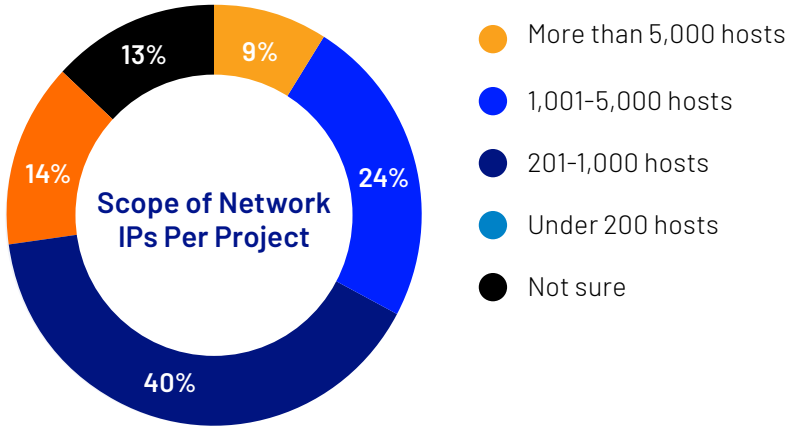
The findings correspond with the feedback we received from cross-vertical conversations stating the need for increased penetration testing frequency in view of the dynamic nature and the number of changes in a modern IT network.

60% of the responders who said penetration testing frequency is sufficient either have an internal red team in place or plan to build one in 2020. This emphasizes the need to continuously test security controls and the inability to budget for more external penetration tests at the current market price.

It's safe to assume that in times of remote work and access limitations, the frequency of manual penetration tests will decrease. Hence increasing the need for an automated solution that can run remotely.

Q4 What is the scope of network IPs you test within a typical pentest project?

54% test less than 1,000 hosts in each pentest run

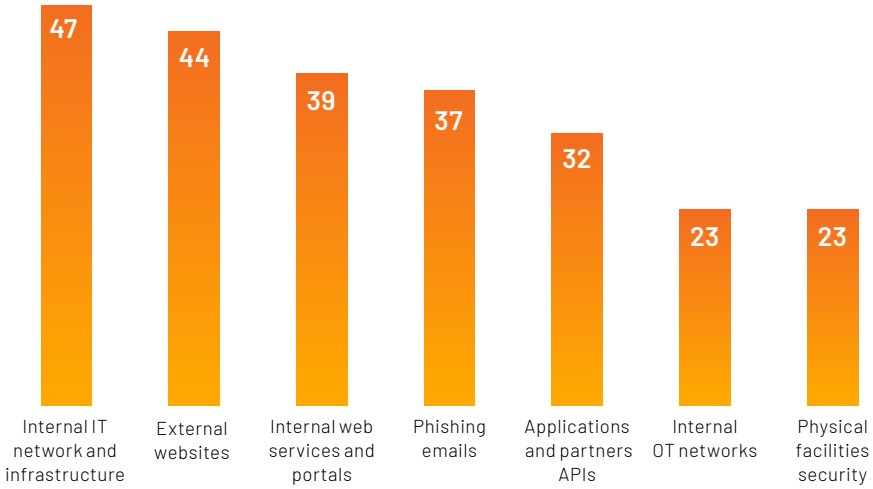


Insights

Limited in scope and time and based on available budget, this makes penetration testing a "sampling" exercise in its innate services nature of billable hours. It's interesting to think about automation changing this reality and providing 100% penetration testing coverage over a much wider designated test scope. This is particularly necessary when you think of how much the attack surface has grown and how many attack vectors and tools have been created in the past decade.

