The Attacker's Perspective

"I hear a lot of solutions..what is the problem?"

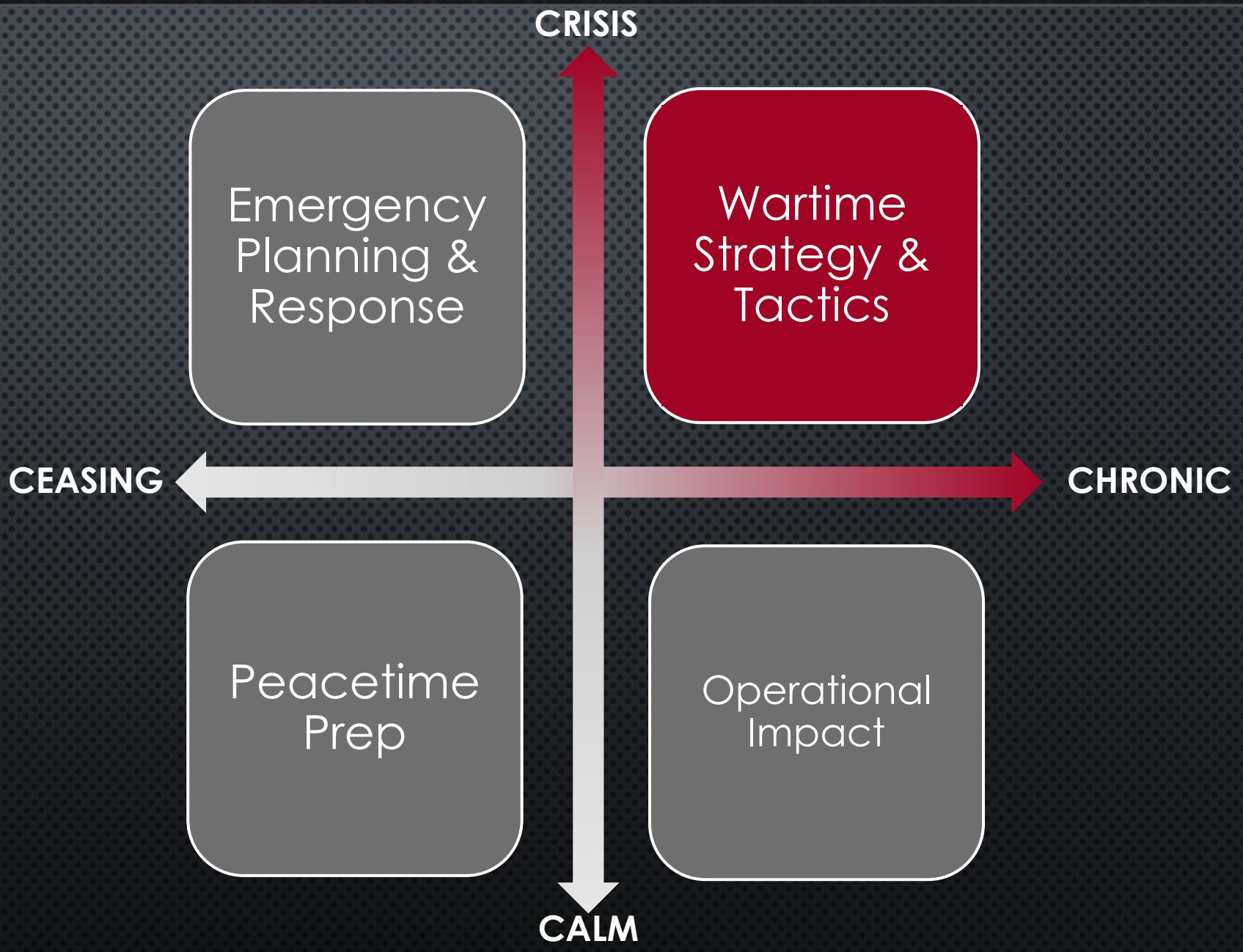
"ARE WE READY?"

