Pentera

Automated Security Validation

Nadav Elkiess

Regional Manager - France, Belgium & Luxembourg

nadav@pentera.io

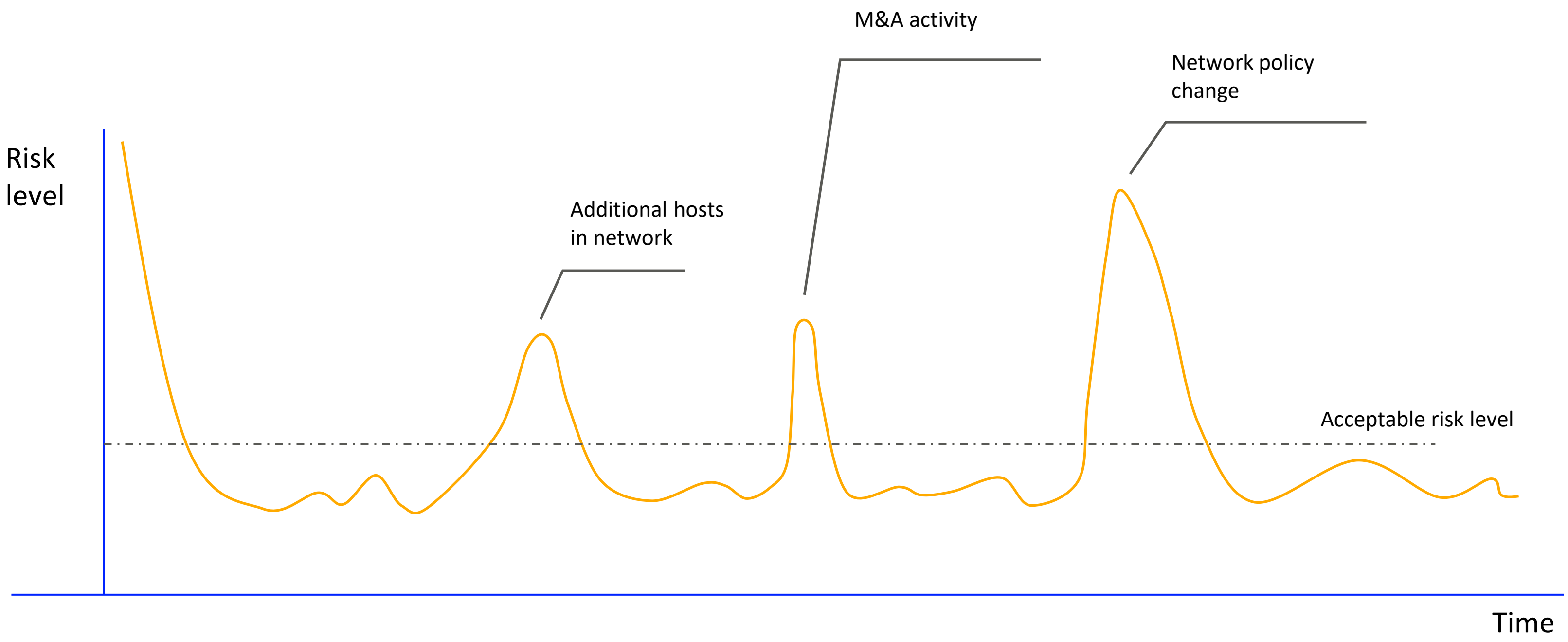
PENTERA

THE CHALLENGE

Enterprises need to *continuously* and *consistently* validate and act on their Cyber Security Risks

Inability to assure your security efficacy 24/7

The problem we solve



OUR SOLUTION

Pentera is the world's first Automated Security Validation Platform

Enabling organizations worldwide to constantly validate and improve their cybersecurity posture.

Automated & Real

2015

FOUNDED

$40M

TOTAL FUNDING

INSIGHT PARTNERS

Blackstone

AWZ HLS FUND I

>220

EMPLOYEES

>350

CUSTOMERS WW

exabeam · NTT · FIS · Blackstone · CYBERARK

NHS · IP Telecom · altice · IDB BANK · Apria Healthcare

Our Customers

Blackstone
IDB BANK It's personal
City National Bank An RBC Company
LA The Port of Los Angeles
CyberArk
Netafim Grow more with less
Bank Yahav
BNP Paribas
Skanska
City of Vienna
enel
NTT

FIS
BTIG
DavidsonKempner Capital Management LLC
Big Y
Mizrahi Tefahot
FIBI First International Bank of Israel
Israel Railways
NHS Bolton NHS Foundation Trust
on2it Zero Trust Innovators
Melbourne Water
IP Telecom
NEC

Dean College
Alliant
exabeam
Empire State Development
cybereason
Yigal Arnon & Co. Law Firm
AICL
Welsh Blood Service
zehnder
Cythera
Fundação Calouste Gulbenkian
WA Police

Diodes Incorporated
Apria Healthcare
中国农业银行 Agricultural Bank of China
BC
AMOS by Spacecom
Harel Insurance & Finance
Ayalon
St Margaret's Hospice Care
Schellenberg Wittmer
eni
AT autoridade tributária e aduaneira
yellowcube

Loblaw Companies Limited
analogic
Promontory Interfinancial Network
CPower
AMOT
Bar-Ilan University
סייבר ישראל Cyber Israel National Cyber Directorate - Prime Minister's Office
NHS East Sussex Healthcare NHS Trust
Leica Geosystems
SG Stevanato Group Engineering Systems
altice
GC Giftcraft

ADR Chambers
Redpoint Cybersecurity LLC
Keystone Dental Group
Silo City Information Technology
Clal Insurance
Israel Electric
Taylor Vinters
Saunderson House
Kambly Excellence Suisse depuis 1910
Acciaierie Valbruna High quality is our standard
absa
Bridge Bank Group Côte d'Ivoire

Export Packers Company Limited
hydro one
Seneca Gaming Corporation
ATEA
Shufersal
Slaughter and May
Pinewood
Spielbanken Bayern
La Martina
access
IP performance

nwmo Nuclear Waste Management Organization
VINCE.
Lipsitz Green Scime Cambria LLP Attorneys at Law
Police משטרת ישראל
מכון הנריטה סאלד
CIFF Children's Investment Fund Foundation
Tideway
Kessler
Tom Ford
Zenith Bank
Yoox Net-a-Porter Group

TBG Security
Gwinnett County Public Schools
Brahman Capital Management Pte Ltd
commIT
משרד ראש הממשלה
משרד הבריאות
charterhouse
Creel García-Cuéllar Aiza y Enríquez
Omicron Seit 1995
Attemptum AG
Rosbank
AA

SkOUT Secure Intelligence
HEXO
sisap
Electra Consider it done
Powys
orbia
Genesis Swiss Team AG
Selution Premium ICT Services
SmartPetro Inc.
EnterpRise Cybersecurity Red
Securicentrix

