The Attacker's Perspective

Presentation by
Rainer M. Richter
Vice President EMEA & APAC

“Are we secure? How do we know?”

Verifying your security posture (the old way)

Justify the budget…

Spend weeks preparing…

Get PWN'd…

Start updating your Linkedin Profile…

HORIZON3.ai
~~TRUST BUT VERIFY~~

Security Testing is on an unsustainable trajectory

Supply < Demand

<5,000

Certified Ethical Hackers in US

~10 years

To become a “Master” Ethical Hacker

~18 weeks

Lead time to schedule a single pentest and receive report

Growing Infrastructure Attack Surface

- Datacenter
- Perimeter
- Insider Threat
- Clouds
- SaaS Access
- WFH
- OSINT
- DarkWeb Data
- IoT

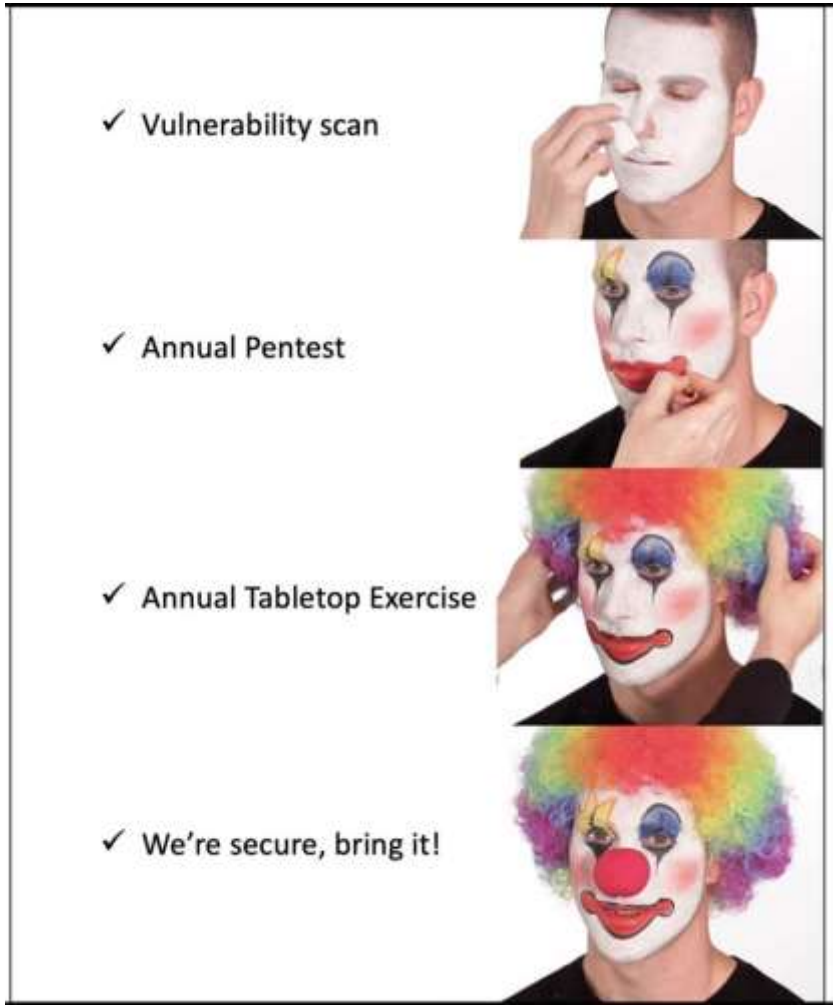
Compliance Requirements

- SOC2
- HIPPA
- PC
- NIS2
- CMMC
- GDPR
- State & Federal laws
- DORA

Continuously Prove Security posture

- To the Board
- To Regulators
- To customers
- To insurance providers
- Justify ROI of ~130 defensive tools
- Validate SOC/MSSP response time
- Keep up with continuous changes in env