HORIZON3.ai
~~TRUST BUT~~ VERIFY

THE PANDEMIC

FEAR AND IGNORANCE

- HEADLINES
- OPINIONS
- ASSUMPTION
- REGULATIONS
- FACTS



"THE CONCEPT THAT ALL COMBAT, INDEED ALL HUMAN COMPETITION FROM CHESS TO SOCCER TO BUSINESS, INVOLVES A CONTINUOUS CYCLE OF…"

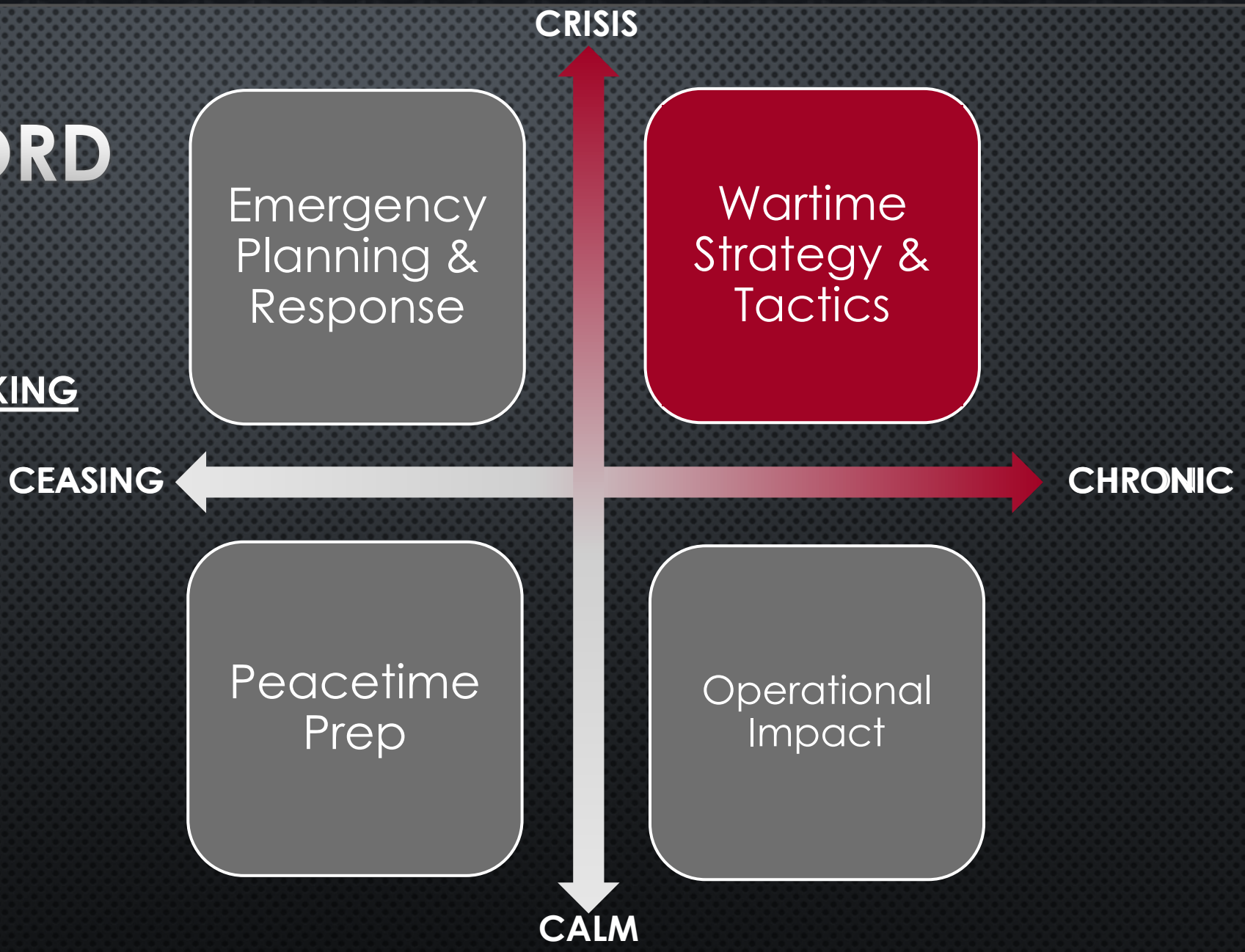
- COL JOHN BOYD (USAF)

HORIZON3.ai
~~TRUST BUT~~ VERIFY

THE PASSWORD PANDEMIC

WARTIME DECISION-MAKING

- HONEST
- ACCURATE
- RELEVANT
- SPEED
- SCALE



“ARE WE READY?”

Russian OSINT : "A recent report from Microsoft said that 2 extremely effective attacks for introducing Ransomware are brute-force and RDP hacking, how do you think, will attack vectors change over time?"

REvil: "Brute force has been alive for 20 years. And he will be alive. RDP is the best vector."