Trusted worldwide

Financial Services

15%

Healthcare & Pharma

13%

Cybersecurity & MSSP

12%

Services & Consulting

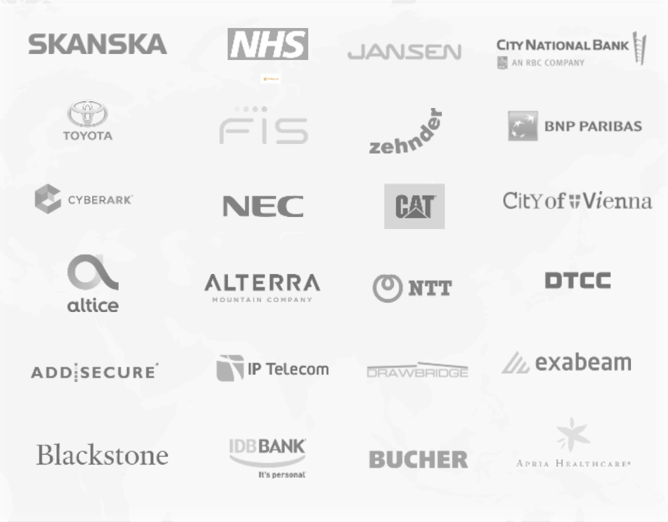
8%

18

Verticals

30

Countries



>300

Customers

We are recognized as

Industry leader & top innovator

CYBERSECURITY BREAKTHROUGH

Pentera Earns 2019 **Enterprise Risk Management Software of the Year**

CYBERSECURITY BREAKTHROUGH AWARDS

RED HERRING

Pentera Named 2019 Red Herring **Top 100 Winner Award** of Cyber Security

RED HERRING WINNER 100 EUROPE

Gartner

Pentera Named a **Cool Vendor** in Gartner's 2020 Cool Vendor Publication

Gartner COOL VENDOR 2020

FROST & SULLIVAN

Pentera Received **Value Leadership Award** for Global Automated Penetration Testing

FROST & SULLIVAN BEST 2019 PRACTICES AWARD GLOBAL AUTOMATED PENETRATION-TESTING CUSTOMER VALUE LEADERSHIP AWARD

Business Intelligence GROUP

Pentera Wins 2019 Fortress Cyber Security Award for **Best Software & Application Threat Detection**

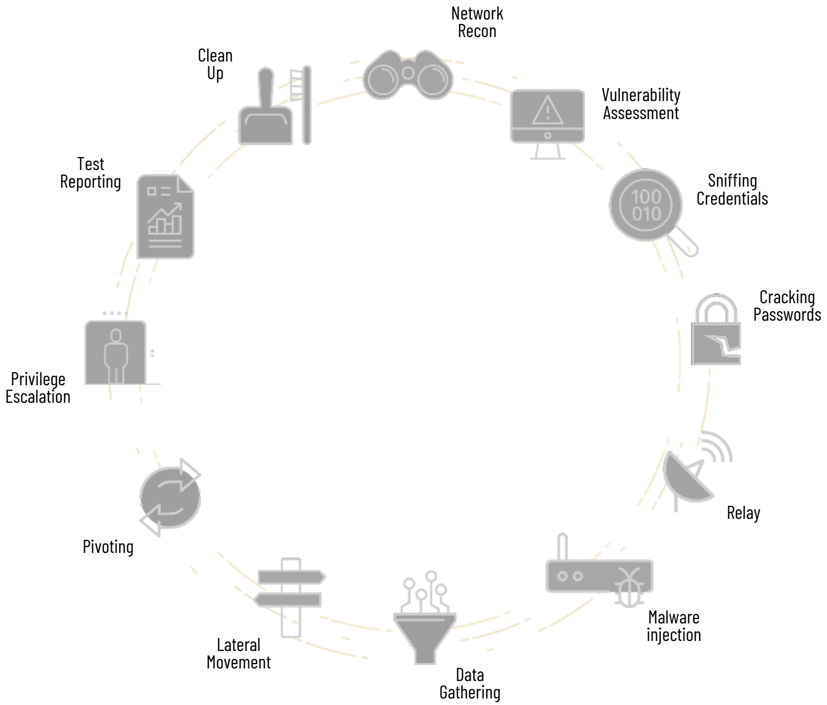
2019 FORTRESS CYBER SECURITY AWARD

CYBER DEFENSE MAGAZINE

Pentera Outperformed All Other Vendors and Awarded **Next Gen Network Penetration Testing Tools**

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019

Pentera Automated Security Validation Platform



Agentless

Real

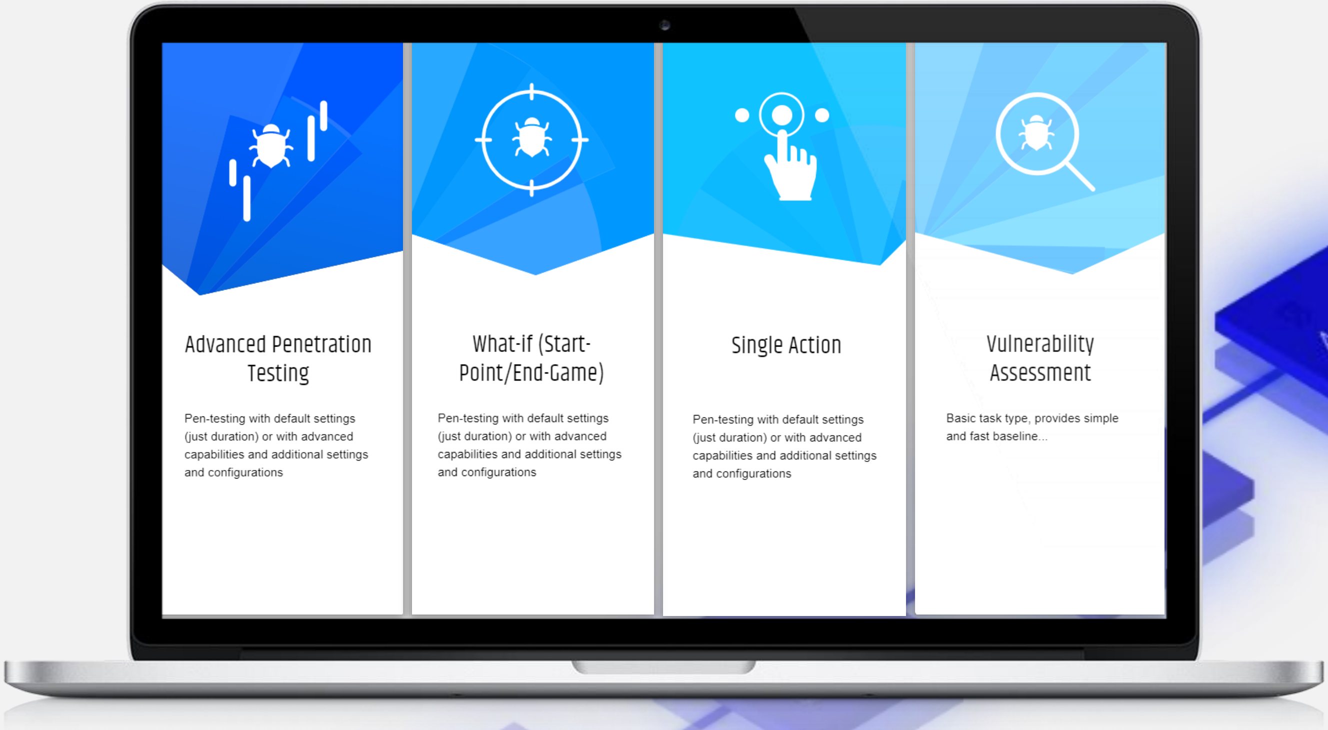
Safe

Complete

Comprehensive

PENTERA

One Platform



Advanced Penetration Testing

Pen-testing with default settings (just duration) or with advanced capabilities and additional settings and configurations

