Research @ Pentera

Alex Spivakovsky, VP of Research

spivi@pentera.io

PENTERACON 2023

Pentera's Annual Customer Summit

PENTERA

C:\Windows\System32\whoami.exe

Red Team Security Researcher

Blue Team Group Manager

Security Researcher

Research Team Leader

Head of Research

VP of Research

2010 2018 2023


C:\Windows\System32\whoareweexe
Experienced Cyber Researchers
Veterans of Elite Cyber Units
Practitioners

PENTERA

Take control of your security validation:

Engage, Interact, and Influence!

Matan

Yahel

PENTERA

Agenda

- Mission Statement
- Year in a Glimpse
- Next Year: Exciting Horizons Ahead
- Summary

Mission Statement

PENTERA

“**Continuously** deliver new and advanced attack capabilities to the platform to **ensure comprehensive security validation**”

PENTERA

How we do it

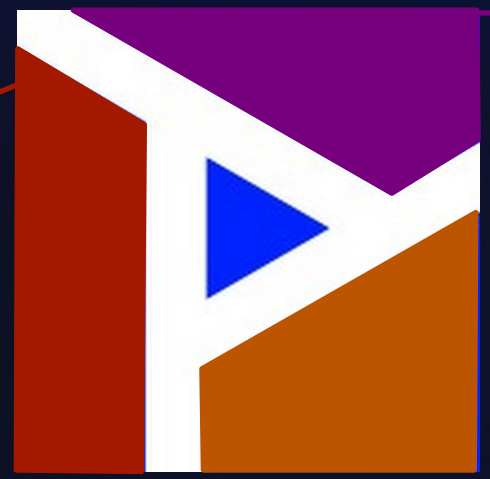
Continuously

How we

Ensure comprehensive security validation

PENTERA

How we Ensure comprehensive security validation

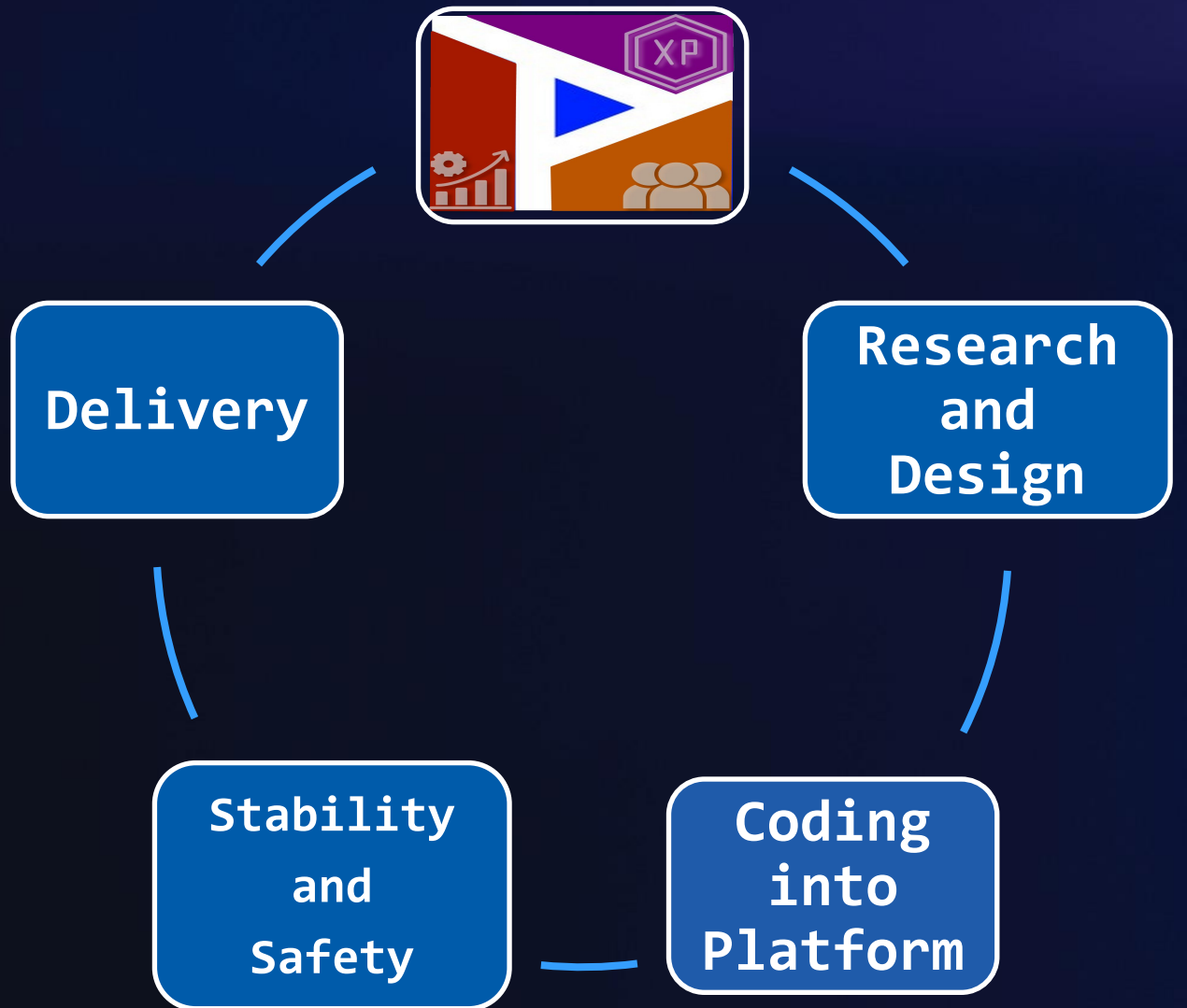


Customers

