PENTERA

Presentazione per:

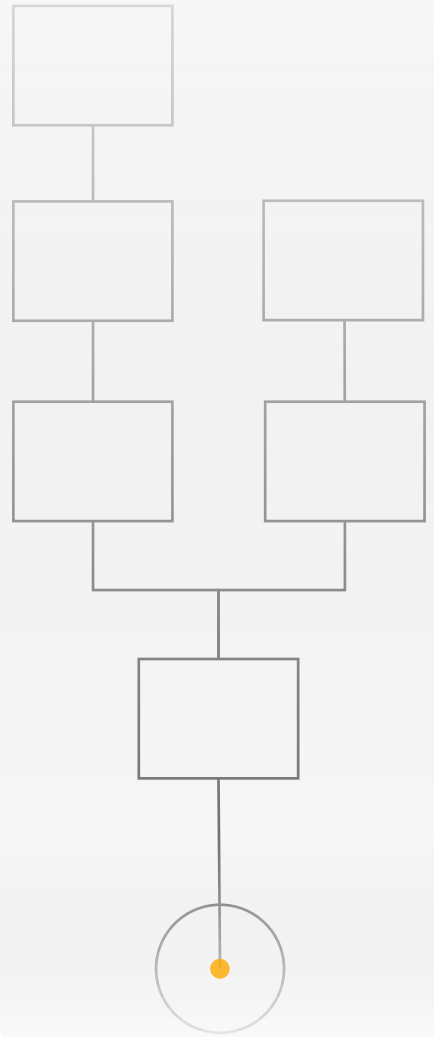
Il Penetration test automatizzato come ausilio all'analisi e alla gestione del rischio operativo aziendale

- Paolo Bufarini - Regional Sales Manager Italy & Malta – Pentera Security Ltd.

 © Pentera

Sommario

- La portata della trasformazione digitale nelle aziende e nelle organizzazioni governative comporta anche un'enorme espansione della superficie attaccabile da parte degli hacker.
- Che si tratti di minacce note o sconosciute, essa introduce importanti lacune nella sicurezza che non si riescono a colmare con i tradizionali approcci incentrati sulla sola verifica delle vulnerabilità note.
- Al giorno d'oggi l'unico modo per salvaguardare efficacemente un'impresa da incidenti di cybersecurity è condurre test di penetrazione comprensivi, continuativi e basati sull'intera infrastruttura dell'ambiente informatico delle aziende per identificare le vulnerabilità sfruttabili e porvi rimedio in modo conveniente e nel tempo minore possibile.



© Pentera

Answering the Question

DO YOUR CYBER DEFENSES TRULY WORK TODAY

Against The Latest Threats?

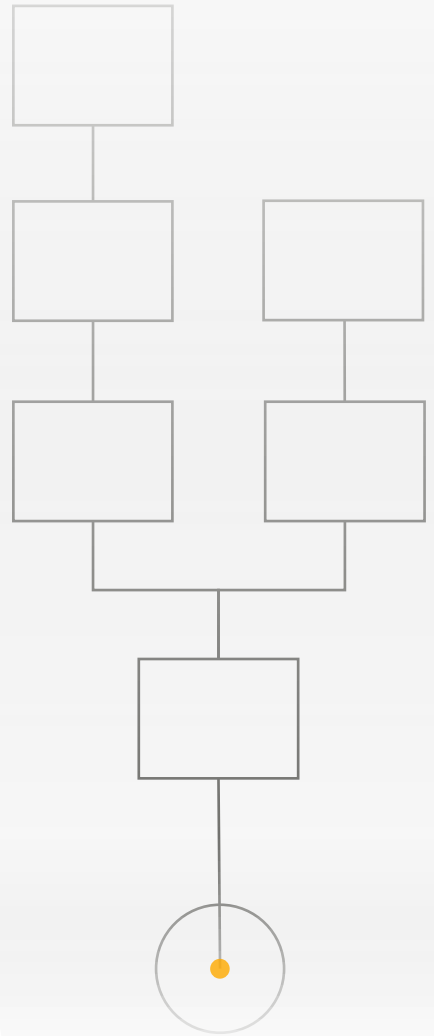
EDR | NDR | EPP | SIEM | WAF | FW | SOAR | ...

 © Pentera

Chi è Pentera?

Automated security validation Platform .

To tests and improve Security Posture and immunity against cyberattacks across organizational networks.



© Pentera

PENTERA

OUR VISION

Becoming the World's Cyber Risk Validation Authority

OUR MISSION STATEMENT

Improve our customers security readiness against cyber threats by emulating adversary attacks

PENTERA Security Ltd.

Profilo aziendale

© Pentera

PENTERA

La storia della fondazione

CTO

Arik Liberzon

Esperto di sicurezza informatica offensiva, che ha prestato servizio per 15 anni presso l'IDF, guidando un'unità d'élite e difendendo le risorse più strategiche di Israele.

"

Dopo aver guidato centinaia di progetti di RED TEAM lavorando con pen tester d'élite, mi sono reso conto che il software, se costruito in modo intelligente, potrebbe fare un lavoro molto migliore nel pen-testing rispetto agli umani ..."

... abbastanza presto, i miei compagni di squadra dell'IDF hanno iniziato a unirsi a me a Pentera, per comporre uno dei migliori team di ricerca informatica al mondo!

PENTERA

La storia di successo

$ 150 MILIONI ROUND C FOUNDING ... ORA SIAMO UN UNICORNO!

 © Pentera

PENTERA

Apprezzata ed adottata in tutto il mondo

2015
Founded

>220
Employees

$190M
Funding

Financial Services
15%

Healthcare & Pharma
13%

Cybersecurity & MSSP
12%

Services & Consulting
8%

19
Verticals

45
Countries

>530
Customers

PENTERA

Alcuni dei principali clienti in Italia

 © Pentera

PENTERA

Tuttavia, le voci dei clienti

Contano di più

Automated Security Validation Platform

★★★★★

Pentera received **4.8/5.0 SCORE** in Gartner Peer Insights 2021

"

The Next Generation Vulnerability Scanner

This is a new kind of vulnerability scanner. It's almost a human pentester working at computer speed. It finds lots of vulnerabilities faster than I could dream doing it myself.

Customer Review,
Gartner Peer Insights, Dec 2021

"

Pentera helped us shift from the focusing on vulnerabilities to remediations

- *The Ransomware Ready module opened our eyes to actual weaknesses and risks we were not aware of*
- *Remediation priority help us reduce risk and validate that fix made solved the problem*

Customer Review,
Gartner Peer Insights, Dec 2021

"

Security validation that by far better than all legacy breach simulation tools

Major focus area for us was to understand our attack surface - both that inside and our external facing. we tested several tools and the "all-in-one" solution Pentera had outmatched all other point tools in the market today.