Q5 The scope of your current pentesting includes:

Internal IT networks are the first priority for penetration testing, followed closely by external website testing



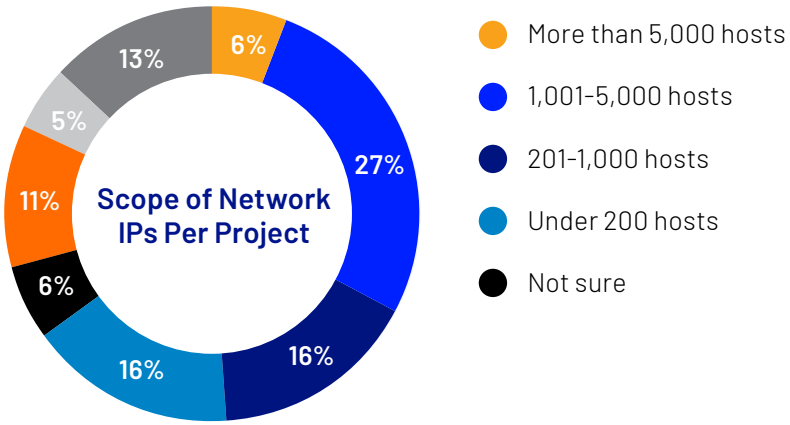
Insights

In an "assume breach" era, it's not surprising that testing the network is top priority. With that in mind, it's clear that security professionals are aware of other elements of the attack surface and want to find ways to test all its components.

In today's world of remote work, the attack surface has grown tremendously allowing for more attack vectors. On the other hand, protecting the organizational crown jewels, in the shape of critical assets, remains the primary goal, increasing the need to validate the internal network security controls as the last line of defense.

Q6 What is your estimated annual pentesting budget?

Close to 50% of respondents have sub $100,000 penetration testing budgets



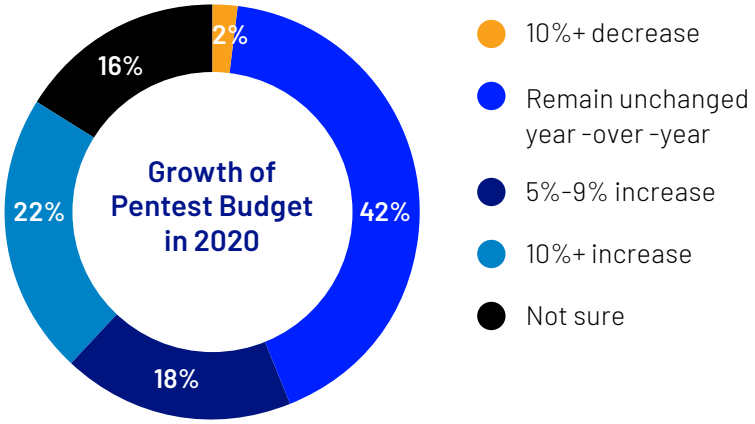
Insights

There's a clear correlation between the size of the organization and size of the pentesting budget. With a more segmented look, the data shows that in regulated industries, such as finance and healthcare, there is a higher level of security testing "maturity", backed by a relatively higher budget allocated to penetration testing.

It is clear from the data that small to medium enterprises cannot afford an increased spend concurrent with the threat or the attack surface growth. This significant gap will probably find it's solution either with technology or with a managed services approach.

Q7 By how much will the pentesting budget change in 2020?

40% of organizations will have increased their pentesting budget by more than 5% in 2020



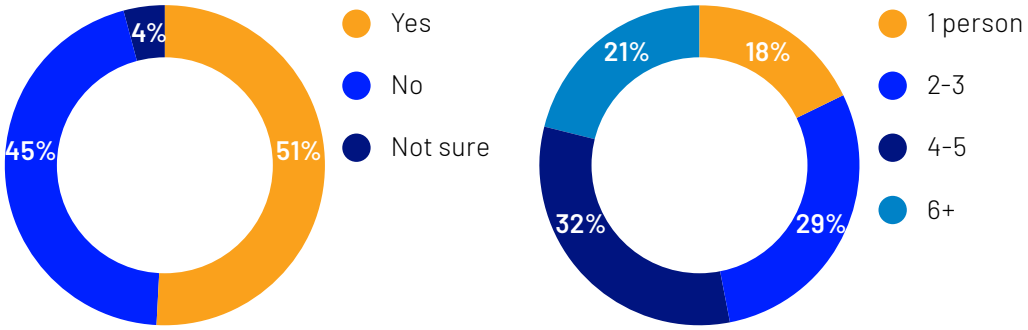
Insights

The results align with the market research indicating the penetration testing market will have a Compound Annual Growth Rate (CAGR) of 21.8% by 2025 in accordance with MarketsAndMarkets Global Penetration Testing Forecast from 2020-2025.