Experience

Community

How we do it
Continuously



Year in a Glimpse

PENTERA

20 Researchers

425 TTPs & Exploits

700% ⬆️ Exploitation
350% ⬆️ MITRE Coverage

Introduced OWASP

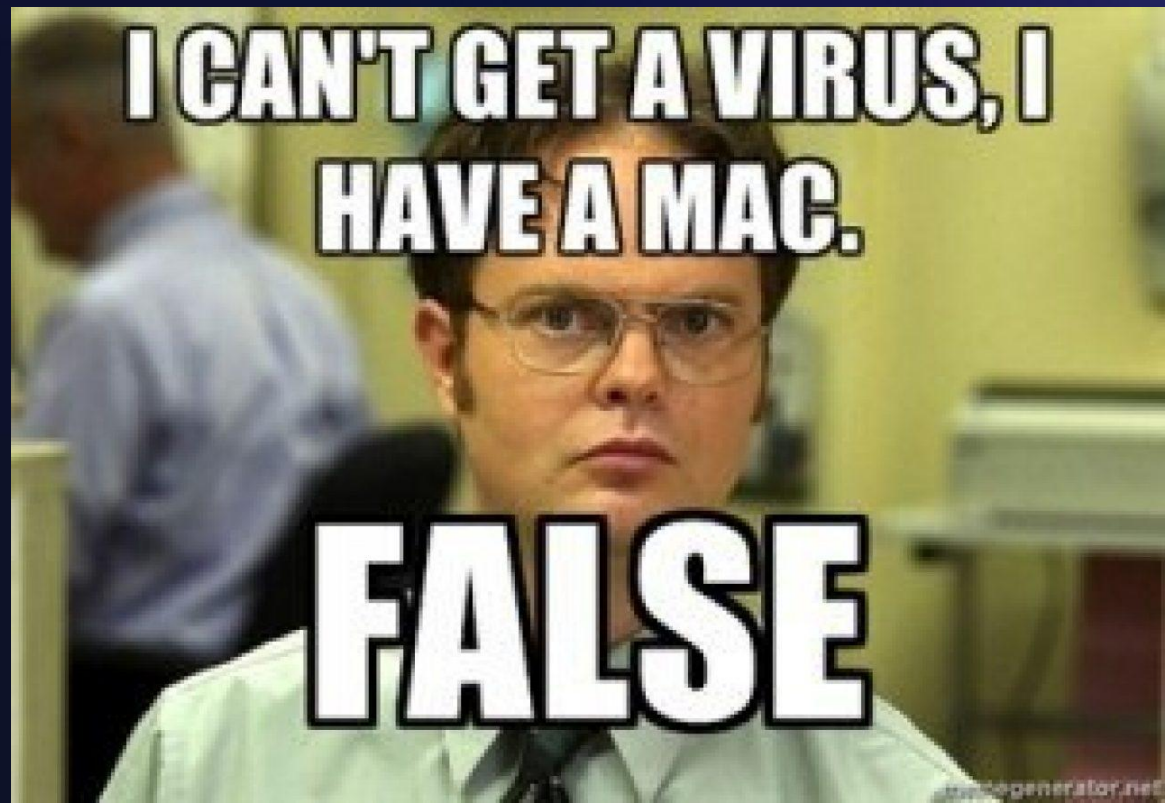
New Domains

Pentera Labs

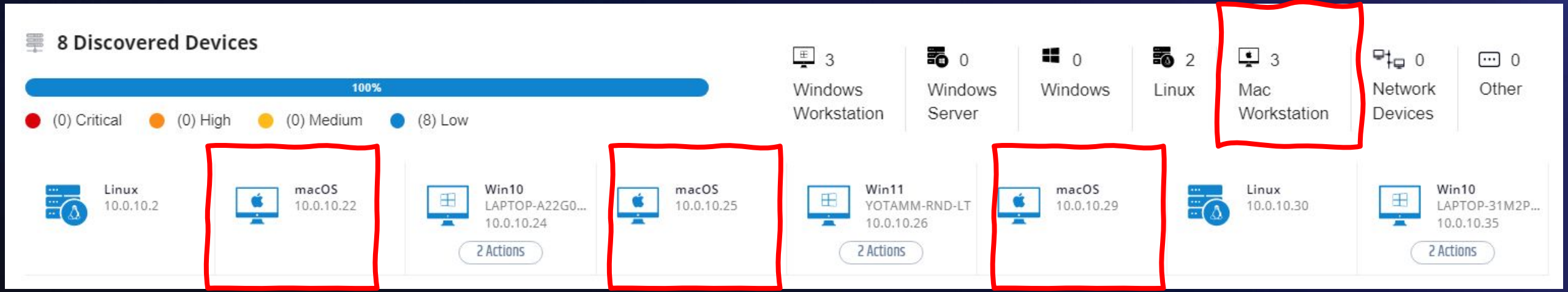
PENTERA

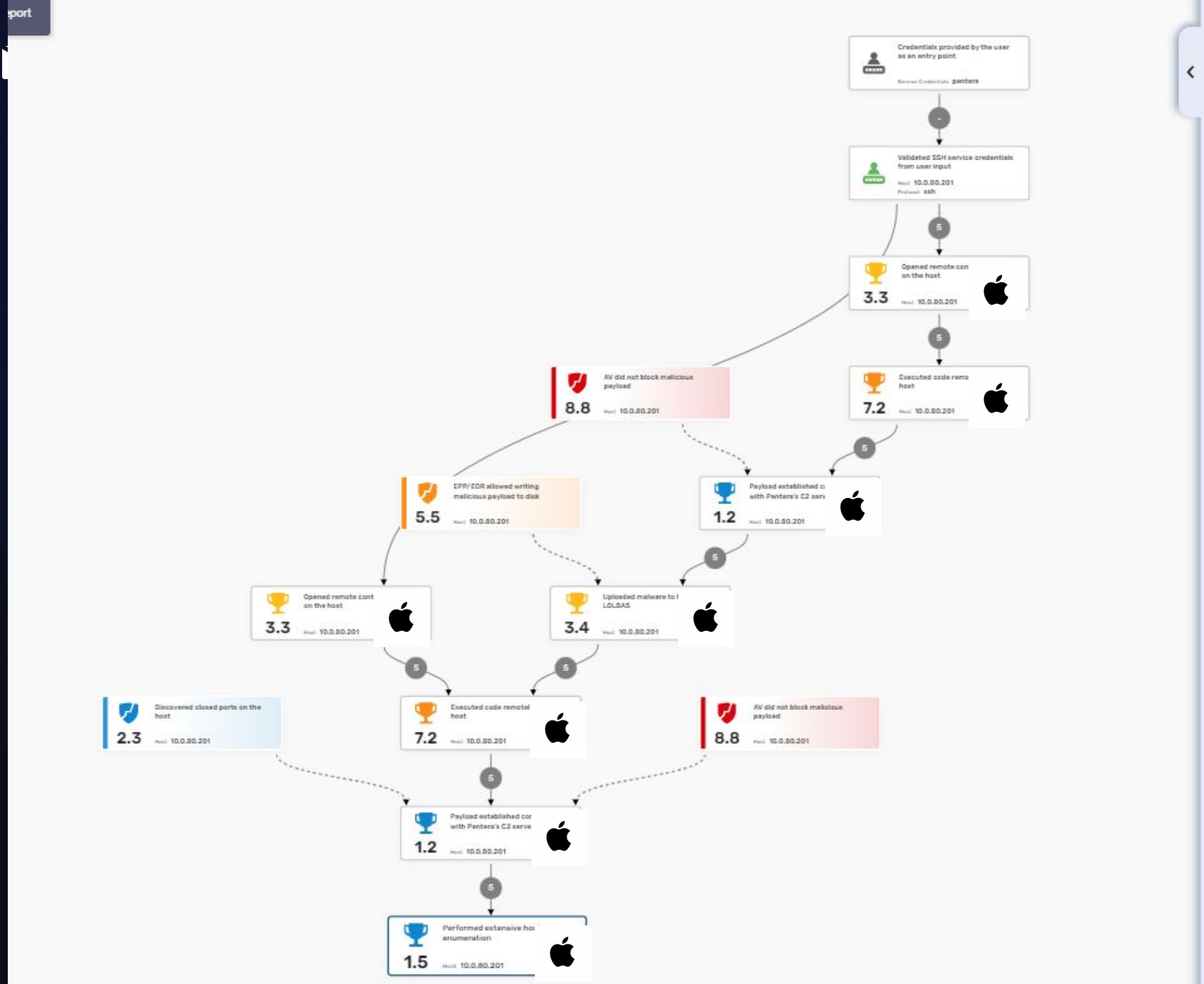
MacOS Attack Surface

- MacOS users often perceive a false sense of security
- Growing macOS usage
- BYOD policy == Shadow IT



PENTERA


8 Discovered Devices
100%
(0) Critical
(0) High
(0) Medium
(8) Low
3 Windows Workstation
0 Windows Server
0 Windows
2 Linux
3 Mac Workstation
0 Network Devices
0 Other
Linux 10.0.10.2
macOS 10.0.10.22
Win10 LAPTOP-A22G0... 10.0.10.24
2 Actions
macOS 10.0.10.25
Win11 YOTAMM-RND-LT 10.0.10.26
2 Actions
macOS 10.0.10.29
Linux 10.0.10.30
Win10 LAPTOP-31M2P... 10.0.10.35
2 Actions



Details

1.5 Performed extensive host enumeration

Parameters

IP: 10.0.80.201

Results

Local Account (2)
Network Interface (1)
Physical Data (1)
Installed Program (271)