Customer Review,
Gartner Peer Insights, Dec 2021

PENTERA

LA CONTINUA SFIDA

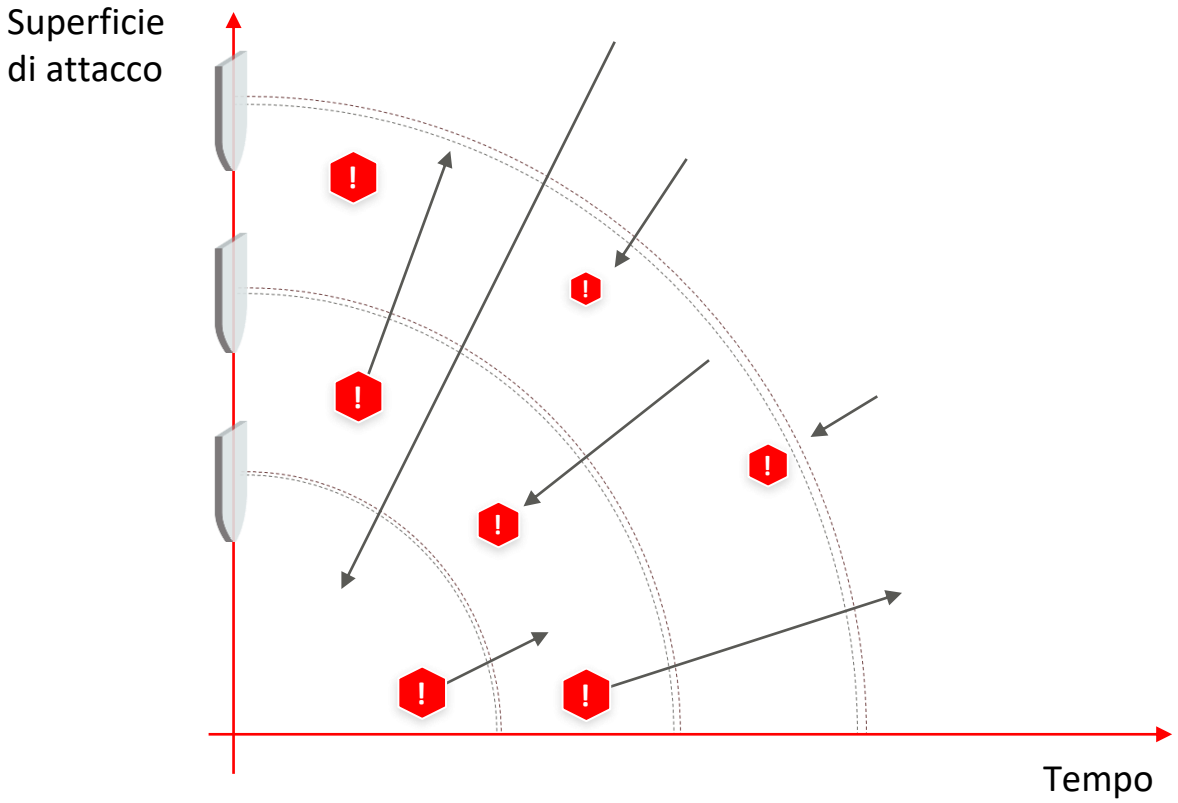
Le aziende devono convalidare e agire in modo continuo e coerente sui loro rischi per la sicurezza informatica

© Pentera

PENTERA

Incapacità di garantire un'efficacia di sicurezza continua

Contro una superficie di attacco in crescita



+ Assets
+ Vulnerabilità ed esposizioni
+ Superficie di attacco
+ Controlli di sicurezza
+ Panorama delle minacce

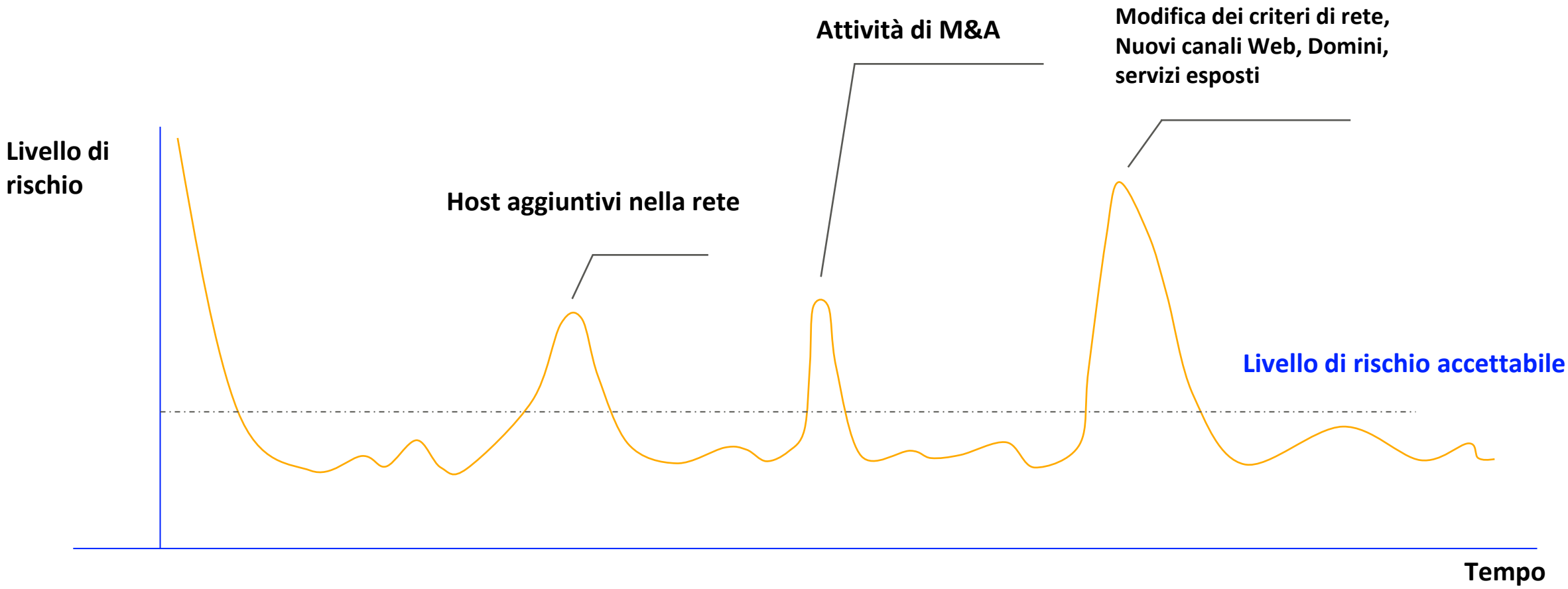
? Efficacia della sicurezza e rischio informatico