This growth in penetration testing budget can also be explained by the increasing number of breaches indicating that security control misconfigurations, confused policies, wrongful privileges and weak credentials are the real causes of most breaches. In other words, it's becoming clear that the human factor is the prime reason for a breach. Validating the effectiveness of the security technology stack is a crutial step before venturing into further acquisitions.

Q8 What is the scope of network IPs you test within a typical pentest project?

51% of respondents have an in-house red team



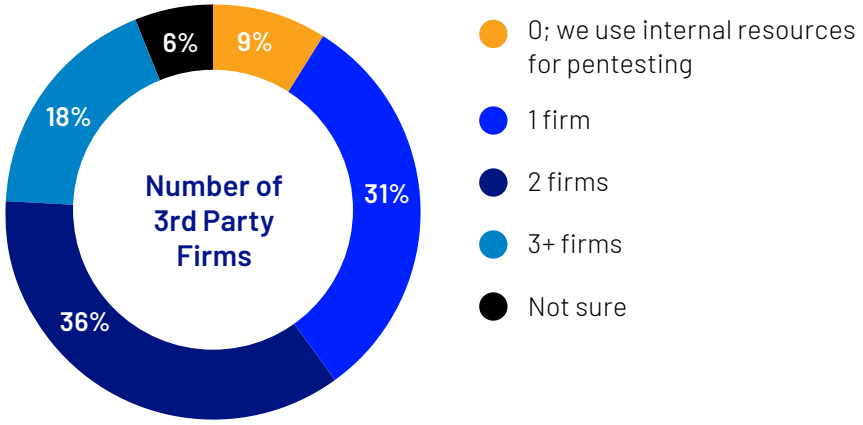
Insights

As the threat landscape changes, organizations recognize the need to continuously validate their security controls, and turn to red team activities as part of their in-house validation cycle.

Taking an in-house function indicates that this practice cannot scale economically if consumed as a service.

Q9 How many 3rd party pentesting consulting firms does your organization use?

54% use two or more firms to run their pentesting activity



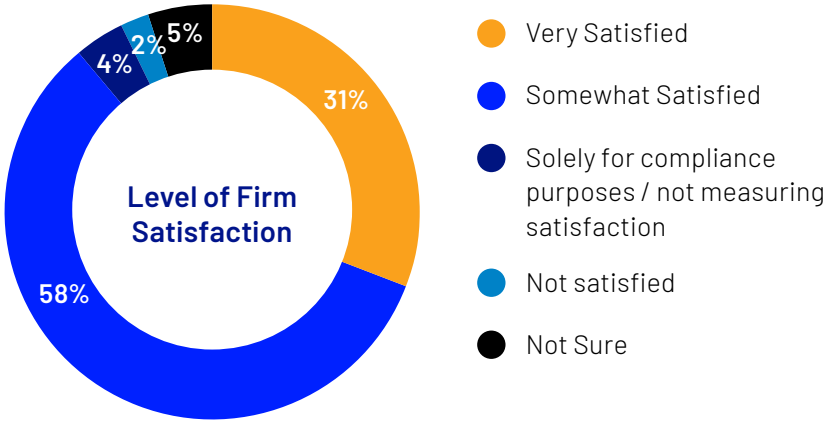
Insights

Organizations are often required to replace pentesting companies by their auditing teams. However, from conversations with prospects, the main reason seems to be the need to test various components while the pentesting company often has a specific expertise. The use of various firms allows organizations to reach a wider range of testing capabilities.

The issue is, of course, that this creates little consistency and the testing cycle which, on paper, is annual becomes much longer.

Q10 How satisfied are you today with your primary pentesting firm?