Brute force. RDP. Not a CVE. Not a zero day.

And your zero trust framework falls apart when they get in and create their own trust.

REvil: aka Ransomware Evil/Sodinokibi is a Russia-based or Russian-speaking private ransomware-as-a-service (RaaS) operation with 2020-2021 earnings: $140M

ATTACKERS DON'T HACK IN...

THEY LOG IN.

HORIZON3.ai
~~TRUST~~ BUT VERIFY

CREDENTIAL ATTACK TTPS

OPEN SOURCE INTELLIGENCE (OSINT)

- LINKEDIN, HUNTER.IO, BREACHES

- SCANADY
- SCAN
- SHAWNC
- SHAWNCAN
- SHAWCANA

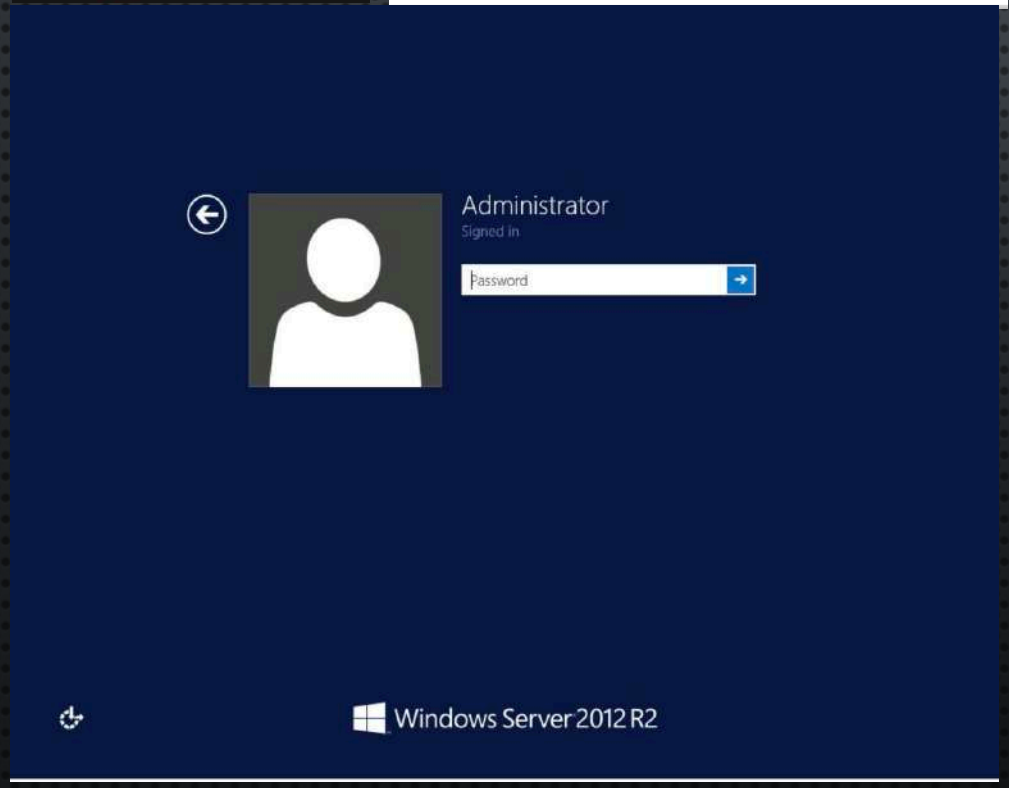
CREDENTIAL ATTACK TTPS

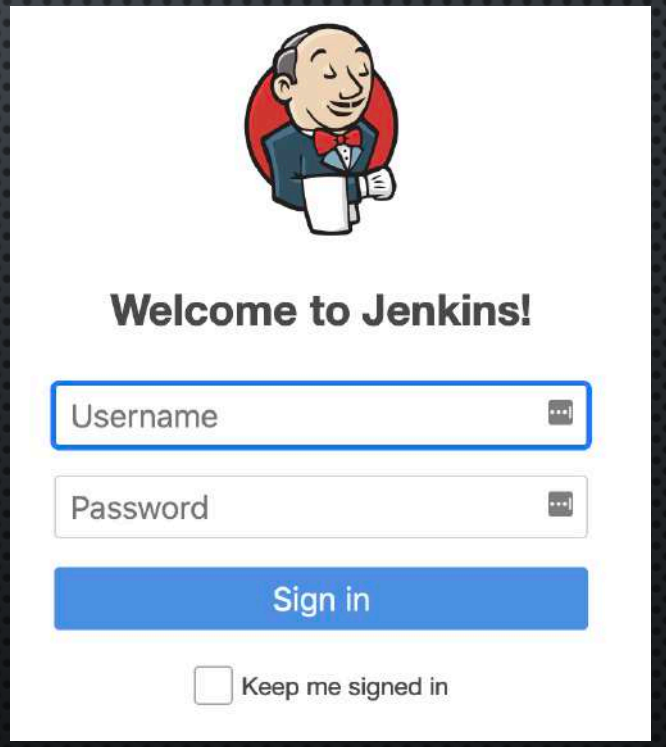
PASSWORD SPRAY

- SENSITIVE PORTS LIKE RDP
- VPNS AND AD-JOINED WEB APPLICATIONS (WITHOUT MFA)

