PENTERA

Automatiserad Pentesting

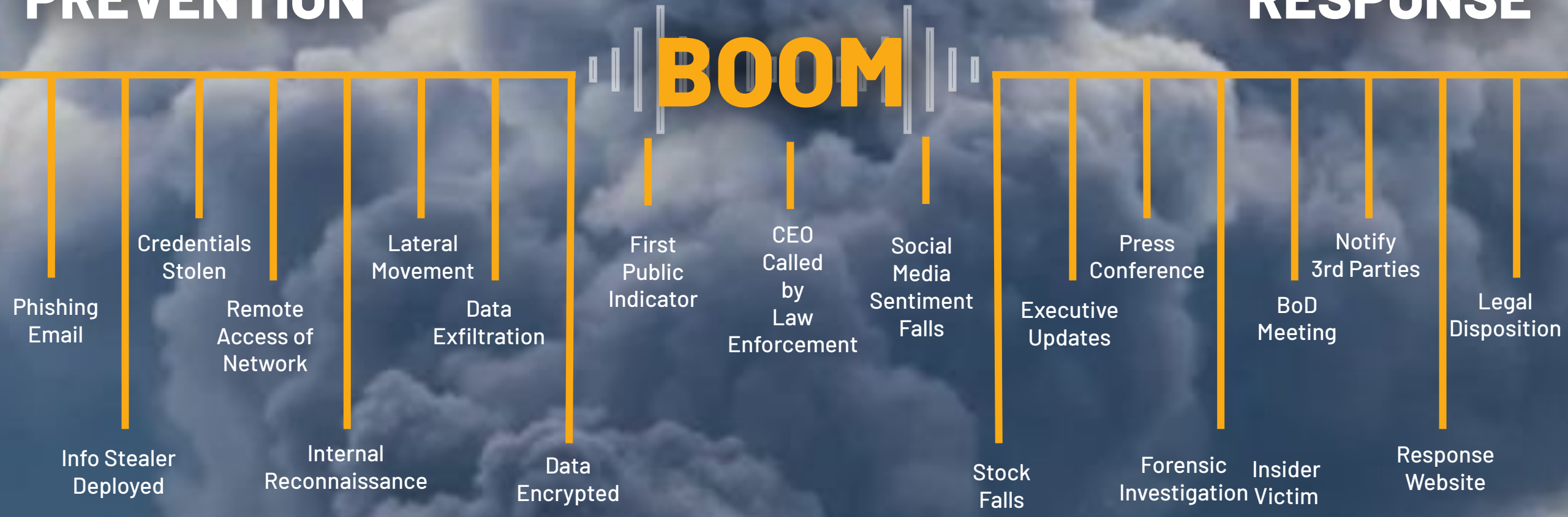
Security Validation at the Heart of **CTEM**