© Pentera

PENTERA

Incapacità di garantire l'efficacia dei controlli di sicurezza

Il problema da risolvere



© Pentera

La sicurezza incentrata sulle vulnerabilità e' carente

15,000 +

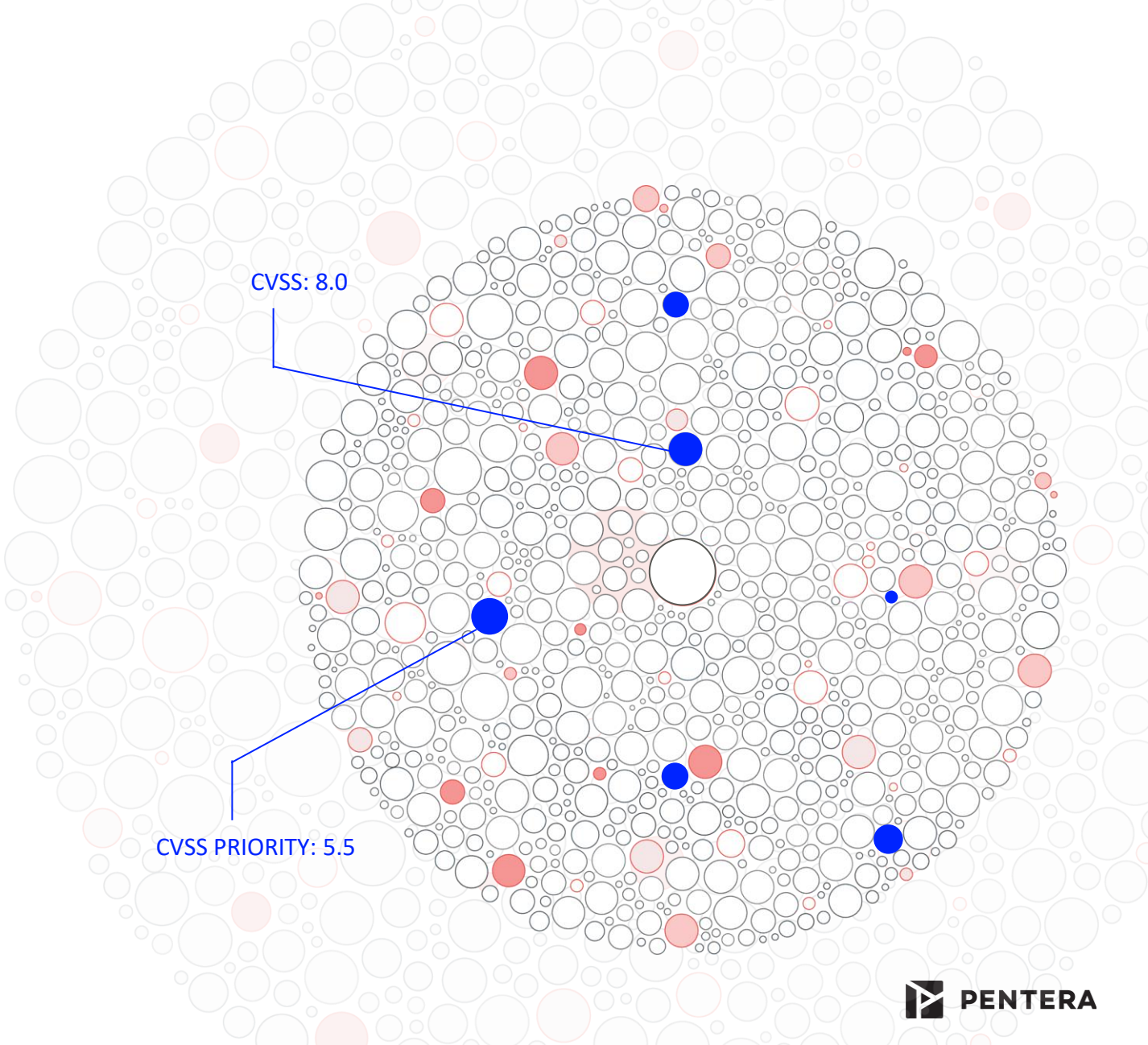
Nuove vulnerabilità scoperte ogni anno
…solamente

> 5%

Hanno un exploit e sono stati
attivamente sfruttati dagli aggressori

~1%

Numero di vulnerabilità di sicurezza sfruttate
attivamente dai gruppi ransomware



 © Pentera

PENTERA

Come migliorare la gestione dei rischi operativi

- Nel panorama delle minacce informatiche di oggi, sta diventando sempre più chiaro che la convalida della sicurezza dei controlli e dei processi di rete devono essere al centro dell'attenzione dell'organizzazione come strategia di sicurezza.
- I penetration test (PT) sono la pratica più comune per la convalida dei rischi aziendali.
- Questi test sono eseguiti principalmente da terze parti o dai RED TEAM interni e si sono evoluti molto lentamente negli ultimi dieci anni.
- E’ chiaro che e carenze pratiche ed organizzative per l’esecuzione di questi test necessitano di automatizzare questi test mantenendo il controllo dell’intero ciclo di controllo dello stato di rischio IT.

© Pentera

La convalida automatizzata dei controlli di sicurezza

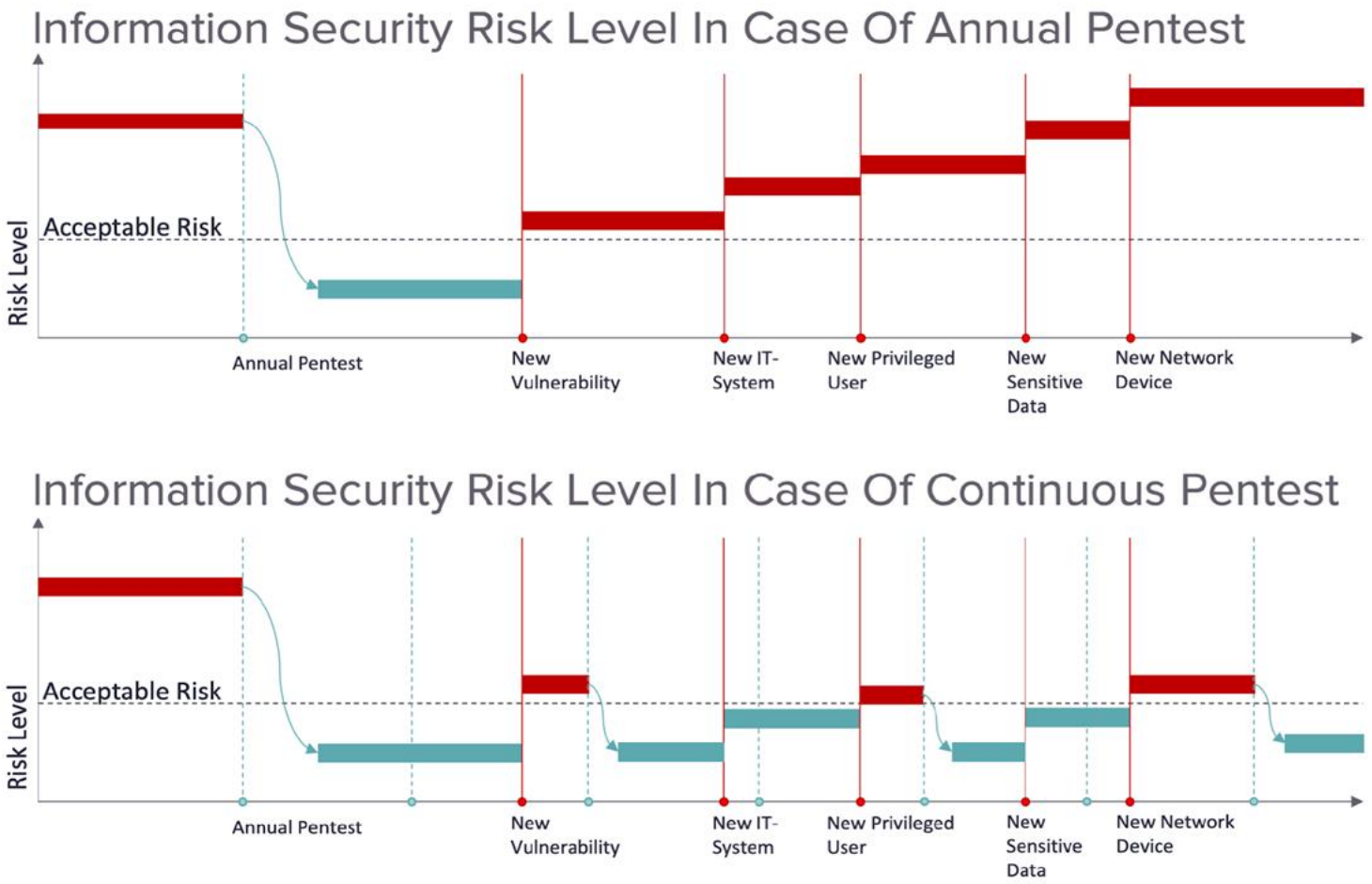
- Un'evoluzione del software di Penetration Test automatizza quello che storicamente è stato un processo manuale. La piattaforma Pentera consente a un'organizzazione di impostare la cadenza dei test in base alle proprie esigenze operative.

