The Attacker's Perspective

"In the military it's called 'turning the map around'...

get inside the mind of the enemy,

see the situation as they do

to anticipate & prepare for

what's to come"

~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

HORIZON3.ai
~~TRUST BUT~~ VERIFY

My Boardroom “Interrogation”

How do you know?

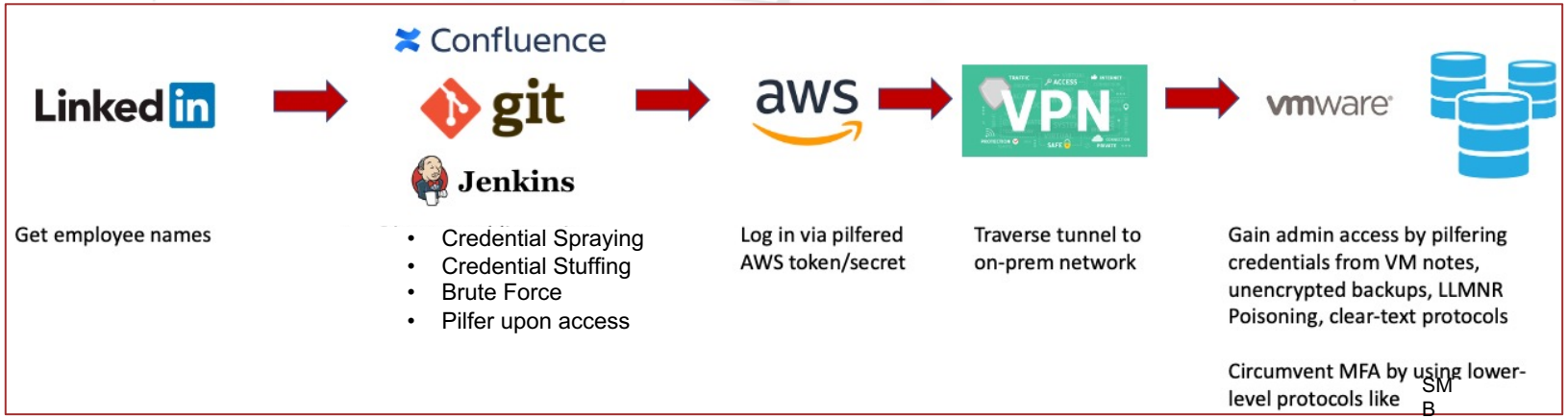
That we are secure?

That our ”Crown Jewels” are protected?

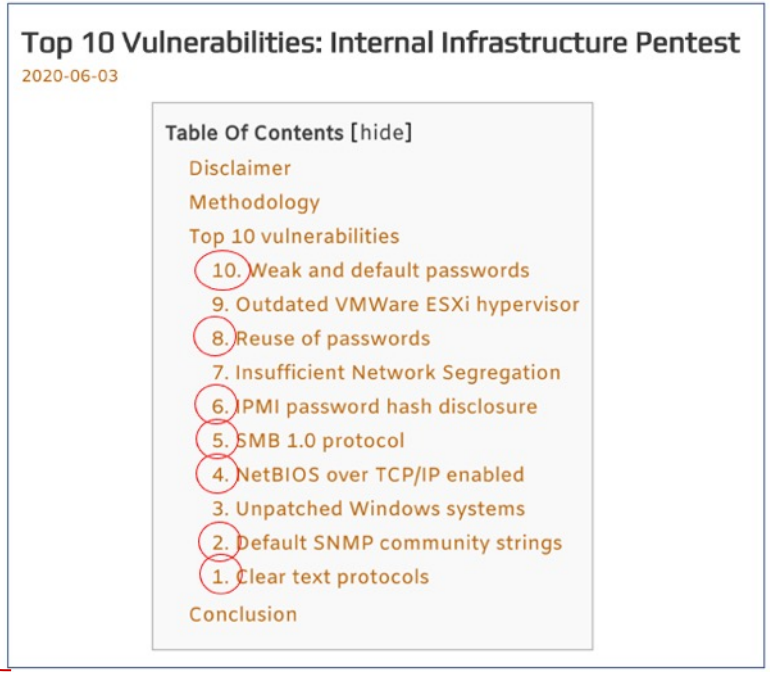
That we are fixing the right vulnerabilities?