PENTERA
Controls not validated,
will degrade over time

PENTERA

THREAT PREVENTION

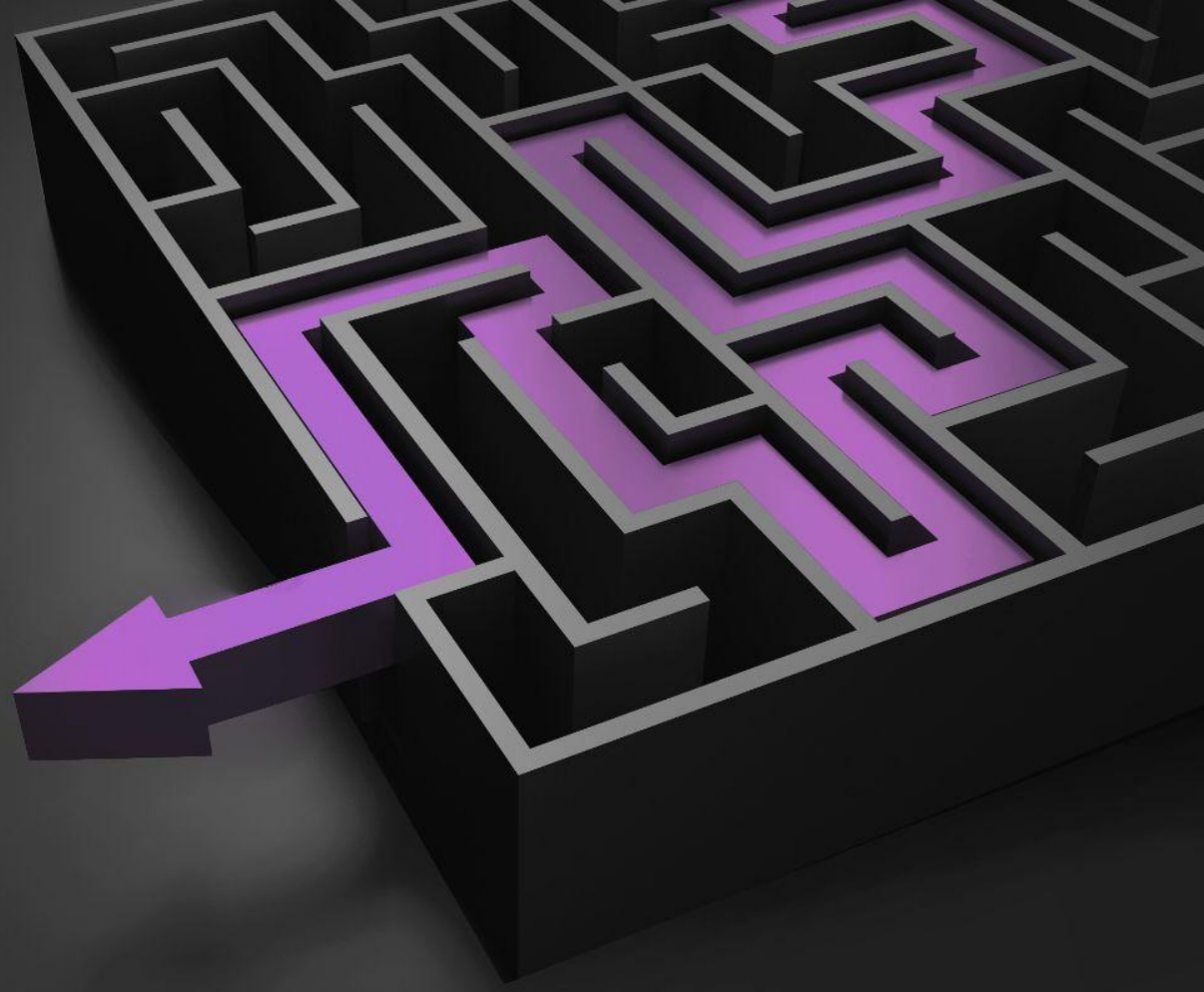
CRISIS RESPONSE



FINANCIAL IMPACT ASSESSMENT

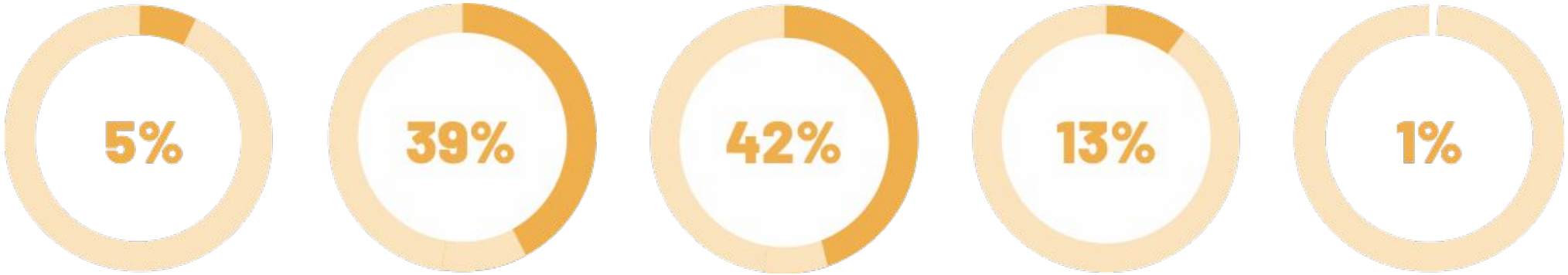
REGULATOR INVESTIGATION

PENTERA

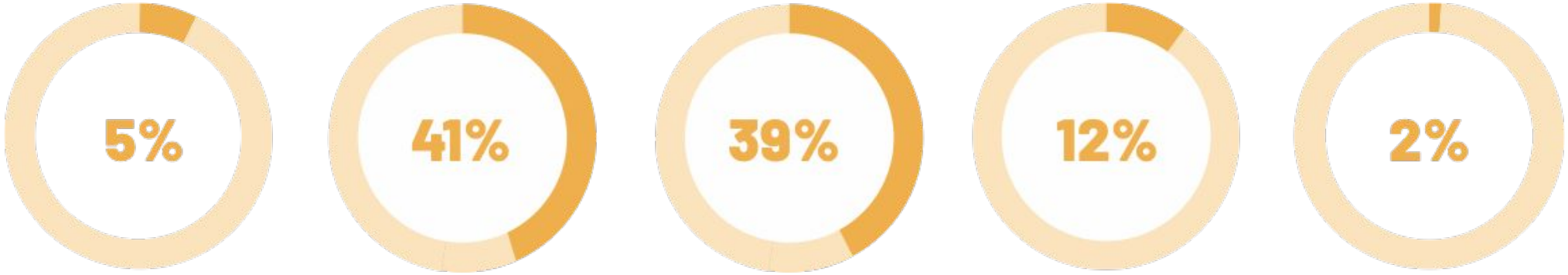


THE STATE OF PENTESTING 2024

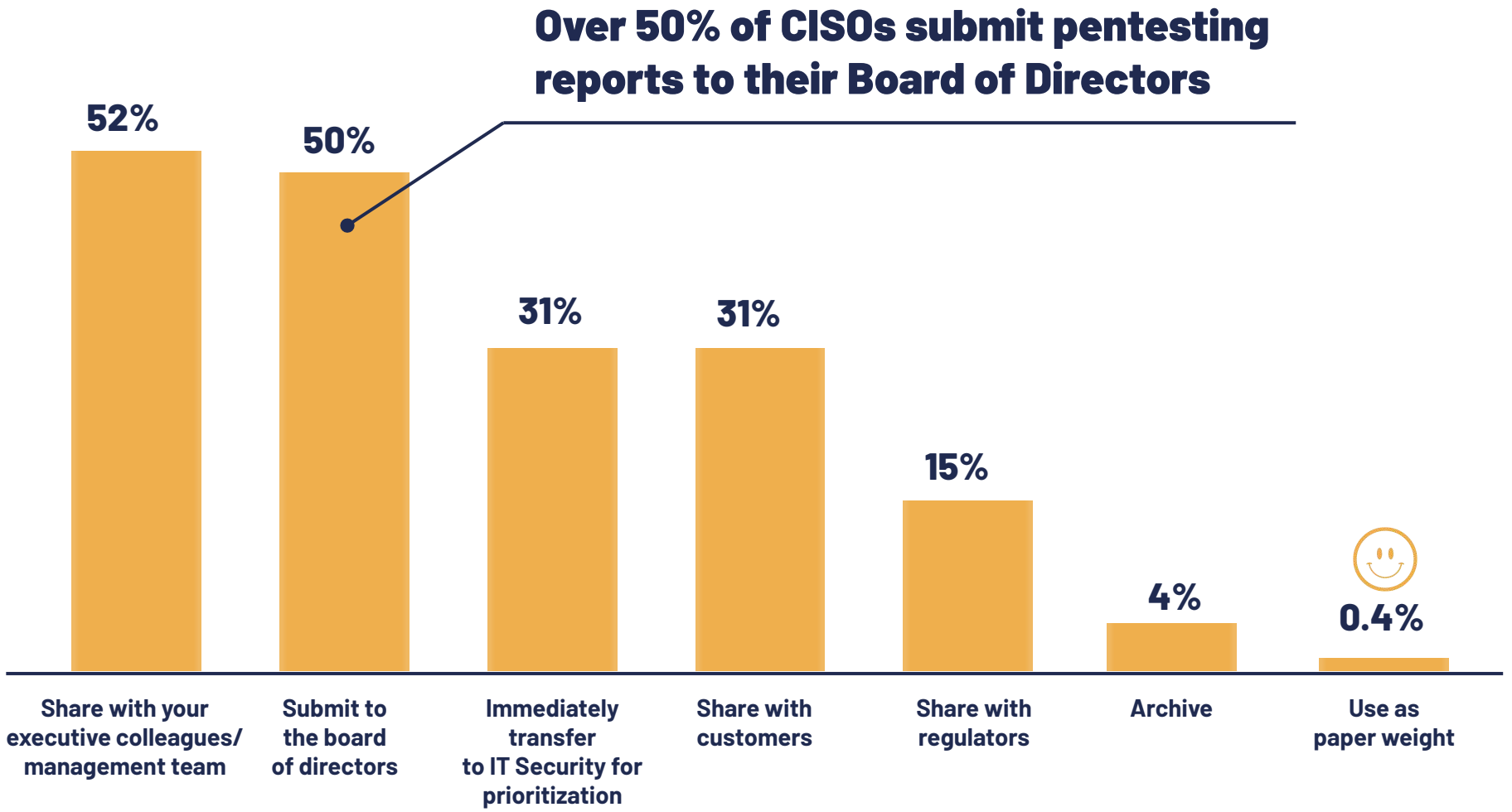
Your annual PENTESTING budget for 2024 is due to:



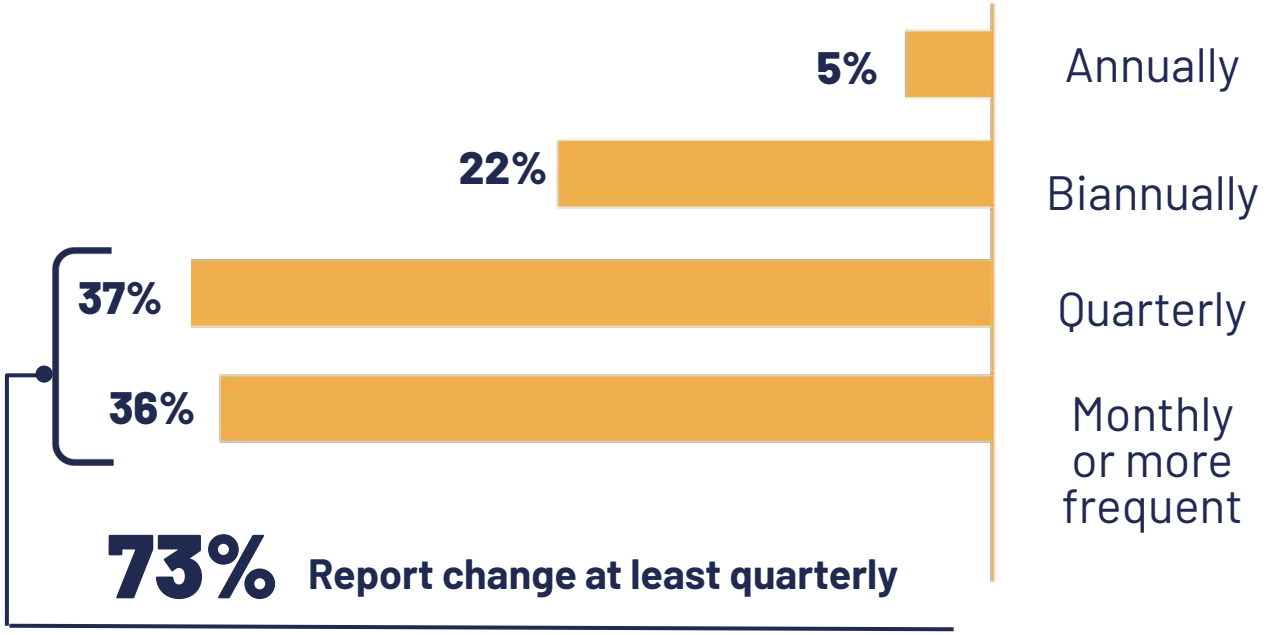
Your annual OVERALL IT Security budget for 2024 is due to:



What CISOs do with their pentesting report

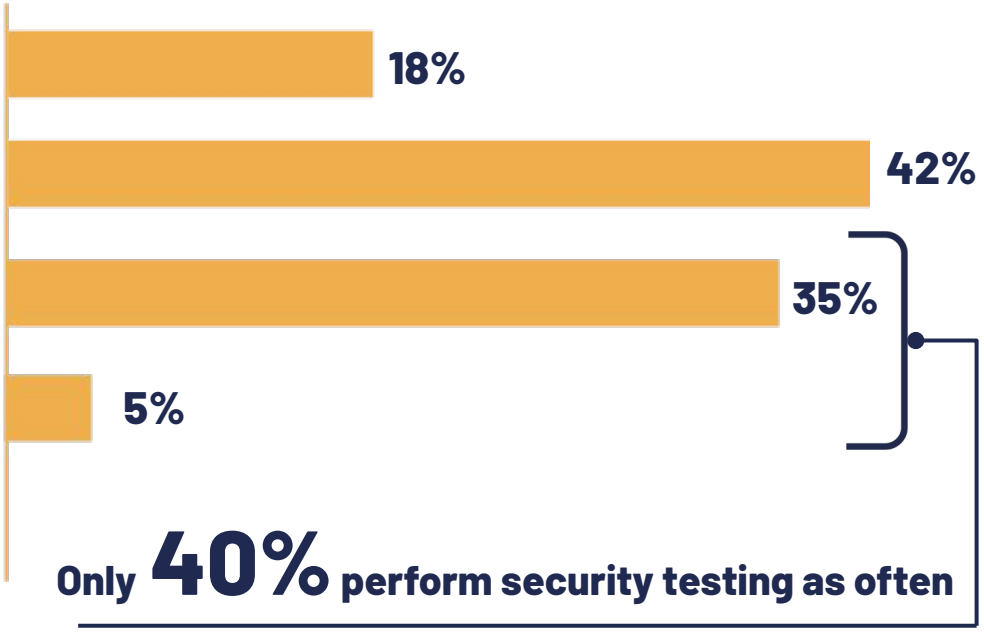


How often are you adding/subtracting resources to/from your network?



