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"

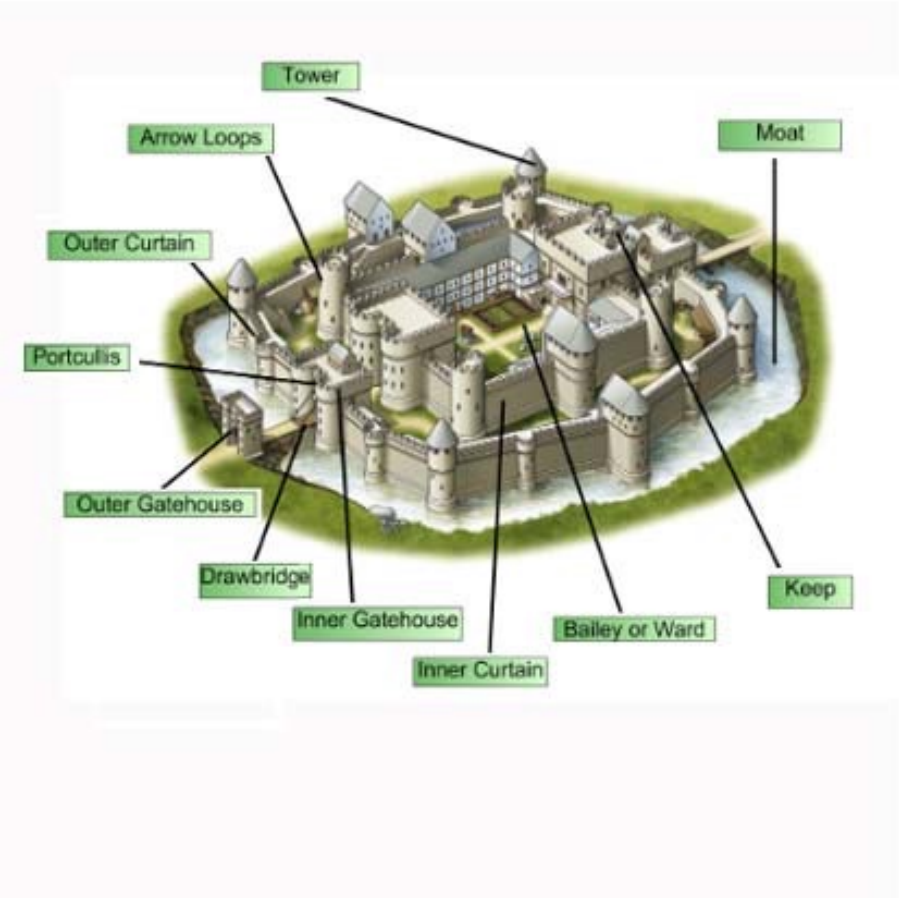
~~Manual~~

~~Crowdsourced~~

~~Automated~~

Autonomous Pentesting

What is Defense-In-Depth?



- Multiple layers of security controls – Perimeter, Identity, Behavioral, etc
- Provides redundancy in the event a single control fails
- “Train like you fight” principle verifies effectiveness

Broadly Accepted Security Principles

- Assume initial access and focus on stifling C2, lateral movement, and exfil
- Proactively find + fix + verify the remediation of security weaknesses to harden systems
- “Train like you fight” to identify weaknesses in your defenses PRIOR to a breach, not during

Porous Defenses

1. ”My EDR should have caught that!”

2. ”I thought we were patched!”

What is LSASS?

- Local Security Authority Subsystem Service Process (LSASS) stores credentials locally or within a Windows domain
- Enables users to access resources without reauthenticating
- Passwords stored in-memory as plaintext, NTLM hashes, and Kerberos Tickets

What is a Domain Administrator?

- In Windows, it is a user account that can edit information in active directory
- Active Directory authenticates and authorizes all users in a windows domain
- Attackers attaining Domain Admin privileges have the keys to your kingdom

NodeZero successfully dumps LSASS and escalated privileges to Domain Admin, Fortinet EDR did NOT detect it

Per Fortinet – “EDR was not properly configured, and Medical Clinic didn’t buy the right add-on products and modules to detect lateral movement”