That our security tools are properly configured and effective?

Attackers don't have to "hack in" – they log in



link



Reused Credentials + Misconfigurations + Dangerous Defaults

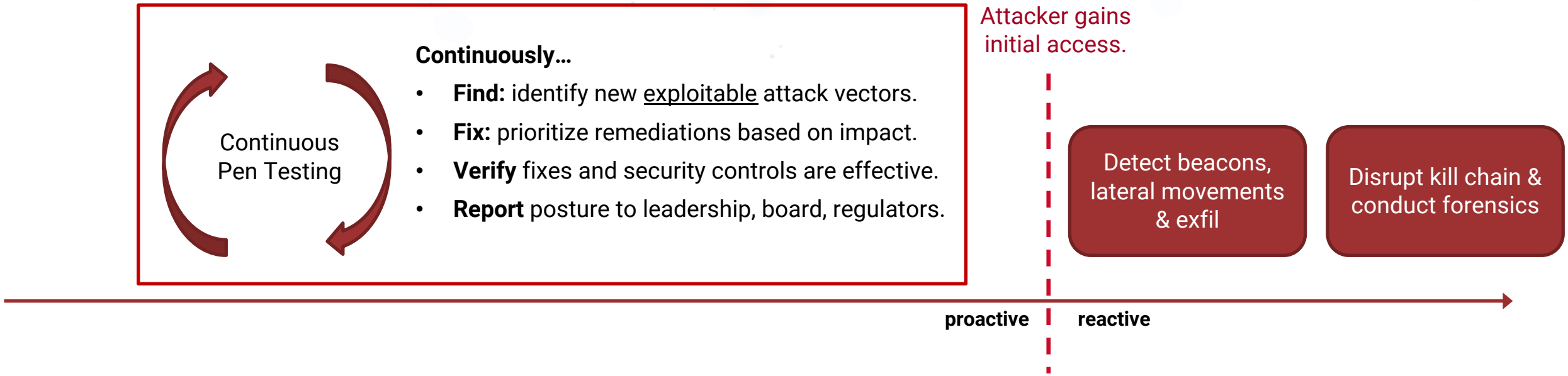
No CVEs or malware were used in this attack.

How quickly can you detect this?

How do you know?

My Vision

Find & fix attack vectors before criminals exploit them.