“Peacetime” Security Mindset…



Waiting for a breach to verify
my security tools work

Prepare for Cyber-enabled Economic Warfare

1000+ companies have withdrawn from the Russian economy

Suppliers →  → Distributors

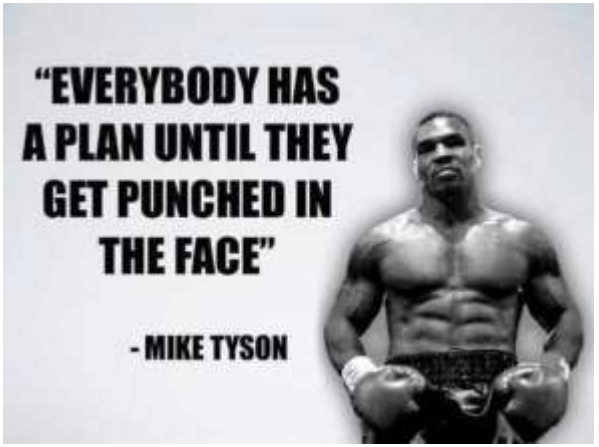
Western Sanctions		**Cyber-Enabled Counter Punch**
Ban Russians from traveling	→	Corrupt airline ticketing database
Ban the sale of luxury goods	→	Attack logistics industry to create product shortages
Ban Russian oil & gas	→	Attack refineries & pipelines to cause 10x spike in gas prices

Wartime Mindset = ~~Trust But~~ Verify

1. **See your enterprise through the eyes of the attacker**
   - Attackers will get in, can you detect and stifle them?
   - Are your "crown jewels" secure?
   - Are your tools & processes effective?

2. **Build your incident response muscle memory**
   - Router crashed due to hack or IT misconfig?
   - Are your processes clearly understood?
   - Who has decision-making authority?

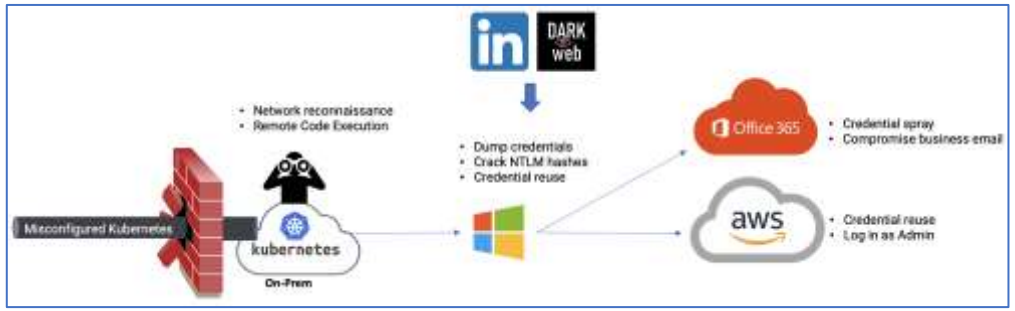
3. **Operational Collaboration**
   - Red + Blue = Purple teams
   - Your suppliers & distributors are part of your security team
   - Operationally-minded ISAC's



