HEXWAY

Why traditional pentesting approach doesn't keep pace with the times

Introduction

Nowadays, when the number of cyberattacks is increasing every day, and the value of vulnerability detection or prevention dramatically enhances, leading companies request a complex approach to providing cybersecurity audits.

The traditional penetration testing process implies that, as a result, clients get "an imprint" of the cybersecurity environment of specific products/hostnames/IPs. This information becomes obsolete right after it is obtained. This is grossly inadequate, considering the needs of the modern cybersecurity market.

If you, as a pentest service provider, want to move with the times and attract more clients, you have to offer more benefits and underscore your advantages as a security service provider. Transform your one-time clients into regular customers by adding PTaaS to the list of your capabilities. In this research, we will spotlight cybersecurity market demands and explain why you need to change.

Table of content

CHAPTER 1

Traditional pentest: How it works

According to Pcysys research[1]

55%

of enterprises that use penetration testing services run them only once or twice a year.

40%

of enterprises feel their penetration testing frequency is insufficient.

58%

of enterprises are only somewhat satisfied with their pentesting firm.

71% of organizations think pentesting is essential for their security posture

This data shows us that companies are getting more serious about their cybersecurity. The Core security research[2] indicates that 71% of organizations think pentesting is essential for their security posture. Companies are ready to increase pentest frequency and choose new providers of pentest services. And do not forget about companies that will conduct pentesting for the first time due to transitioning to remote work and universal digitalization.

Pentest companies should be able to prove their benefits to both types of clients: seasoned or not. Competition for clients has just begun.

The typical pentest process from planning to report writing takes about 6-7 weeks

As for the fixing stage, on average, it can take 3-4 weeks

2-3 weeks
planning stage

1-2 weeks
execution stage

1-2 weeks
analysis and report writing

1 day
presentation of findings

1.5 month

wait for pentesting results

1 month

remediating stage

Imagine you are a company that takes care of your cybersecurity. You need to maintain cybersecurity resilience and be flexible to react to possible vulnerabilities.

At the same time, you have to wait for pentesting results for about 1,5 months. After that, you spend about 1 month remediating it, while new vulnerabilities can happen continuously.

Sounds weird, doesn't it?

CHAPTER 2

Cybersecurity trends

AustCyver[3] predicted that global spending on external cybersecurity products and services will increase by 8.4% annually.

We want to explain what is the basis for this growth and emphasize the main 5 cybersecurity market trends

Five cybersecurity market trends

$6 trillion — cybercrime expected damage

1. A significant increase in cybercrime harms' cost

Cybersecurity Ventures[4] expects global cybercrime to inflict damages totaling **$6 trillion** globally in 2021.

2. Forestalling cybersecurity risks

Methods that hackers use are improving day by day. Companies that want to avoid critical data breaches and everything related to it need to be more proactive in order not to lose money from the previous item.

The price of fixing consequences is much higher than the price of prevention.

predictive security cloud gained a 261% ROI

3. Cloud migration

More and more companies are beginning to use cloud solutions. That comes with new possibilities to be hacked, and consequently – a new cybersecurity field – cloud security. To understand the scope, Finance Online[5] found that predictive security cloud gained a **261% ROI** in the last three years.

4. Extensive introduction of AI and ML

Many companies hope for AI (Artificial intelligence) and ML (Machine Learning) to decrease the number of successful attacks and provide a consistent quality of response. It's impossible to cover all cybersecurity only with a human resource without automation. As well as AI and ML can't carry out all the pentest stages without human intervention. Cybersecurity these days is more complicated and requires complementarity between handwork and automation.

100%
of large enterprises

5. Complexness and agility

Based on the foregoing, pentest clients have to be ready to react at any time. For it, they should have real-time information from plenty of sources in a single view. Also, this information should be easy to interpret and convert to an action plan.

Gartner[6] claimed that by 2020, **100%** of large enterprises were asked to report to their board of directors about cybersecurity and technology risk at least annually. Therefore, reports should be understandable for any level at the customers' company.

Five cybersecurity market trends

And the cherry on the top of these cybersecurity trends – a lack of professionals that influences both sides of the pentest process. The demand for high-quality cybersecurity specialists considerably exceeds the supply in the rapidly growing cybersecurity market.