- No agents to install
- No scripts to develop
- No consultants to hire

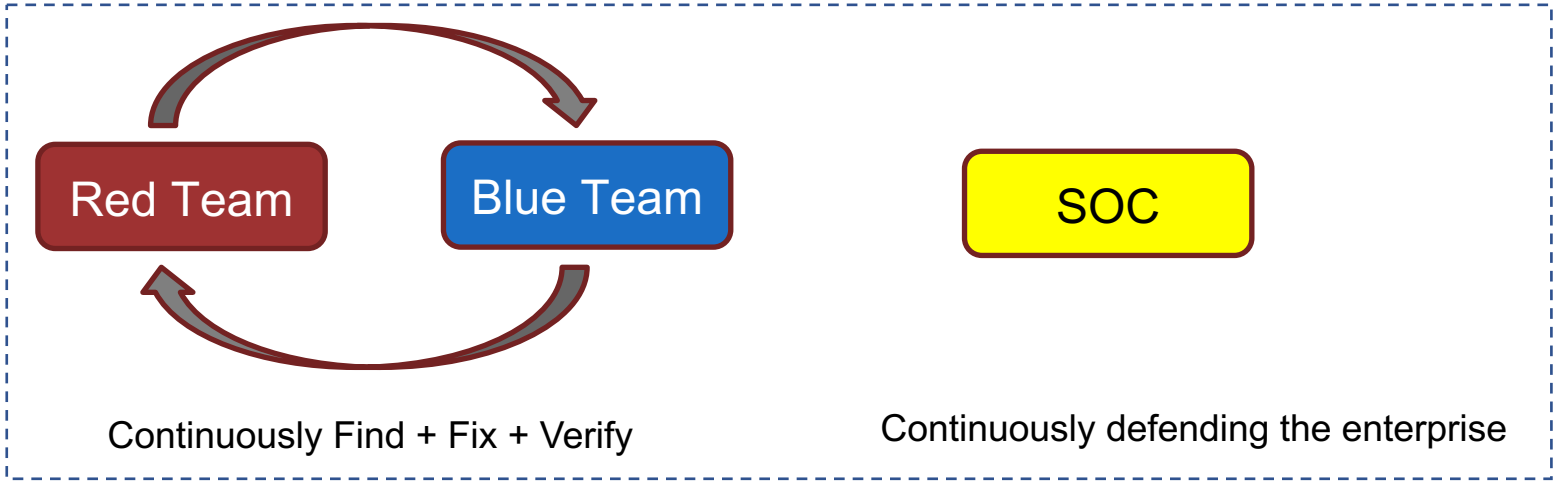
HORIZON3.ai
TRUST BUT VERIFY

How I Tried to Organize

Red Team: Continuously assess my security posture

Blue Team: IT Admins, Network Engineers, and Security Tool focused on fixing problems

SOC: Focused on defending the enterprise (detect beacons, lateral movement, exfil, etc)



HORIZON3.ai
TRUST BUT VERIFY

My Reality

"I don't know if my security tools work, or if I fixed the right vulnerabilities until I'm breached, and by then its too late!!"

Assess

nessus

RAPID7 insightVM

tcs | TATA CONSULTANCY SERVICES

VERODIN

Prioritize

Remediate

Report

Vulnerability Scanners: Noisy and Vulnerable ≠ Exploitable

Manual Pen Tests: Incomplete Snapshot

Security Risk Management Tools: Garbage in, Garbage out

Breach Attack Simulation: Install more agents & script fake tests

HORIZON3.ai
~~TRUST~~ BUT VERIFY

Who we are

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

[Tony Pillitiere](#)
CTO & Co-Founder
Former US Special Ops
MSgt (Ret), USAF

What we do

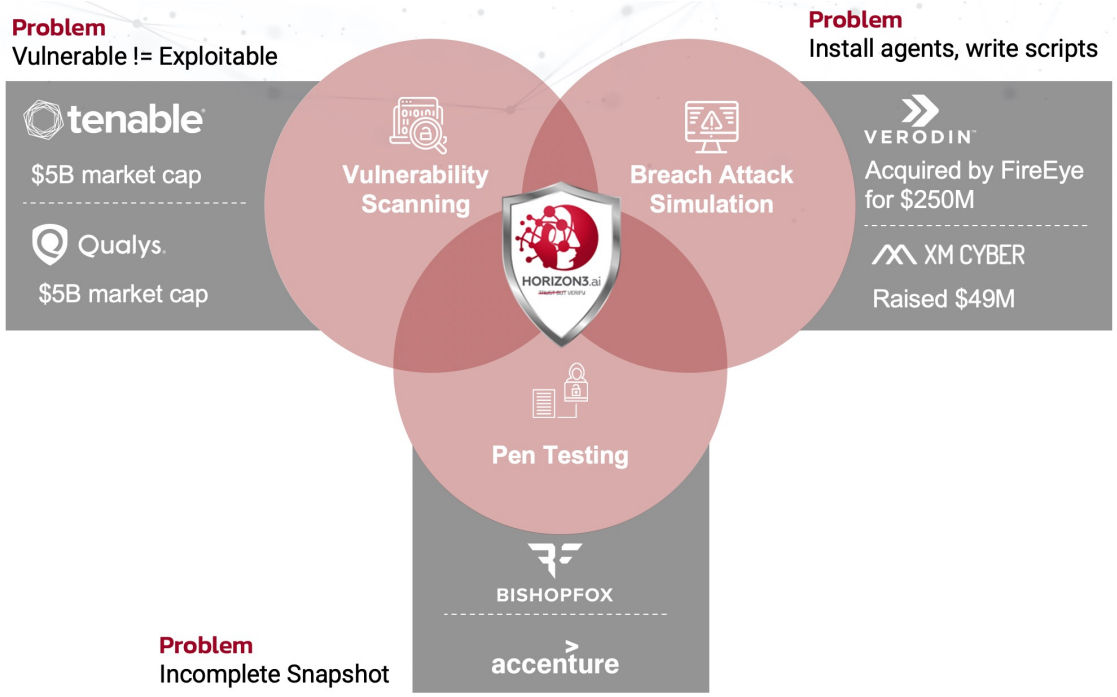
~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