58% of organizations are only somewhat satisfied with their pentesting firm



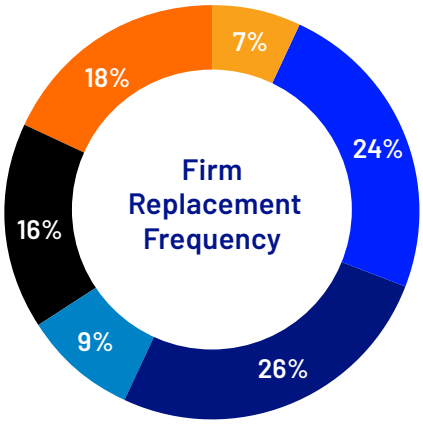
Insights

Dissatisfaction with a firm is usually linked to dissatisfaction with the cost benefit in relation to the provided results. There are many costs, some of them hidden, that accumulate when onboarding a firm - payment, project management, 3rd party vulnerabilities, remediation management and others. Some complaints might also have to do with level of expertise, reporting processes or remediation recommendations.

The majority of organizations that marked themselves as satisfied with their pentesting firms have internal red team personnel. This could be an indicator of the amount of resources needed to successfully run manual security testing and how automation can improve team productivity and reduce costs.

Q11 How often do you replace your primary pentesting firm?

57% of organizations change penetration testing firms at least every 3 years

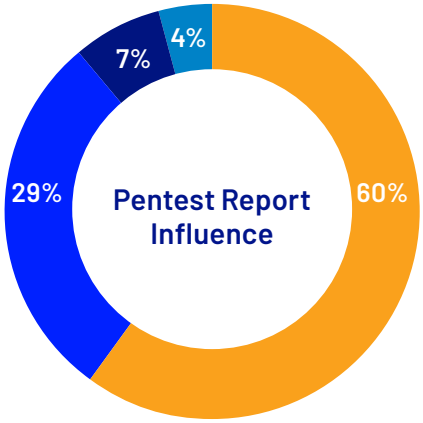


Insights

There are many hidden costs in hiring 3rd party firms, mainly in sourcing and managing them. Organizations need to allocate internal resources to find the best firms, ensure the pentests are run properly and that reporting is sufficient. When multiplying this by many firms and the frequency of which firms are replaced, due to dissatisfaction with the performance, the overhead becomes disproportionate.

Q12 How much does the pentesting report influence your decision making?

29% state that the pentesting report drives decision making at the highest levels

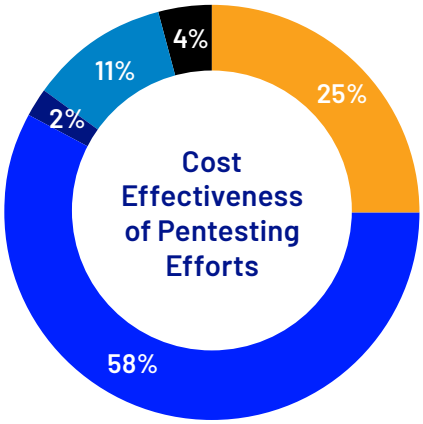


Insights

It's clear that penetration testing has an influence on the cyber security strategy and decision making process. After all it provides an independent test against a skilled "challenger" actor. Incorporating automation and increasing the cadence of testing, will establish a cyber posture benchmark that will allow reporting to further improve over time.

Q13 Overall, how cost-effective are your pentesting efforts towards improving your security posture over time?

Only 25% of organizations have stated that their penetration testing efforts are effective

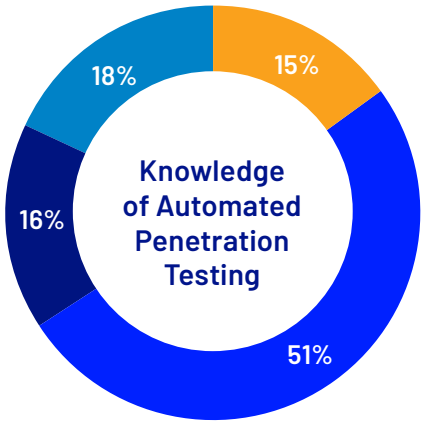


Insights

As seen throughout the survey, most organizations that are satisfied with their pentesting activities, and find them cost effective, also have internal red teams. This again shows the level of resources needed to effectively run security testing and the role automation can play in increasing its cost-effectiveness.