HORIZON3.ai
TRUST BUT VERIFY

Porous Defenses

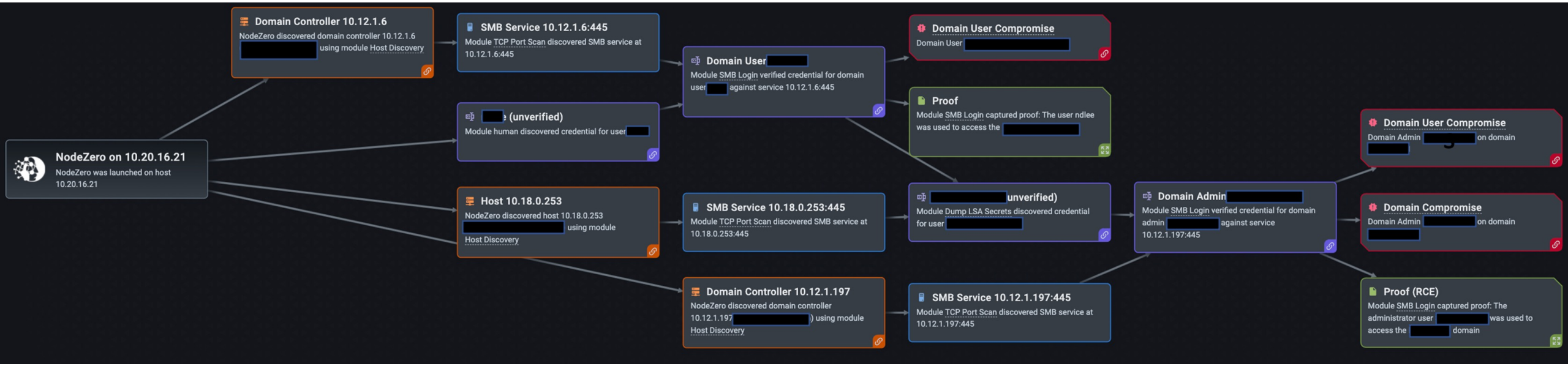
1. ”My EDR should have caught that!”

2. ”I thought we were patched!”

What is ZeroLogon (CVE-2020-1472)?

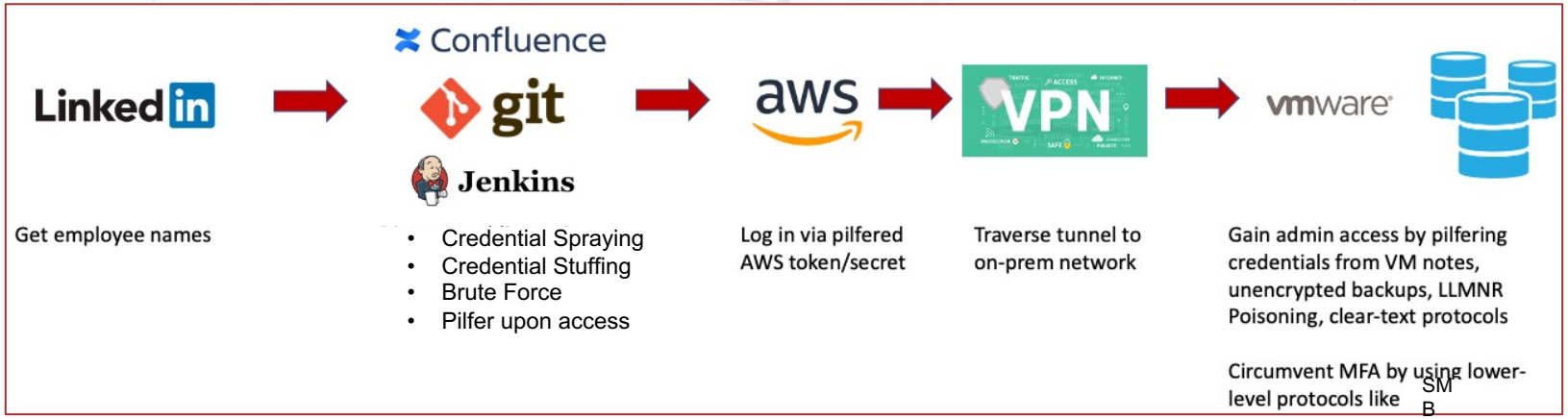
- Critical vulnerability in the Microsoft authentication protocol
- Allows attackers to access all valid usernames & passwords in the network
- Harvested credentials are used to escalate privileges and access sensitive data

