

3 16,000 Pentests später...

Man versus Machine – autonomes Pentesting in der Praxis

Jens Egger, Senior Solution Architect

“

When I was a CIO, I had no idea I was secure until the bad guys showed up. I either wait to get hacked or...
hack myself.

”



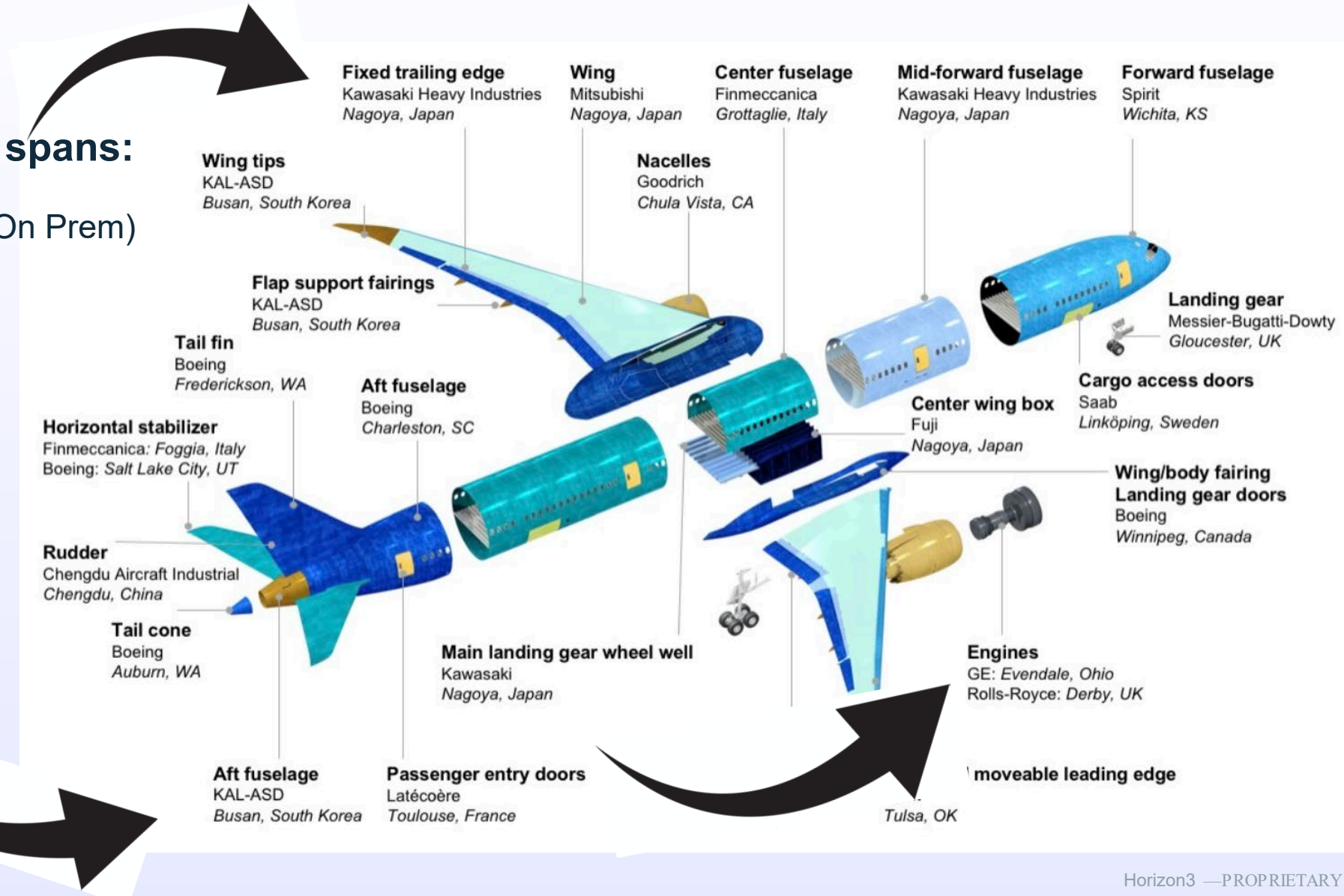
Snehal Antani

CEO and Co-Founder Horizon3.ai

Do you attack the main target or the supplier?

Cyber Attack Surface now spans:

- Enterprise IT (SaaS + Cloud + On Prem)
- Vibe Coded Apps
- Data leakage to ChatGPT
- **Suppliers**
- **Distributors**





The “Cyber” Monkey Business Illusion

Perceptual Blindness

“Inattentional or perceptual blindness” the failure to see something obvious when focusing attention on something else.

