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”
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

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”
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

Reused Credentials + Misconfigurations + Dangerous Defaults

No CVEs or malware were used in this attack.

How quickly can you detect this?

How do you know?
## Layered Defense

1. **Perimeter Security**
2. **Endpoint Detection & Response**
3. **Data loss prevention**
4. **Privileged account management**
5. **SIEM (Focus on beacons & exfil)**
6. **Asset Discovery & Mgmt**
7. **SOAR**

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

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

### Recommended priority

## Layered Assessment

1. **Unauthenticated External Pentests**
2. **Unauthenticated Internal Pentests**
3. **No-Notice Pentests to verify SOC reaction time**
4. **Yes-Notice Pentests to build purple team**
5. **Application Security Testing of external apps**
6. **Authenticated Internal Vulnerability Mgmt**
7. **Authenticated Application Pentest**

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

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

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

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

<table>
<thead>
<tr>
<th>Run NodeZero</th>
<th>Fix</th>
<th>Re-Run NodeZero</th>
<th>Find</th>
<th>Fix</th>
<th>Verify /Find</th>
<th>Fix</th>
<th>Verify /Find</th>
<th>Fix</th>
<th>Verify /Find</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours (Find)</td>
<td>1 Day</td>
<td>Hours (Verify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

aka “Purple Teaming”
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

Continuous Pen Testing

- 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.

Attacker gains initial access.

- Detect beacons, lateral movements & exfil
- Disrupt kill chain & conduct forensics

---

8
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)
Zero Trust
Moving Target Defense
Active Defense Measures

Horizon 3 – Stay Ahead
Attribute-Based Access Control (ABAC)
Data Protection
Standardized Operating Procedures
Orchestration & Automated Response (SOAR)
User-Behavior Analytics (UBA)
Static & Dynamic Application Security Testing (SAST/DAST)

Horizon 2 – Keep Up
Enterprise Logging, Monitoring, & Alerting (ELM)
IT Service Management (ITSM)
Identity & Access Management (IDAM)
Threat Surface Reduction
End-point Protection
Email Protection.
Strong Credentials

Horizon 1 – Catch Up

Think: Only access what you need, when you need it, from an authorized device
Think: Frequency hopping, but for IP addresses
Think: Applications can detect abuse and shut themselves down

Who has access to what data?
What if I lose control of my data?
How should I respond to an incident?
How can I automate incident response?
How can I detect unusual behavior?
Are my applications & their configurations secure?

What activity is happening in my environment?
What things, devices, software, & systems are in my environment?
Who is in my environment?
Am I using the latest patches & reducing complexity?
Are my end-points secure?
Is my email secure?
Is my login robust?
What urgent issues must I triage or fix?
Am I improving my detection & remediation time?
How should I prioritize my efforts?
Are my “Crown Jewels” secure?
What does my attack surface look like to hackers?

Zero Trust
Moving Target Defense
Active Defense Measures
Horizon 3 – Stay Ahead
Attribute-Based Access Control (ABAC)
Data Protection
Standardized Operating Procedures
Orchestration & Automated Response (SOAR)
User-Behavior Analytics (UBA)
Static & Dynamic Application Security Testing (SAST/DAST)

Think: Only access what you need, when you need it, from an authorized device
Think: Frequency hopping, but for IP addresses
Think: Applications can detect abuse and shut themselves down

Who has access to what data?
What if I lose control of my data?
How should I respond to an incident?
How can I automate incident response?
How can I detect unusual behavior?
Are my applications & their configurations secure?

Think: Only access what you need, when you need it, from an authorized device
Think: Frequency hopping, but for IP addresses
Think: Applications can detect abuse and shut themselves down

What activity is happening in my environment?
What things, devices, software, & systems are in my environment?
Am I using the latest patches & reducing complexity?
Are my end-points secure?
Is my email secure?
Is my login robust?

Horizon 2 – Keep Up
Enterprise Logging, Monitoring, & Alerting (ELM)
IT Service Management (ITSM)
Identity & Access Management (IDAM)
Threat Surface Reduction
End-point Protection
Email Protection.
Strong Credentials

Horizon 1 – Catch Up

Continuously assess your security posture & effectiveness
<table>
<thead>
<tr>
<th>Horizon 1 - Catch Up</th>
<th>Horizon 2 - Keep Up</th>
<th>Horizon 3 - Stay Ahead</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Assess posture via PenTesting</td>
<td><strong>Frequently</strong> assess posture via PenTesting</td>
<td>1. <strong>Continuously</strong> assess posture via PenTesting</td>
</tr>
<tr>
<td>2. Reduce attack surface:</td>
<td><strong>Reduce attack surface</strong></td>
<td>2. <strong>Reduce attack surface</strong></td>
</tr>
<tr>
<td>• Remove unnecessary software</td>
<td>• Discovery &amp; Manage all assets</td>
<td>• Segment network to stifle lateral movement</td>
</tr>
<tr>
<td>• Remove old hardware</td>
<td>• Govern &amp; Monitor all changes</td>
<td>• Replace persistent admin access with Just-in-time admin access</td>
</tr>
<tr>
<td>• Remove unneeded users</td>
<td>• Reduce # of admin accounts</td>
<td>• Continuously identify, prioritize, remediate exploitable vulnerabilities</td>
</tr>
<tr>
<td>• Reduce # of admin accounts</td>
<td>• Monitor privileged access</td>
<td>• Continuously identify &amp; remediate 0-days in custom applications</td>
</tr>
<tr>
<td>• Patch &amp; upgrade software</td>
<td>• Establish patch mgmt. process</td>
<td></td>
</tr>
<tr>
<td>• Secure perimeter</td>
<td>• Secure endpoints</td>
<td></td>
</tr>
<tr>
<td>• Secure endpoints</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Accelerate threat detection</strong></td>
<td>3. <strong>Automated Threat Detection</strong></td>
</tr>
<tr>
<td></td>
<td>• Log, Monitor, Alert critical events</td>
<td>• Detect abnormal user &amp; systems behavior</td>
</tr>
<tr>
<td>3. Accelerate threat detection</td>
<td></td>
<td>• Optimize incident “reaction time”</td>
</tr>
<tr>
<td></td>
<td>• Log, Monitor, Alert critical events</td>
<td>4. <strong>Automated remediation</strong></td>
</tr>
<tr>
<td>4. Accelerate remediation</td>
<td></td>
<td>• Automate remediation of high-impact issues</td>
</tr>
<tr>
<td></td>
<td>• Define and implement SOP’s</td>
<td>• Optimize incident “remediation time”</td>
</tr>
<tr>
<td></td>
<td>• Identify, locate, and remove unnecessary access to critical data and systems</td>
<td>• Isolate network access to all critical data and systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Monitor, baseline, and identify anomalous inbound/outbound communications</td>
</tr>
</tbody>
</table>
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)

Disrupting the $25B Security Testing Market

Continuous...

- Find exploitable chained vulnerabilities
- Fix what matters
- Verify your posture

Effective Security

Domain Admin in 7 minutes 19 seconds
No Security Alerts Triggered
Fix the Effectiveness Problem

© 2022, Horizon 3 AI, All Rights Reserved
Schedule a demo
www.horizon3.ai/demo

Start your free trial now
www.horizon3.ai/trial