NodeZero proves ZeroLogon was NOT patched despite Microsoft & Qualys Reports

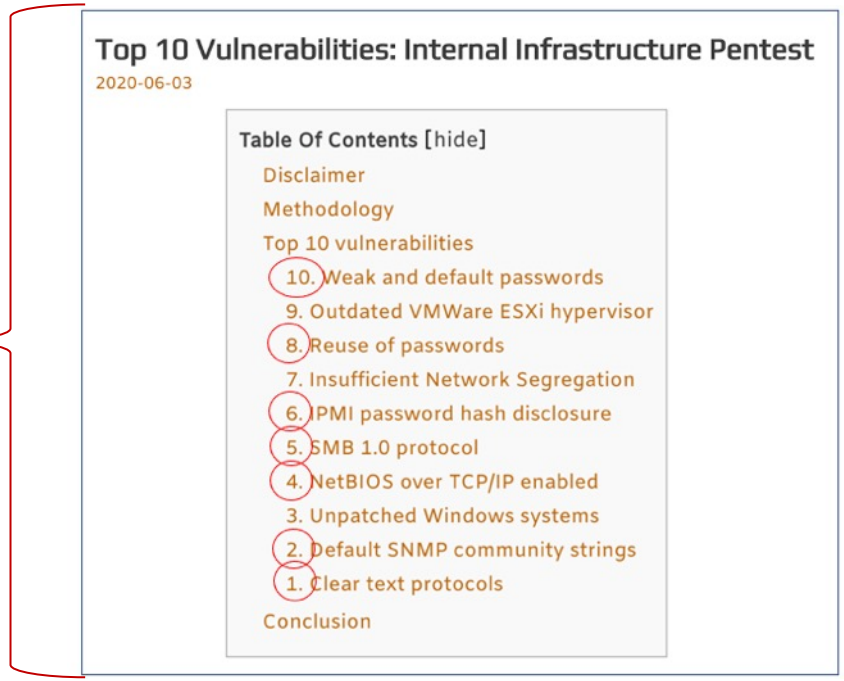


Per Customer – “We had been misreporting our ZeroLogon status for 18 months, in addition to ’Patch Tuesday’, we’ve now implemented ‘Pentest Wednesday’”

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?

Defense & Assess in-depth Approach

Layered Defense

1
- Perimeter Security
- Endpoint Detection & Response
- Data loss prevention
- Privileged account management

Bare minimum to fend off bad guys and not be in the news

2
- SIEM (Focus on beacons & exfil)
- Asset Discovery & Mgmt
- SOAR

Detect advanced threat vectors, reduce attack surface, disrupt kill chains, and accelerate forensics

4
- SIEM (add more log types)
- User Behavior Analytics
- Network Segmentation

Understand user & system behavior, detect abnormal behavior, and isolate the impact of exploitation

Recommended priority

Layered Assessment

Identify threat vectors that require minimum effort by attackers to exploit, as well as verify that layered defense is working

1
- Unauthenticated External Pentests
- Unauthenticated Internal Pentests
- No-Notice Pentests to verify SOC reaction time
- Yes-Notice Pentests to build purple team

Identify app-specific & machine-specific threat vectors that require attackers invest significant time researching & building custom exploits

3
- Application Security Testing of external apps
- Authenticated Internal Vulnerability Mgmt
- Authenticated Application Pentest

Identify app-specific threat vectors for INTERNAL applications that require attackers and insider threats to invest significant time researching & building custom exploits.

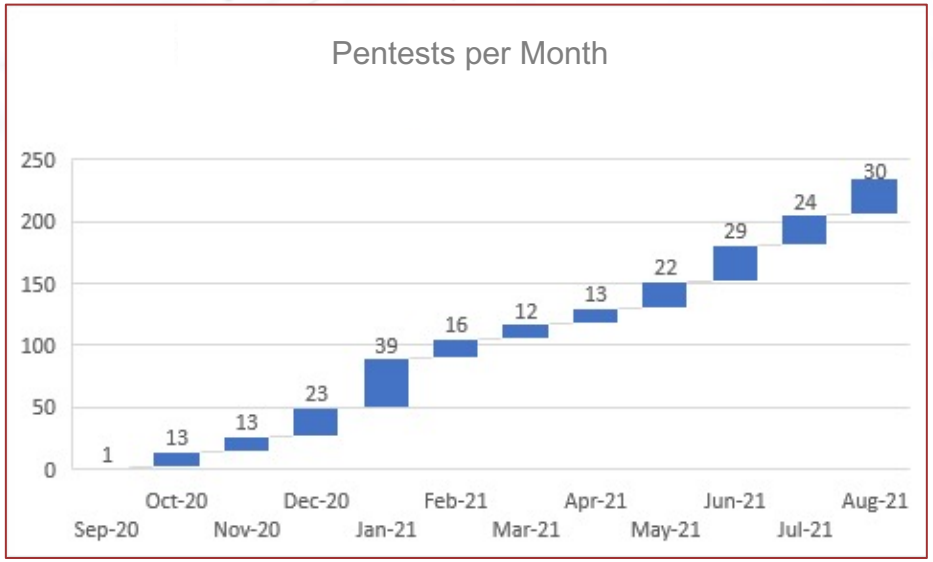
5
- Application Security Testing internal apps
- Tools, Policy, & Training Effectiveness