Don't tell me we're secure, show me

HORIZON3.ai
TRUST BUT VERIFY

Continuously verify your security posture



FIND

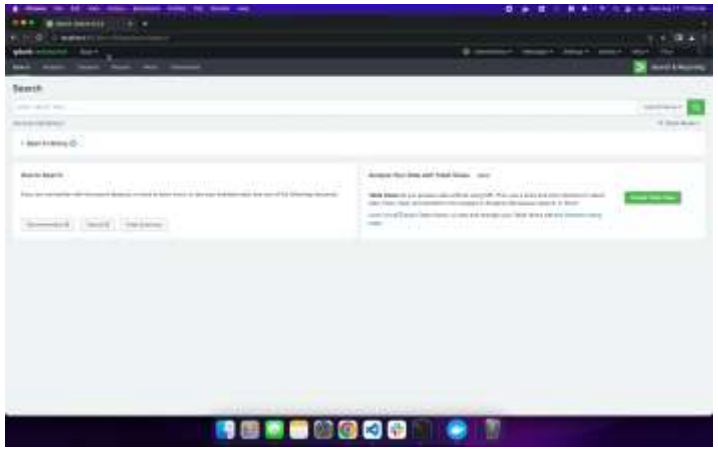
Via Continuous Pentesting

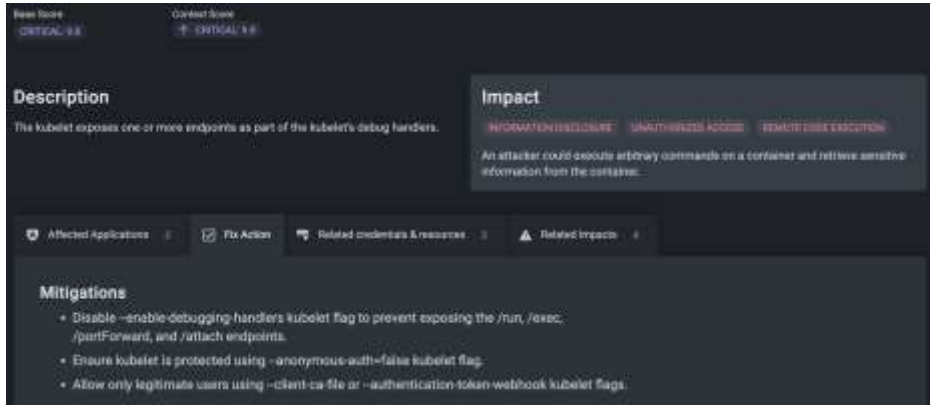
FIX

Via SOAR

VERIFY

Via Detection Engineering





Story 1: My EDR should have caught that!

Environment

- Internal infrastructure pentest
- ~5,000 hosts
- EDR & UBA tools installed

Windows SMB RCE

Proof

Proof of remote command execution: Output of 'whoami' command showing current user.

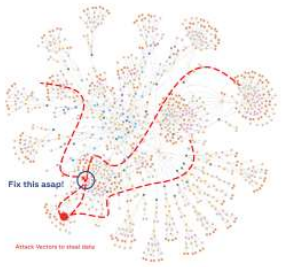
```
python3 /opt/h3/smbrun.py
VERBOSE => false
RPORT => 445
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
DCERPC::max_frag_size => 4096
DCERPC::fake_bind_multi => true
DCERPC::fake_bind_multi_prepend => 0
DCERPC::fake_bind_multi_append => 0
DCERPC::smb_pipeio => rw
DCERPC::ReadTimeout => 10
```

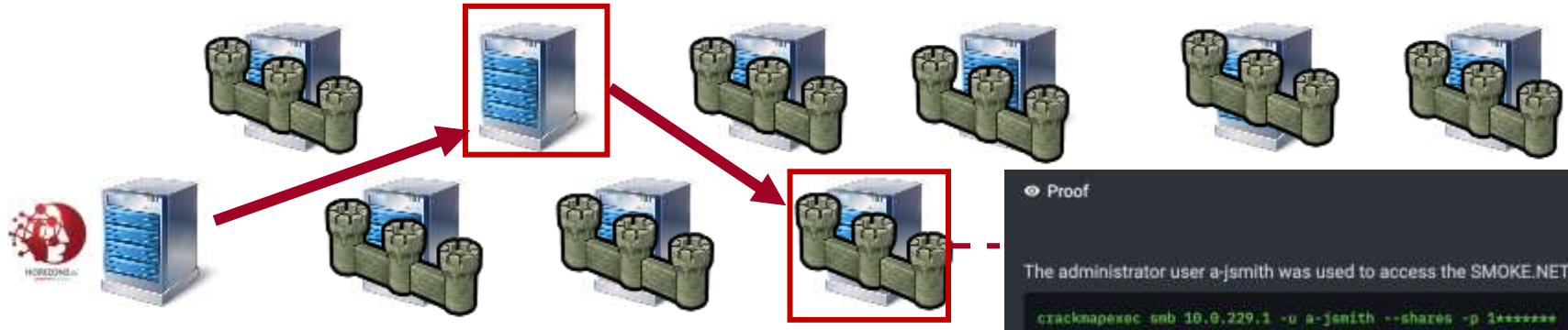
Dump LSASS to harvest credentials

Proof

The administrator user administrator was used to access the endpoint 10.0.220.55

```
crackmapexec smb 10.0.220.55 -u administrator --shares -H 8**********************************c --local-auth
SMB         10.0.220.55     445    WIN2K3           [*] Windows Server 2003 3790 Service Pack 2 (name:WI
SMB         10.0.220.55     445    WIN2K3           [+] WIN2K3\administrator 8**********************
SMB         10.0.220.55     445    WIN2K3           [+] Enumerated shares
SMB         10.0.220.55     445    WIN2K3           Share           Permissions     Remark
SMB         10.0.220.55     445    WIN2K3           -----           -----------     ------
SMB         10.0.220.55     445    WIN2K3           C$              READ,WRITE      Default share
SMB         10.0.220.55     445    WIN2K3           IPC$                            Remote IPC
SMB         10.0.220.55     445    WIN2K3           ADMIN$          READ,WRITE      Remote Admin
```