Details

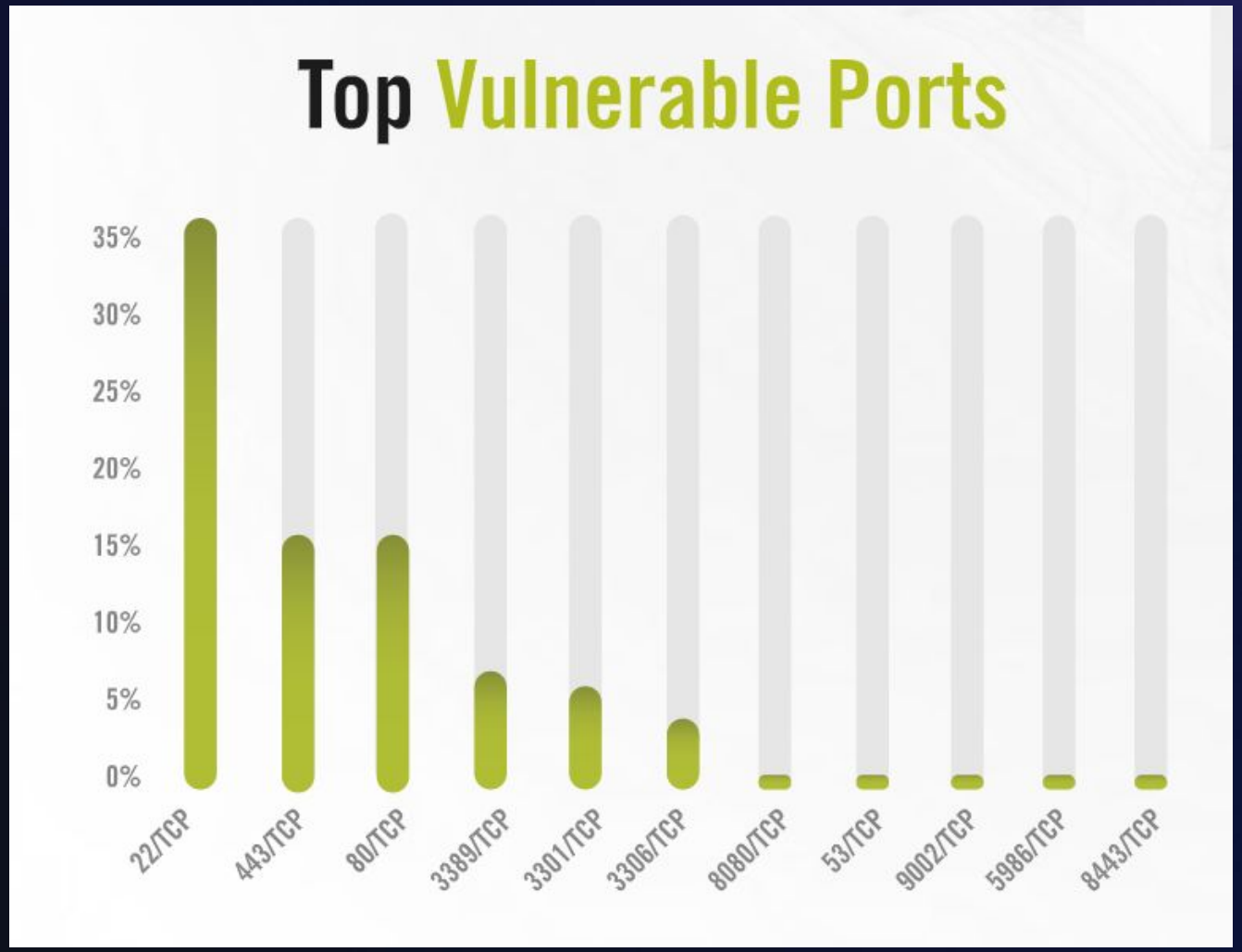
Time: Apr 24, 2023 12:56
IPv4: 10.0.80.201
OS: macOS Monterey
Vendor: Apple
MITRE Technique(s): Data from Local System (T1005) ,Process Discovery (T1057) ,Application Layer Protocol (T1071) ,Web Protocols (T1071.001) ,File Transfer Protocols (T1071.002) ,Non-Application Layer Protocol (T1095) ,Ingress Tool Transfer (T1105) ,System Services (T1569) ,Service Execution (T1569.002) ,Exfiltration Over Alternative Protocol (T1048) ,Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) ,Indicator Removal (T1070) ,File Deletion (T1070.004)

Related Actions

OsaScriptInvokerLolbas
Execution of a command over SSH
Deleted malware's payload
Established connection with remote malware
Host profiling
Injected malware to host
MacOSHostRecon
CurlLolbas