- È possibile che la maggior parte dei sistemi necessiti solo di un test di penetrazione mensile, ma un sistema critico necessita di un test di penetrazione settimanale. Ad oggi era proibitivo manualmente a causa di vincoli di risorse o di costi.

- Un altro vantaggio chiave è la segnalazione immediata una volta concluso il test. Dai rapporti esecutivi utilizzati come input nella linea di reporting ERM (Enterprise Risk Management) alle attività di remediation dettagliate, prioritarie in base agli exploit realizzabili, consegnate a un team operativo.

PENTERA

Il valore del Pen-testing continuativo



 © Pentera

ERA

Pen-test tramite automazione in numeri

“MACHINE BASED SCALABILITY” - MTM = 54 : 1 (Source PWC)

Combinazione dei vettori di attacco

Protocol X **Access type** X **Payload type** X **Evasion technique** X **C2 technique**

~4 Vettori di attacco/ giorno

~2000 Vettori di attacco/ giorno

 © Pentera

PENTERA

PenTera: I 4 elementi di ROI (Ritorno dell'Investimento)

Risparmio sull'effort dei servizi di Test di 3ze parti

Riduzione dell'esposizione a incidenti di sicurezza

Miglioramento della produttivita' del Red Team

Incremento della produttivita' del Blue Team

© Pentera

PENTERA

LA NOSTRA SOLUZIONE

Pentera è la prima **Piattaforma di convalida della sicurezza automatizzata al mondo**

Consente alle organizzazioni di tutto il mondo di **convalidare e migliorare costantemente la propria postura di sicurezza informatica**.

© Pentera

PENTERA

Pentera: I suoi Valori

Ritorno dell'investimento (ROI)

- ✓ Risparmio sui costi per l'impegno di terze parti. Riduzione dell'esposizione agli incidenti di sicurezza. Miglioramento della produttività di Red-Teams/Blue-Teams.

Agentless

- ✓ Nessuna configurazione o installazione richiesta; il pen test inizia accedendo alla rete proprio come farebbe un hacker.

Leggi, Regolamenti e Standards

- ✓ Aiuto nella risposta di audit per diversi elementi su GDPR, NIST, PCI-DSS come esempi.

Remediation Prioritizzata

- ✓ Ricevi un riepilogo chiaro e attuabile della correzione critica in base alle priorità funzionali incontrate.

Visibilita’ della Kill-Chain

- ✓ Ogni passaggio nel vettore di attacco è descritto in dettaglio per spiegare ed evidenziare la "**Causa principale**".

Enterprise Risk Management (ERM)

- ✓ Può essere facilmente integrato nei processi aziendali ERM e migliorare la visibilità e il controllo sul "***Livello di rischio accettabile***" definito.

Harmless Exploits

- ✓ Come hacker etici eseguiamo exploit reali ***senza*** causare alcun danno.

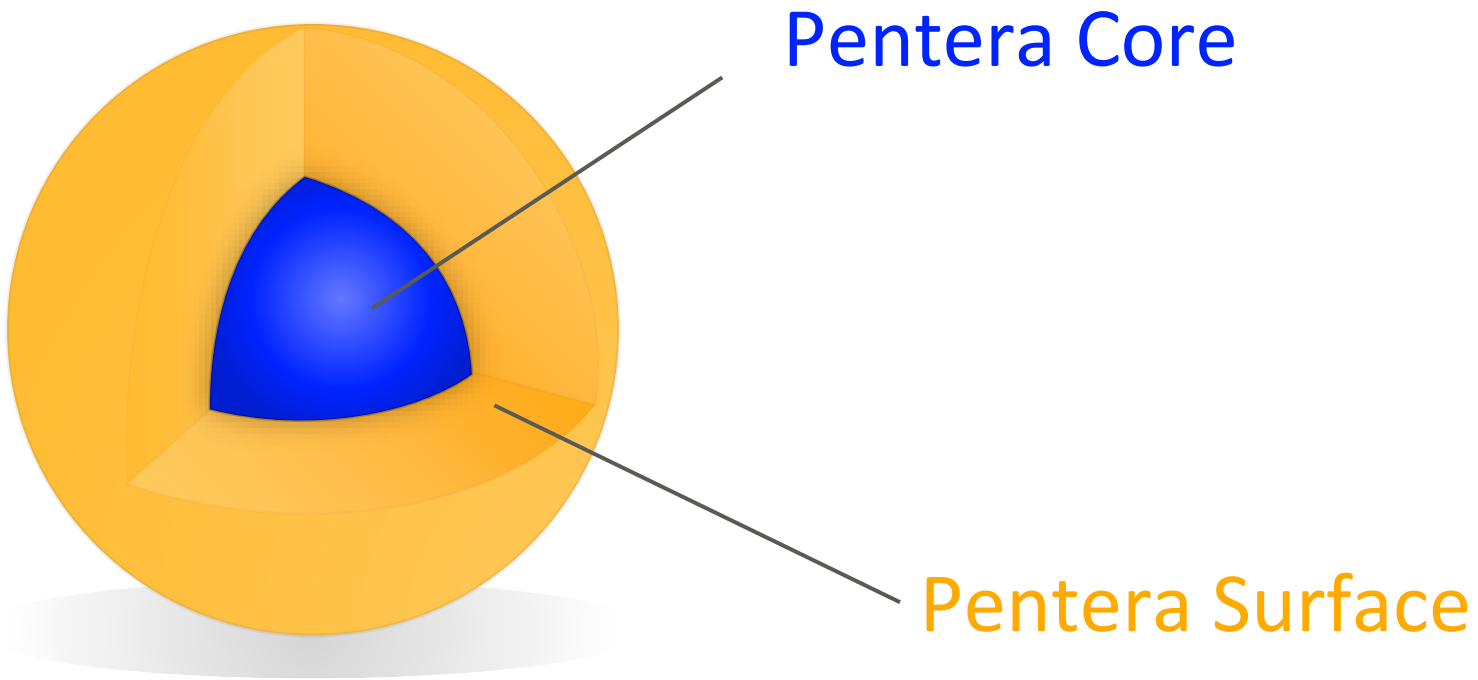
Automatico

- ✓ Premi “Play” e focalizzati su altro mentre la convalida procede.