Proof

The administrator user a-jsmith was used to access the SMOKE.NET domain

```
crackmapexec smb 10.0.229.1 -u a-jsmith --shares -p 1*******
SMB         10.0.229.1      445    DC               [*] Windows Server 2012 R2 Standard 9600 x64 (name:D
SMB         10.0.229.1      445    DC               [+] smoke.net\a-jsmith:1******* (Pwn3d!)
SMB         10.0.229.1      445    DC               [+] Enumerated shares
SMB         10.0.229.1      445    DC               Share           Permissions     Remark
SMB         10.0.229.1      445    DC               -----           -----------     ------
SMB         10.0.229.1      445    DC               ADMIN$          READ,WRITE      Remote Admin
SMB         10.0.229.1      445    DC               C$              READ,WRITE      Default share
SMB         10.0.229.1      445    DC               IPC$                            Remote IPC
SMB         10.0.229.1      445    DC               NETLOGON        READ,WRITE      Logon server share
SMB         10.0.229.1      445    DC               SYSVOL          READ            Logon server share
```

Credential reuse leads to Domain Compromise

What happened?

- Fortinet was misconfigured on 3/5000 machines
- “Buy why didn’t Fortinet stop the credential pivot?”
- Per Fortinet, “Customer didn’t buy the right UBA modules”

Story 2: I thought we patched that!

Environment

- Internal infrastructure pentest
- ~10,000 hosts
- Robust patching processes
- Cylance for AV
- Qualys for VM & reporting

Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472)

Zerologon

Base Score

CRITICAL: 10

Impact

REMOTE CODE EXECUTION | UNAUTHORIZED ACCESS | PRIVILEGE ESCALATION

What happened?

- ZeroLogon patch has 2 steps
  1. Update registry files to show patch was applied
  2. Apply the binaries
- Cylance blocked the binaries from applying
- Qualys relies on registry files to report patching status
- Went unnoticed for 18 months, had to rebuild network

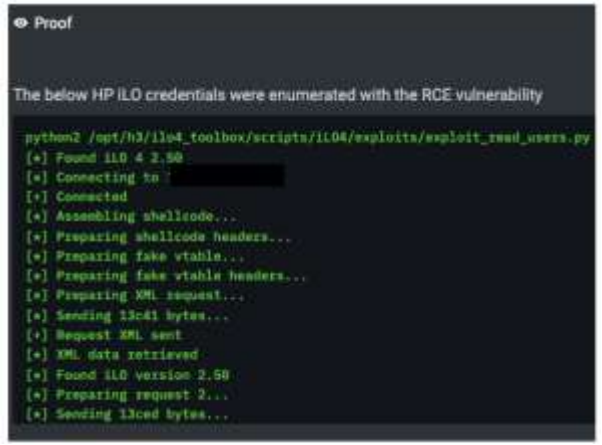
CYLANCE

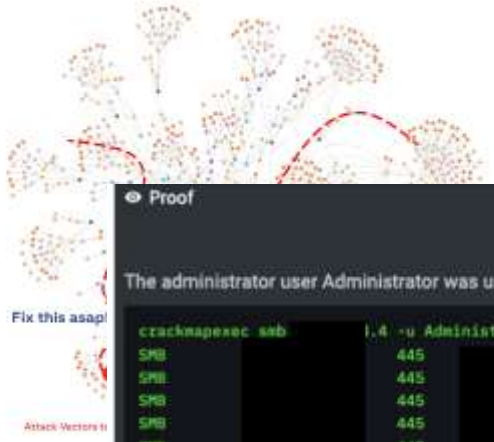
Qualys.