PENTERA

HTTP/HTTPS Attack Surface



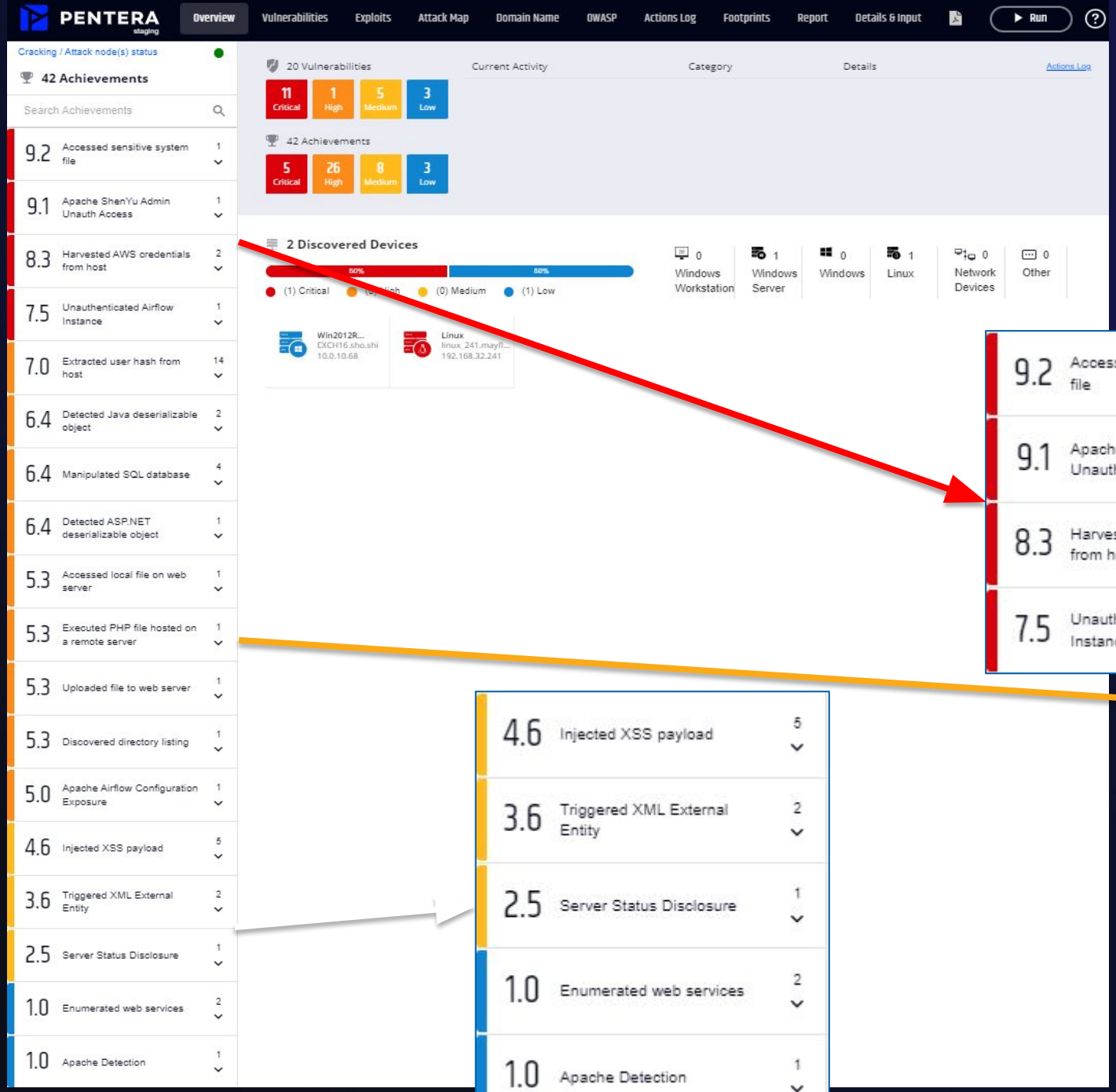
PENTERA

HTTP/HTTPS Attack Surface

PENTERA

HTTP/HTTPS Attack Surface

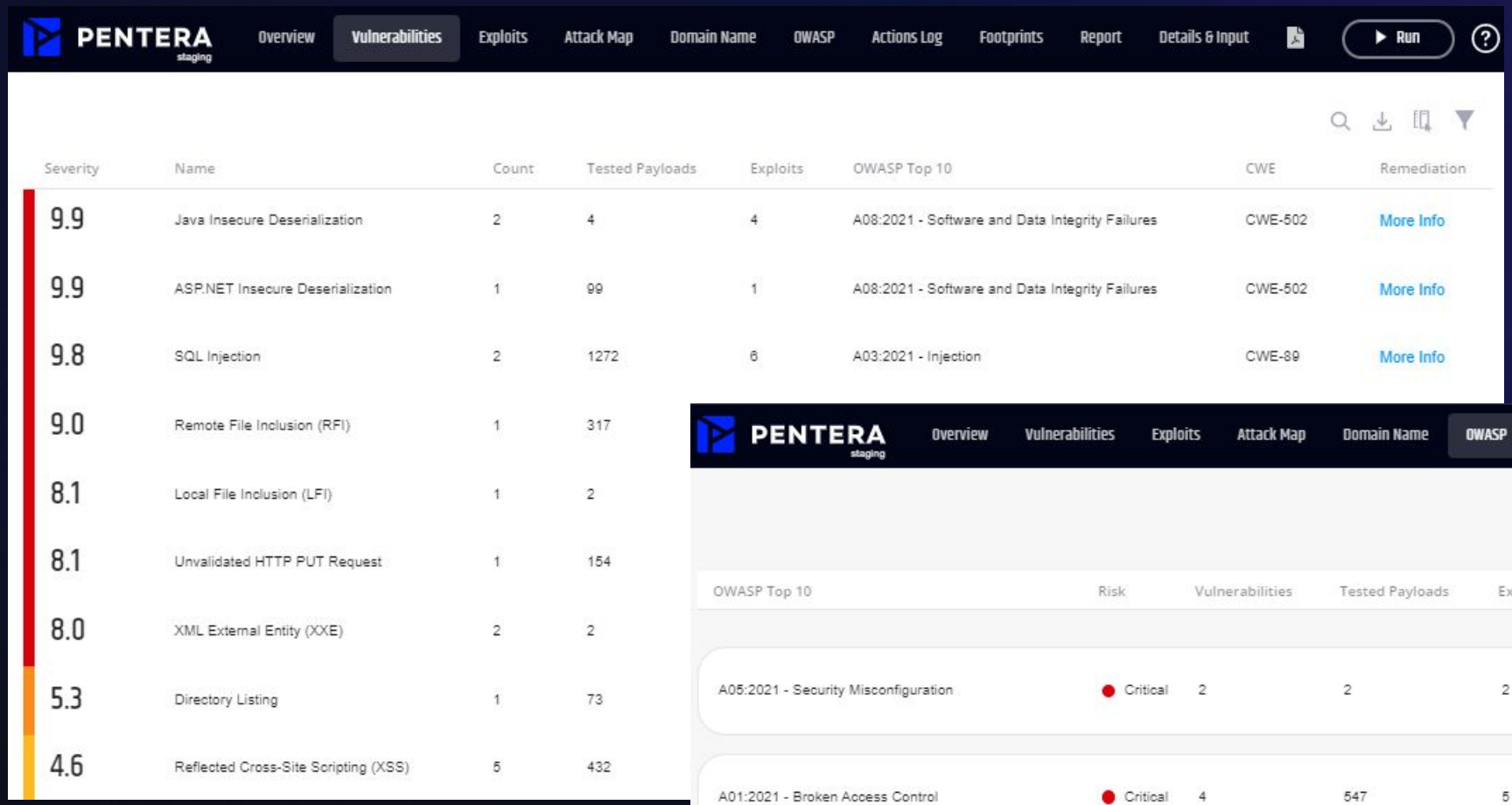
- Data protection
- Access control
- ompliance
- Secure communications
- Application Security
- Secure APIs

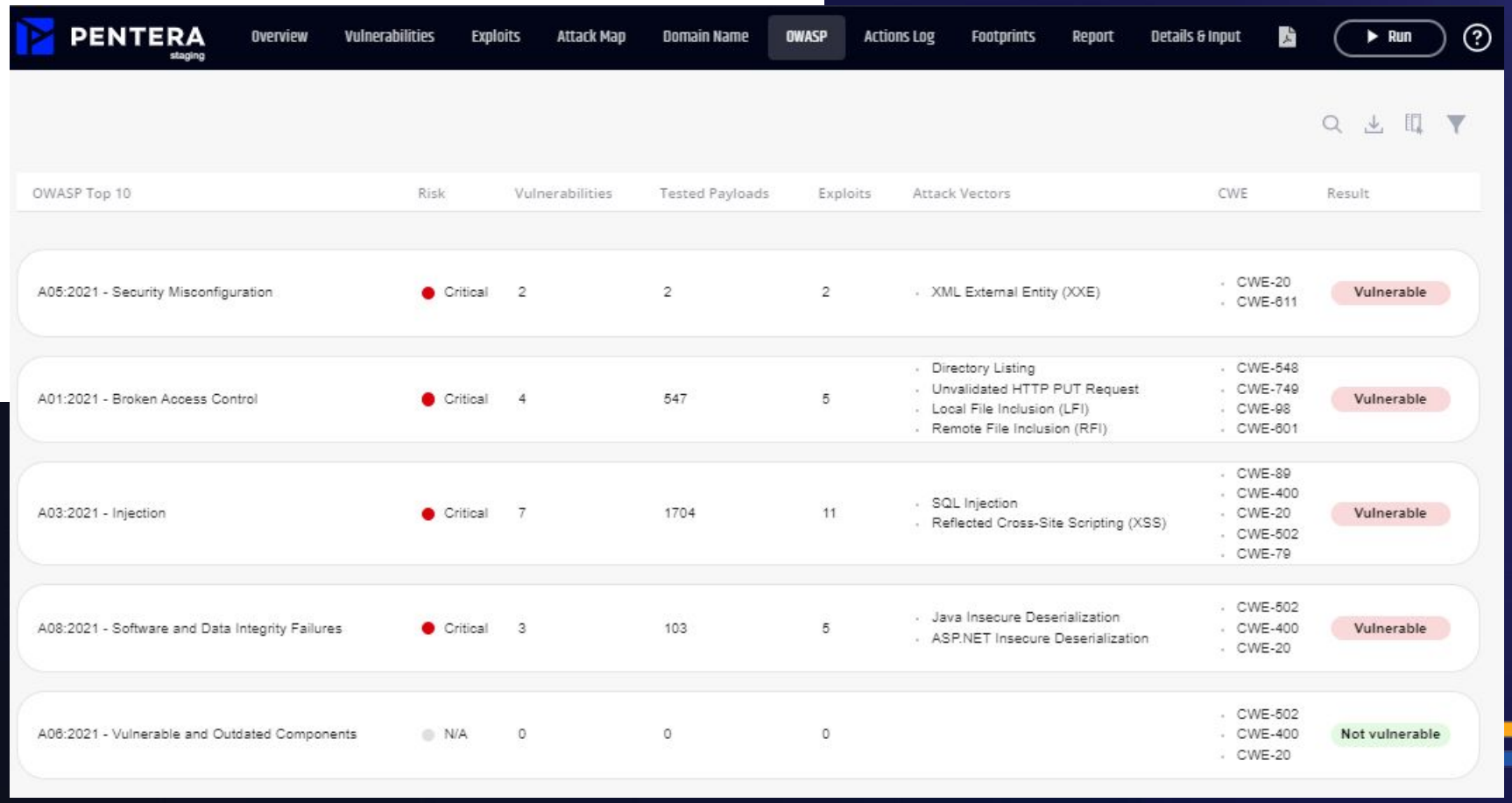


9.2 Accessed sensitive system file 1
9.1 Apache ShenYu Admin Unauth Access 1
8.3 Harvested AWS credentials from host 2
7.5 Unauthenticated Airflow Instance 1