Manufacturing Customer with 37 Global Datacenters

Motivation

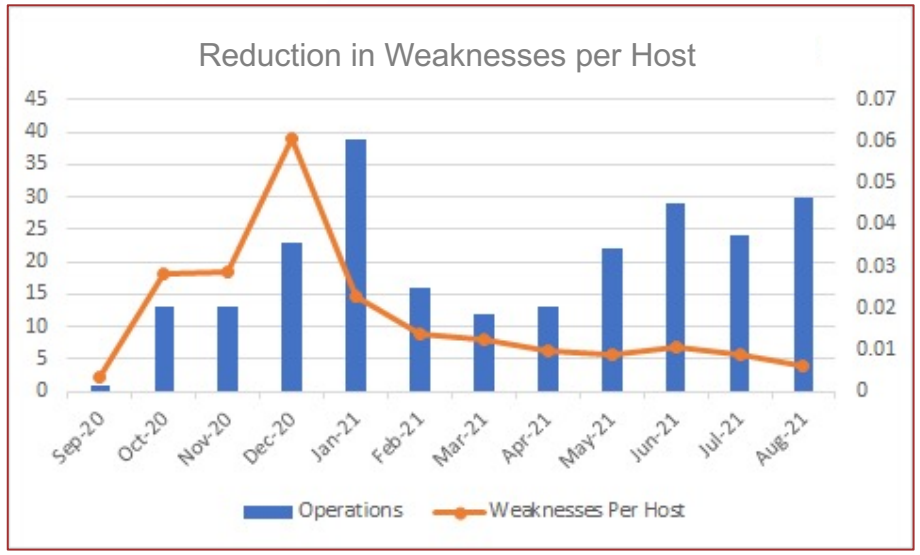
- $35k per pentest to consultants
- CISO recently fired for breach
- Cold email to deal close in 8 weeks

Adoption

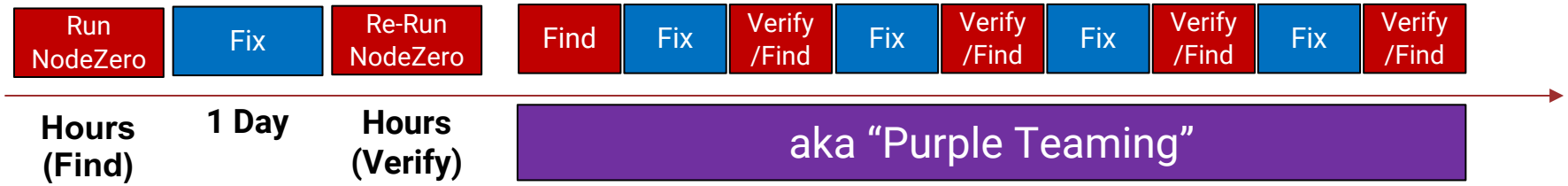


- Averaging 16 pentests per month
- ”Sparring partner” for the SOC
- Network Engineers with security “superpowers”

