Pentera

Automated Security Validation

Nadav Elkiess
Regional Manager - France, Belgium & Luxembourg
nadav@pentera.io
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

- Inability to assure your security efficacy 24/7
- Risk level
- Time
- Additional hosts in network
- M&A activity
- Network policy change
- Acceptable risk level
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

>220
EMPLOYEES

>350
CUSTOMERS WW
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

- Pentera Earns 2019 Enterprise Risk Management Software of the Year
- Pentera Named 2019 Red Herring Top 100 Winner Award of Cyber Security
- Pentera Named a Cool Vendor in Gartner’s 2020 Cool Vendor Publication
- Pentera Received Value Leadership Award for Global Automated Penetration Testing
- Pentera Wins 2019 Fortress Cyber Security Award for Best Software & Application Threat Detection
- Pentera Outperformed All Other Vendors and Awarded Next Gen Network Penetration Testing Tools
Pentera Automated Security Validation Platform

Agentless

Real

Safe

Complete

Comprehensive
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
Instant & actionable Report
Validate security control efficacy by using the same tactics and techniques adversaries do
What does a Ransomware attack look like?

Lateral Expansion

Encryption & Exfiltration
Become RansomwareReady™

Automatic framework of ransomware emulation – safe by design

Alignment to MITRE ATT&CK framework
2010-2020
We are on a technology arms race
Stacking the security stack
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

Alignment to MITRE ATT&CK framework
Become RansomwareReady™

Pinpoint the root vulnerability

Focus on true root vulnerability
Launch attack

Process injection
Encrypt
Execute payload
Exfiltrate data
C&C (Real IOC)

Endpoint
Network
Data
Access

Cleanup
Ransomware Ready Emulation

One-click exposure

Agentless Real Safe
RansomwareReady Emulation

Autonomous validation

- 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...

Initial access
- Privileged user
- Template configurations

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

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

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

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

Cleanup
- Clean encrypted files
- Clean payload
- Complete sanitation

Alignment to MITRE ATT&CK framework
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 compromised

Endpoint Security bypass results

Resilience Score including:
- Encryption
- Data Exfil
- Achievements
- EDR bypass
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
THANK YOU