4.6 Injected XSS payload 5
3.6 Triggered XML External Entity 2
2.5 Server Status Disclosure 1
1.0 Enumerated web services 2
1.0 Apache Detection 1

7.0 Extracted user hash from host 14
6.4 Detected Java deserializable object 2
6.4 Manipulated SQL database 4
6.4 Detected ASP.NET deserializable object 1
5.3 Accessed local file on web server 1
5.3 Executed PHP file hosted on a remote server 1
5.3 Uploaded file to web server 1
5.3 Discovered directory listing 1
5.0 Apache Airflow Configuration Exposure 1


PENTERA
staging
Overview
Vulnerabilities
Exploits
Attack Map
Domain Name
OWASP
Actions Log
Footprints
Report
Details & Input
Run
Severity
Name
Count
Tested Payloads
Exploits
OWASP Top 10
CWE
Remediation
9.9
Java Insecure Deserialization
2
4
4
A08:2021 - Software and Data Integrity Failures
CWE-502
More Info
9.9
ASP.NET Insecure Deserialization
1
99
1
A08:2021 - Software and Data Integrity Failures
CWE-502
More Info
9.8
SQL Injection
2
1272
6
A03:2021 - Injection
CWE-89
More Info
9.0
Remote File Inclusion (RFI)
1
317
8.1
Local File Inclusion (LFI)
1
2
8.1
Unvalidated HTTP PUT Request
1
154
8.0
XML External Entity (XXE)
2
2
5.3
Directory Listing
1
73
4.6
Reflected Cross-Site Scripting (XSS)
5
432


PENTERA
staging
Overview
Vulnerabilities
Exploits
Attack Map
Domain Name
OWASP
Actions Log
Footprints
Report
Details & Input
Run
OWASP Top 10
Risk
Vulnerabilities
Tested Payloads
Exploits
Attack Vectors
CWE
Result
A05:2021 - Security Misconfiguration
Critical
2
2
2
XML External Entity (XXE)
CWE-20
CWE-611
Vulnerable
A01:2021 - Broken Access Control
Critical
4
547
5
Directory Listing
Unvalidated HTTP PUT Request
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
CWE-548
CWE-749
CWE-98
CWE-601
Vulnerable
A03:2021 - Injection
Critical
7
1704
11
SQL Injection
Reflected Cross-Site Scripting (XSS)
CWE-89
CWE-400
CWE-20
CWE-502
CWE-79
Vulnerable
A08:2021 - Software and Data Integrity Failures
Critical
3
103
5
Java Insecure Deserialization
ASP.NET Insecure Deserialization
CWE-502
CWE-400
CWE-20
Vulnerable
A06:2021 - Vulnerable and Outdated Components
N/A
0
0
0
CWE-502
CWE-400
CWE-20
Not vulnerable

PENTERA

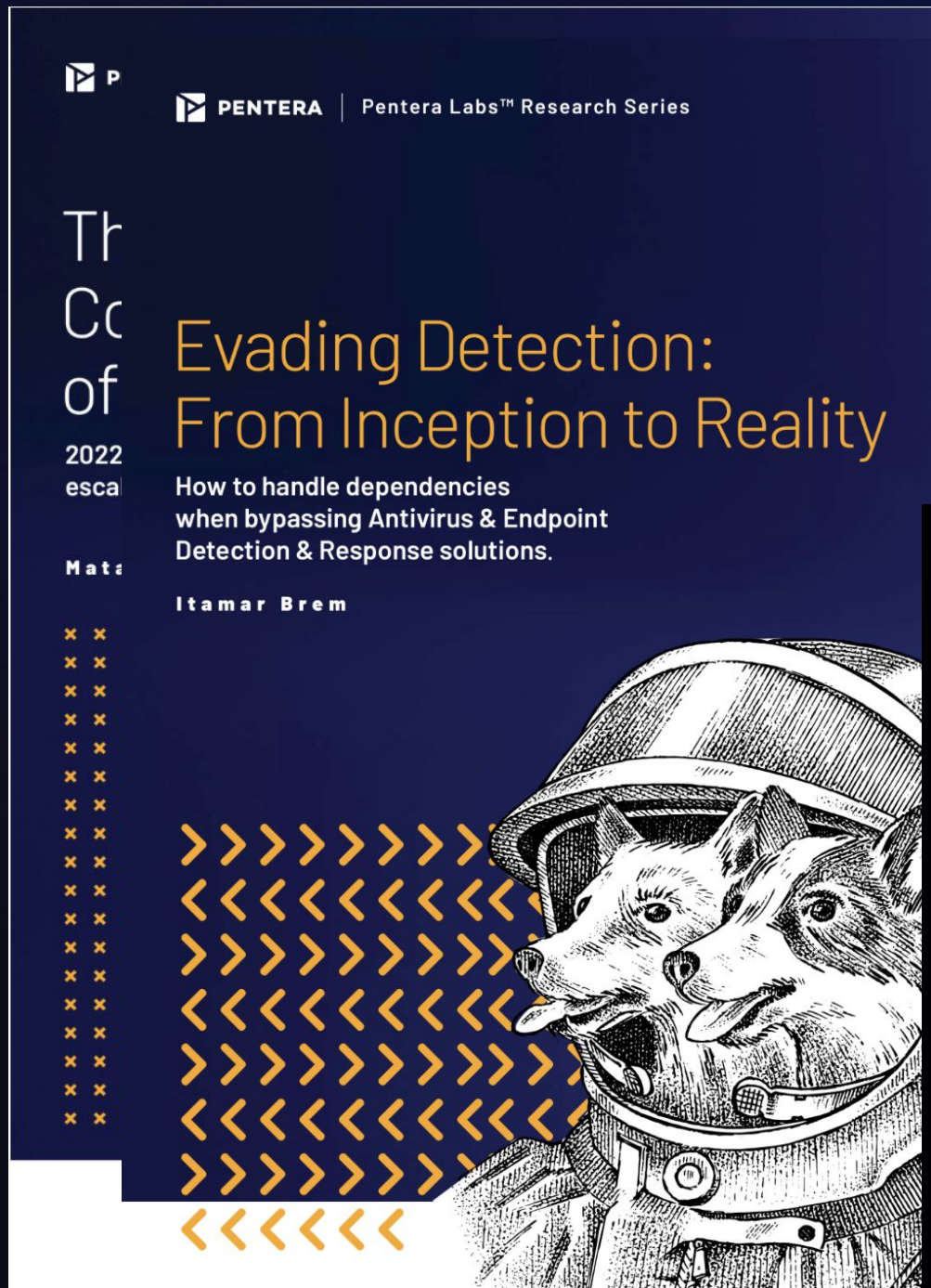
Outcomes of Customer Engagement

PENTERA

HTTP/HTTPS Attack Surface

Leaked Credentials

Web Platform



Pentera Labs

SUBSCRIBE NOW

Next Year:
Exciting Horizons Ahead

Email Attack Delivery

91% of Cyber Attacks Start with an Email

(Source: Security Middle East Magazine)

PENTERA

Why Emails Pose an Ongoing Pain?