Impact

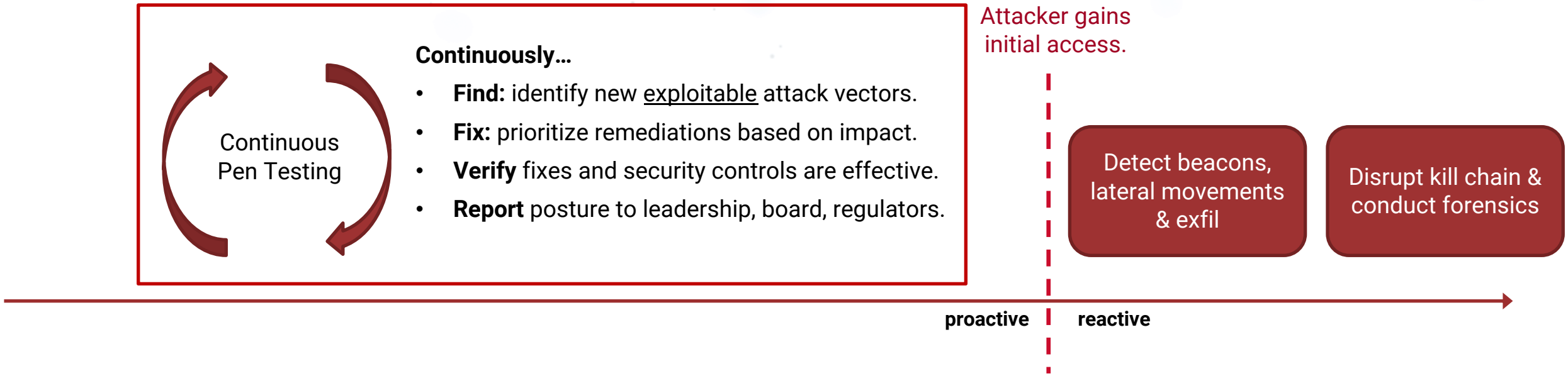


- Cut weaknesses-per-host by 95%
- Accelerated MTTR by 90%
- Saving 600+ person-hours per pentest



NodeZero – Self-Service, Agentless, Adaptive

Find & fix attack vectors before criminals exploit them.