What-if (Start-Point/End-Game)

Pen-testing with default settings (just duration) or with advanced capabilities and additional settings and configurations

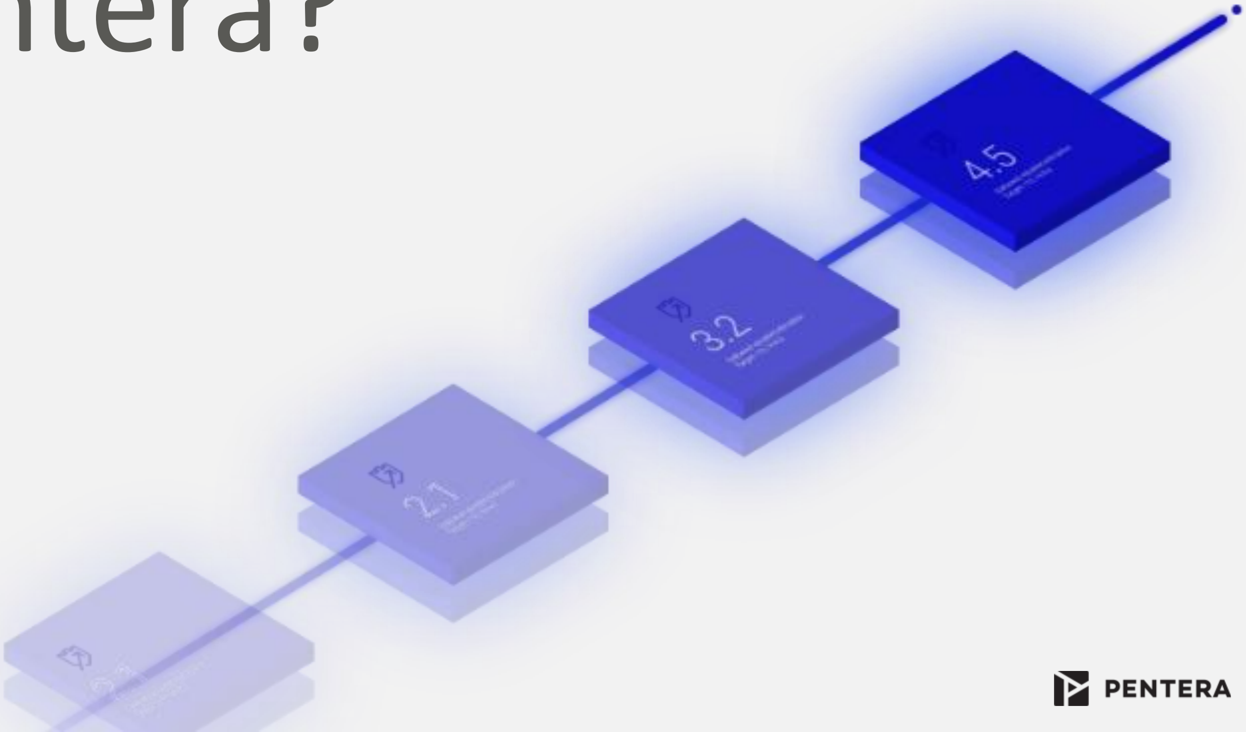
Single Action

Pen-testing with default settings (just duration) or with advanced capabilities and additional settings and configurations

Vulnerability Assessment

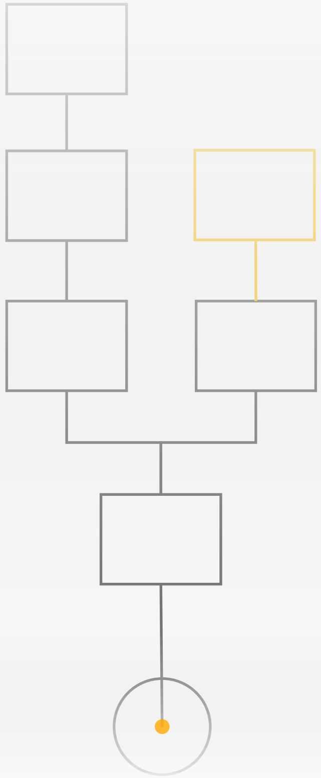
Basic task type, provides simple and fast baseline...

Why Pentera?