Human Factor

Accessibility

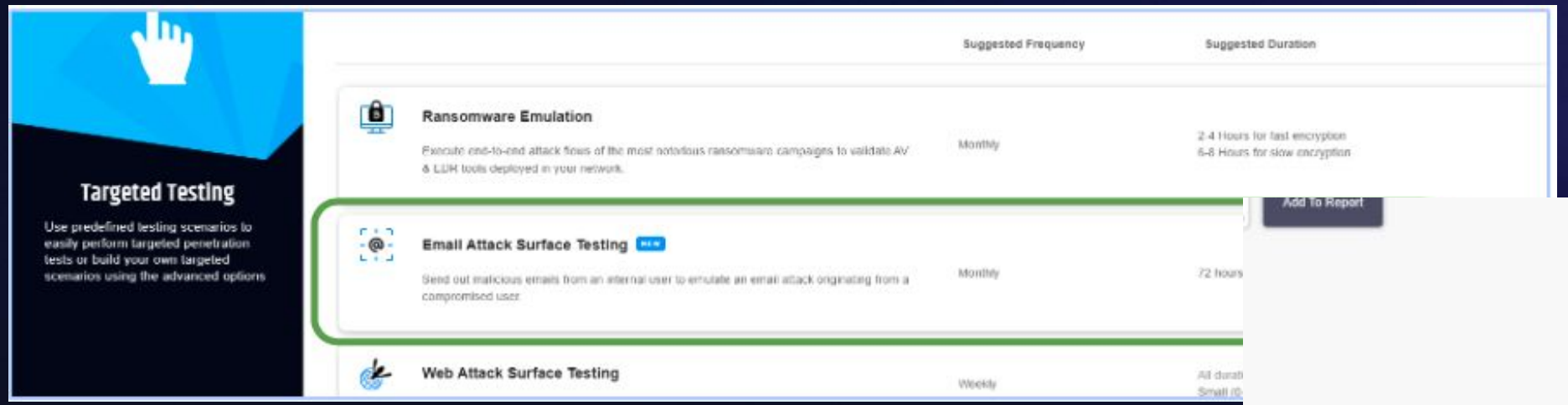
Increased Attack Surface

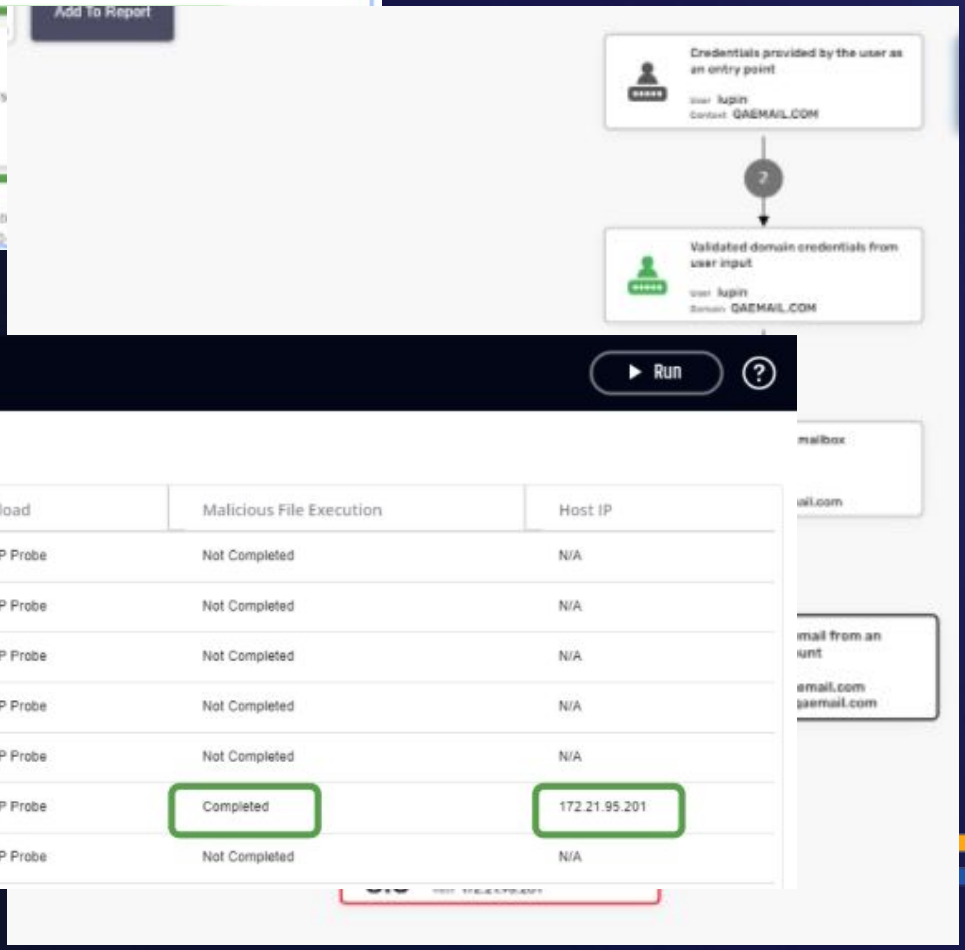
PENTERA

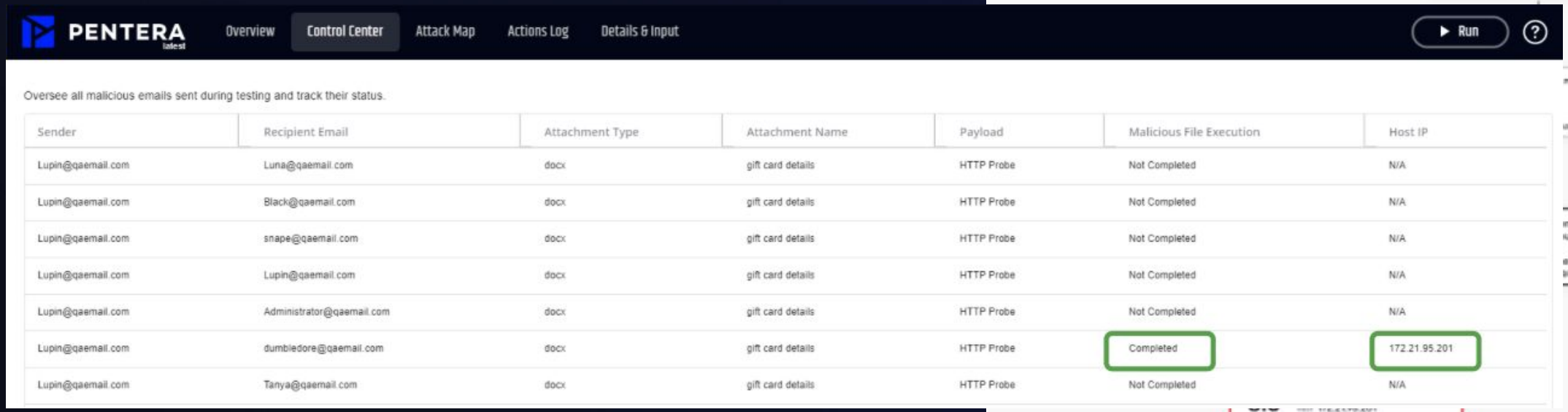
Email security checklist

- [ ] Employee Awareness
- [ ] EDR Controls
- [ ] Segmentation
- [ ] Spam filtering
- [ ] Incident Response Protocols