CHAPTER 3

What Customers need

It is no surprise that clients want to reduce costs and enhance the quality of the services received. This is too obvious to stop there. Let's take a closer look at the details.

30%

of a CISO's effectiveness will be measured by the ability to create value for the business.

Gartner[7] showed that by 2023, 30% of a CISO's effectiveness will be directly measured by the ability **to create value for the business.** It means that if you want to attract more clients, you need to think in terms of benefits for clients' business.

Daniel Kennedy[4], research director for information security and networking for 451 Research, said that customers need **to identify problems during the software development** lifecycle before a new product is released. It's all about the price of mistakes – if you detect vulnerabilities after your product is released, you'll lose more money.

60 times

more expensive to fix a vulnerability if it makes it into production

Ajay Arora[4], a founder of BluBracket, maker of a security tool for code, has estimated that "it's **60 times more expensive** to fix a vulnerability if it makes it into production than if it were caught earlier in the development cycle". In our opinion, this argument looks very convincing.

To meet the demands of time, your pentest company needs to offer the following solutions for the client:

Provide an opportunity to coordinate a penetration test

We know that this point sounds grisly for pentesters because usually, it means that clients can distract you. But in case you ensure the transparency of the process, clients will cooperate with your team, not bother.

57%

of organizations change penetration testing firms at least every 3 years

Provide access to aggregated vulnerability information

As the frequency of pentests increases, more and more data appears. Customers need to analyze it.

Pcysys research[1] shows that **57% of organizations** change penetration testing firms at least every 3 years. It's inevitable, however, if you deliver a structured and detailed view of the process, they will return to you more likely.

Establish a process so the client can fix vulnerabilities faster

This item should manifest in timely information about critical vulnerabilities, automation routine tasks, an easy transformation of your data into an action plan, and more.

The fixing process is a necessary stage in the development process, and, therefore, the faster bugs will be fixed, the faster a product will be released.

We tried to cover the main customers' pain points, nevertheless the most important is to hear your clients' needs and make efforts to solve their unique problems.

CHAPTER 4

What is wrong with modern pentest approaches?

To summarize all of the above, let's list the disadvantages of traditional pentests, which have been extensively described in the Cobalt research[9]:

Disadvantages of traditional pentests

1. Too much time is spent on the planning stage
2. No information until the final report
3. Long response time
4. Inaccuracy and incompleteness of results
5. Lack of transparency in the project
6. Non-actionable results
7. Security and development teams aren't synchronized
8. Inflexibility – limited optimization or automation opportunities
9. Expensive in comparison with other offers

And so on...

Automation, red team, and agile development create a challenging future for pentesters. In this changing environment, pentesters must adapt to remain relevant.

The crucial angle with the traditional approach that it can't match the modern development approach when product updates could be released daily or weekly. Our time asks for continuous and reliable methods of maintaining the proper safety level from pentest companies

CHAPTER 5

Possible ways to adapt and transform pentest organizing approaches

We've considered the market environment around cybersecurity services our days.

Let's look at **3 ways companies try to deal with** the discrepancy between modern market requests and the usual conduct of the pentest

Using task manager programs

We agree that task management tools like Jira, Youtrack, Trello, and the like are a really good way to streamline some project management processes. But at the same time, such platforms are not cut out for a unique penetration testing process that has a lot of specific aspects like import scan results, creating reports, real-time connection between clients and pentesters, etc.

Through these half-solutions, you still need to customize features or add other external plugins to tailor your needs. As a result, money and time are wasted, and the number of Slack chats continues to rise without stopping.

Automating routine tasks

Also, you can use tools that cover only a bit of the whole penetration testing process. For instance, the least favorite part of pentest - creating a report. Let's imagine that you bought the tool that focuses on report generation.

At first glance, you save time, avoid routine tasks, and you and your team should be happy. But it appears that your clients aren't happy because their companies still have to wait for the report till the end of the pentest and put efforts into converting your report to the action plan. As a consequence, you had optimized the process on your side but didn't answer the client's demands.

Creating own pentest management platform

Several companies find the courage to develop a pentest platform by themselves. We respect their choice but can't understand why to reallocate resources from the main goal - providing high-quality pentest service to creating and maintaining the platform.

This way is long and expensive. Is it worth it? Especially when you consider the other existing solutions which are quickly built into the pentest process.