PENTERA

Piattaforma Pentera

Un'unica soluzione per la convalida totale della sicurezza

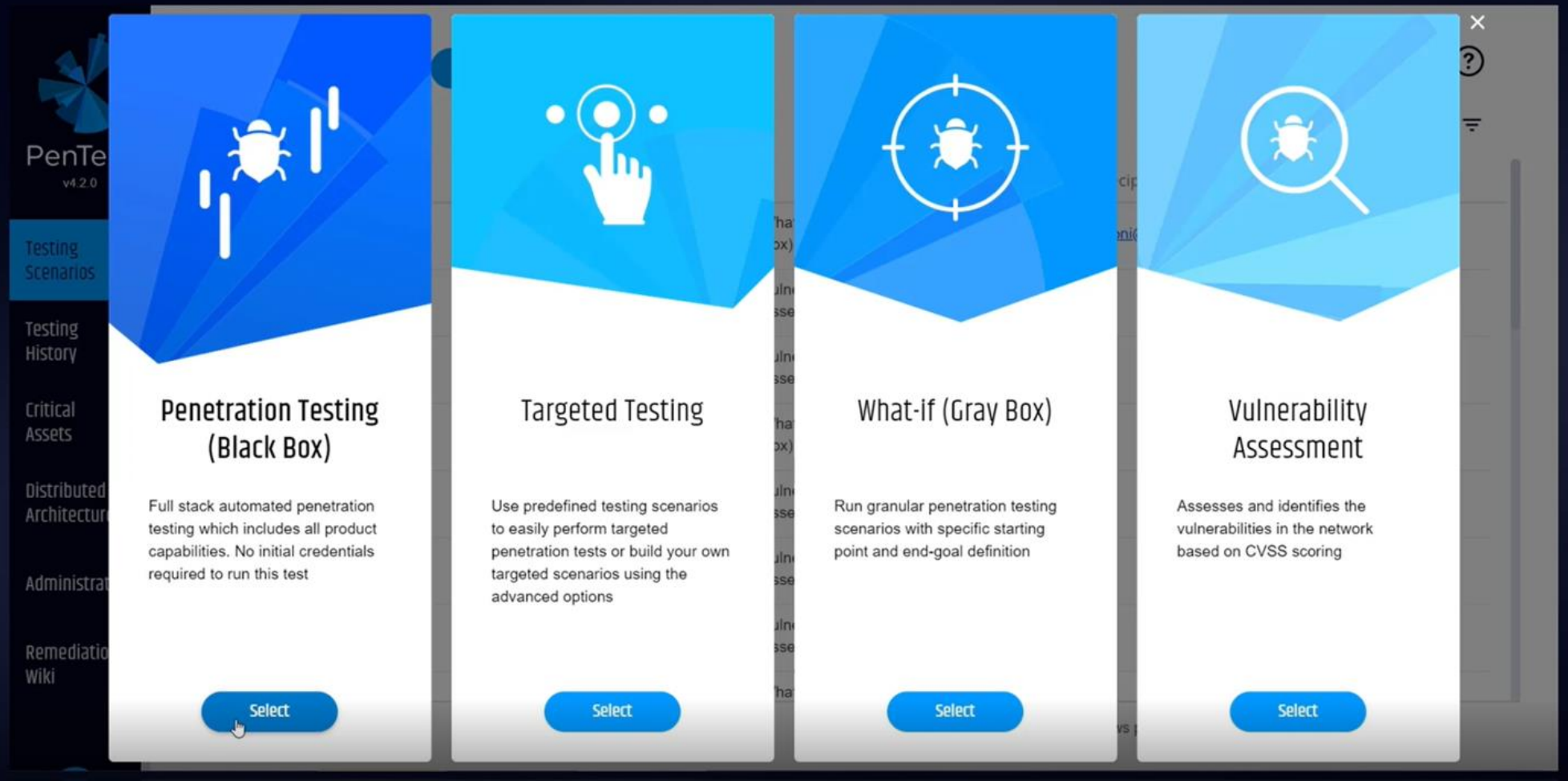


COPERTURA COMPLETA DELLA SUPERFICIE DI ATTACCO

Un'unica soluzione per tutte le operazioni di convalida della sicurezza

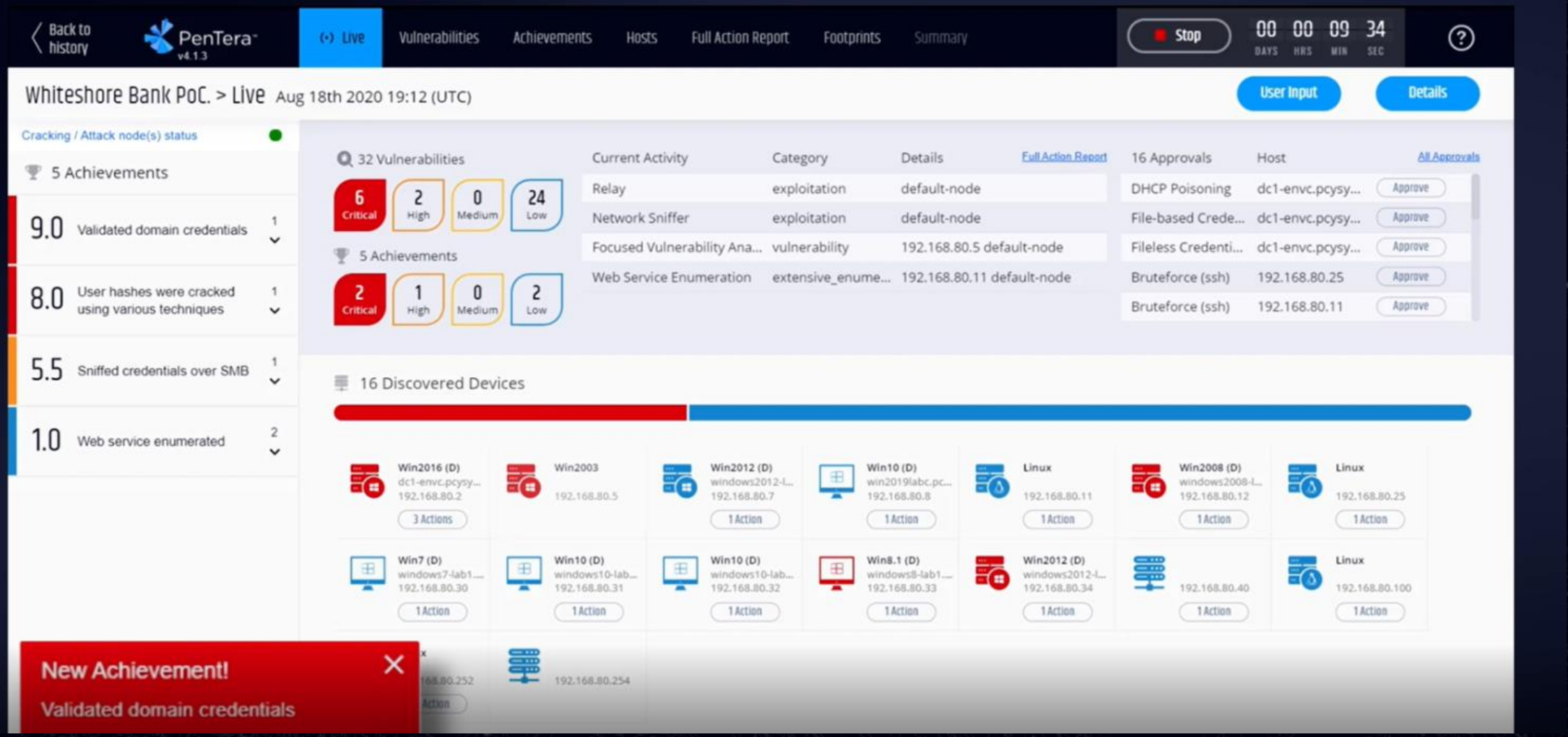
PENTERA

Pentera – 4 scenari di test



PENTERA

Pentera – achievements



 © Pentera

PENTERA

Report - remediation priority

Severity	Remediation Priority	Name	Count	Found On	Remediation
5.5	1	Sensitive information can be sniffed due to network misconfiguration	1	DIM	It is recommended to disable the LLMNR Protocol in the group policy settings. By going to 'Computer Configuration/Policies/Administrative Templates/Network/DNS Client/Turn off Multicast Name Resolution'. The...
6.0	2	Multiple authentication attempts to an untrusted source	2	DIM	It is recommended to disable the LLMNR Protocol in the group policy settings. By going to 'Computer Configuration/Policies/Administrative Templates/Network/DNS Client/Turn off Multicast Name Resolution'. The...
9.8	3	The host is vulnerable to BlueKeep (CVE-2019-0708)	5	192.168.10.13, 192.168.20.13,...	In order to mitigate this vulnerability, any of the following actions can be taken (Although it is recommended to apply all of them): (1) Patch the vulnerable host for BlueKeep (CVE-2019-0708). The following link contains...
9.3	4	The host is vulnerable to MS17-010	3	192.168.10.16 (dc2003x64.old.do...	It is recommended to patch the host for the vulnerability. check the following link for more information: https://technet.microsoft.com/library/security/MS17-010
10	5	The host is vulnerable to MS08-067	1	192.168.10.16 (dc2003x64.old.dom)	It is recommended to patch the host for MS08-067. The following link contains information about the patch and vulnerability: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067. Download th...
8.2	6	Using commonly used password(s)	1	CREDENTIALS	It is recommended to set a stronger password policy for every use or service that requires authentication. The following is a list of minimal requirements for password complexity: A. The password should contain at least 8...
8.0	7	Using easy to guess password(s)	25	CREDENTIALS	It is recommended to set a stronger password policy for every use or service that requires authentication. The following is a list of minimal requirements for password complexity: A. The password should contain at least 8...
7.8	8	Using crackable password(s)	1	CREDENTIALS	It is recommended to set a stronger password policy for every use or service that requires authentication. The following is a list of minimal requirements for password complexity: A. The password should contain at least 8...