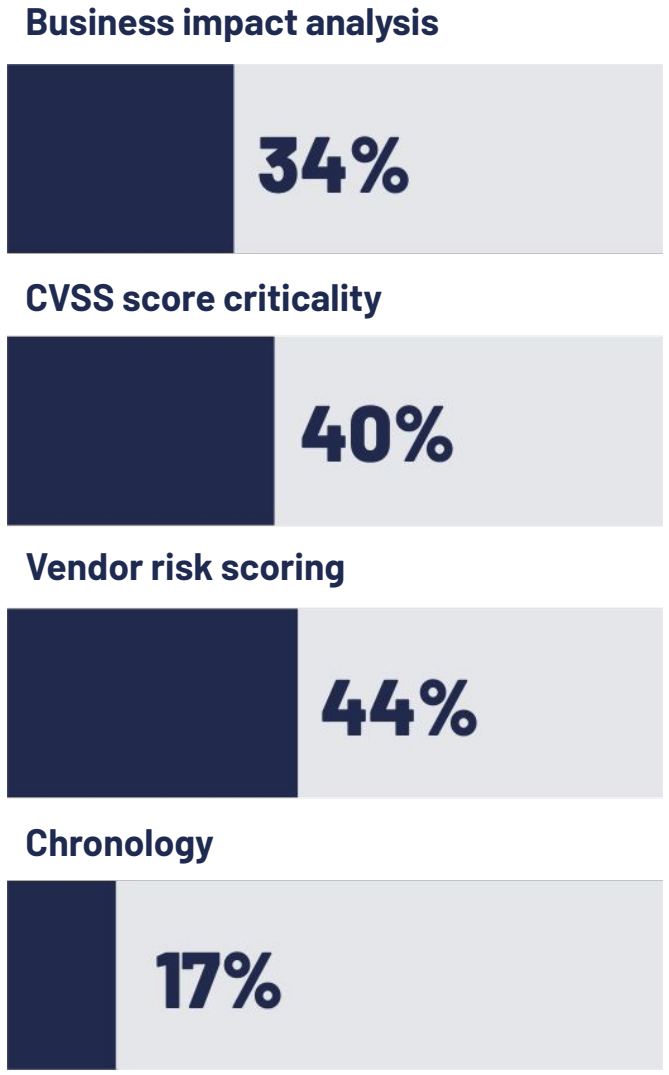
73% Report change at least quarterly

How often does your organization conduct manual pentest assessments?

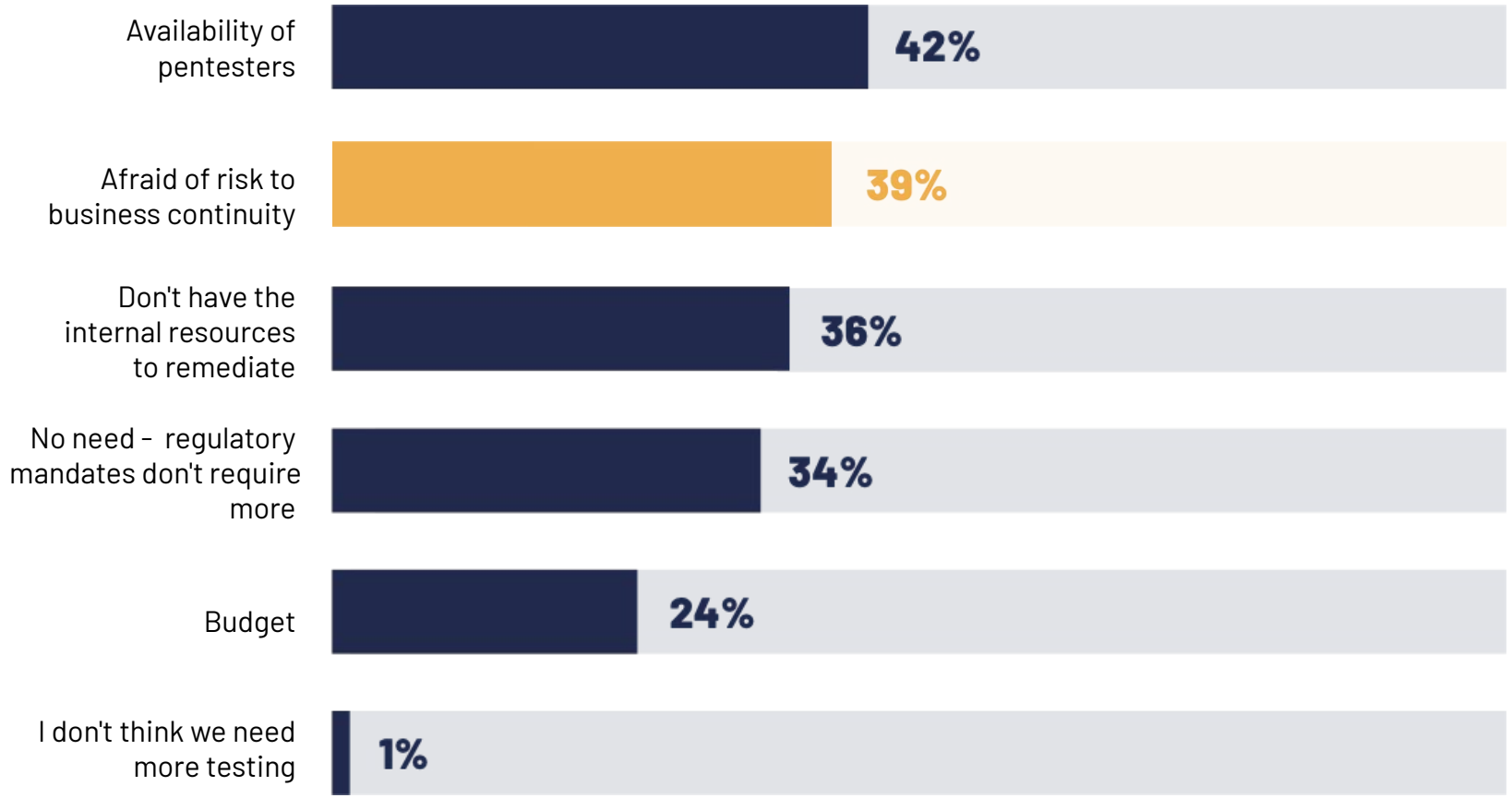


Only **40%** perform security testing as often

How are remediations prioritized?

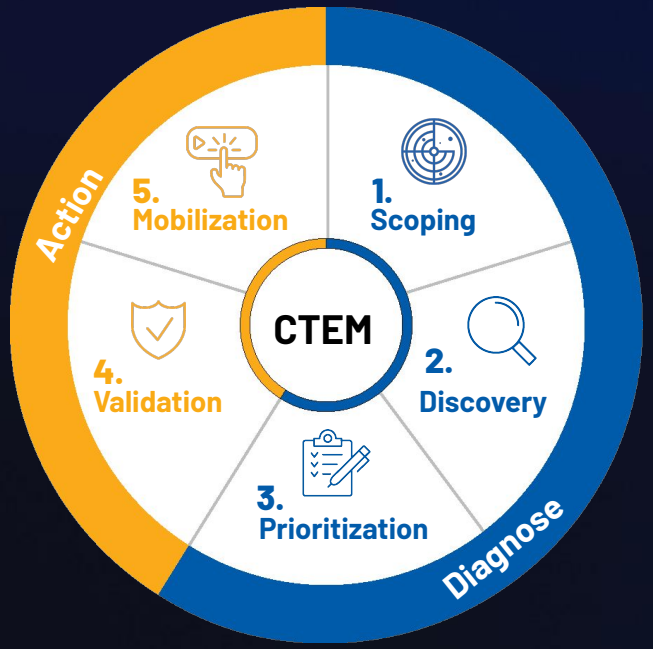


Barriers to pentesting



PENTERA

Continuous Threat Exposure Management (CTEM)



By 2026, organizations that **prioritize** their security investments based on a **continuous exposure** management program will be 3x less likely to suffer a breach