SHODAN

port:3389 has_screenshot:true





CREDENTIAL ATTACK TTPS

BRUTE FORCE DEFAULT CREDENTIALS

- SSH
- ADMIN ACCESS TO WEB APPLICATIONS

HORIZON3.ai

~~TRUST BUT~~ VERIFY

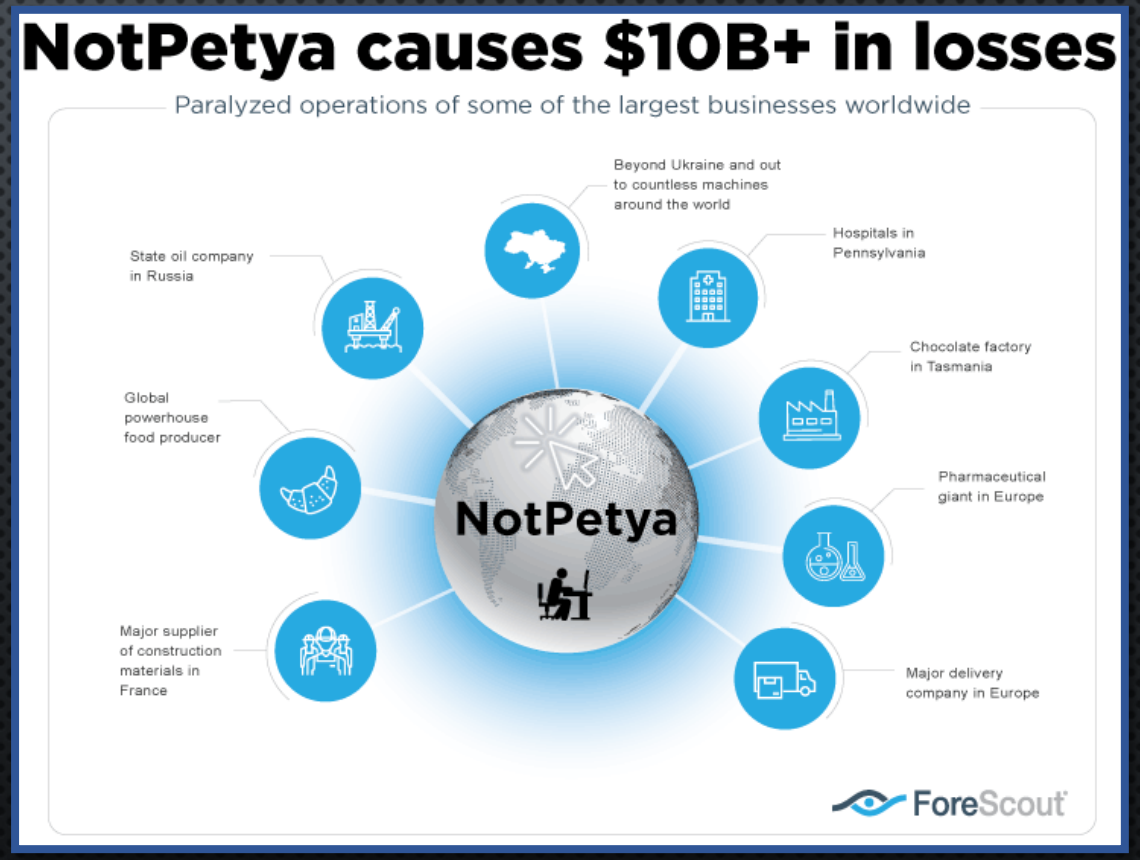
CREDENTIAL ATTACK TTPS

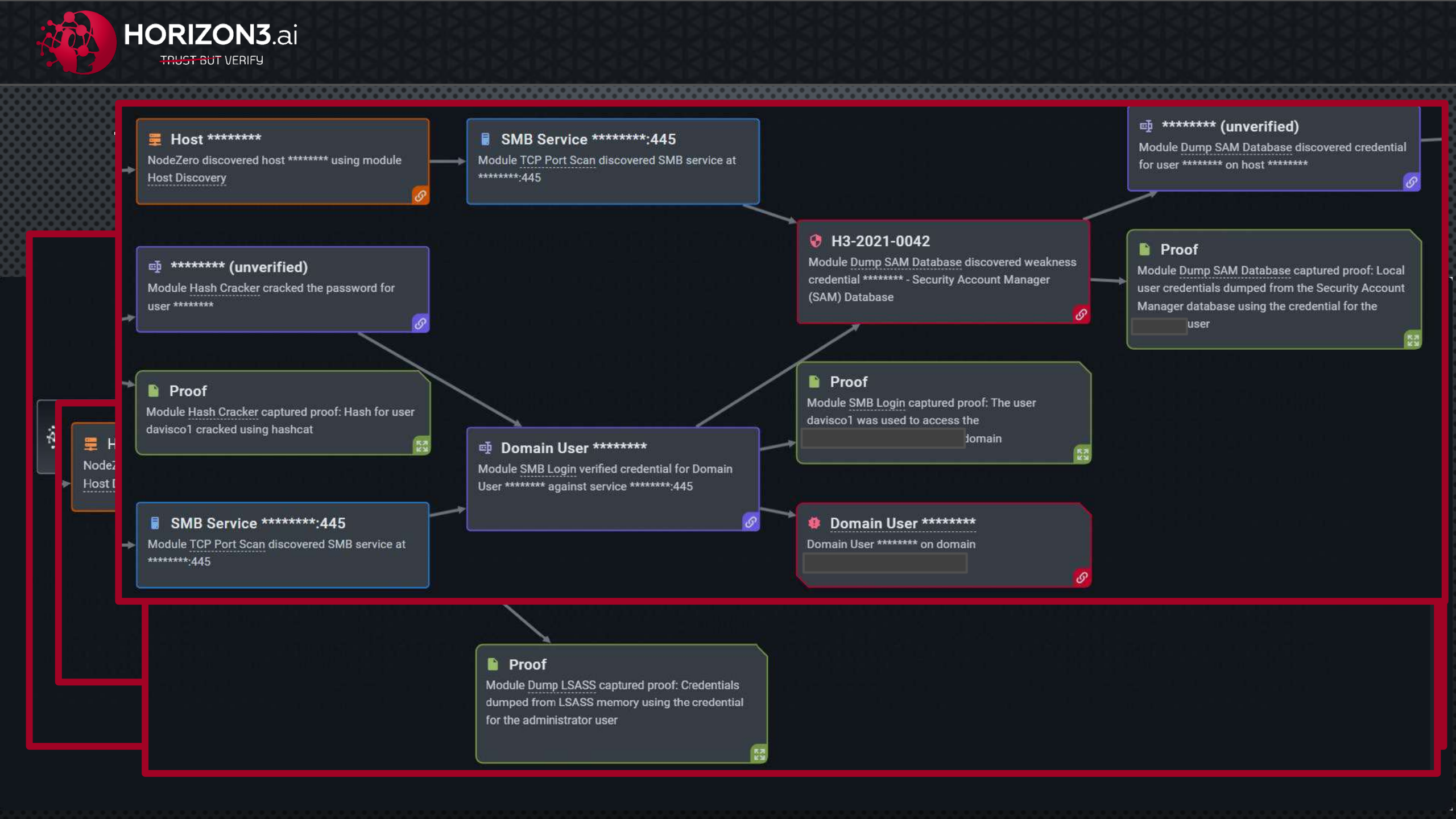
- OSINT
  - LinkedIn, hunter.io, breaches
- User validation
  - Misconfigured mail servers, OWA, Office365, Kerberos
- Password spray
  - Weak password policy, no MFA
- Default credentials
  - SSH, admin access to web applications
- Credential re-use
- Credential dumping via misconfigurations, vulnerabilities
  - Critical applications, e.g. build servers, network monitoring systems, databases
  - Network sniffing, OS credential dumping, cloud metadata URLs
- Credentials in data
  - Github repos, AWS S3 buckets, SMB/NFS shares, web sites