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

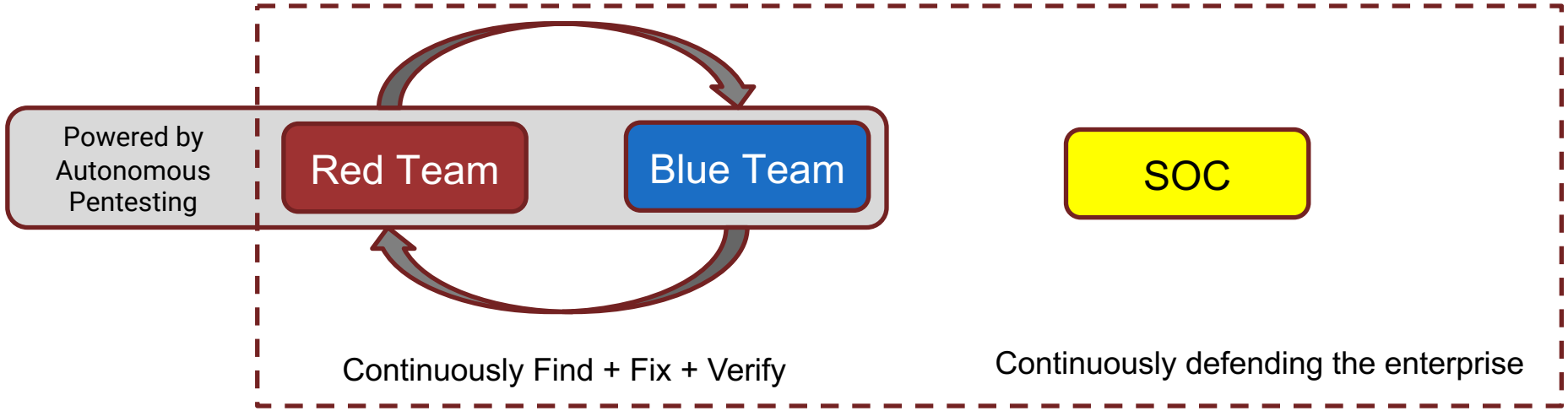
HORIZON3.ai
TRUST BUT VERIFY

Purple Team Culture

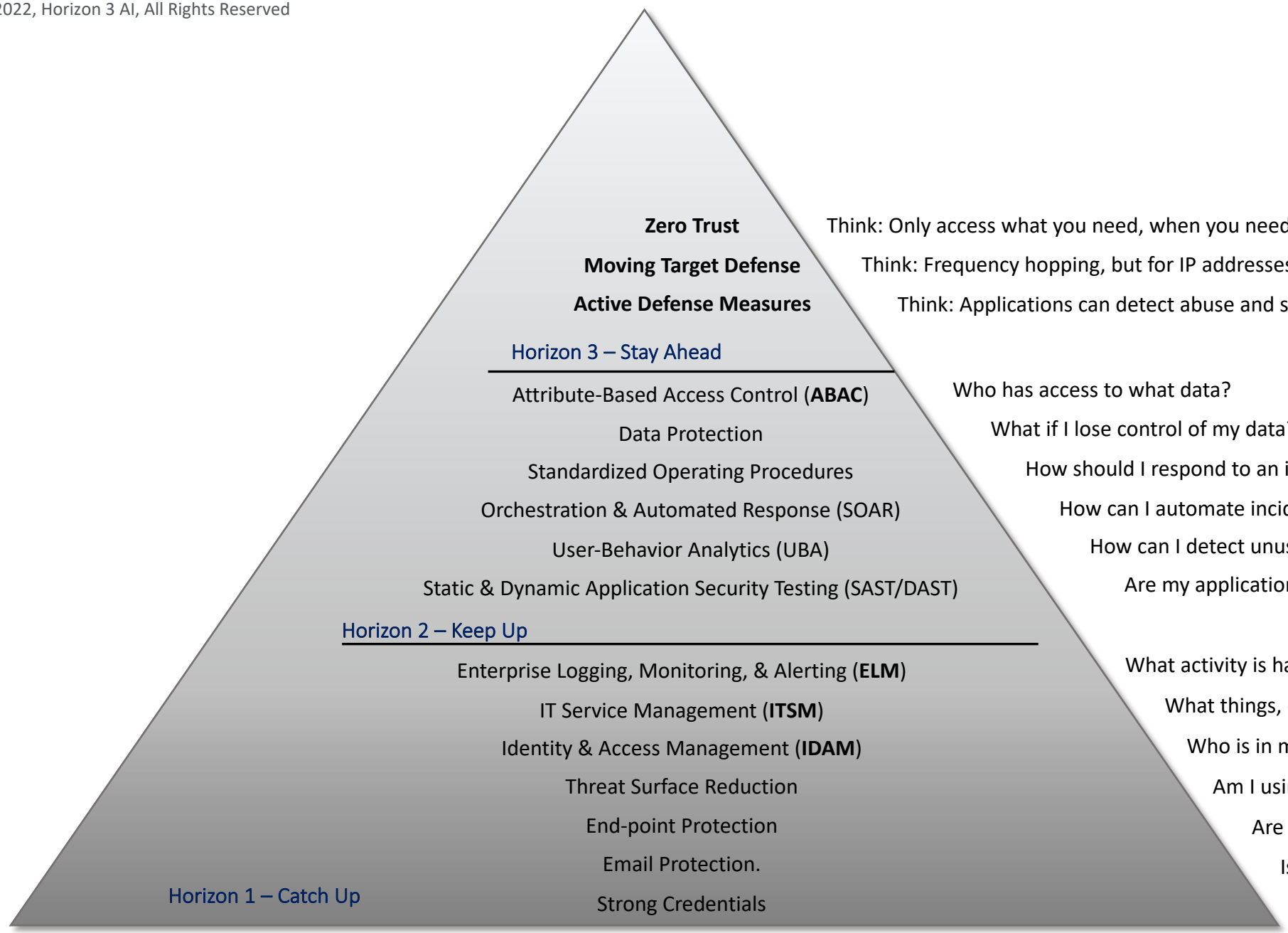
Red Team: Continuously find exploitable attack paths and hopefully trigger security alerts

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)



Hierarchy of Security Needs



Zero Trust — Think: Only access what you need, when you need it, from an authorized device

Moving Target Defense — Think: Frequency hopping, but for IP addresses

Active Defense Measures — Think: Applications can detect abuse and shut themselves down

Horizon 3 – Stay Ahead

Attribute-Based Access Control (**ABAC**) — Who has access to what data?

Data Protection — What if I lose control of my data?

Standardized Operating Procedures — How should I respond to an incident?

Orchestration & Automated Response (SOAR) — How can I automate incident response?

User-Behavior Analytics (UBA) — How can I detect unusual behavior?

Static & Dynamic Application Security Testing (SAST/DAST) — Are my applications & their configurations secure?

Horizon 2 – Keep Up

Enterprise Logging, Monitoring, & Alerting (**ELM**) — What activity is happening in my environment?

IT Service Management (**ITSM**) — What things, devices, software, & systems are in my environment?

Identity & Access Management (**IDAM**) — Who is in my environment?