Q14 Have you heard of Automated Penetration Testing?

18% of respondents are currently using automated pentesting technology



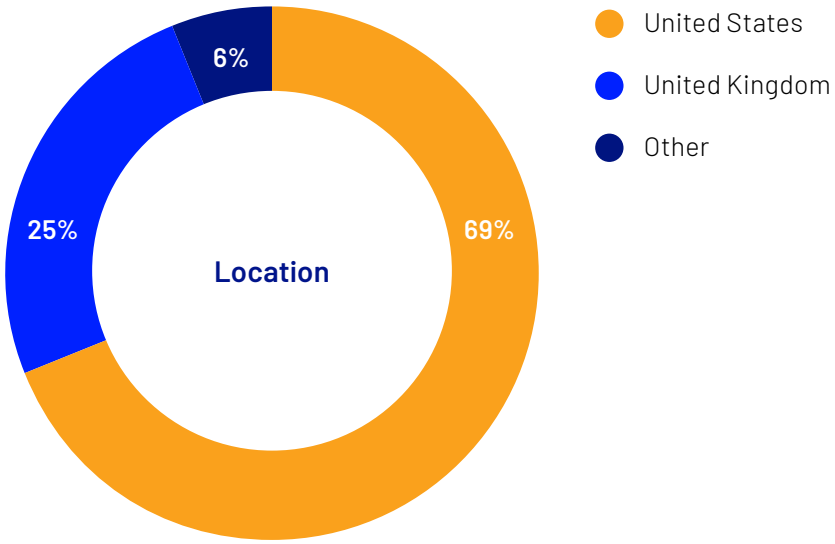
Insights

This is a strong indicator of a shift in the mindset of security professionals from assuming security measures are set up properly to proving they are and measuring their effectiveness.

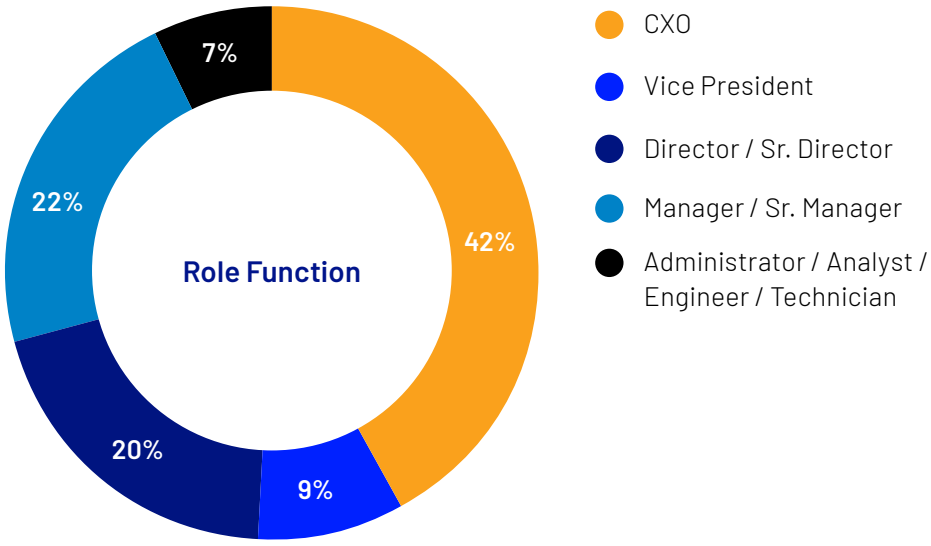
In today's work-from-home (WFH) era, with many home devices logging into the corporate network, the need to continuously pentest seems more important than ever.