HORIZON3.ai
~~TRUST~~ BUT VERIFY

THE PASSWORD PANDEMIC

- **Attacker Trends**
  - Brute force or the use of lost, stolen, or compromised passwords
  - Credential Stuffing in the Financial Sector
  - Malware-free attacks
- **Industry Trends**
  - Non-expiring passwords
  - Post-breach inaction
  - Expanding attack surface
- **Personal Trends**
  - More devices, more apps, more accounts
  - Password reuse across work and home

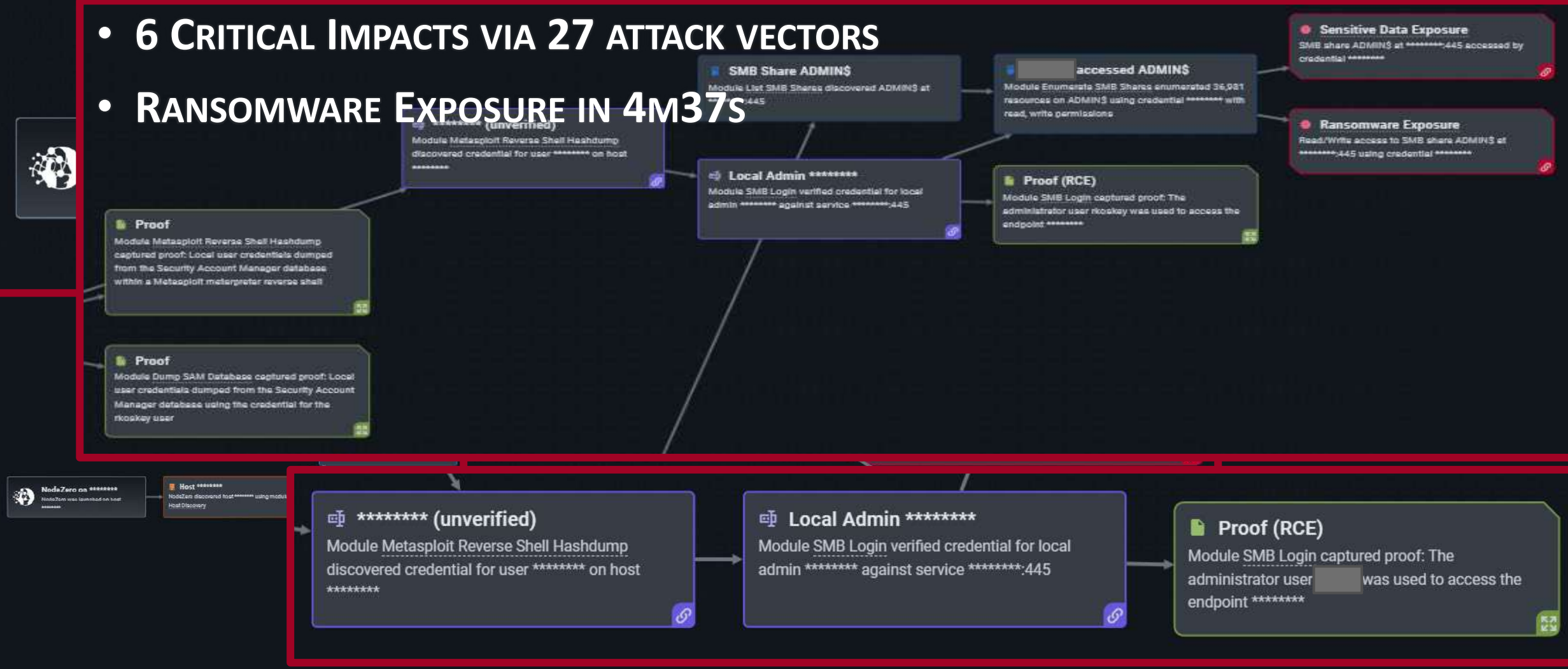



HORIZON3.ai
TRUST BUT VERIFY
Host ********
NodeZero discovered host ******** using module Host Discovery
SMB Service ********:445
Module TCP Port Scan discovered SMB service at ********:445
******** (unverified)
Module Dump SAM Database discovered credential for user ******** on host ********
H3-2021-0042
Module Dump SAM Database discovered weakness credential ******** - Security Account Manager (SAM) Database
Proof
Module Dump SAM Database captured proof: Local user credentials dumped from the Security Account Manager database using the credential for the user