Threat Surface Reduction — Am I using the latest patches & reducing complexity?

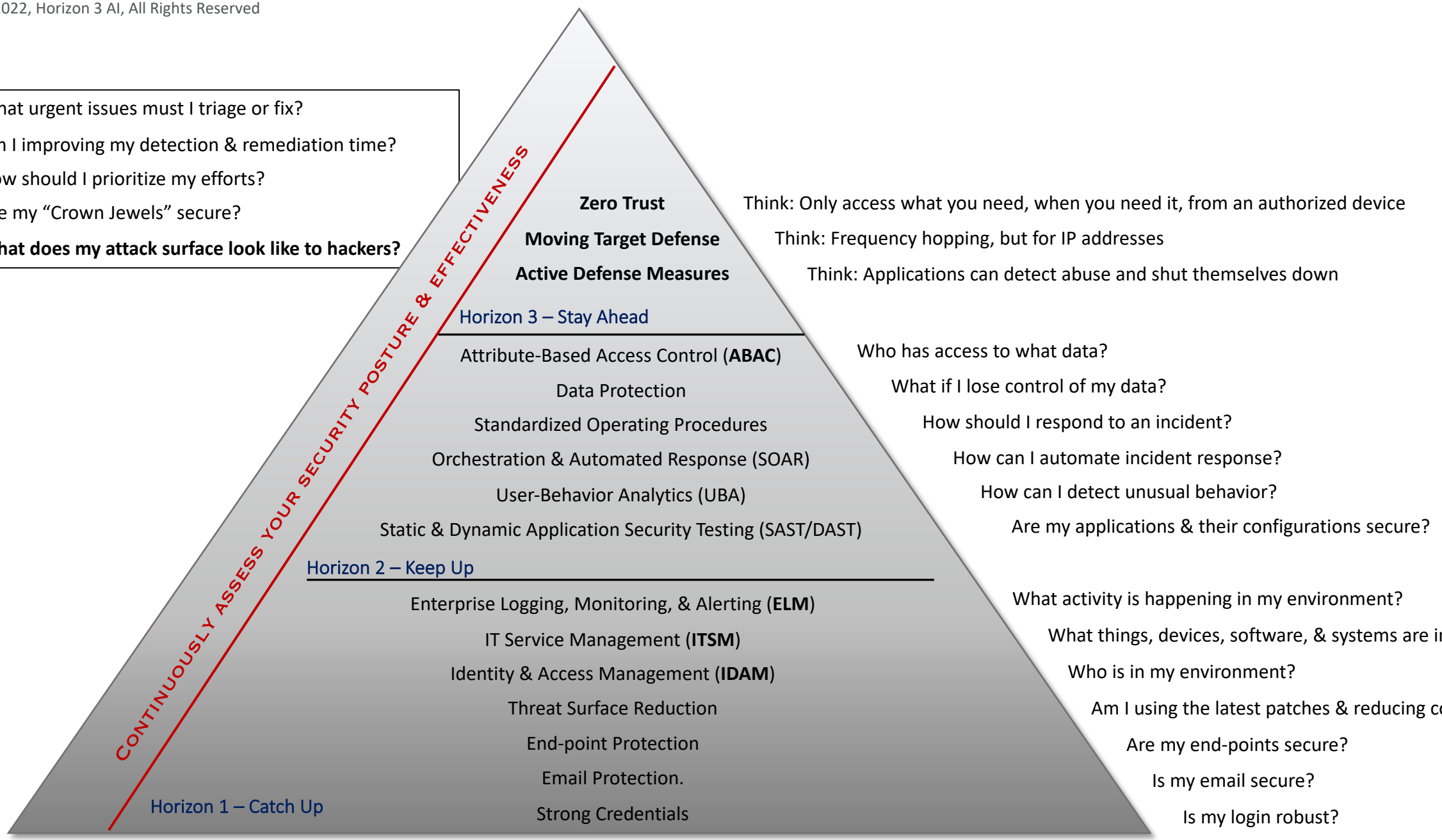
End-point Protection — Are my end-points secure?

Email Protection. — Is my email secure?

Horizon 1 – Catch Up

Strong Credentials — Is my login robust?