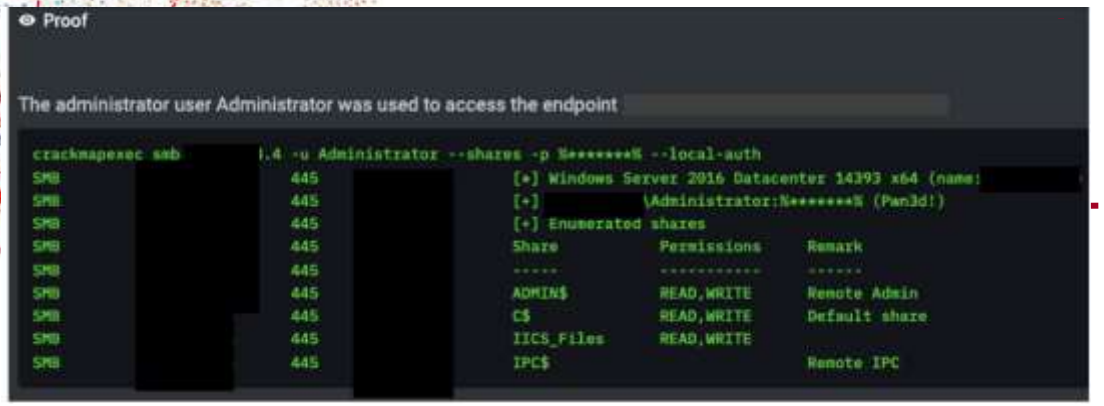
Exploitation isn't required

Story 4: Becoming AWS Admin

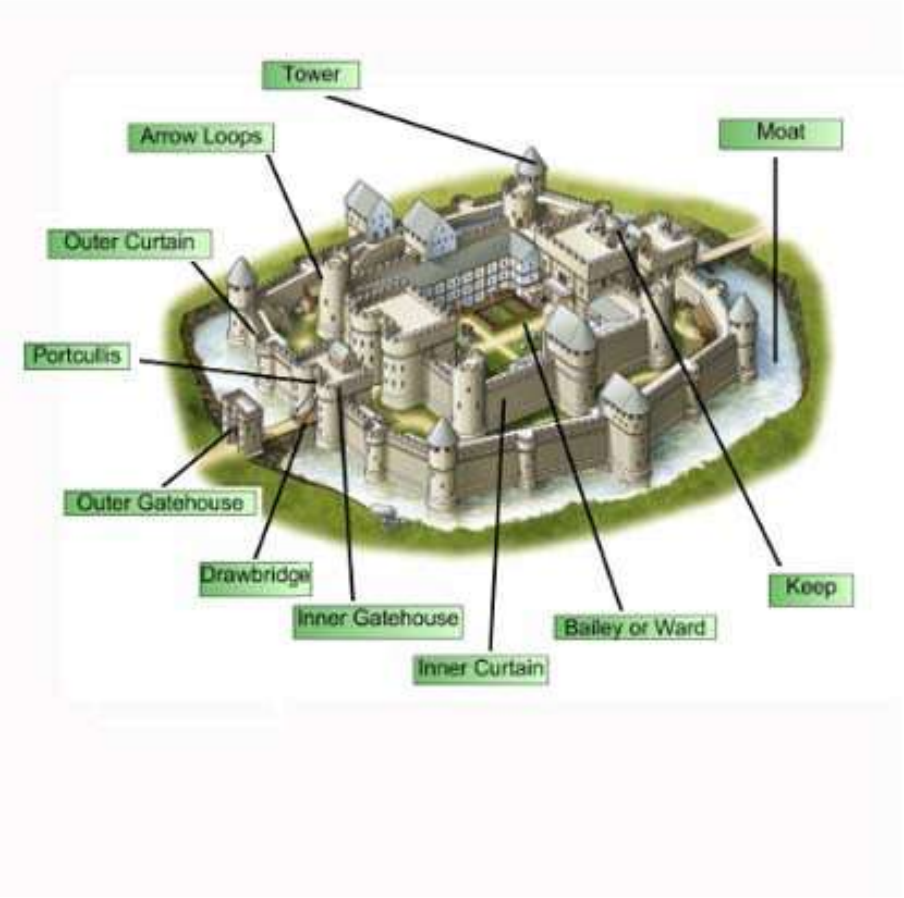
1. NodeZero given initial access
2. NodeZero discovers **2,000** hosts on the network
3. NodeZero identifies HP iLO running on 5 hosts
4. NodeZero successfully gains RCE via HP iLO CVE-2017-12542
5. NodeZero successfully dumps creds via HP iLO RCE
6. NodeZero identifies admin credential from dump, pivots to gain Admin access to adjacent Windows box
7. NodeZero searches local filesystem and identifies password.txt file that contains AWS admin creds
8. NodeZero utilizes harvested credentials to become AWS Admin