Methodology and Demographics

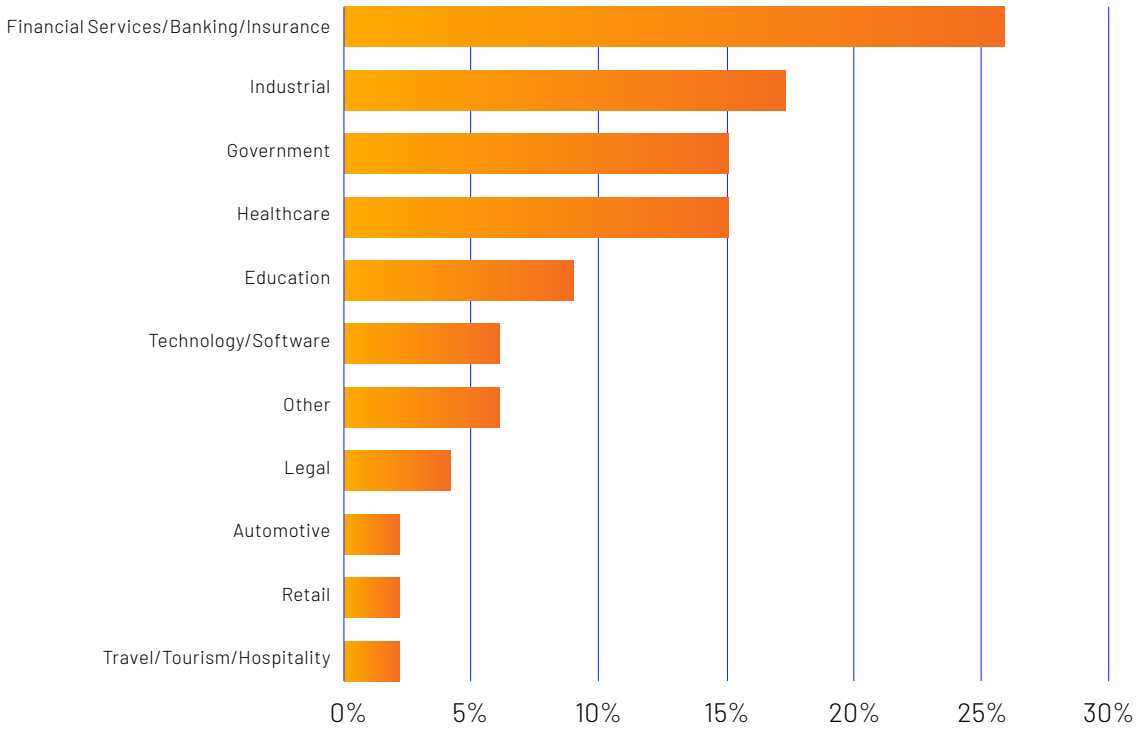
Security professionals in the United States and United Kingdom were the primary target regions of the survey. Responses were received primarily from the U.S. (69%) and U.K. (25%). 6% of the respondents came from an additional 14 countries.



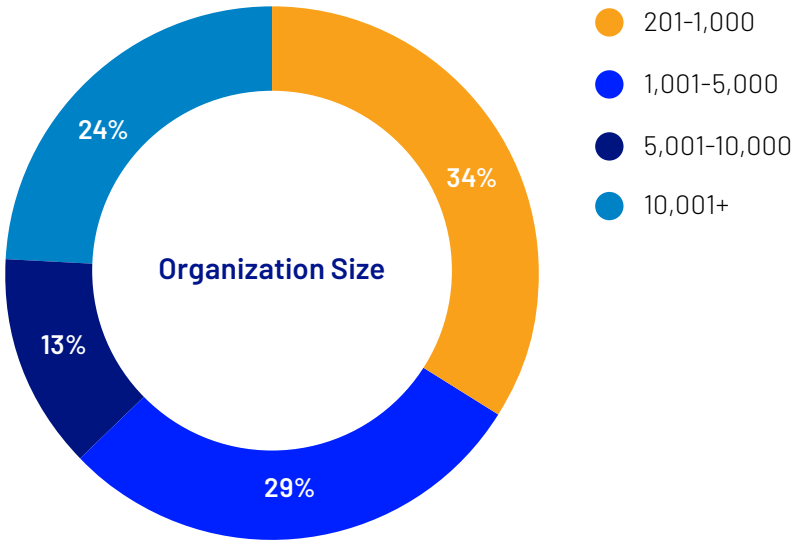
Enterprise cyber security influencers and decision-makers have a variety of roles in their organizations. 42% of the respondents have an executive position, such as CISO or CIO, while 29% said they serve in a Vice President or Director role.