Hierarchy of Security Needs



Funding Approach – Planning your Multi-year Journey

Horizon1- Catch Up

1. **Assess posture via PenTesting**

2. **Reduce attack surface:**
   - Remove unnecessary software
   - Remove old hardware
   - Remove unneeded users
   - Reduce # of admin accounts
   - Patch & upgrade software
   - Secure perimeter
   - Secure endpoints

3. **Accelerate threat detection**
   - Log, Monitor, Alert critical events

4. **Accelerate remediation**
   - Define and implement SOP's

5. **Identify, locate, protect "Crown Jewels"**
   - Identify, locate, and remove unnecessary access to critical data and systems

Horizon2- Keep Up

1. **Frequently assess posture via PenTesting**

2. **Reduce attack surface**
   - Discovery & Manage all assets
   - Govern & Monitor all changes
   - Reduce # of admin accounts
   - Monitor privileged access
   - Establish patch mgmt. process

3. **Automated Threat Detection**
   - Log, monitor, alert all security events
   - Measure incident "reaction time"

4. **Automated remediation**
   - Automate remediation of high-volume alerts
   - Implement Security Orchestration
   - Measure incident "remediation time"

5. **Identify, locate, protect "Crown Jewels"**
   - Enable identify & access management to monitor access to all critical data & systems

Horizon3 - Stay Ahead

1. **Continuously assess posture via PenTesting**

2. **Reduce attack surface**
   - Segment network to stifle lateral movement
   - Replace persistent admin access with Just-in-time admin access
   - Continuously identify, prioritize, remediate exploitable vulnerabilities
   - Continuously identify & remediate 0-days in custom applications

3. **Automated Threat Detection**
   - Detect abnormal user & systems behavior
   - Optimize incident "reaction time"

4. **Automated remediation**
   - Automate remediation of high-impact issues
   - Optimize incident "remediation time"

5. **Identify, locate, protect "Crown Jewels"**
   - Isolate network access to all critical data and systems
   - Monitor, baseline, and identify anomalous inbound/outbound communications

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Who we are

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

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

What we do

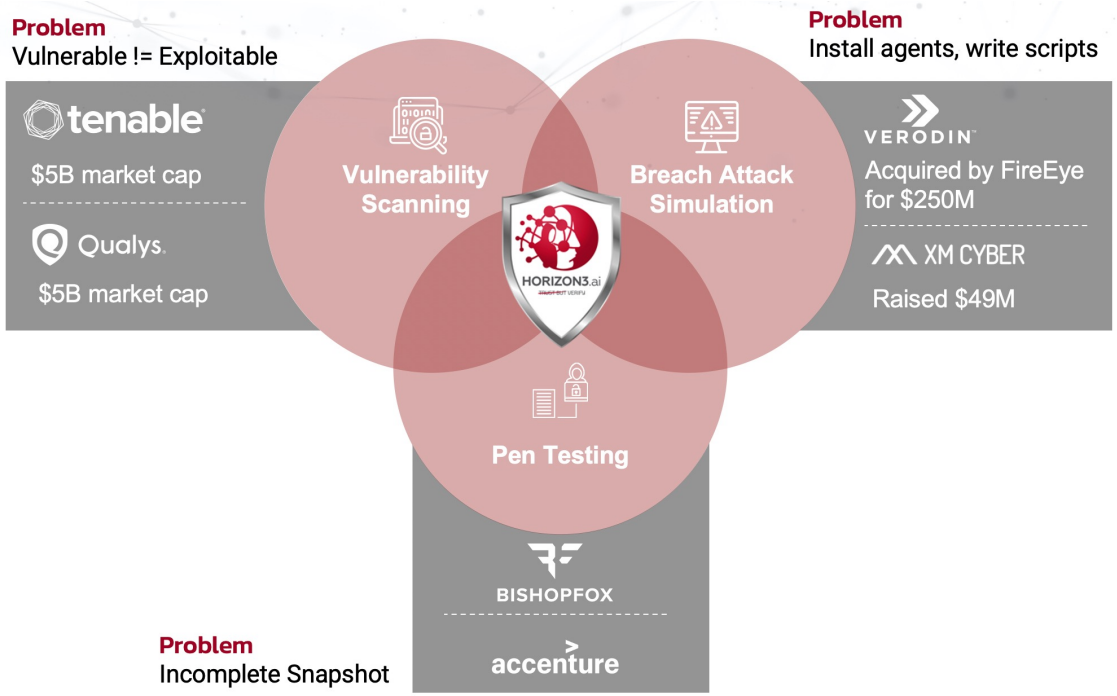
~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

(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

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