Source: Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023

PENTERA

CHALLENGES

PENTERA

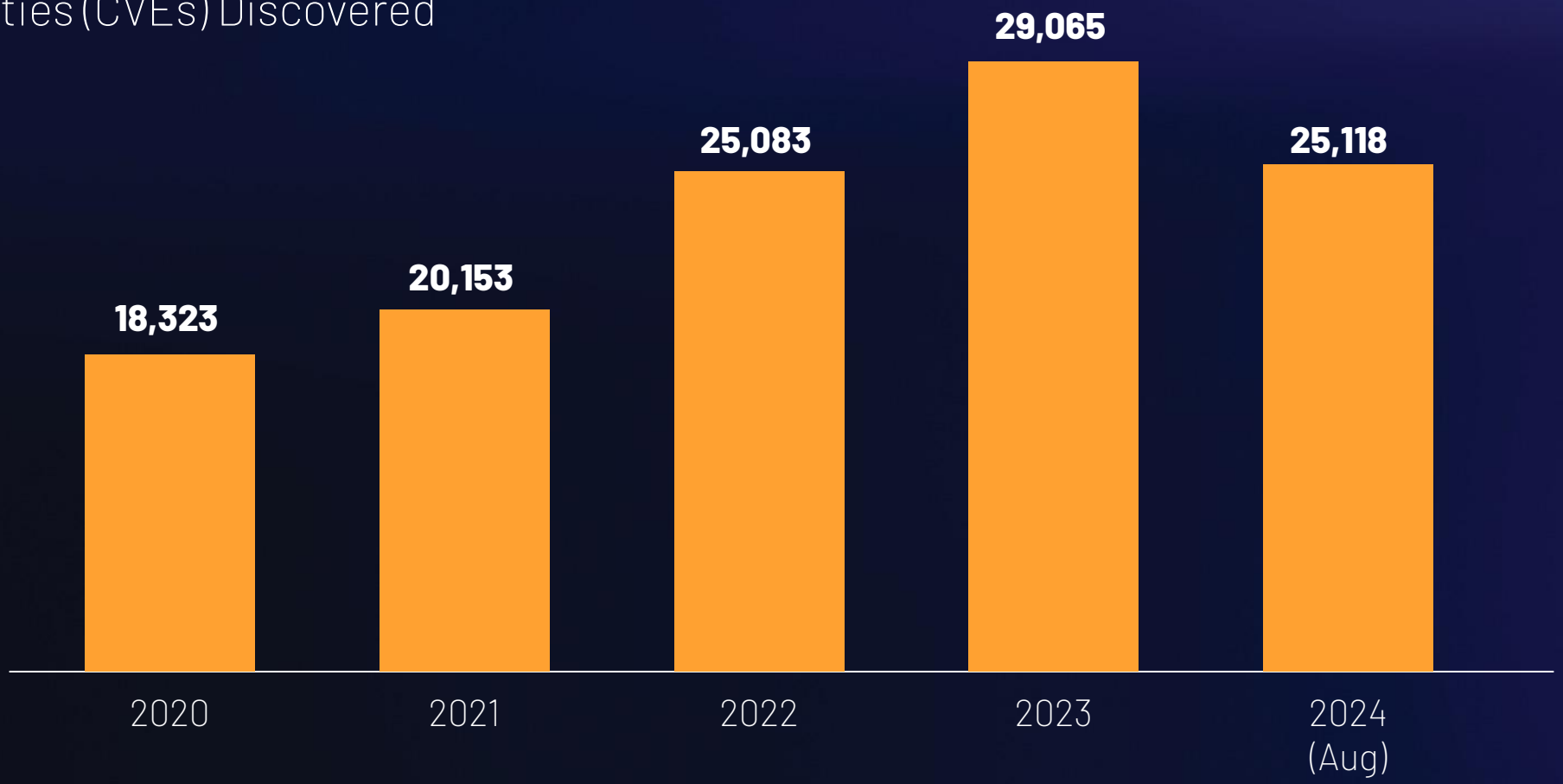
The traditional mindset

> **...a vulnerability is something I can patch**

PENTERA

Reality Check - We Can Never be **Patch Perfect**

Vulnerabilities (CVEs) Discovered

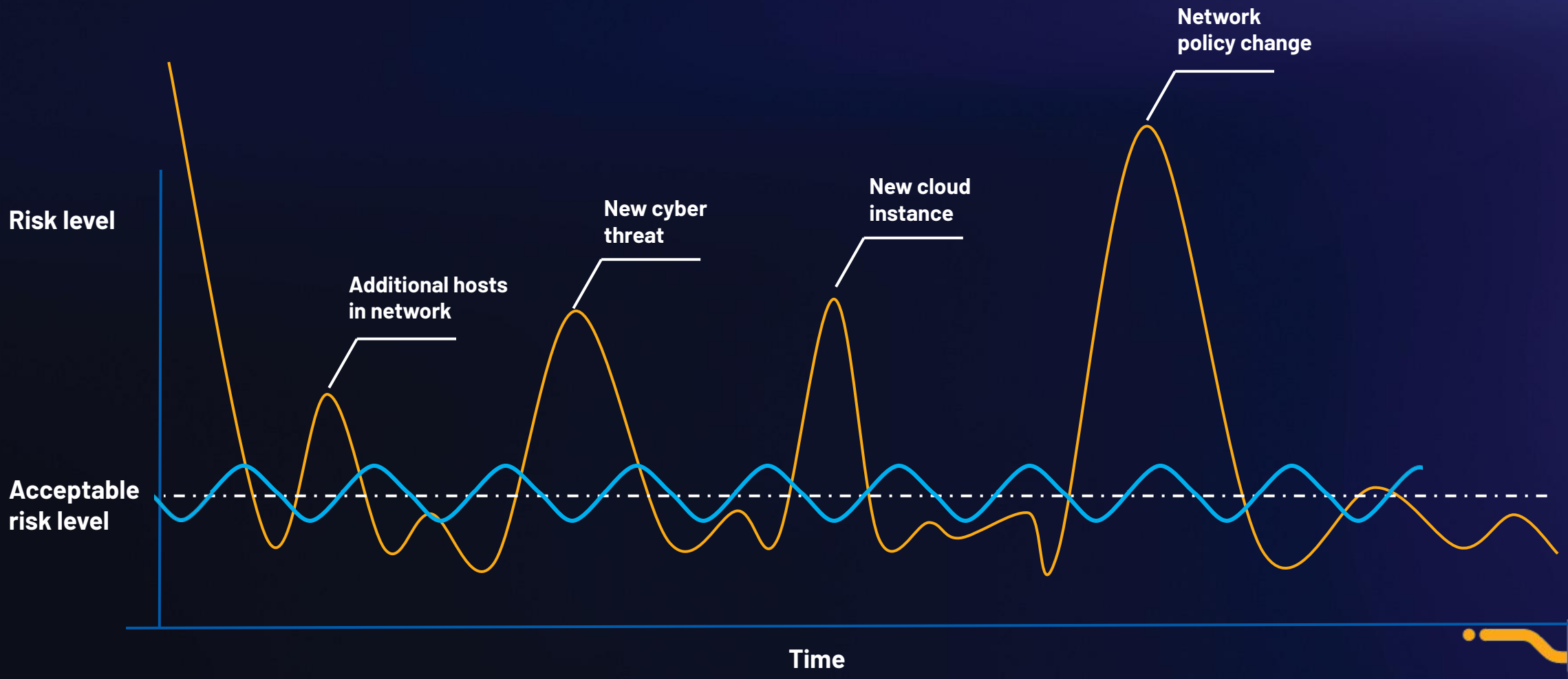


Source: https://www.cvedetails.com/

PENTERA

Challenge #1: Constantly Changing

Attack Surfaces and Risk Exposure



PENTERA

Challenge #2: Ineffective Remediation
with Traditional Vulnerability-Centric Approaches

> Non-patchable attack surfaces will account for **over 50%** of enterprise exposure by 2026.
>
> Gartner®

MISCONFIGURATION

PRIVILEGES

HUMAN ERROR

LEAKED CREDENTIALS

DATA HYGIENE

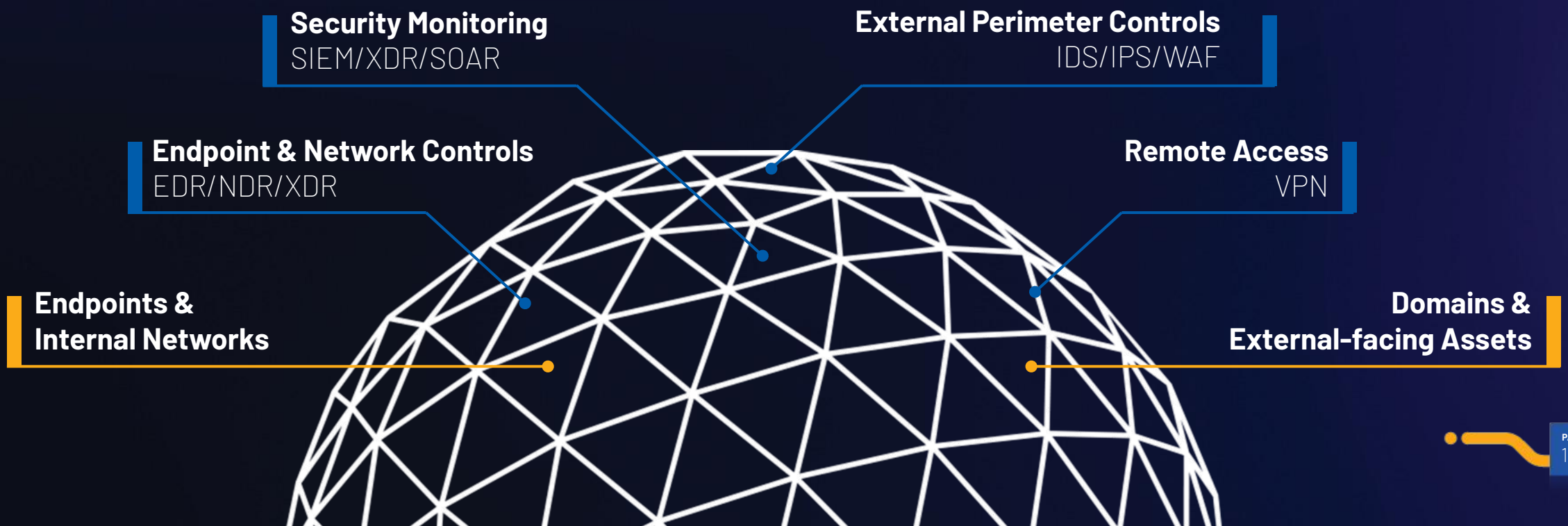
Source: Gartner, “Predicts 2023: Enterprises Must Expand From Threat to Exposure Management”, December 2022

PENTERA

Challenge #3: Security & Policy gaps

DO YOUR CYBER DEFENSES TRULY WORK TODAY

Against The Latest Threats?