(No Consultants, No Agents, No Custom Scripting)

Continuously…

- **Find** exploitable **chained** vulnerabilities
- **Fix** what matters
- **Verify** your posture
- **Report** board & regulators.

Disrupting the $25B Security Testing Market



Effective Security

Domain Admin in 7 minutes 19 seconds

No Security Alerts Triggered

Fix the Effectiveness Problem

Self-Service, Agentless, Adaptive

Weaknesses (2)

Weak or Default Credentials - Cracked Credentials (H3-2021-0020)

Mitigations

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References

- CWE-521: Weak Password Requirements
- T1110: Brute Force

LLMNR/NBT-NS Poisoning Possible (H3-2020-0012)

Mitigations

- Disable LLMNR using Group Policy to enable 'Turn OFF Multicast Name Resolution' setting under 'Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client'.
- Disable NBT-NS in the network adapter settings by selecting 'Disable NetBIOS over TCP/IP. Alternatively, disable by using a registry key.

References

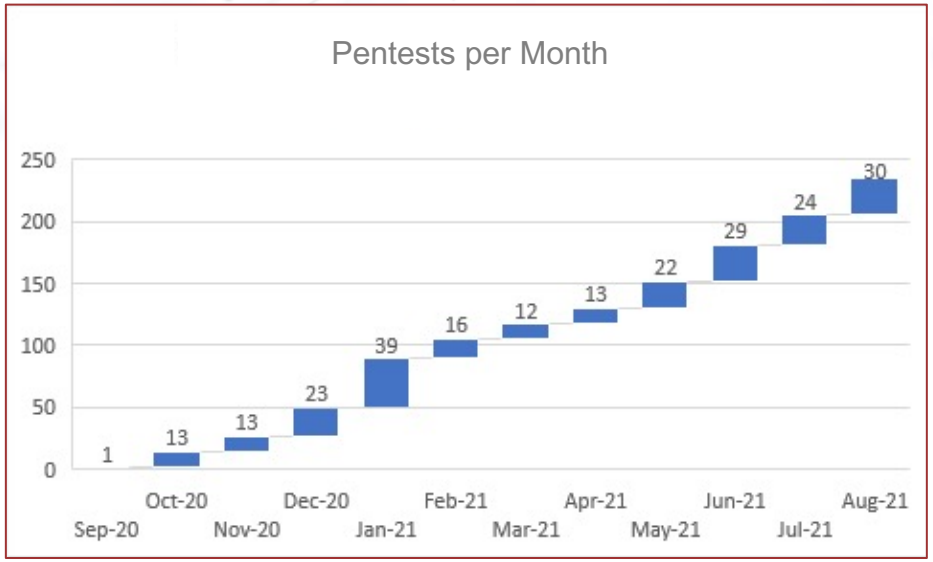
- T1171 - LLMNR/NBT-NS Poisoning and Relay
- Local network vulnerabilities - LLMNR and NTB-NS Poisoning
- LLMNR and NBT-NS Mitigation