7.9	9	Local user account has remote code execution privileges on several hosts (more than 2)	1	LOCALHOST	It is recommended to use a different password for each high privileges local account. Consider implementing the Microsoft LAPS solution, as seen in the following link: https://www.microsoft.com/en-us/download/details.aspx?...
7.7	10	Domain user has remote code execution privileges on several hosts (more than 2)	1	DIM	Consider limiting the access of users across the network and also consider limiting the number of high privileged users.
7.0	11	Possibly storing cleartext credentials in script file(s)	6	192.168.10.26 (enva-win81x64.dim.x),...	It is recommended to keep credentials in encrypted files or documents and never store cleartext passwords in any file.
7.6	12	Using crackable password(s)	2	CREDENTIALS	It is recommended to set a stronger password policy for every use or service that requires authentication with special focus on privilaged accounts. The following is a list of minimal requirements for password complexity: A...
5.4	13	Relay techniques in the network are possible	7	DIM	Use signing mechanism on windows stations and servers.Use precautions against man-in-the-middle attacks. Consider implementing monitoring tools to detect spoofing attacks or run script to identify spoofers on the...

PENTERA

468 ACHIEVEMENTS | 70 VULNERABILITIES

5.1	Executed remote WMI query	23
5.1	Valuable data was gathered from the Active Directory...	1
5.0	Found pivot machine	11
3.5	Validated local credentials	48
3.4	Malware was uploaded to host (LOLBAS)	14
3.3	Opened Remote Control Channel	102
3.2	Found circular nested groups in the domain	2
2.8	Revealed domain's groups and users	2
2.0	Enumerated a builtin domain group with...	3
2.0	Accessible shares using domain credentials	6

Adversary Level | Add To Report

1.0 Security Account Manager Re...
Host: 192.168.10.1

7.5 Anonymous bind to Security A...
Domain: DUBLIN-INFRA

1.0 Security Account Manager Re...
Host: 192.168.10.2

1.0 Enumerated local admi...
Host IP: 192.168.10.1, D...

1.0 Enumerated local administrat...
Host IP: 192.168.10.2, Domain:...

5.1 Valuable data was gathered fr...
Domain: DUBLIN-INFRA

2.0 Enume...
Domai...

2.0 Enumerated a builtin domain ...
Domain: DUB.X, Group: DOMA...

2.0 Enumerated a builtin domain ...
Domain: DUB.X, Group: ENTER...

Action Details

Valuable data was gathered from the Active Directory using domain credentials

Adversary Level: 4

1. Cyber-hobbyist / Script Kiddie
2. Cyber-hacktivists / Malicious Insiders
3. Cyber-criminals / Commercial hacking
4. **Cyber-terrorist / Foreign espionage**
5. State-sponsored / State influenced

MITRE Technique:

System Owner/User Discovery Mitigation (T1033),
Permission Groups Discovery Mitigation (T1069),
System Information Discovery Mitigation (T1082)

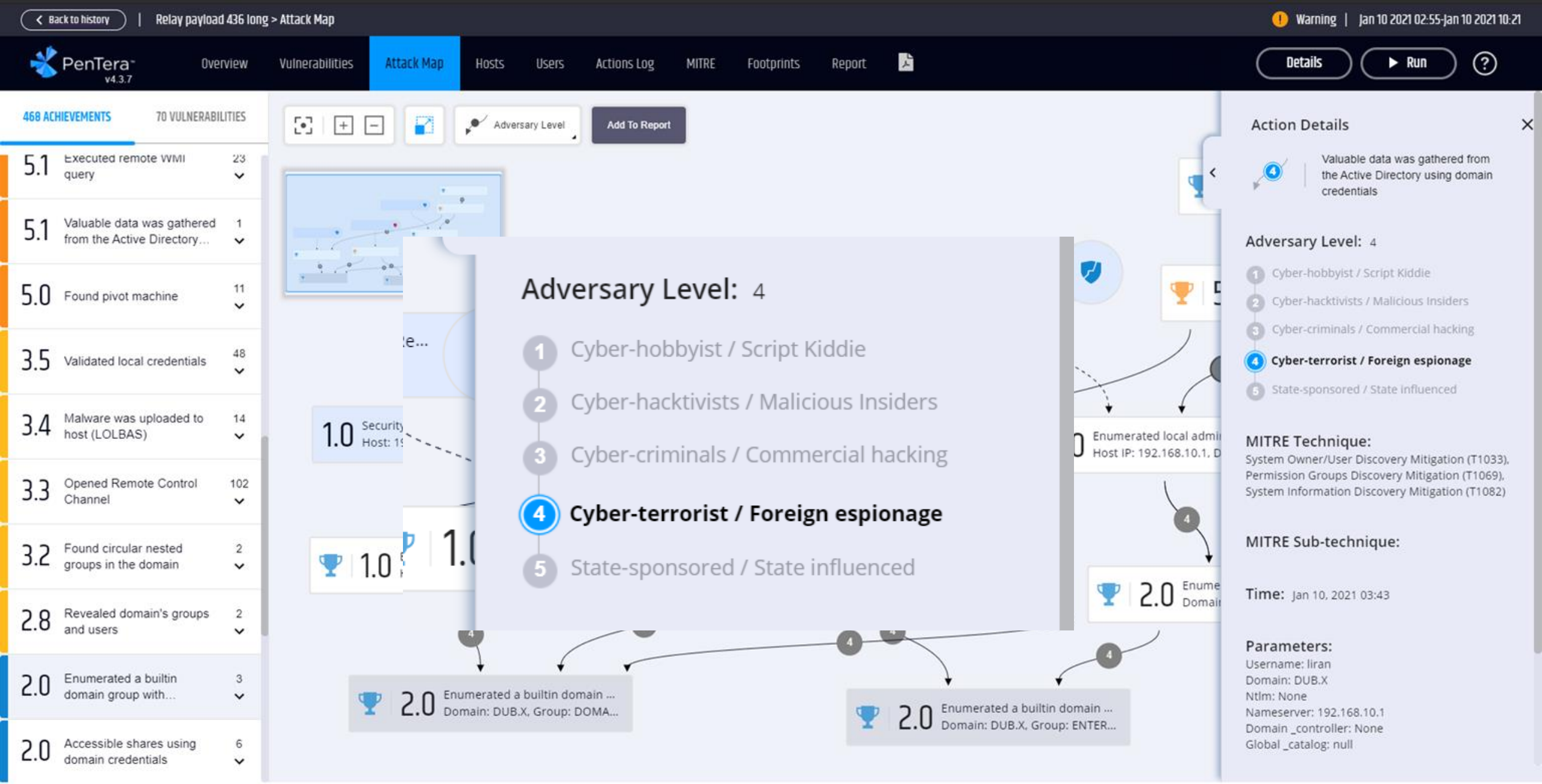
MITRE Sub-technique:

Time: Jan 10, 2021 03:43

Parameters:

Username: liran
Domain: DUB.X
Ntlm: None
Nameserver: 192.168.10.1
Domain _controller: None
Global _catalog: null

PENTERA


Back to history
Relay payload 436 long > Attack Map
Warning | Jan 10 2021 02:55-Jan 10 2021 10:21
PenTera v4.3.7
Overview
Vulnerabilities
Attack Map
Hosts
Users
Actions Log
MITRE
Footprints
Report
Details
Run
468 ACHIEVEMENTS
70 VULNERABILITIES
5.1 Executed remote WMI query 23
5.1 Valuable data was gathered from the Active Directory... 1
5.0 Found pivot machine 11
3.5 Validated local credentials 48
3.4 Malware was uploaded to host (LOLBAS) 14
3.3 Opened Remote Control Channel 102
3.2 Found circular nested groups in the domain 2
2.8 Revealed domain's groups and users 2
2.0 Enumerated a builtin domain group with... 3
2.0 Accessible shares using domain credentials 6
Adversary Level
Add To Report
Adversary Level: 4
1 Cyber-hobbyist / Script Kiddie
2 Cyber-hacktivists / Malicious Insiders
3 Cyber-criminals / Commercial hacking
4 Cyber-terrorist / Foreign espionage
5 State-sponsored / State influenced
1.0 Security Host: 19
1.0
Enumerated local admi Host IP: 192.168.10.1, D
2.0 Enume Domai
2.0 Enumerated a builtin domain ... Domain: DUB.X, Group: DOMA...
2.0 Enumerated a builtin domain ... Domain: DUB.X, Group: ENTER...
Action Details
Valuable data was gathered from the Active Directory using domain credentials
Adversary Level: 4
1 Cyber-hobbyist / Script Kiddie
2 Cyber-hacktivists / Malicious Insiders
3 Cyber-criminals / Commercial hacking
4 Cyber-terrorist / Foreign espionage
5 State-sponsored / State influenced
MITRE Technique:
System Owner/User Discovery Mitigation (T1033),
Permission Groups Discovery Mitigation (T1069),
System Information Discovery Mitigation (T1082)
MITRE Sub-technique:
Time: Jan 10, 2021 03:43
Parameters:
Username: liran
Domain: DUB.X
Ntlm: None
Nameserver: 192.168.10.1
Domain _controller: None
Global _catalog: null

PENTERA

Report - Criticita’ e gravita’

Resilience score card

Critical assets	We have taken over 5 critical assets	Critical
Privileged users	Got 2 Domain Admin Users	Critical
Sniffing	Sniffed 1 Domain Admin and 5 Domain Users	Medium
Password strength	58/234 passwords	High
Lateral movement	Lateral Movement - 78/200 Hosts	High
Payload Exploation	26 Hosts	Critical
Fileless Exploation	Exploited 60 Hosts and bypassed the AV/EDR	High

33% Host take overs

240 hosts

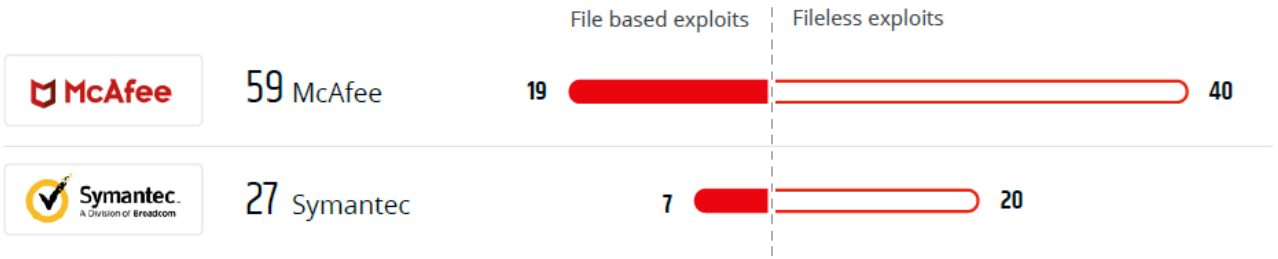
- 78 take overs (33%)
- 162 others (77%)

Total 78 take overs, 5 critical assets

- Regular hosts
- Critical assets

7 Linux servers	2 Critical
5 Window servers	1 Critical
66 Window workstations	2 Critical

86 AV/EDR bypass



 © Pentera

PENTERA

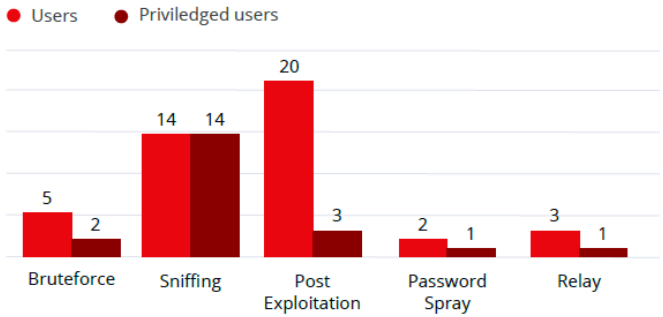
Risultati di dettaglio con approfondimenti

Accounts and credentials

58 Obtained accounts

- 20 priviledged users (34%)
- 38 others (66%)

Techniques



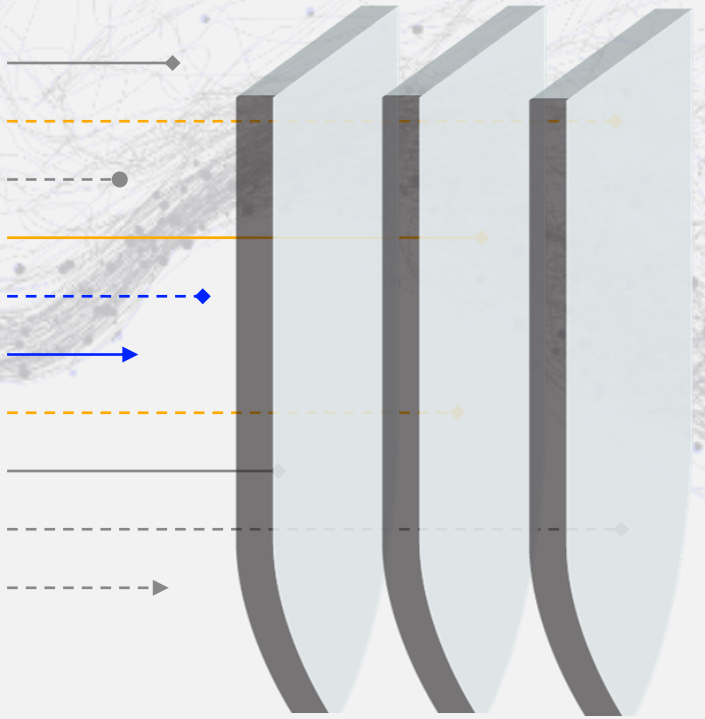
	User Name	Type	Obtained From	Cracking Difficulty
1	yan	Domain admin	Sniffing	Strong
2	pol	Domain admin	Post Exploitation	Trivial
3	na	Domain admin	Brute Force	Strong

Password Cracking Difficulty

PENTERA

Come la tua azienda puo’ diventare

Ransomware ready?