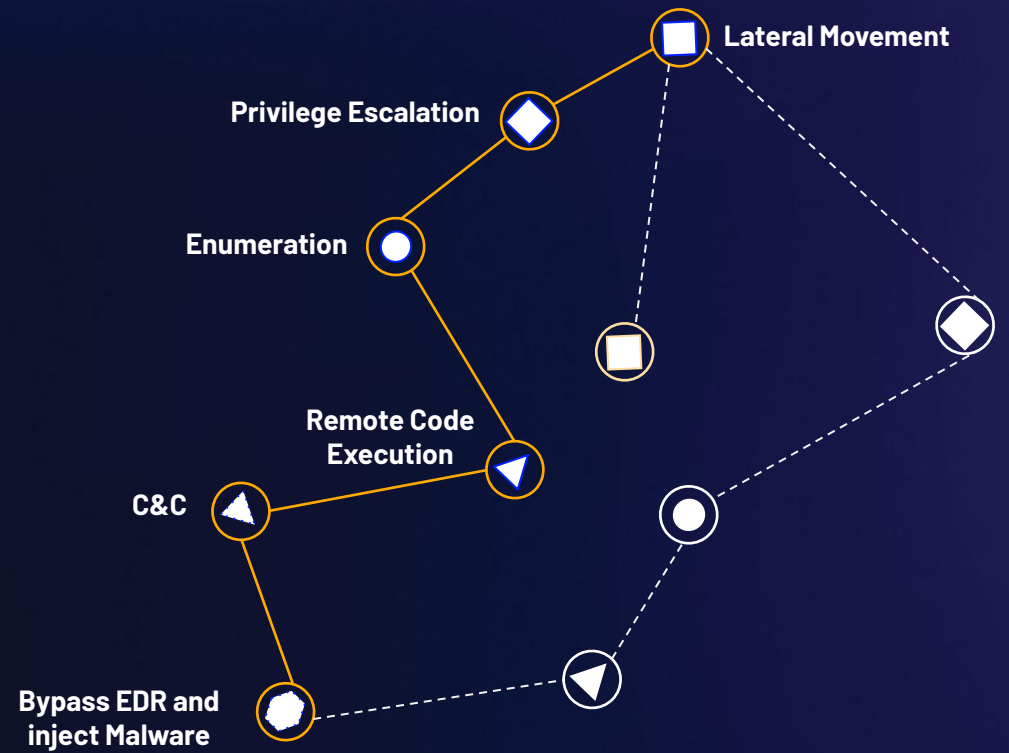


PENTERA

Take the Attacker's View with

SECURITY VALIDATION

Test your entire attack surface
Reveal true exposure
Prioritize fixes based on risk impact