PENTERA


Targeted Testing
Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options
Suggested Frequency
Suggested Duration
Ransomware Emulation
Execute end-to-end attack flows of the most notorious ransomware campaigns to validate AV & EDR tools deployed in your network.
Monthly
2-4 Hours for fast encryption
6-8 Hours for slow encryption
Email Attack Surface Testing
NEW
Send out malicious emails from an internal user to emulate an email attack originating from a compromised user
Monthly
72 hours
Web Attack Surface Testing
Weekly


Add To Report
Credentials provided by the user as an entry point
User lupin
Context QAEMAIL.COM
Validated domain credentials from user input
User lupin
Domain QAEMAIL.COM


PENTERA
latest
Overview
Control Center
Attack Map
Actions Log
Details & Input
Run
Oversee all malicious emails sent during testing and track their status.
Sender
Recipient Email
Attachment Type
Attachment Name
Payload
Malicious File Execution
Host IP
Lupin@qaemail.com
Luna@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A
Lupin@qaemail.com
Black@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A
Lupin@qaemail.com
snape@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A
Lupin@qaemail.com
Lupin@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A
Lupin@qaemail.com
Administrator@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A
Lupin@qaemail.com
dumbledore@qaemail.com
docx
gift card details
HTTP Probe
Completed
172.21.95.201
Lupin@qaemail.com
Tanya@qaemail.com
docx
gift card details
HTTP Probe
Not Completed
N/A

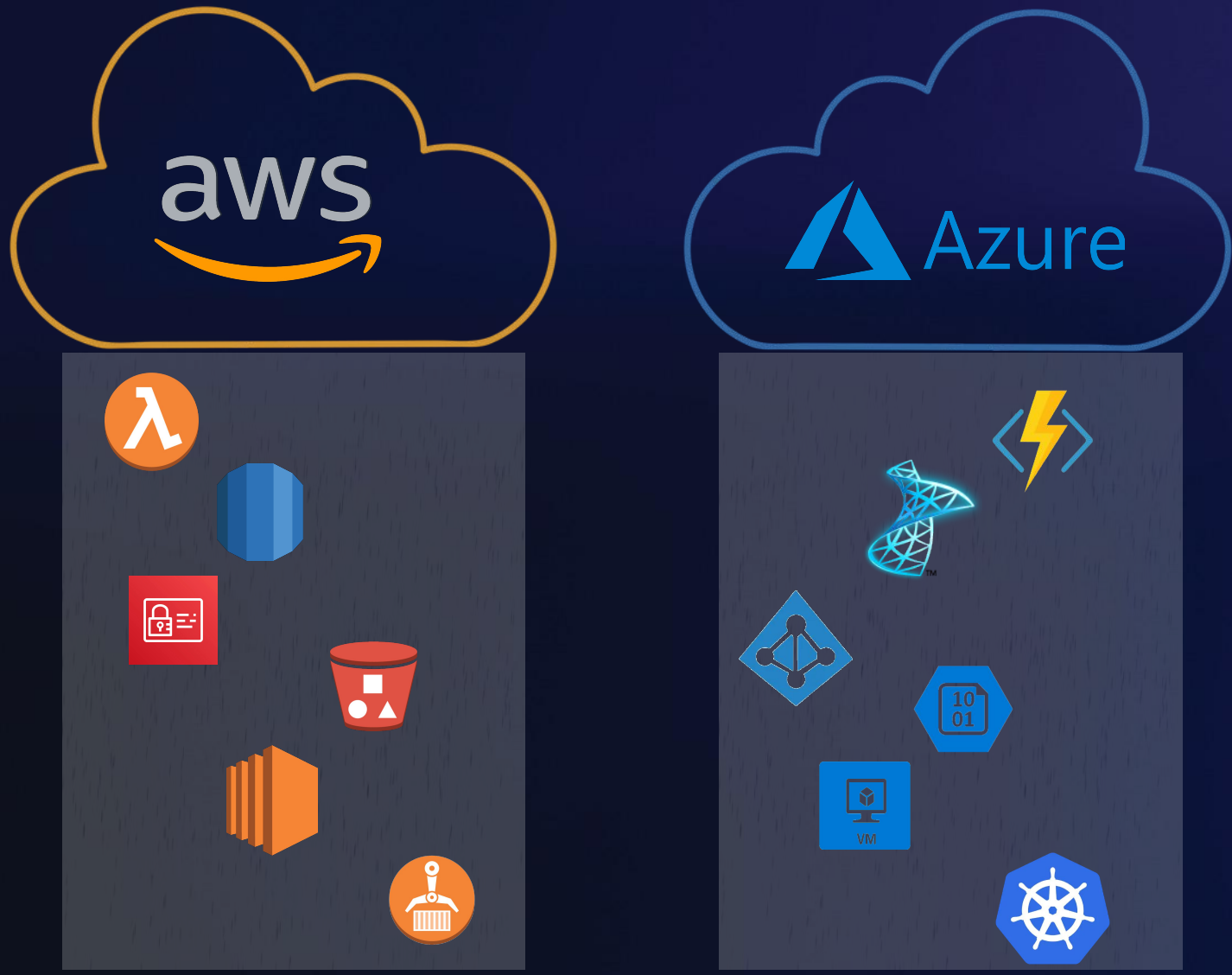
PENTERA

Email security checklist

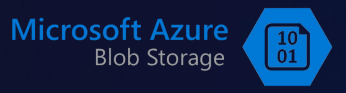
- ✓ Employee Awareness
- ✓ EDR Controls
- ✓ Segmentation
- ✓ Spam filtering
- ✓ Incident Response Protocols

PENTERA

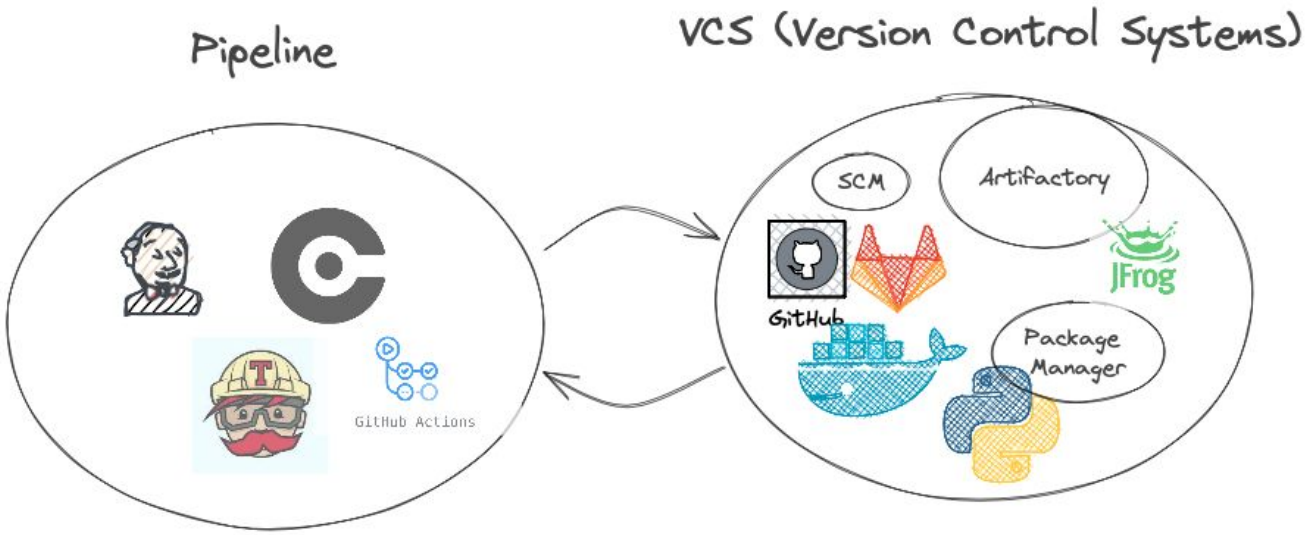
Cloud Services (”Cloud Only”)