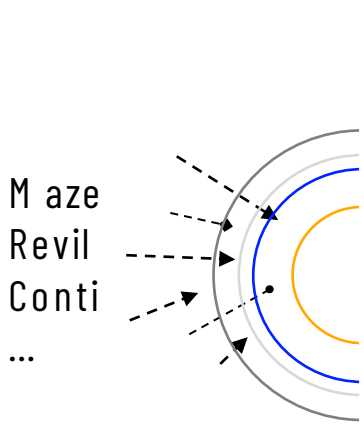


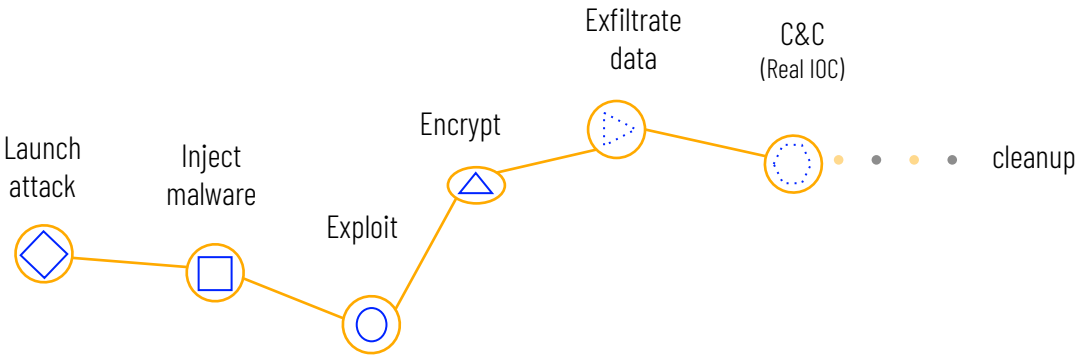
© Pentera

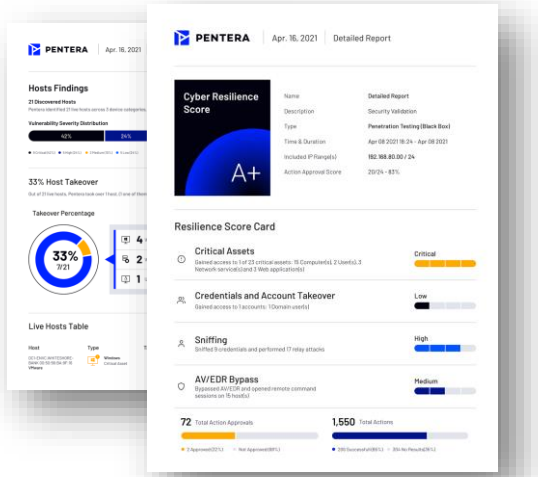
PENTERA

Diventa ransomware ready™

Framework automatico di emulazione ransomware – **Safe by design**







AV/EDR bypass

Vulnerabilities & achievements

Guided remediation

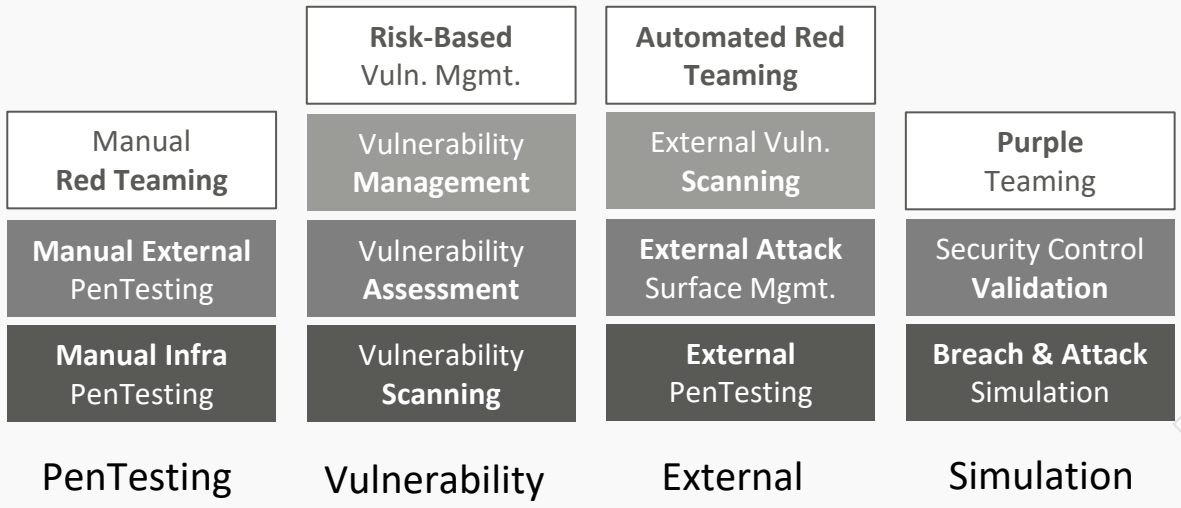
Allineamento al MITRE ATT&CK framework

© Pentera

PENTERA

Piattaforma di convalida della sicurezza

Consolida le soluzioni puntuali in un'unica piattaforma



- Real-time **Reporting**
- Guided **Remediation**
- **External Attack** Surface Mgmt.
- Vulnerability **Prioritization**
- **Risk-Based** Vuln. Mgmt.
- Security Control **Validation**
- **Breach & Attack** Emulation
- **Automated** Red Teaming
- **Vulnerability** Scanning
- **Automated** PenTesting

PENTERA

© Pentera

PENTERA

Confronto tra la convalida della sicurezza automatizzata e™ il vecchio mondo

Un'unica piattaforma che combina il meglio di tutte le funzionalità di convalida della sicurezza.

	Automated Security Validation	Vulnerability Assessment	Breach & Attack Simulation (BAS)	Penetration Testing	External Attack Surface Management
Vulnerability scanning	✓	✓	✗	✓	✓
Control validation	✓	✗	✓	✓	✗
100% Automation	✓	✓	✗	✗	✗
Agentless	✓	✗	✗	✗	✓
Real exploitation / no simulation	✓	✗	✗	✓	✗
Risk-based remediation	✓	✗	✗	✗	✗
Complete Attack Surface Management	✓	✗	✗	✗	✗

PENTERA

Confronto tra la convalida della sicurezza automatizzata e™ il vecchio mondo

Un'unica piattaforma che combina il meglio di tutte le funzionalità di convalida della sicurezza.

	Automated Security Validation	Vulnerability Assessment	Breach & Attack Simulation (BAS)	Penetration Testing	External Attack Surface Management
Vulnerability scanning	✓	✓	✗	✓	✓
Control validation	✓	✗	✓	✓	✗
100% Automation	✓	✓	✗	✗	✗
Agentless	✓	✗	✗	✗	✓
Real exploitation / no simulation	✓	✗	✗	✓	✗
Risk-based remediation	✓	✗	✗	✗	✗
Complete Attack Surface Management	✓	✗	✗	✗	✗

THANK YOU