PENTERA

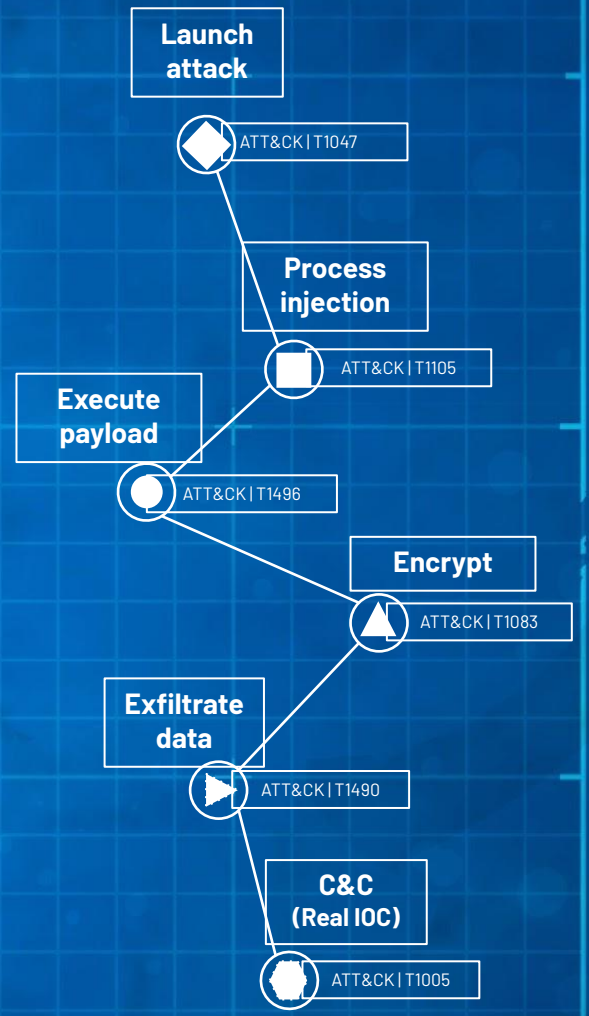
Ransomware Readiness Blueprint

Account Susceptibility

Credentials provided by the user as an entry point

User veritas

Context PENTERA.LAB



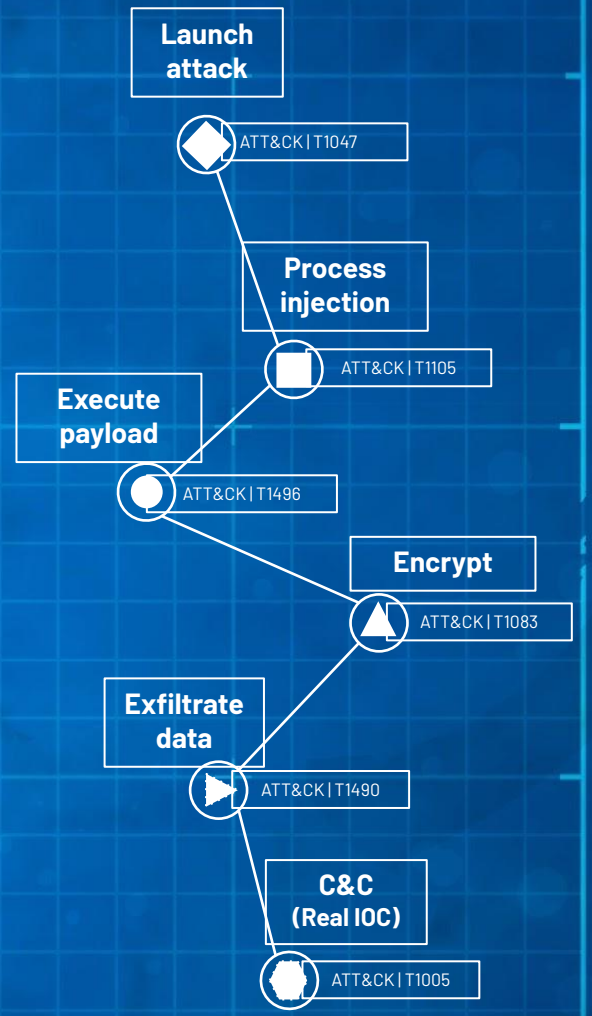
PENTERA

Ransomware Readiness Blueprint

Validate Credentials

Validated domain credentials from user input

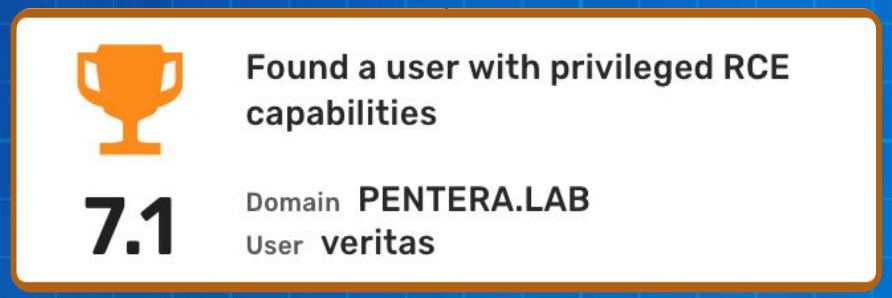
User veritas
Domain PENTERA.LAB

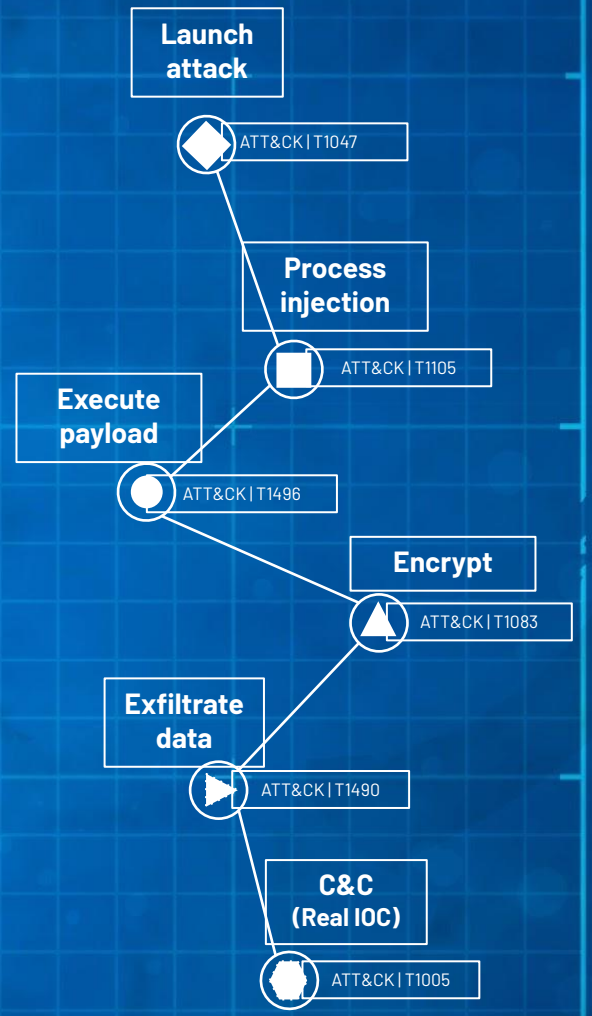


PENTERA

Ransomware Readiness Blueprint

Privilege Escalation





PENTERA

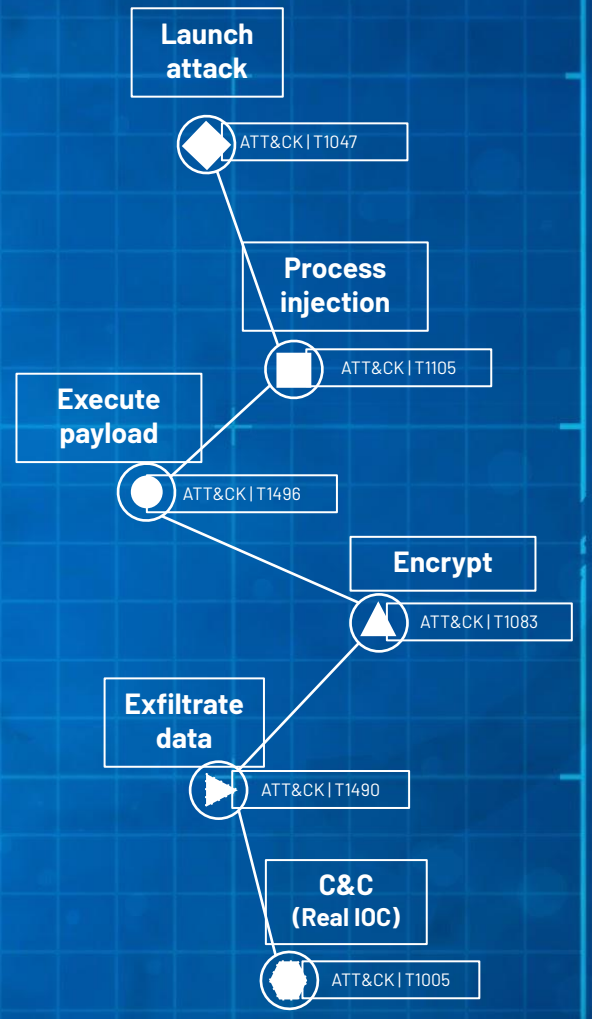
Ransomware Readiness Blueprint

Remote Access

Opened remote control channel on the host

3.3

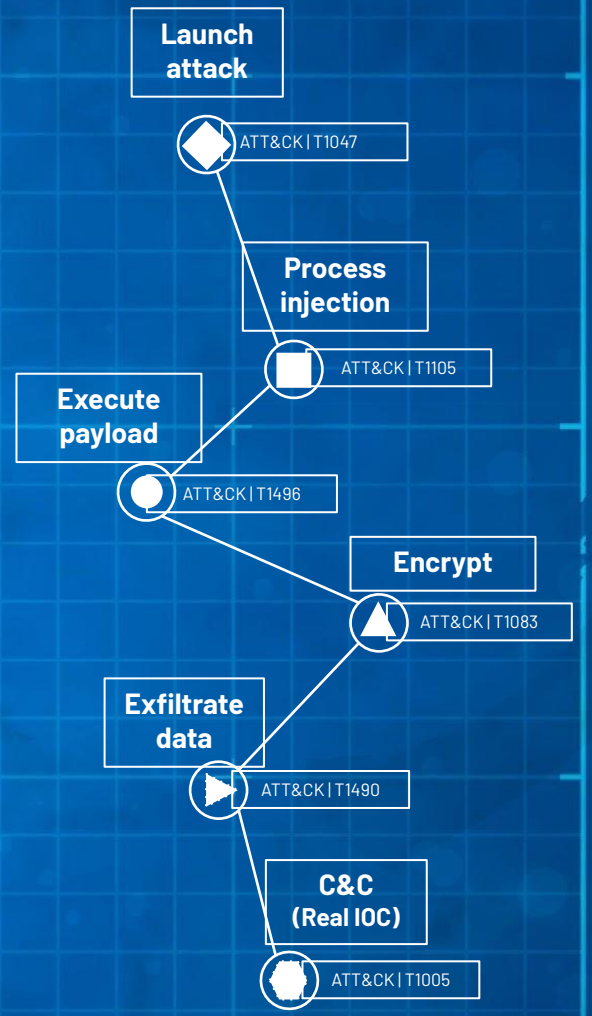
Host 192.168.120.37



PENTERA

Ransomware Readiness Blueprint

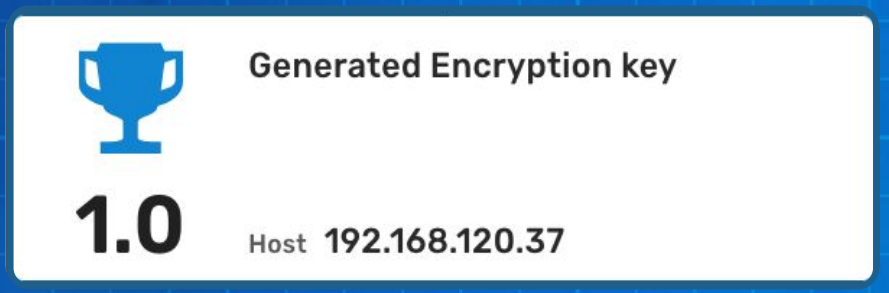
Lateral Movement

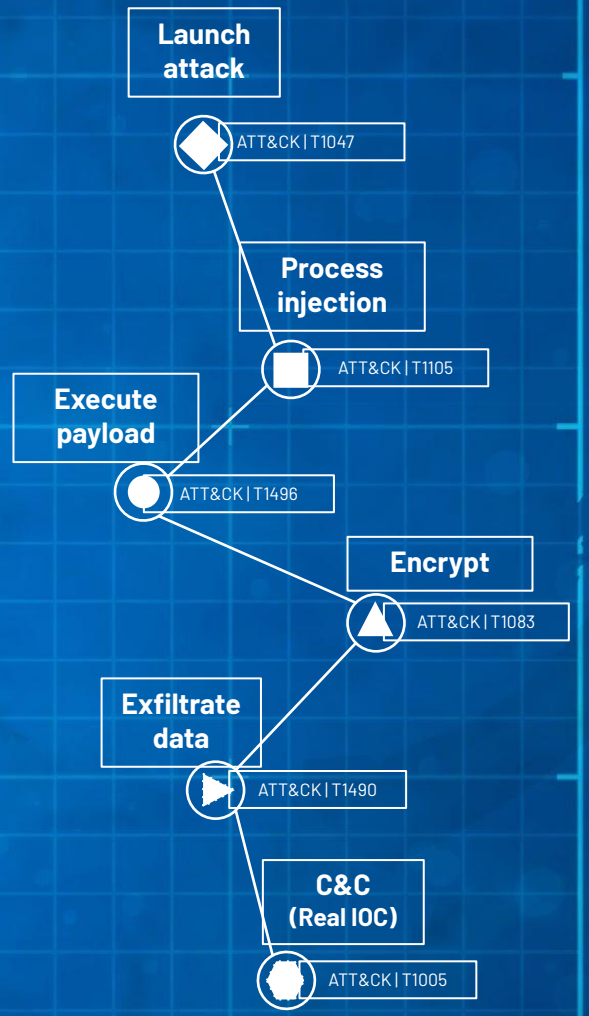


PENTERA

Ransomware Readiness Blueprint

Encryption Preparation





PENTERA

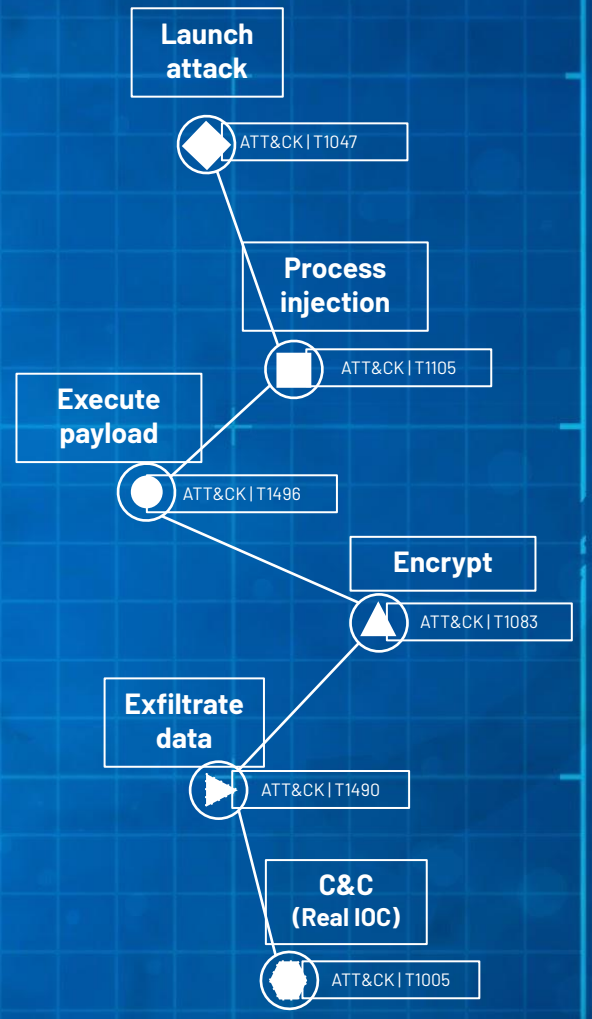
Ransomware Readiness Blueprint