Principles of Good Security Organizations



- Assume attackers can gain initial access
- Implement multiple layers of security controls – Perimeter, Identity, Behavioral, etc
- Provides redundancy in the event a single control fails
- BUT… on average, you have **130** security tools deployed
- **Reality**: these security tools aren't designed to work together

After running a NodeZero pentest…

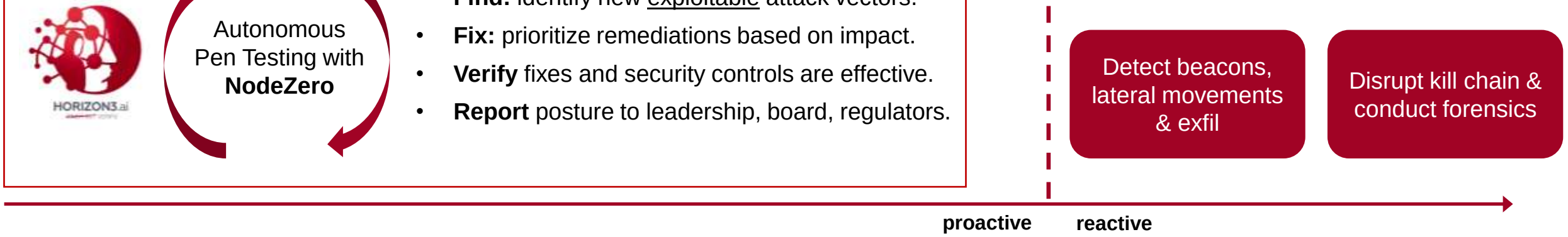
1. Did you detect us?
2. Did you log us?
3. Did you alert on us?
4. Did you stop us?

Our Mission with NodeZero

Autonomous Pen Testing with **NodeZero**

Continuously…

- **Find:** identify new exploitable attack vectors.
- **Fix:** prioritize remediations based on impact.
- **Verify** fixes and security controls are effective.
- **Report** posture to leadership, board, regulators.