Agentless

Network plug & play



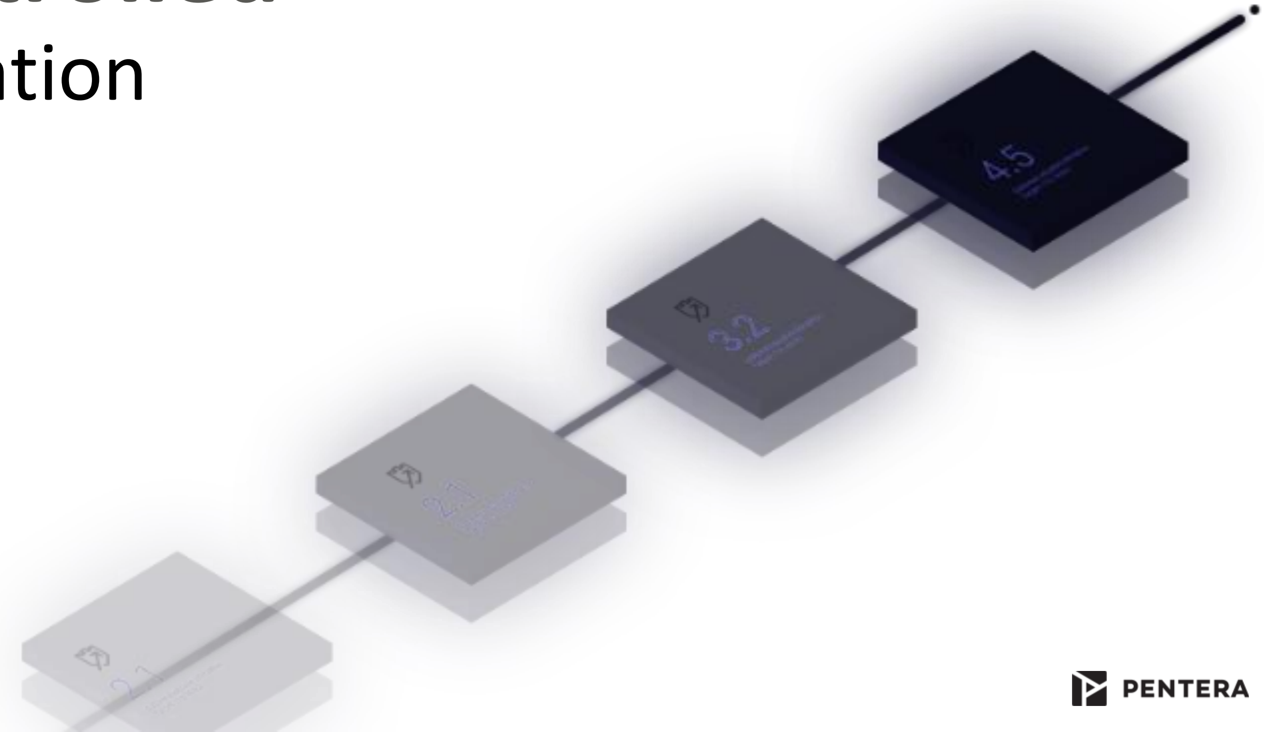
No simulation.
Ethical exploits

Measure attack readiness with minimum false positives

Safe & controlled

security validation

#Do-No-Harm

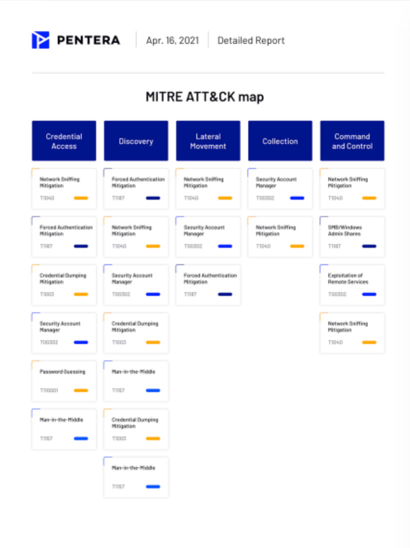


Pentera™
Penetration Test
Detailed Report

Apr. 16, 2021 | Detailed Report

Pentera Automated Security Validation report summarizes the vulnerabilities, exploit achievements and remediation action items recommended in your network based on the latest ethical hacking pentesting techniques.

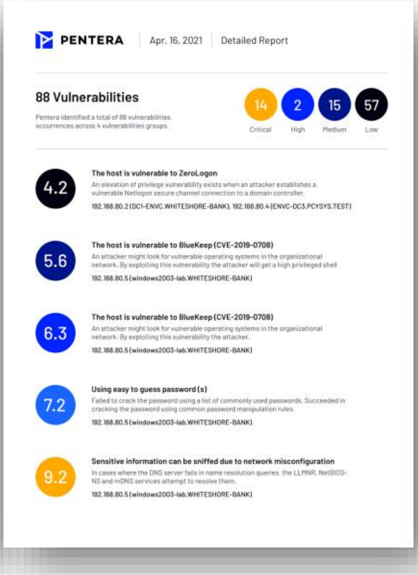
PENTERA



PENTERA | Apr. 16, 2021 | Detailed Report

MITRE ATT&CK map

Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Network Sniffing Mitigation T1040	Forced Authentication Mitigation T1187	Network Sniffing Mitigation T1040	Security Account Manager T00302	Network Sniffing Mitigation T1040
Forced Authentication Mitigation T1187	Network Sniffing Mitigation T1040	Security Account Manager T00302	Network Sniffing Mitigation T1040	SMB/Windows Admin Shares T1187
Credential Dumping Mitigation T1003	Security Account Manager T00302	Forced Authentication Mitigation T1187		Exploitation of Remote Services T00302
Security Account Manager T00302	Credential Dumping Mitigation T1003			Network Sniffing Mitigation T1040
Password Guessing T110001	Man-in-the-Middle T1557			
Man-in-the-Middle T1557	Credential Dumping Mitigation T1003			
	Man-in-the-Middle T1557			



PENTERA | Apr. 16, 2021 | Detailed Report

88 Vulnerabilities

Pentera identified a total of 88 vulnerabilities occurrences across 4 vulnerabilities groups.

14	2	15	57
Critical	High	Medium	Low

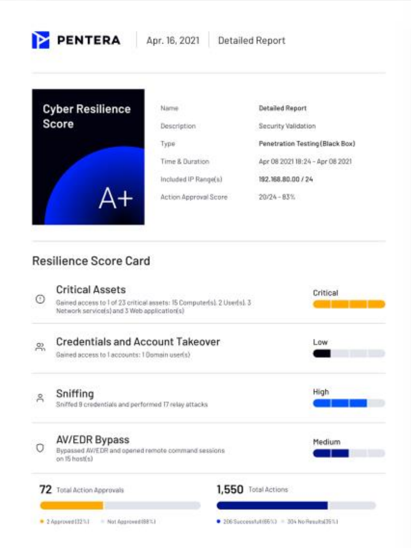
4.2 **The host is vulnerable to ZeroLogon**
An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller.
192.168.80.2 (DC1-ENVC.WHITESHORE-BANK), 192.168.80.4 (ENVC-DC3.PCYSYS.TEST)

5.6 **The host is vulnerable to BlueKeep (CVE-2019-0708)**
An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability the attacker will get a high privileged shell
192.168.80.5 (windows2003-lab.WHITESHORE-BANK)

6.3 **The host is vulnerable to BlueKeep (CVE-2019-0708)**
An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability the attacker.
192.168.80.5 (windows2003-lab.WHITESHORE-BANK)

7.2 **Using easy to guess password (s)**
Failed to crack the password using a list of commonly used passwords. Succeeded in cracking the password using common password manipulation rules.
192.168.80.5 (windows2003-lab.WHITESHORE-BANK)

9.2 **Sensitive information can be sniffed due to network misconfiguration**
In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them.
192.168.80.5 (windows2003-lab.WHITESHORE-BANK)



PENTERA | Apr. 16, 2021 | Detailed Report

Cyber Resilience Score
A+

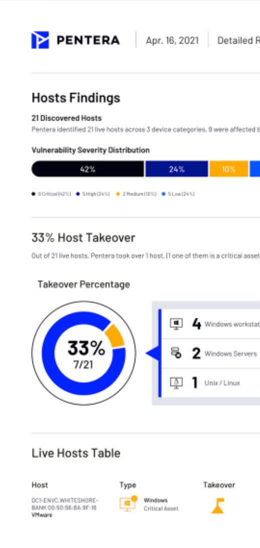
Name	Detailed Report
Description	Security Validation
Type	Penetration Testing (Black Box)
Time & Duration	Apr 08 2021 18:24 - Apr 08 2021
Included IP Range(s)	192.168.80.00 / 24
Action Approval Score	20/24 - 83%

Resilience Score Card

Critical Assets Gained access to 1 of 23 critical assets: 15 Computer(s), 2 User(s), 3 Network service(s) and 3 Web application(s)	Critical
Credentials and Account Takeover Gained access to 1 accounts: 1 Domain user(s)	Low
Sniffing Sniffed 9 credentials and performed 17 relay attacks	High
AV/EDR Bypass Bypassed AV/EDR and opened remote command sessions on 15 host(s)	Medium

72 Total Action Approvals
● 2 Approved (32%) ● Not Approved (68%)

1,550 Total Actions
● 206 Successfull (65%) ● 304 No Results (35%)