Manufacturing Customer with 37 Global Datacenters

Motivation

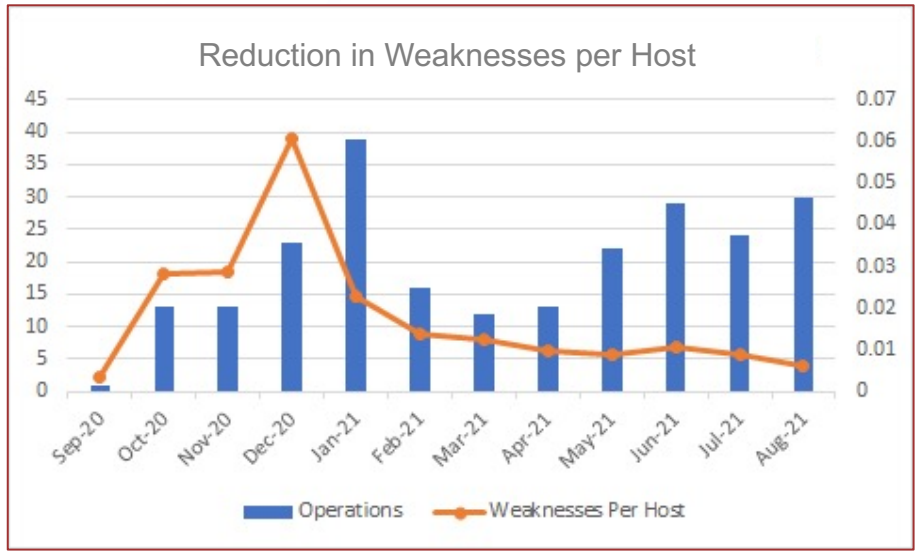
- $35k per pentest to consultants
- CISO recently fired for breach
- Cold email to deal close in 8 weeks

Adoption

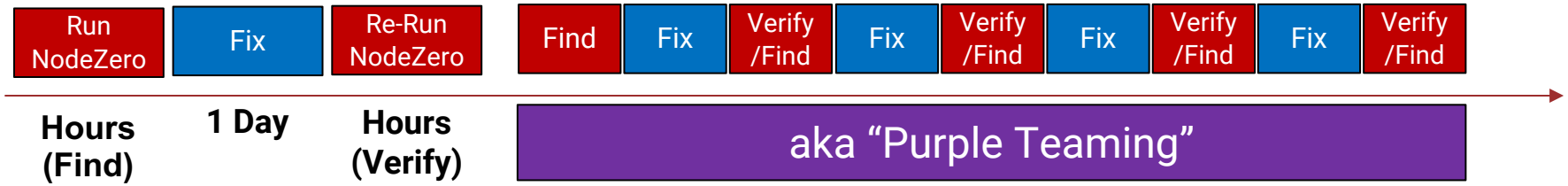


- Averaging 16 pentests per month
- ”Sparring partner” for the SOC
- Network Engineers with security “superpowers”

Impact



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



Why Autonomous Pentesting

Emerging Use-Cases	Why?
"**Sparring Partner**" to tune the SOC	NodeZero gained domain admin in ~ 7 mins and **did not** trigger any SOC alerts
Empower "Fixers"	IT Teams can quickly & proactively find + fix + verify security weaknesses
Force Multiplier for Ethical Hackers	Maximize coverage using human + machine teaming

Red Team: Continuously test and verify my security posture with autonomous pentesting