******** (unverified)
Module Hash Cracker cracked the password for user ********
Proof
Module Hash Cracker captured proof: Hash for user davisco1 cracked using hashcat
Proof
Module SMB Login captured proof: The user davisco1 was used to access the domain
Domain User ********
Module SMB Login verified credential for Domain User ******** against service ********:445
SMB Service ********:445
Module TCP Port Scan discovered SMB service at ********:445
Domain User ********
Domain User ******** on domain
Proof
Module Dump LSASS captured proof: Credentials dumped from LSASS memory using the credential for the administrator user

HORIZON3.ai
TRUST BUT VERIFY

EDUCATION

- UNSPECIFIED SCOPE DISCOVERED 173 HOSTS
- 6 CRITICAL IMPACTS VIA 27 ATTACK VECTORS
- RANSOMWARE EXPOSURE IN 4M37S



"ARE WE READY?"

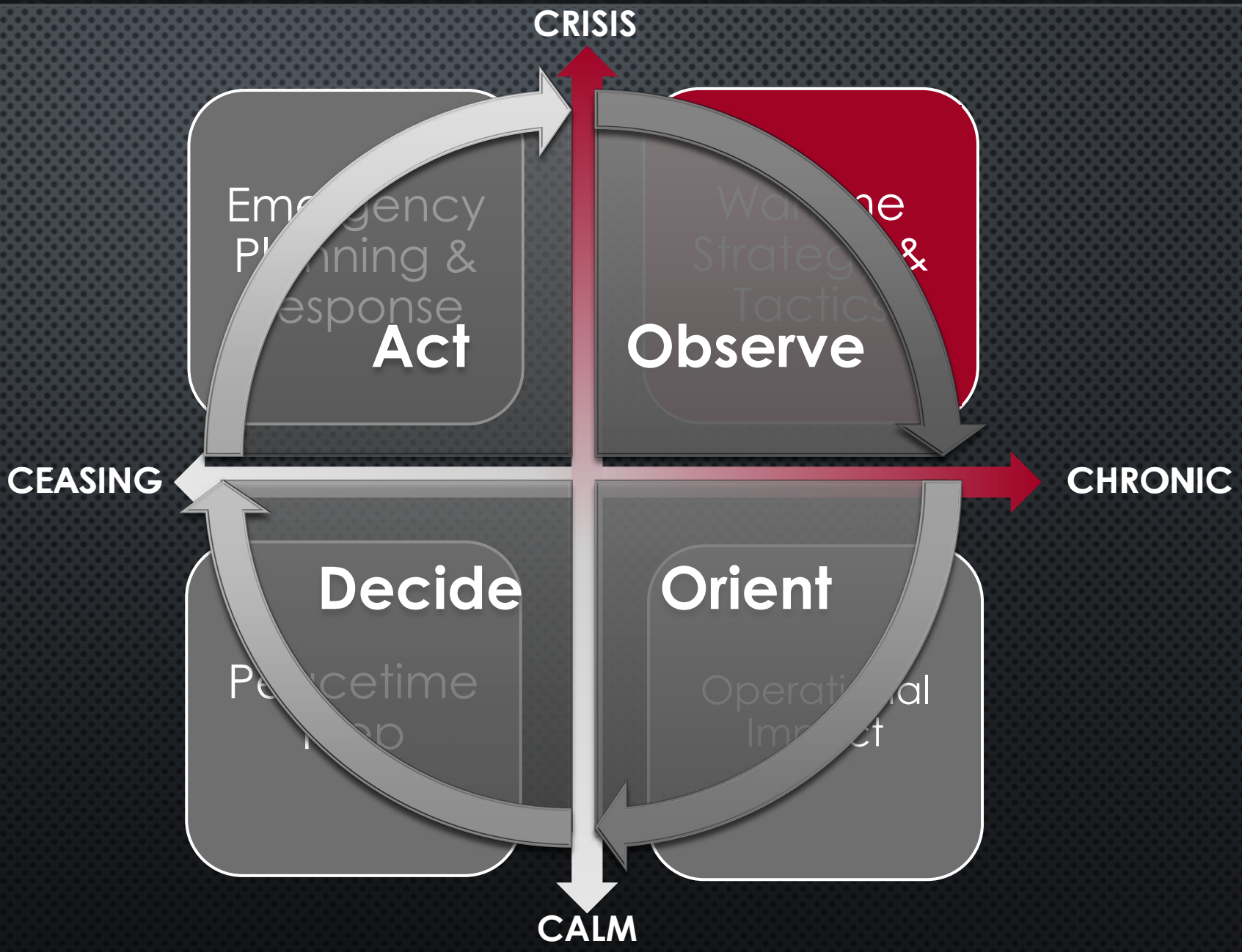
HORIZON3.ai
~~TRUST BUT~~ VERIFY

How do you know?