Identify Critical Data for Exfiltration

Enumerated files on the host

7.2

Host 192.168.120.37



PENTERA

Ransomware Readiness Blueprint

Bypass EDR & Encryption

Encrypted files on the host

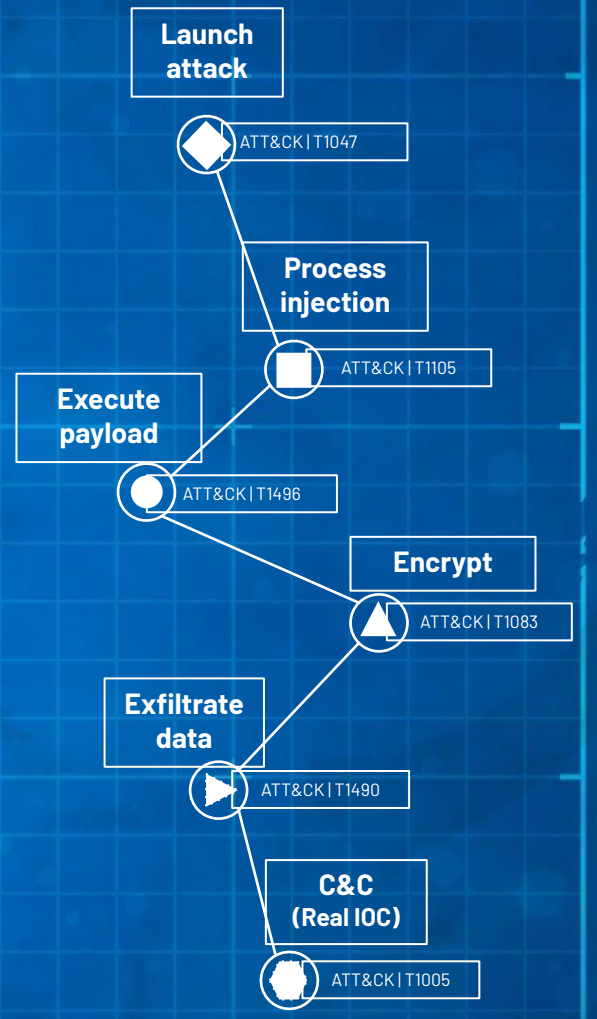
9.2

Host 192.168.120.37

AV did not block malicious payload

8.8

Host 192.168.120.37



PENTERA

Ransomware Readiness Blueprint

Disable Recovery & Clean Up Tracks

Emulated Windows Event Log deletion

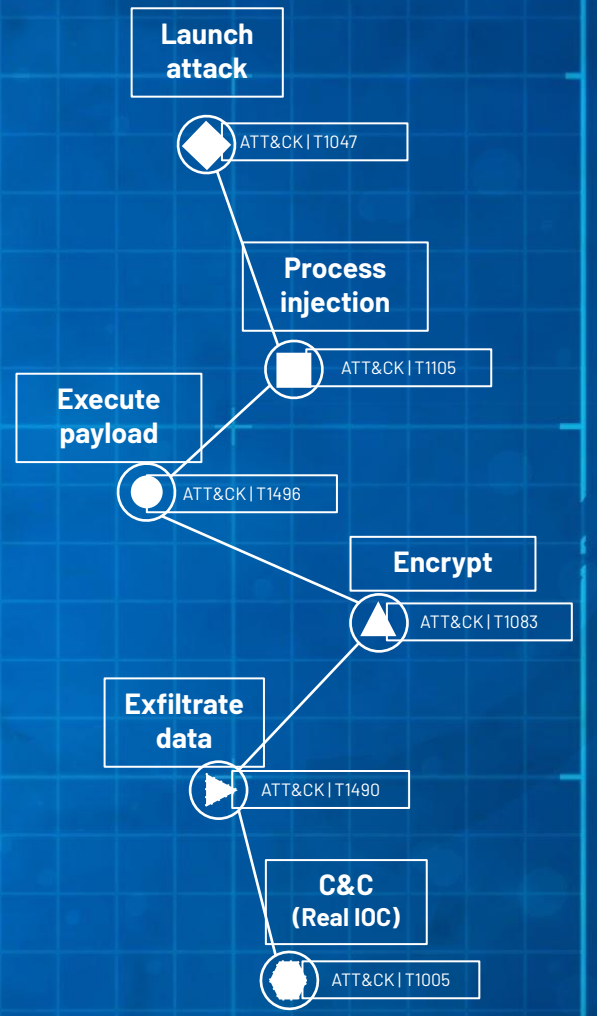
7.9

Host 192.168.120.37

Emulated deletion of shadow copies

7.9

Host 192.168.120.37



PENTERA

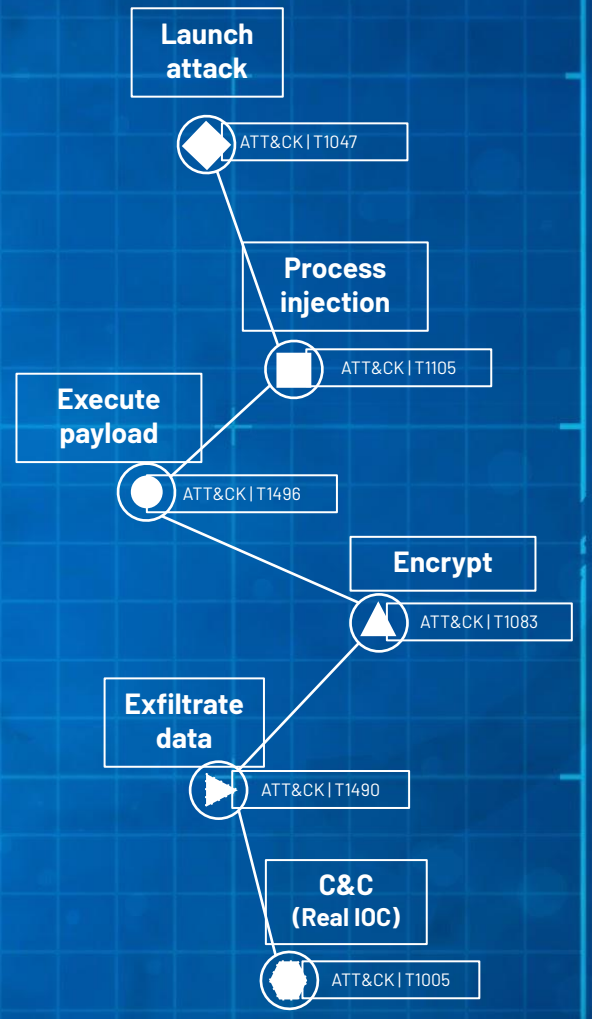
Ransomware Readiness Blueprint

Establish Communication

Payload established connection with Pentera's C2 server

1.2

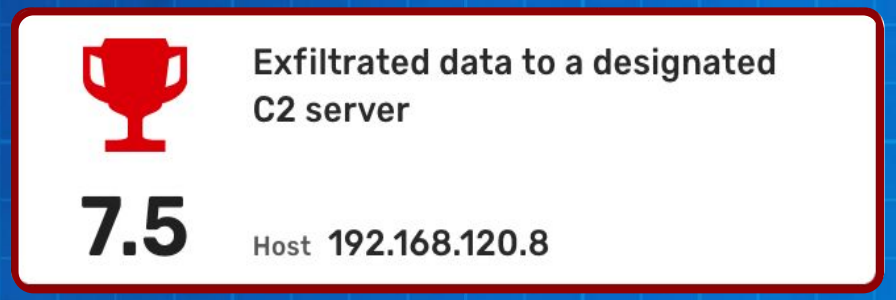
Host 192.168.120.37

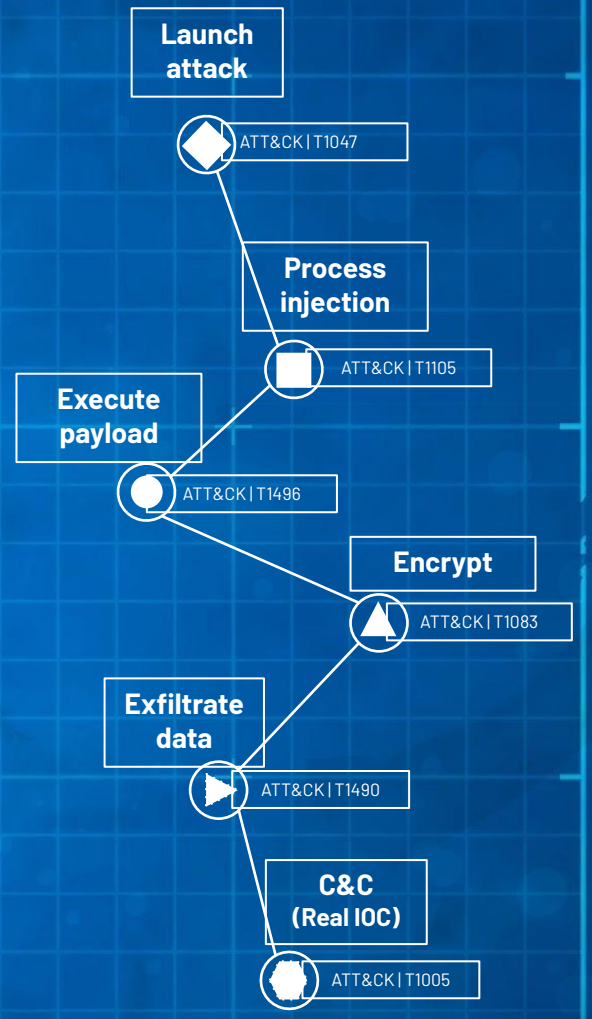


PENTERA

Ransomware Readiness Blueprint

Exfiltrate the Crown Jewels






Didn't you turn on the XDR?
Yes, but apparently just in monitoring mode
PENTERA
HOW DO OTHER COMPANIE S REDUCE EXPOSURE ?