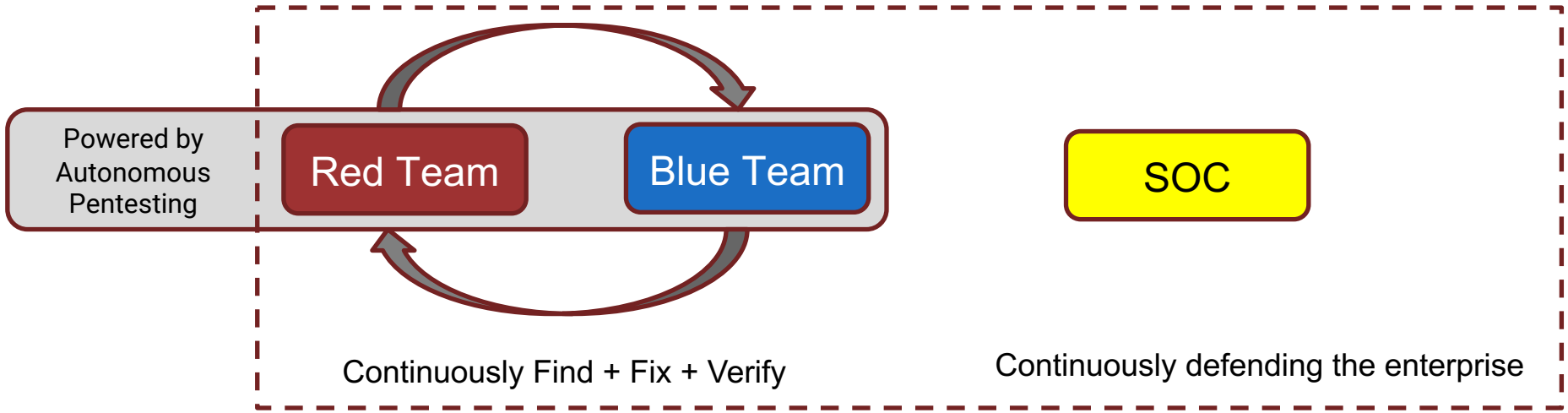
NodeZero compromises HackTheBox-Active in 3 minutes and 30 seconds, auto-describes attack
https://www.horizon3.ai/iamnodezero/iamnodezero-active

Revisiting the Team Structure

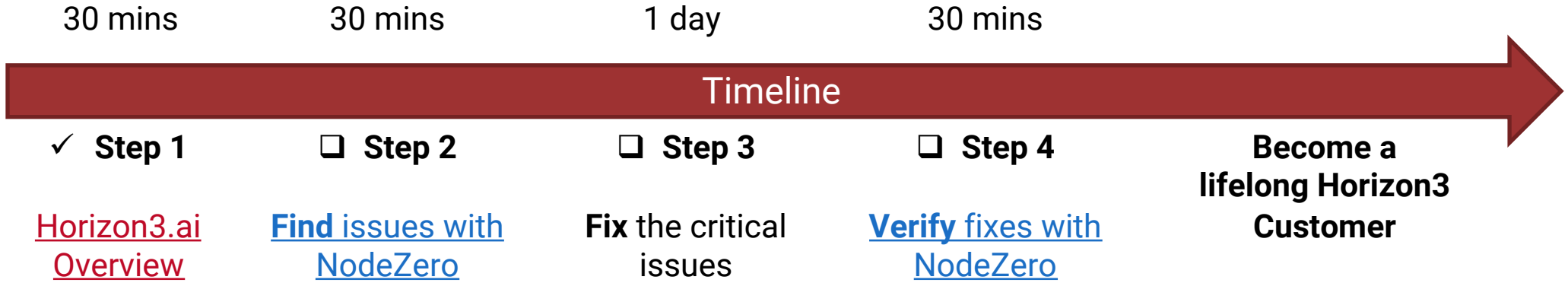
Red Team: Continuously find exploitable attack paths and hopefully trigger security alerts

Blue Team: IT Admins, Network Engineers, and Security Tool focused on quickly fixing problems

SOC: Focused on defending the enterprise (detect beacons, lateral movement, exfil, etc)



Thesis: Find & Fix what Matters



There's no downside

1. If NodeZero finds something – you fix it, then verify the fix
2. If NodeZero finds nothing – your controls are working

Schedule a demo

www.horizon3.ai/demo

Start your free trial now

www.horizon3.ai/trial

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