PENTERA | Apr. 16, 2021 | Detailed R

Hosts Findings

21 Discovered Hosts
Pentera identified 21 live hosts across 3 device categories, 9 were affected b

Vulnerability Severity Distribution

● 9 Critical (42%) ● 5 High (24%) ● 2 Medium (10%) ● 5 Low (24%)

33% Host Takeover

Out of 21 live hosts, Pentera took over 1 host, (1 one of them is a critical asset

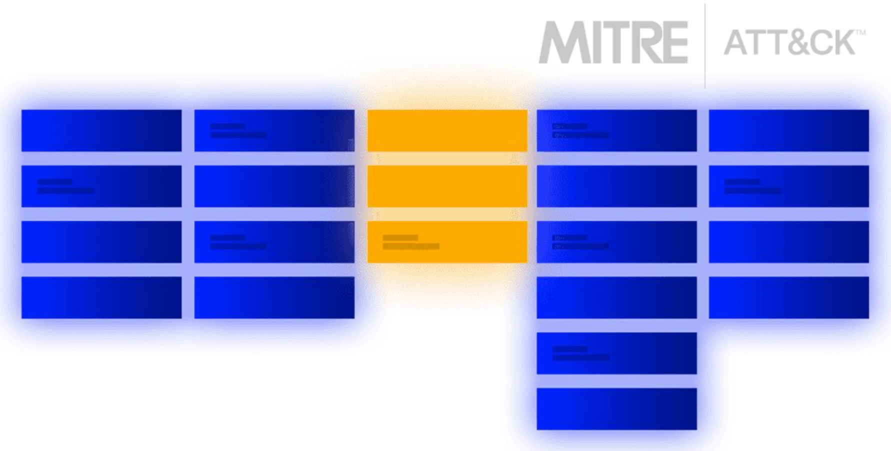
Takeover Percentage

4 Windows workstat
2 Windows Servers
1 Unix / Linux

Live Hosts Table

Host	Type	Takeover
DC1-ENVC.WHITESHORE-BANK 00:50:56:BA:9F:18 VMware	Windows Critical Asset	

Instant & actionable
Report

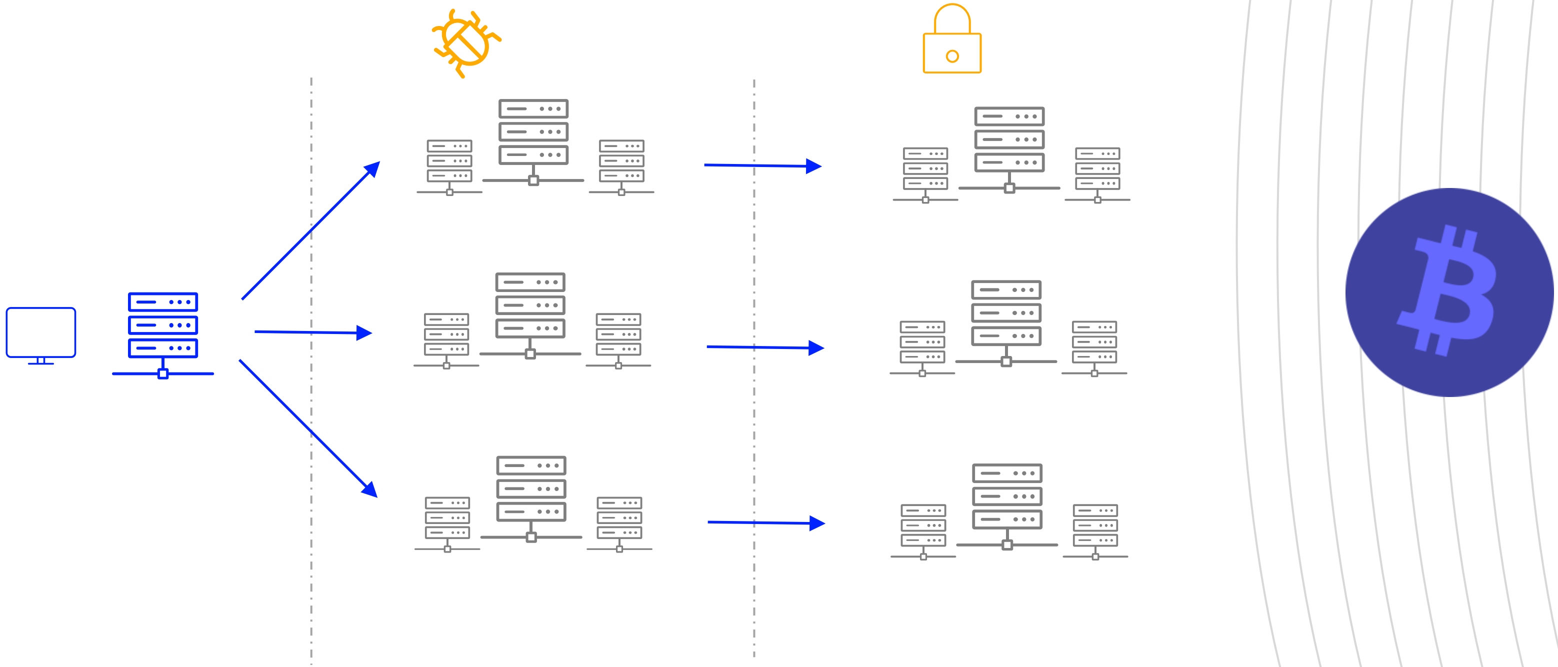


Attack for

ATT&CK

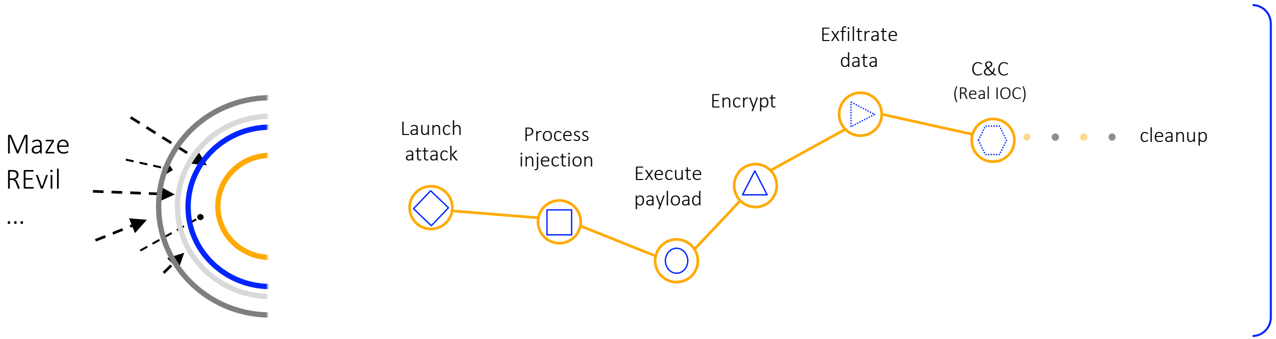
Validate security control efficacy by using the same tactics and techniques adversaries do

What does a Ransomware attack look like?