The largest segment of security professionals completing the survey represent the Financial Services / Banking / Insurance industry (26%) followed by Industrial sectors (17%), Healthcare and Government/Public Sector/Military (15%) and Education (9%). Approximately 94% of respondents are associated with one of the 10 identified industries.



24% of respondents are from organizations with more than 10k employees while the majority of enterprises (63%) span two organization sizes: 201-1,000 and 1,001-5,000.



Executive Q&A

An Interview with Aviv Cohen, CMO Pentera

Q

What are the main motives driving enterprises to automate their penetration testing?

A

As seen in this survey, but also from talking to many security executives, it's clear that the need to increase the cadence

and scope of security testing is imminent. It's the only way to survive and prioritize investment and remediation with today's budgetary dynamics.

Let's do the math - the threat landscape is evolving, the pace of change in IT networks and cloud is increasing, yet the budgets are at a stand still or growing moderately. The net effect of this is that security executives today understand that without security testing automation, it's impossible to validate the entire scope of network controls and processes.

Q

How does automated penetration testing apply to compliance? their penetration testing?

A

Compliance revolves around a set of regulations and standards an organization needs to adhere to with the intent that following these guidelines will help maintain the integrity of private personal consumer data as well as the business operations. If you look past the checkboxes, by continuously testing the efficacy of network controls, an organization can, in fact, make sure its security controls consistently comply with regulations.

Automated penetration testing provides on-demand reporting of the organization's cyber posture. While compliance regulations might still require the annual 3rd party pentest, by running continuous testing, an organization can ensure its held to the highest standard at all times. For example, PCI-DSS penetration testing requirement 11.3.2/3 can be 100% catered for by automated penetration testing.

Q

What primary use cases should security professionals considering automated penetration testing lean on to get the organization's buy-in?

A

There are several use cases for implementing automated penetration testing:

1. First and foremost is validating that the security controls are working as designed, justifying past large investments in security products by making sure they are effective.

2. The second use case is prioritizing remediation on what is a 100% exploitable vulnerability or weakness, lacking effective compensating control. I have yet to meet an organization that has enough resources to remediate all their vulnerabilities. Automated penetration testing assures you focus on the 10% of vulnerabilities carrying 90% of the risk.

3. The third use case is increasing the red team or purple team productivity. Tests need to be done, but the talented red team professionals should focus on the unique application and other bespoke or more exotic tests, while a software can take away most of the repetitive mundane work.

4. The fourth use case worth mentioning has to do with change management, whether it's system migration, cloud adoption or digital transformation. Every change creates exposures and the ability to continually test throughout a multi-month process assures there are no exposures and cross-talk between systems.

5. The fifth common use case has to do with testing partners or businesses prior to acquisition and integration. Cyber security is determined by the weakest link and sometimes that link is actually in another organization. Applying machine-based penetration testing to the process is inexpensive and can be done in hours.

In summary, the survey shows that pentesting automation technology is here but not yet known by and familiar to more than 50% of security professionals. My hope is that the trend will continue to pick up to allow people to move forward and become more cyber-resilient than before.

About Pentera

Pentera delivers Pentera, the automated network penetration-testing platform, that assesses and reduces cybersecurity risk. The platform runs on the Cloud or on-site to identify, analyze, and focus remediation efforts on vulnerabilities. Hundreds of security professionals and service providers around the world use Pentera to perform continuous machine-based penetration tests that improve their immunity against cyber-attacks across their organizational networks. www.pentera.io

PENTERA

Learn more at www.Pentera.io

Book A Demo By Clicking Here