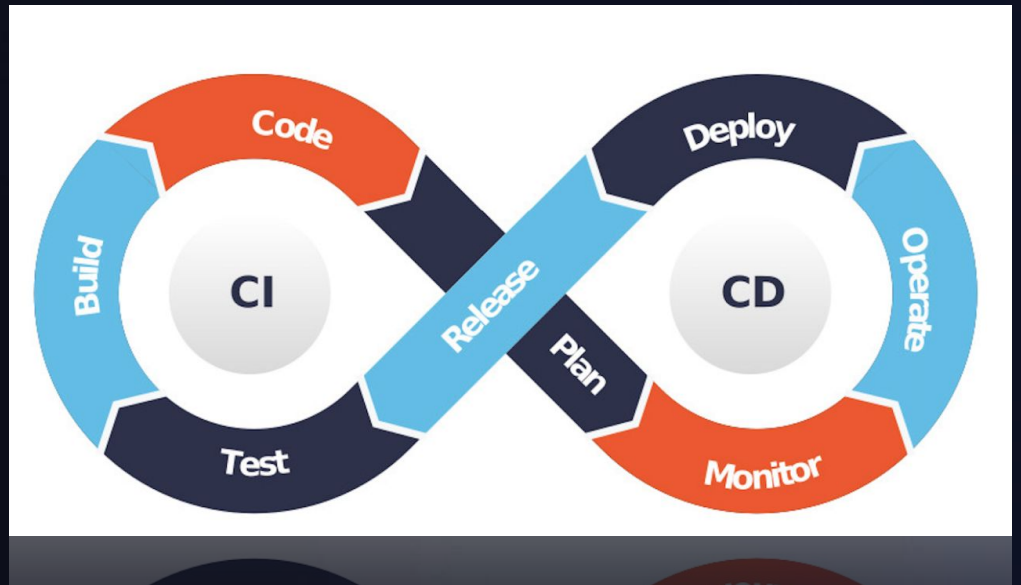
PENTERA

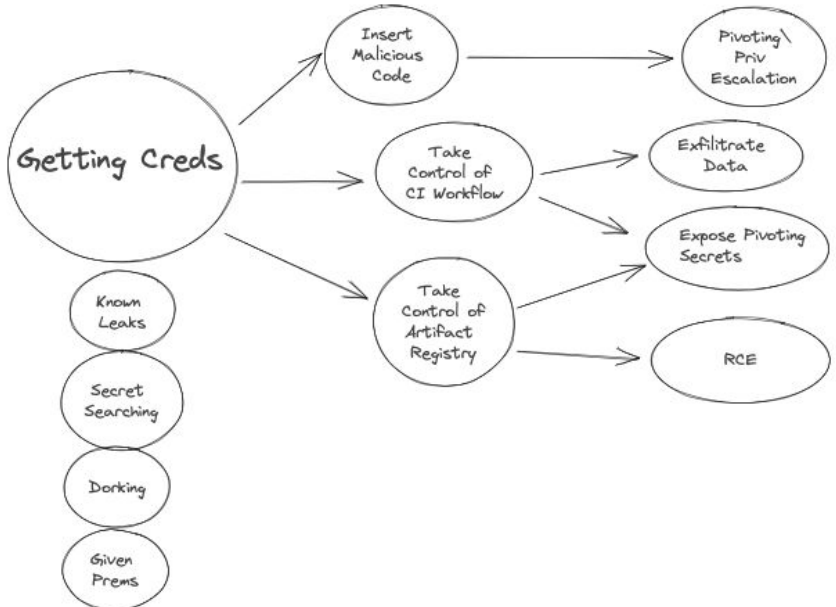
	amazon	Microsoft
Serverless Computing		
Rationale DB		
Identity Management		
Storage		
Computing		
Containerized Environments	 AWS ECR	

PENTERA



CI/CD Pipelines



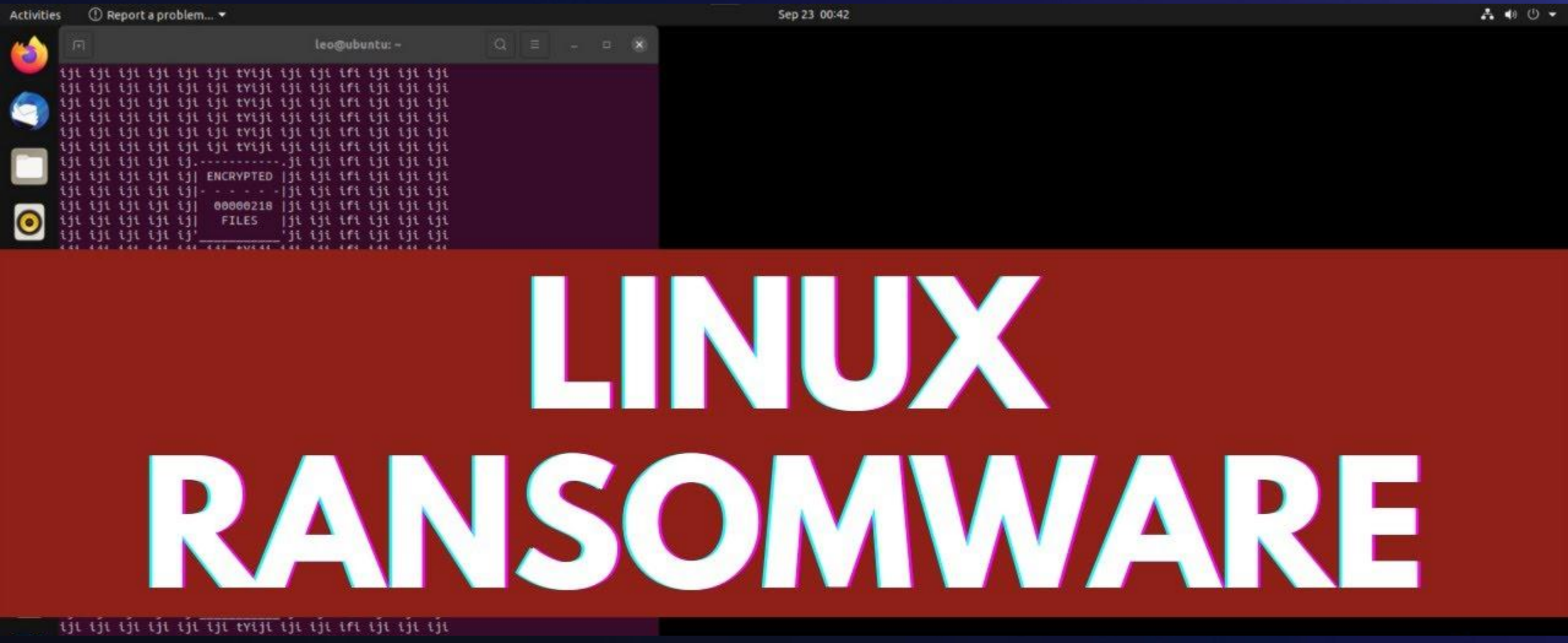


PENTERA

What About Ransomware?

PENTERA

RANSOMWARE is Alive and Kicking!



Summary

- We're committed to delivering comprehensive cyber validation, leveraging top-tier talent
- Over the past year, we've significantly expanded our capabilities, ventured into new domains, and launched the ”Pentera Labs” knowledge base
- We're just getting started!
- **Engage** with us **and become more secure!**

PENTERA

Thank You!