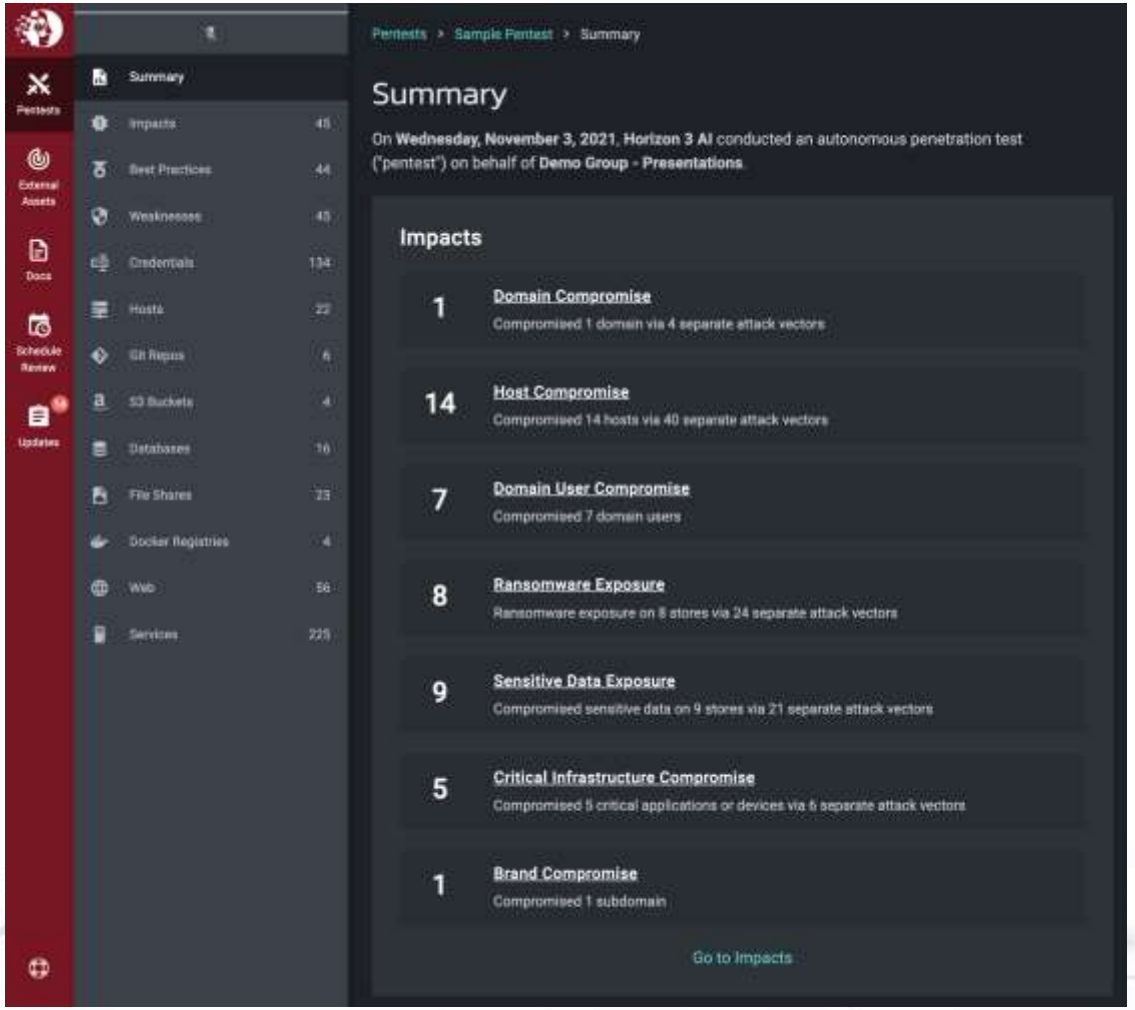
- Delivered as SaaS – no agents, custom scripts, or credentials required.
  - EU instance in Frankfurt/Main, operated by Horizon3.aI Europe GmbH
- Up and running in <10 minutes via self-service UI or API.
- No consultants or professional services required.
- Helping to fulfill mandatory requirements NIS-2 and DORA

10 most frequently used techniques used by NodeZero

Top 10 techniques used

1. **Brute force weak and default credentials** across protocols (SSH, FTP, web, etc)
2. **Credential dumping & reuse** across Windows & Linux hosts
3. Public-facing asset discovery and **perimeter host exploitation**
4. **Lateral movement** via insufficient network segmentation
5. **Man-in-the-middle** and relay attacks
6. Windows Active Directory **privilege escalation** vectors such as Kerberoasting
7. Exploitation of **misconfigurations** & vulnerabilities in routers, iLOs, iDRACs, etc.
8. Open-Source Intelligence and **password spraying** credentials
9. Exploitation of misconfigurations and vulnerabilities in DevOps tools such as Jenkins, GitLab, Kubernetes, Docker
10. Exploitation of **critical CISA recognized vulnerabilities** & remote code execution

… To achieve critical impacts



HORIZON3.ai
~~TRUST~~ BUT VERIFY

Continuously verify your security posture

1. On-demand, self-service pentests
2. Attack paths spanning on-prem, cloud, perimeter
3. Chain misconfigurations, defaults, vulnerabilities, and credentials at-scale

1. Verify detection & response
2. Verify cyber resilience & systems hardening
3. Verify compliance posture

1. Prioritize exploitable vulnerabilities
2. Secure critical data
3. Quickly remediate & retest

Thank You!

rainer@horizon3.ai

itsa

Hall 7, booth is 724

www.horizon3.ai
www.linkedin.com/company/horizon3ai
https://twitter.com/Horizon3ai