HORIZON3.ai
~~TRUST BUT~~ VERIFY

How Do You Know:

- Honest
- Accurate
- Relevant
- Speed
- Scale



HORIZON3.ai
~~TRUST BUT~~ VERIFY

Continuously Verify your Security Posture..in 3 clicks

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

Bob Cariddi
Chief Revenue Officer
Former SVP Sales,
SentinelOne, Whitehat

What We Do

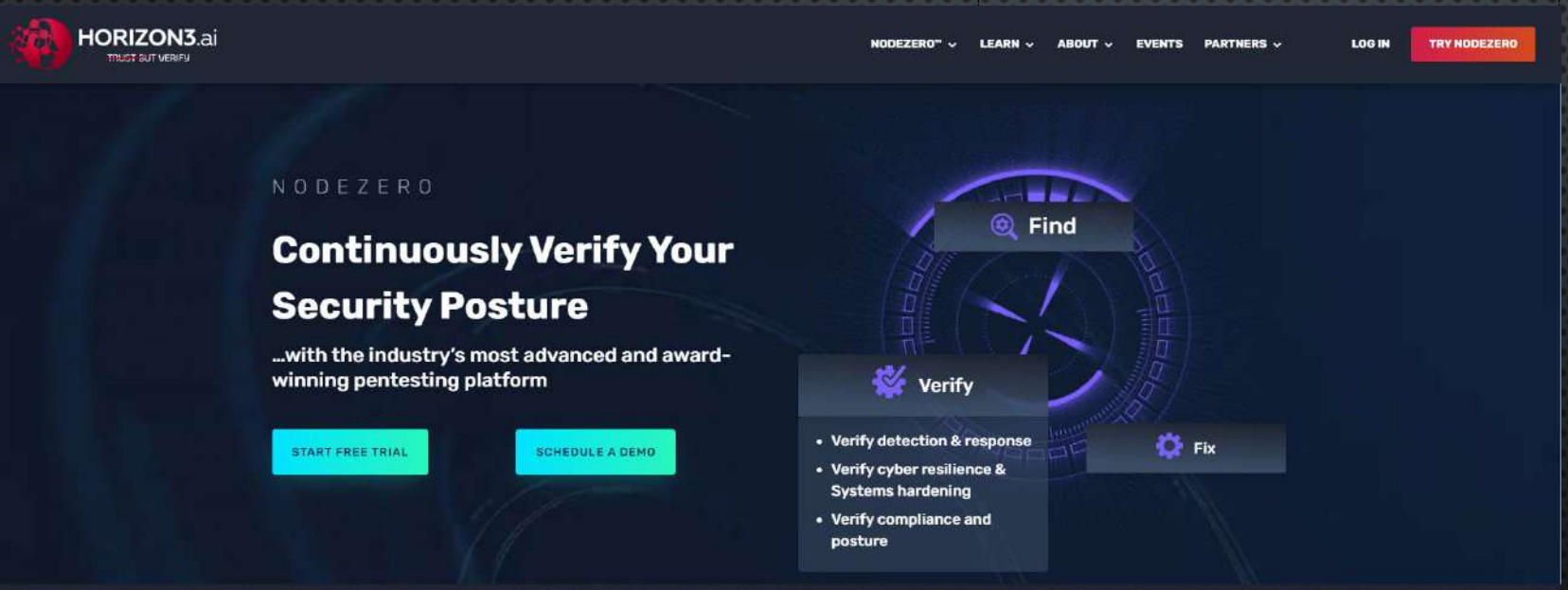
~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

Our AHA Moment

Run NodeZero → Fix Issues → Re-Run NodeZero

Hours (Find) | 1 Day | Hours (Verify)

No Scripting, No Credentialed Agents, No Consulting



Recognized and Trusted

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

Find
attack paths

Fix
what matters

Verify
your teams, tools, & rules

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