PENTERA

Making the financial case for Exposure Validation

PENTERA

Severity Reduction Factor

Industry average cost of a breach in 2023:

- **$4.45M** for organizations prioritizing vulnerabilities **by CVE score only**
- **$3.98M** when **risk-based analysis** is used for prioritization

11% breach severity reduction with Exposure Validation

Cost of a data breach by vulnerability management prioritization approach

Source: IBM Cost of a Data Breach Report 2023

PENTERA

Probability Reduction Factor

Industry average
breach probability

vs.

Pentera customer
breach probability

Cyentia INSTITUTE

Customer data -
230 customer years

Public breach data -
VERIS Community DB +
online research

Pentera customers have
81% lower probability of being breached

PENTERA

Qualitative ROI

Cybersecurity employee satisfaction and retention

Improved day-to-day security operations

Improved communication with management

Support for compliance processes

Reduced cyber insurance premiums

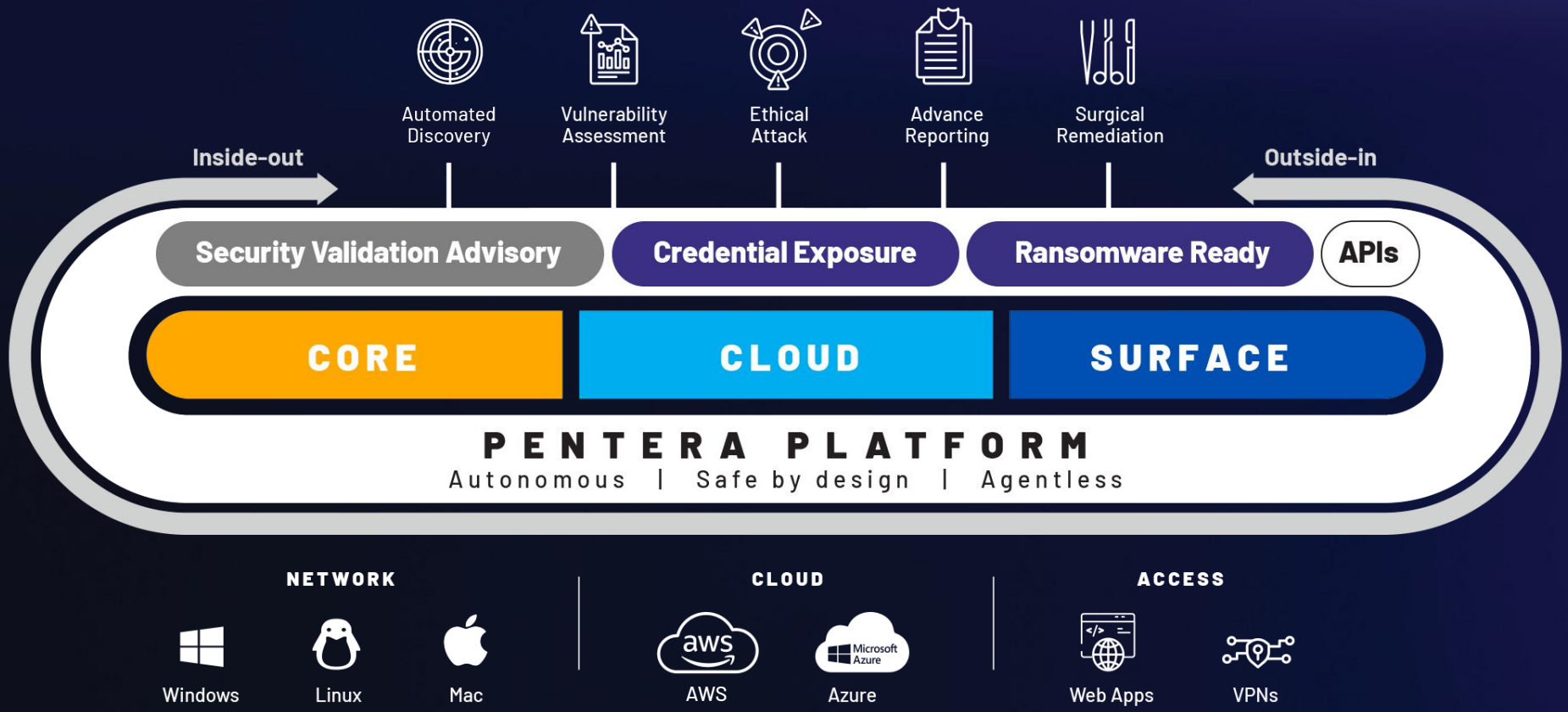
Evidence for security product evaluations (bake-offs)

PENTERA

The Platform

One Platform for All Your Validation and Exposure Management Needs

Pentera Platform: Total Security Validation



PENTERA

1-Day Proof of Value (PoV)

Agreement on PoV
PoV Guide

Quote, Questionnaire

2 weeks before PoV starts

PoV Scoping Call

1 week before PoV starts

PoV day

- **Kick off**
- **Summary**

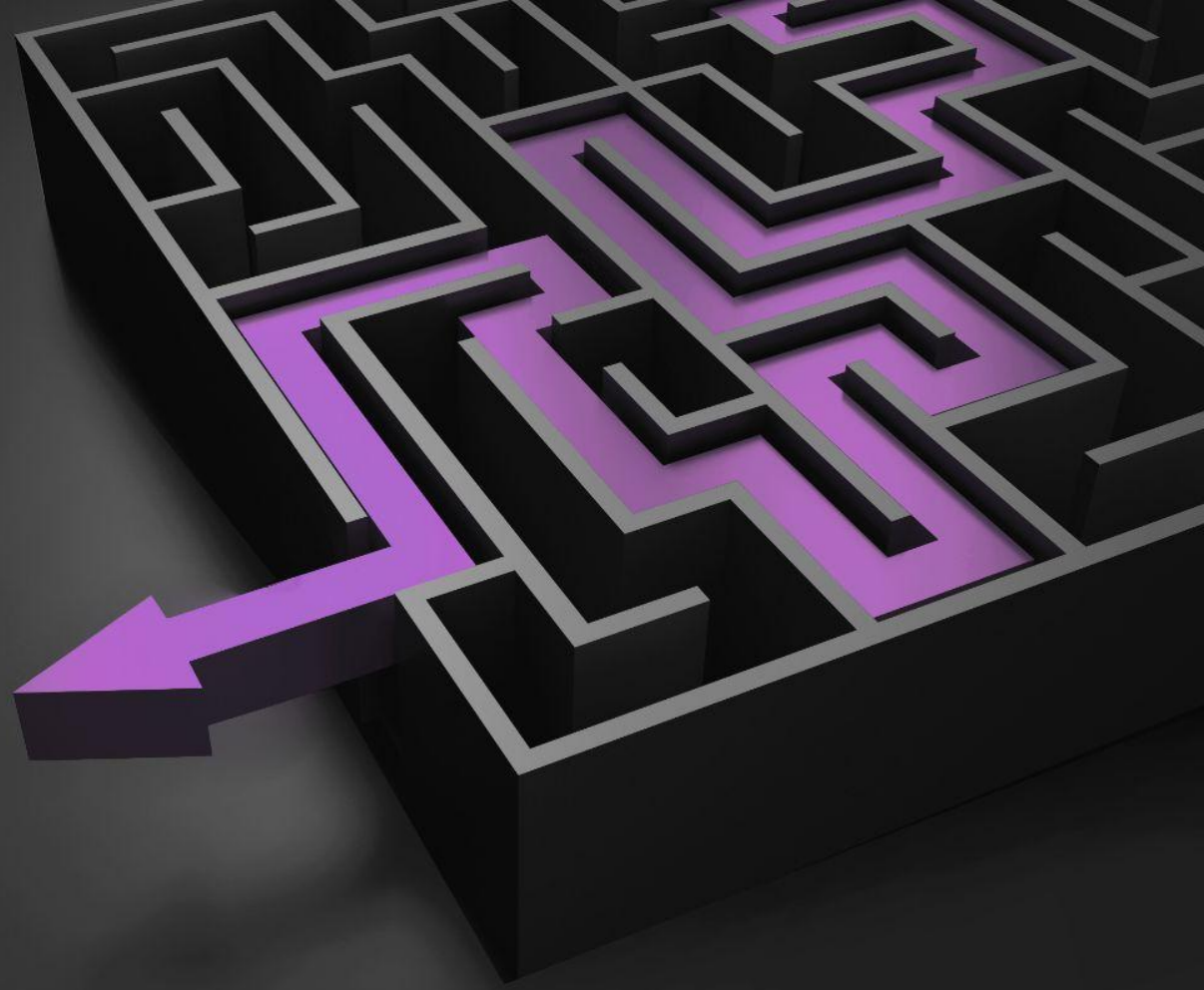
Pentera Surface 3 weeks lead time (domain ownership, asset & domains)

PoV fundamentals:

- Save and controlled
- Pentera Core: No learning phase: no artificial intelligence requiring cloud data matching
- Pentera Core: On-prem approach – all information stays


PENTERA
All systems check,
ready for takeoff!

PENTERA



THANK YOU!