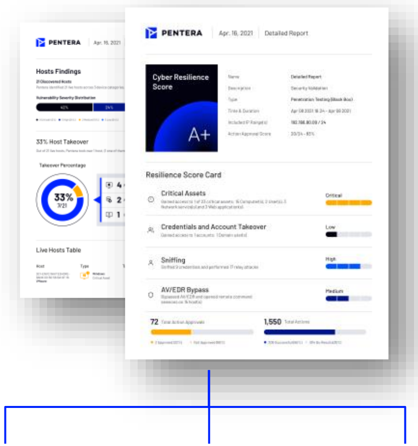


Become RansomwareReady™

Automatic framework of ransomware emulation – safe by design



Alignment to MITRE ATT&CK framework



PENTERA | Apr. 16, 2021

Hosts Findings

21 Discovered Hosts

Vulnerability Severity Distribution

42% 24%

33% Host Takeover

Takeover Percentage

33% 7/21

4 2 1

Live Hosts Table

Host Type

PENTERA | Apr. 16, 2021 | Detailed Report

Cyber Resilience Score

A+

Name	Detailed Report
Description	Security Validation
Type	Penetration Testing (Black Box)
Time & Duration	Apr 08 2021 16:34 - Apr 09 2021
Included IP Range(s)	192.168.80.0 / 24
Action Approval Score	20/24 - 83%

Resilience Score Card

Critical Assets — Critical

Credentials and Account Takeover — Low

Sniffing — High

AV/EDR Bypass — Medium

72 Total Action Approvals

1,550 Total Actions

AV/EDR bypass

Vulnerabilities & achievements

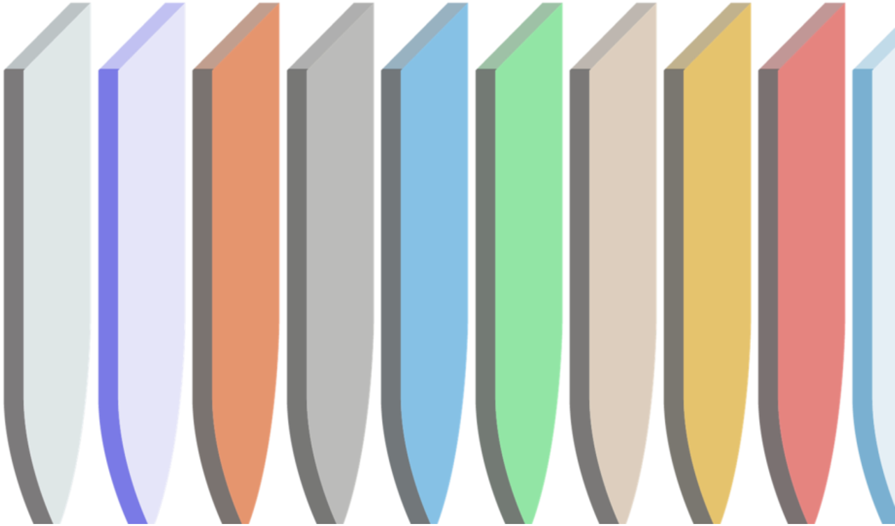
Guided remediation

PENTERA

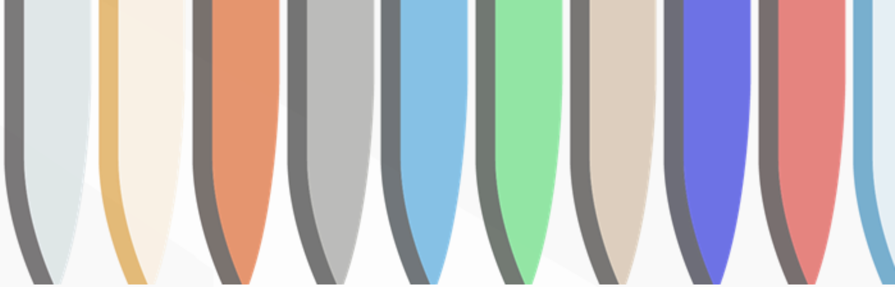
2010-2020

We are on a technology arms race

Stacking the security stack



PENTERA



EDR NDR SIEM NGAV DLP FW VA NAC …

Have we stopped to validate that investments made truly work?

Ransomware is not going anywhere!

Prevention & detection as the only approach… is failing

$20 Billion

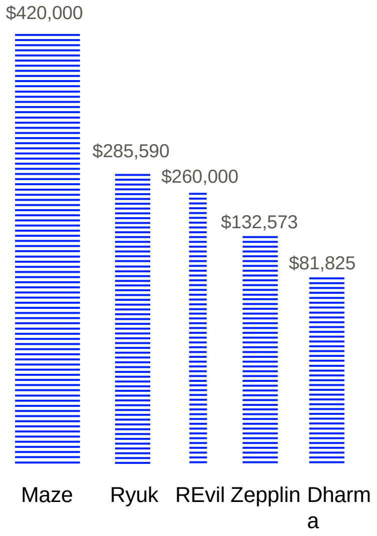
Projected ransomware damages costs to be paid in 2021

x2.5

Number of organizations impacted by ransomware (1H 2021 compared with 2020)

>50%

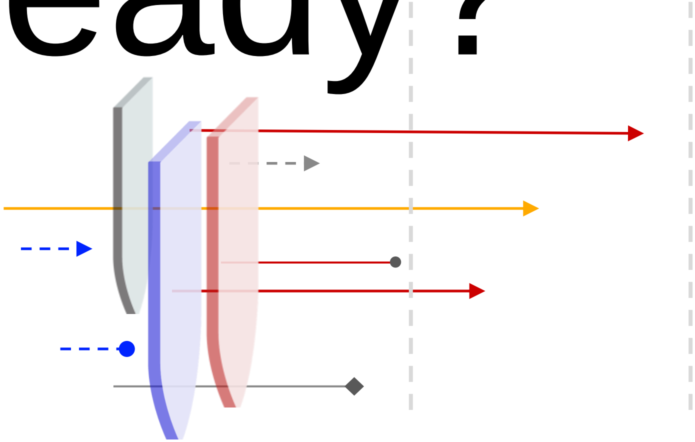
of all cyber insurance claims accounted for ransomware in 2020



Reference: Checkpoint, Cybersecurity ventures, Coalition

How confident are you – with the question

Am I ready?

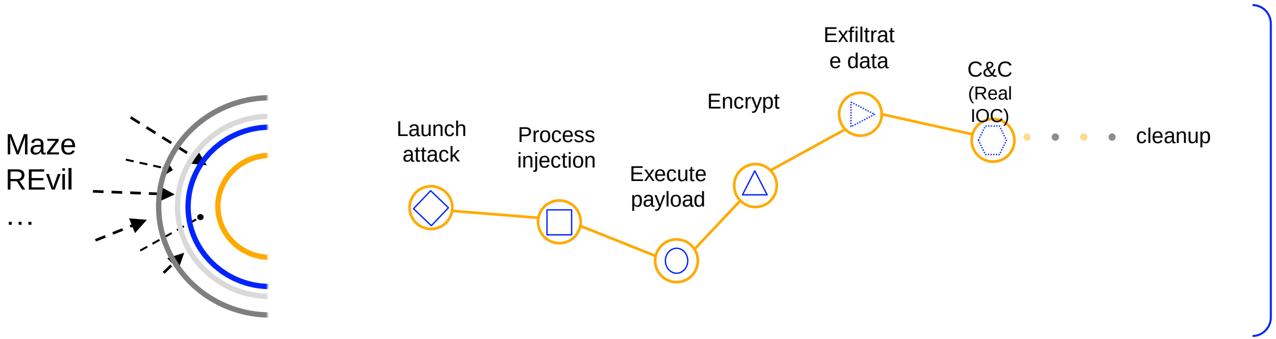


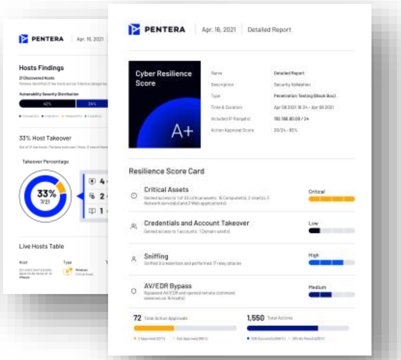
Unfortunately,

assumptions are different from **reality**.