CHAPTER 6

PTaaS (Penetration testing as a Service)

PTaaS helps companies implement the continuous penetration testing process. The main features of this service are scalability and profitability. Penetration testing as a Service fits in the ongoing development process and other flexible approaches that require continuous testing.

Apart from displaying the actual pentest data, PTaaS simplifies for customers supporting the work of their systems by delivering information when each step is implemented.

5 practical advantages of the PTaaS platform for both sides

1. Run more projects simultaneously due to routine optimization
2. Manage project data (import, export, interact) in a convenient way
3. Enhance the performance with the tool that cut out specifically for pentesting
4. Deliver high-quality results to the clients promptly
5. Easy to get into the development process

PtaaS platform features

To ensure the integrated approach, each PtaaS platform should have the following features that were perfectly described by Cyver[10]

1. Scanner tool connections and advanced import possibilities
2. Comprehensive knowledge base of Issues
3. Client portal that is specific to convenient pentest management
4. Customizable report generation feature
5. Project management capacity like creating tasks and notes, assigning a responsible person, setting notifications, etc.

+35%

of revenue by providing PTaaS delivery model

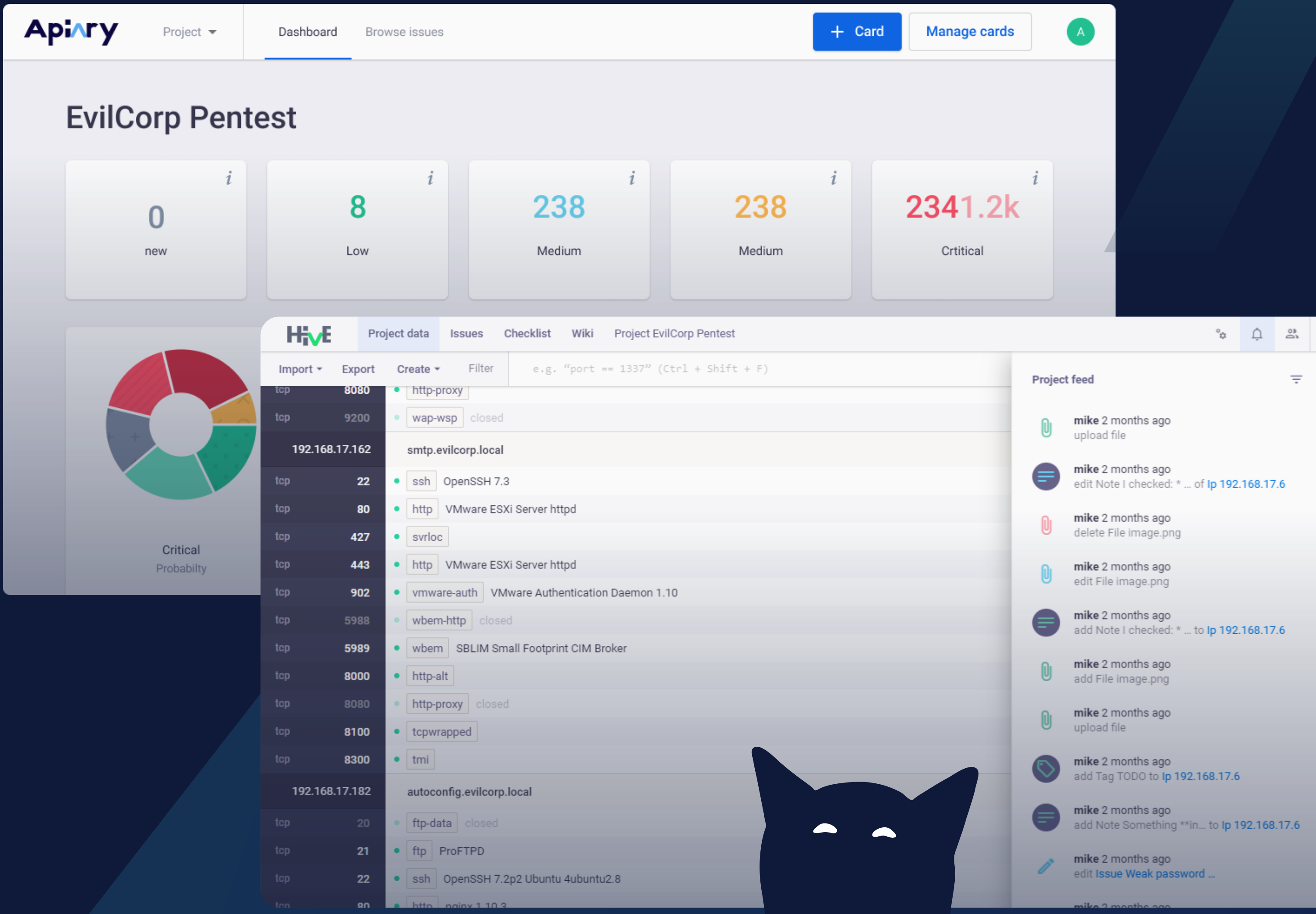
96%

higher ROI than traditional pen testing

Moreover, as NetSPI estimated[11], they earned +35% of revenue by providing PTaaS delivery model. It was the argument for you, and one more important proof for your clients that was calculated by Cobalt[12] — PTaaS model has a 96% higher ROI than traditional pen testing.

CHAPTER 7

Our solution: Hexway Platform



Apiary · Project · Dashboard · Browse issues · + Card · Manage cards · A

EvilCorp Pentest

0	8	238	238	2341.2k
new	Low	Medium	Medium	Crtitical

Critical · Probabilty

HIVE · Project data · Issues · Checklist · Wiki · Project EvilCorp Pentest

Import · Export · Create · Filter · e.g. "port == 1337" (Ctrl + Shift + F)

tcp	8080	http-proxy	
tcp	9200	wap-wsp	closed
192.168.17.162		smtp.evilcorp.local	
tcp	22	ssh	OpenSSH 7.3
tcp	80	http	VMware ESXi Server httpd
tcp	427	svrloc	
tcp	443	http	VMware ESXi Server httpd
tcp	902	vmware-auth	VMware Authentication Daemon 1.10