Become RansomwareReady™

Automatic framework of ransomware emulation – safe by design




PENTERA | Apr. 16, 2021

Hosts Findings

33% Host Takeover

Takeover Percentage

33%
7/21

Live Hosts Table

PENTERA | Apr. 16, 2021 | Detailed Report

Cyber Resilience Score

A+

Resilience Score Card

Critical Assets — Critical

Credentials and Account Takeover — Low

Sniffing — High

AV/EDR Bypass — Medium

72 Total Action Approvals

1,550 Total Actions

AV/ED R bypass

Vulnerabilities & achievements

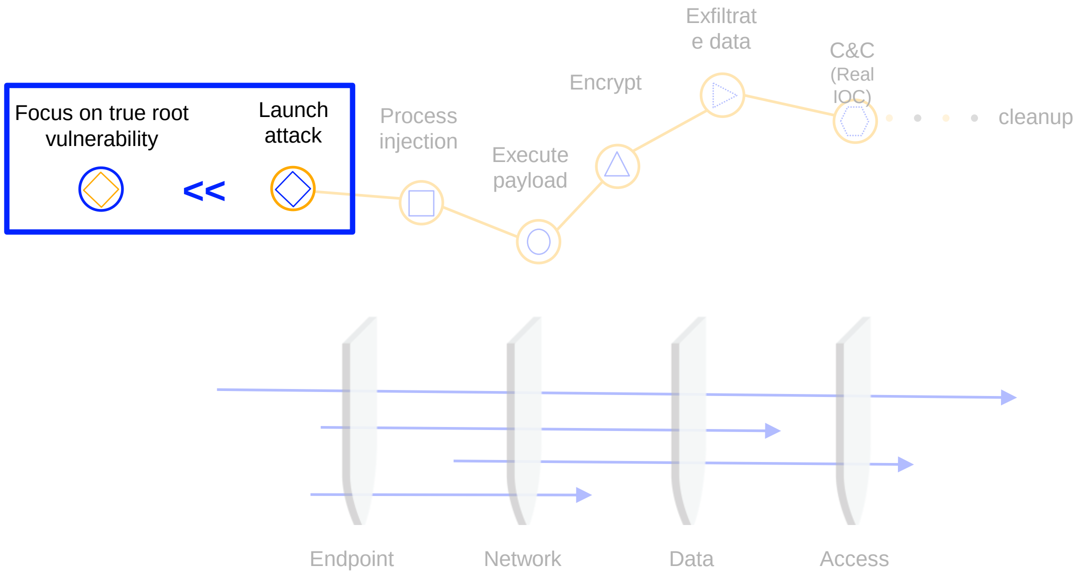
Guided remediation

Alignment to MITRE ATT&CK framework

PENTERA

Become RansomwareReady™

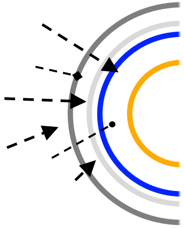
Pinpoint the root vulnerability

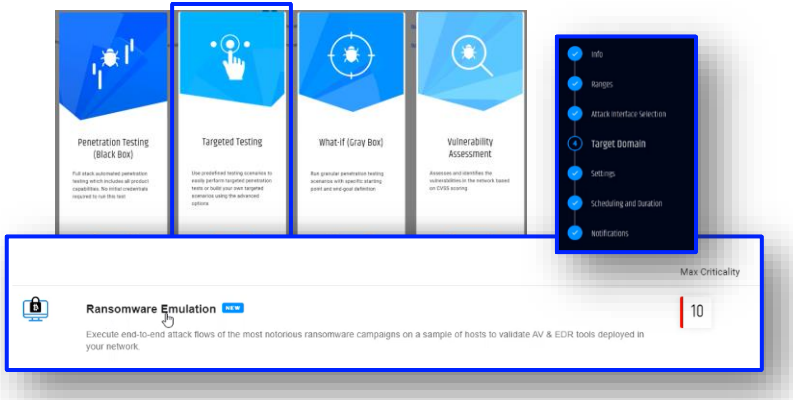


RansomwareReady Emulation

One-click exposure

Maze
REvil
…





Penetration Testing (Black Box)

Full stack automated penetration testing which includes all product capabilities. No initial credentials required to run this test

Targeted Testing

Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options

What-If (Gray Box)

Run granular penetration testing scenarios with specific starting point and end-goal definition

Vulnerability Assessment

Assesses and identifies the vulnerabilities in the network based on CVSS scoring

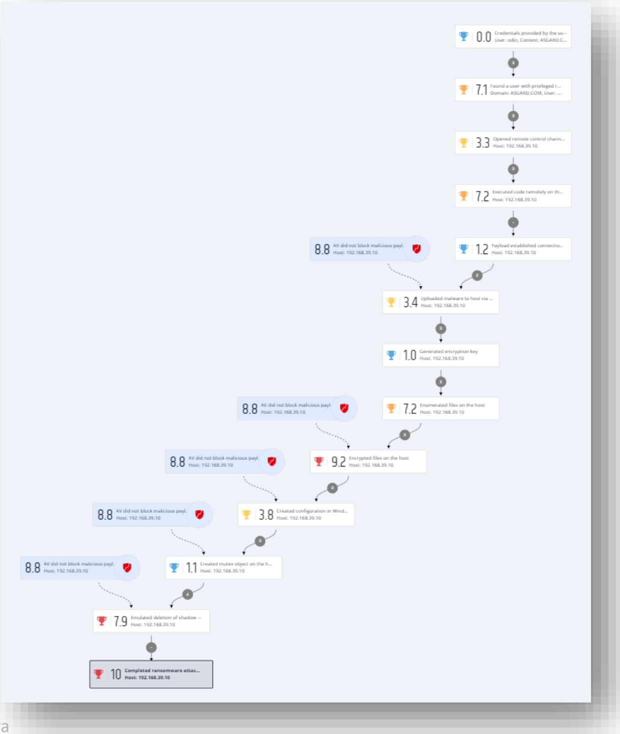
- ✓ Info
- ✓ Ranges
- ✓ Attack Interface Selection
- 4 Target Domain
- ✓ Settings
- ✓ Scheduling and Duration
- ✓ Notifications