tcp	5988	wbem-http	closed
tcp	5989	wbem	SBLIM Small Footprint CIM Broker
tcp	8000	http-alt	
tcp	8080	http-proxy	closed
tcp	8100	tcpwrapped	
tcp	8300	tmi	
192.168.17.182		autoconfig.evilcorp.local	
tcp	20	ftp-data	closed
tcp	21	ftp	ProFTPD
tcp	22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8
tcp	80	http	nginx 1.10.3

Project feed

mike 2 months ago
upload file

mike 2 months ago
edit Note I checked: * ... of Ip 192.168.17.6

mike 2 months ago
delete File image.png

mike 2 months ago
edit File image.png

mike 2 months ago
add Note I checked: * ... to Ip 192.168.17.6

mike 2 months ago
add File image.png

mike 2 months ago
upload file

mike 2 months ago
add Tag TODO to Ip 192.168.17.6

mike 2 months ago
add Note Something **in... to Ip 192.168.17.6

mike 2 months ago
edit Issue Weak password ...

You don't need to waste your time on creating your pentest management platform. We have already made it for you according to the clients' and market's needs.

Using the Hexway platform, you can:

1. Consolidate the team in a single environment enhances
2. Use a comprehensive knowledge base with plenty of checklists' and reports' templates
3. Import data from popular scanners directly to the platform or using custom rules
4. Interact with the project data by using an advanced filters system
5. Create reports and delivery them to the clients

And so on...

You can learn more about Hexway benefits and features on our website.
To test the platform: try out the online demo version of Hexway Hive and Apiary.
Or contact us with any questions, proposals, and feature requests.

References

1. The State of Penetration Testing Global Research 2020
2. Prioritizing Pen Testing: 2021 Survey Results
3. Australian Cyber Security Growth Network, SCP - Chapter 1 - The global outlook for cybersecurity, 2020.
4. Cybersecurity Ventures, Special Report: Cyberwarfare In The C-Suite.
5. 10 Cybersecurity Trends for 2021/2022: Latest Predictions You Should Know
6. Gartner, Cybersecurity and Digital Business Risk Management
7. Gartner, How Security and Risk Leaders Can Prepare for Reduced Budgets
8. TechBeacon, 10 application
9. Cobalt, Analyst Research: Pentest as a Service Impact Report 2020
10. Cyver, How Pentest-as-a-Service Delivers Scaling & Growth
11. NetSPI, NetSPI Celebrates 35% Organic Revenue Growth in 2020
12. Cobalt, ROI of Pentesting as a Service