	Max Criticality
Ransomware Emulation NEW Execute end-to-end attack flows of the most notorious ransomware campaigns on a sample of hosts to validate AV & EDR tools deployed in your network.	10

Agentle ss **Real** **Safe**

RansomwareReady Emulation

Autonomous validation



0.0 Credentials provided by the us...
User: odin, Context: ASGARD.C...

7.1 Found a user with privileged r...
Domain: ASGARD.COM, User: ...

3.3 Opened remote control chann...
Host: 192.168.39.10

7.2 Executed code remotely on th...
Host: 192.168.39.10

8.8 AV did not block malicious payl.
Host: 192.168.39.10

1.2 Payload established connectio...
Host: 192.168.39.10

3.4 Uploaded malware to host via ...
Host: 192.168.39.10

1.0 Generated encryption key
Host: 192.168.39.10

8.8 AV did not block malicious payl.
Host: 192.168.39.10

7.2 Enumerated files on the host
Host: 192.168.39.10

8.8 AV did not block malicious payl.
Host: 192.168.39.10

9.2 Encrypted files on the host
Host: 192.168.39.10

8.8 AV did not block malicious payl.
Host: 192.168.39.10

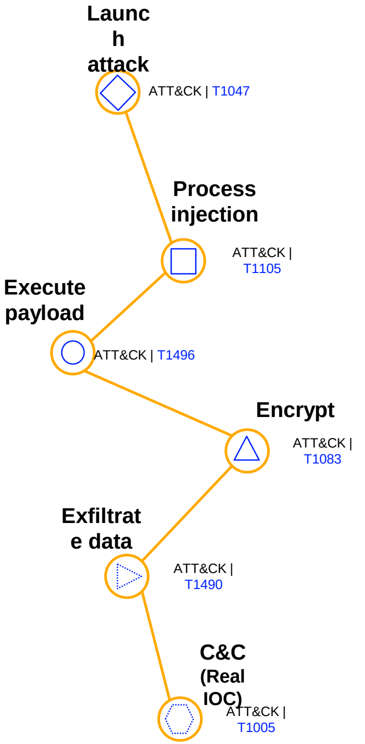
3.8 Created configuration in Wind...
Host: 192.168.39.10

8.8 AV did not block malicious payl.
Host: 192.168.39.10

1.1 Created mutex object on the h...
Host: 192.168.39.10

7.9 Emulated deletion of shadow ...
Host: 192.168.39.10

10 Completed ransomware attac...
Host: 192.168.39.10

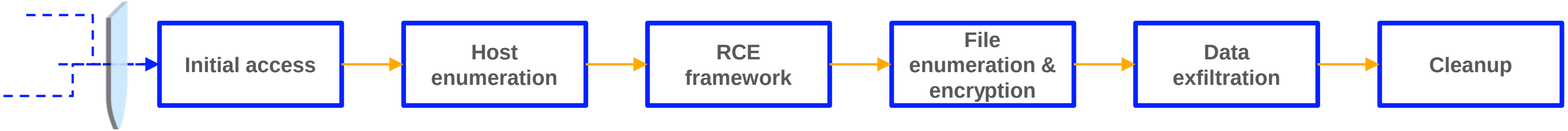


- End-to-end ransomware attack operation
- Complete alignment to the MITRE ATT&CK framework
- ‘`Salsa20`’ encryption algorithm
- Shadow copies access tested
- Safety controls
- Data exfiltration options
    - *c2.ransomware-emulation.com*
    - *Known IOCs*

Become RansomwareReady™

Maze emulation targeted testing - under the hood view

Assume breach…



- Privileged user
- Template configurations

- Windows only
- 50 hosts / validation
- Approval per host

- SMB protocol
- Remote code execution
- Connection established
- Payload loaded to memory

- Compromise user (logged-in/last modified)
- User related files (<150MB)
- Shadow copy
- Data encryption (original algorithm salsa20)
- NGAV/EDR bypass

- Beacon dummy messages
- (optional) real IOCs or dedicated URL
- Validate NDR/FW/TIP
- Report completion to Pentera

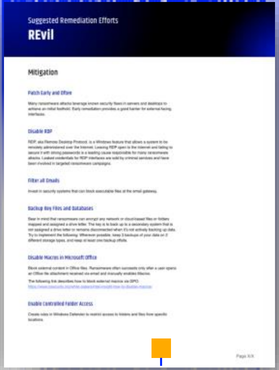
- Clean encrypted files
- Clean payload
- Complete sanitation

Alignment to MITRE ATT&CK framework

309 Achievements

MITRE ATT&CK Matrix for Enterprise - Heat Map (2 of 2)

REvil



Suggested Remediation Efforts

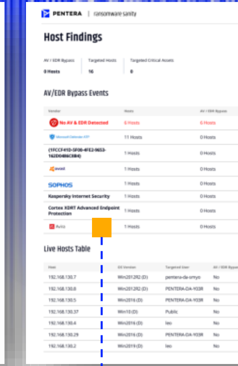
REvil

Mitigation

Maze Ransomware

Indicators of Compromise (IOCs)

Executive Summary



Host Findings

AV/EDR Bypass Events

Live Hosts Table

Prioritized achievements based on true-risk

MITRE ATT&CK Tactics & Techniques successfully executed

Info & context to better understand risk and impact

Guided remediation steps

Hosts compromise d

Resilience Score including
Encryption
Data Exfil
Achievements
EDR bypass

Endpoint Security bypass results

Evaluate your organization's readiness today

__Pentera Free Ransomware Readiness Assessment__ & (a lot) more

☑ Asset discovery

- ☑ Workstation / server / network device
- ☑ Windows / Linux
- ☑ Azure cloud

☑ Enumeration

☑ Attack operation

- ☑ Complete attack vector
- ☑ No operational & system impact
- ☑ Safe exploit
- ☑ Safe approval

☑ Report

- ☑ Cyber resilience scorecard
- ☑ Executive summary report
- ☑ MITRE ATT&CK TTP mapping
- ☑ Vulnerabilities & remediation priority

☑ Impact & remediation

- ☑ Remediation guidance

☑ Business considerations

- ☑ No false positives
- ☑ Scalable
- ☑ Do-no-harm / safety
- ☑ Automated scheduling
- ☑ Multi-segment / domain / site

☑ Penetration testing

- ☑ Black box testing
- ☑ Targeted scenario / Grey box testing
- ☑ Prioritized achievements

☑ Security validation

- ☑ Prevention / detection controls (EPP, EDR, SASE, NDR…)
- ☑ Infrastructure policy (FW, Zero Trust)
- ☑ Security configurations
- ☑ Blue team / IR practice
- ☑ Data hygiene

☑ Password management

- ☑ Password strength assessment
- ☑ Password policy
- ☑ Password cracking

☑ Vulnerability management

- ☑ Static vulnerability scanning
- ☑ Vulnerability prioritization

☑ **Ransomware Readiness**

- ☑ Controls validation
- ☑ Data encryption
- ☑ Data exfiltration
- ☑ Ransomware risk & impact
- ☑ Root vulnerabilities

PENTERA

THANK YOU