1

“Don’t Tell
me I’m
secure,
show me”

2

Take the
Attacker's
Perspective

CVE-2021-20035	CVE-2024-57968	CVE-2020-29574	CVE-2018-14933	CVE-2013-0648	CVE-2019-17621
CVE-2024-53150	CVE-2025-25181	CVE-2024-21413	CVE-2024-55956	CVE-2013-0643	CVE-2019-20500
CVE-2024-53197	CVE-2025-22226	CVE-2022-23748	CVE-2024-35250	CVE-2014-0497	CVE-2021-25487
CVE-2025-29824	CVE-2025-22225	CVE-2025-0411	CVE-2024-20767	CVE-2024-6670	CVE-2021-25489
CVE-2025-30406	CVE-2025-22224	CVE-2024-53104	CVE-2024-50623	CVE-2024-43461	CVE-2021-25394
CVE-2025-31161	CVE-2024-50302	CVE-2018-19410	CVE-2024-49138	CVE-2024-8190	CVE-2021-25395
CVE-2025-22457	CVE-2024-4885	CVE-2018-9276	CVE-2024-51378	CVE-2024-38217	CVE-2021-25371
CVE-2025-24813	CVE-2018-8639	CVE-2024-29059	CVE-2024-11667	CVE-2024-38014	CVE-2021-25372
CVE-2024-20439	CVE-2022-43769	CVE-2024-45195	CVE-2024-11680	CVE-2024-38226	CVE-2023-32434
CVE-2025-2783	CVE-2022-43939	CVE-2025-24085	CVE-2023-45727	CVE-2024-40766	CVE-2023-32435
CVE-2019-9875	CVE-2023-20118	CVE-2025-23006	CVE-2023-28461	CVE-2017-1000253	CVE-2023-32439
CVE-2019-9874	CVE-2023-34192	CVE-2020-11023	CVE-2024-21287	CVE-2016-3714	CVE-2023-20867
CVE-2025-30154	CVE-2024-49035	CVE-2024-50603	CVE-2024-44309	CVE-2024-7262	CVE-2023-27992
CVE-2017-12637	CVE-2024-20953	CVE-2025-21335	CVE-2024-44308	CVE-2021-20124	CVE-2023-20887
CVE-2024-48248	CVE-2017-3066	CVE-2025-21334	CVE-2024-38813	CVE-2021-20123	CVE-2020-35730
CVE-2025-1316	CVE-2025-24989	CVE-2025-21333	CVE-2024-38812	CVE-2024-7965	CVE-2020-12641
CVE-2025-30066	CVE-2025-0111	CVE-2024-55591	CVE-2024-9474	CVE-2024-38856	CVE-2021-44026
CVE-2025-24472	CVE-2025-23209	CVE-2023-48365	CVE-2024-0012	CVE-2024-7971	CVE-2016-9079
CVE-2025-21590	CVE-2025-0108	CVE-2024-12686	CVE-2024-1212	CVE-2024-39717	CVE-2016-0165
CVE-2025-24201	CVE-2024-53704	CVE-2025-0282	CVE-2024-9465	CVE-2021-31196	CVE-2023-27997
CVE-2025-24993	CVE-2024-57727	CVE-2020-2883	CVE-2024-9463	CVE-2024-35250	CVE-2023-3079
CVE-2025-24991	CVE-2025-24200	CVE-2024-55550	CVE-2021-26086	CVE-2024-20767	CVE-2023-33009
CVE-2025-24985	CVE-2024-41710	CVE-2024-41713	CVE-2014-2120	CVE-2024-50623	CVE-2023-33010
CVE-2025-24984	CVE-2024-40891	CVE-2024-3393	CVE-2021-41277	CVE-2024-49138	CVE-2023-34362
CVE-2025-24983	CVE-2024-40890	CVE-2021-44207	CVE-2024-43451	CVE-2024-51378	CVE-2023-28771
CVE-2025-26633	CVE-2025-21418	CVE-2024-12356	CVE-2024-49039	CVE-2024-11667	CVE-2024-21287
CVE-2024-13161	CVE-2025-21391	CVE-2021-40407	CVE-2019-16278	CVE-2024-11680	CVE-2024-44309
CVE-2024-13160	CVE-2025-0994	CVE-2019-11001	CVE-2024-51567	CVE-2023-45727	CVE-2024-44308
CVE-2024-13159	CVE-2020-15069	CVE-2022-23227	CVE-2024-43093	CVE-2023-28461	CVE-2024-38813
CVE-2024-38226	CVE-2021-37973	CVE-2024-39717	CVE-2021-21220	CVE-2019-1388	CVE-2020-15505
CVE-2024-40766	CVE-2021-30551	CVE-2021-31196	CVE-2021-30563	CVE-2023-26083	CVE-2021-30116
CVE-2017-1000253	CVE-2021-37975	CVE-2022-0185	CVE-2020-4430	CVE-2022-27926	CVE-2020-7961
CVE-2016-3714	CVE-2020-6418	CVE-2021-33045	CVE-2020-4427	CVE-2013-3163	CVE-2021-23874
CVE-2024-7262	CVE-2021-30554	CVE-2021-33044	CVE-2020-4428	CVE-2017-7494	CVE-2021-22506

PROBLEM 1

GUESSING FROM A CHECKLIST.

Passive scanning can't tell you what's actually risky.

- ⚠ Vulnerable / exploitable
- ⚠ Lacks proven business impact
- ⚠ Creates noise without priority

<2% Of vulnerabilities added in 2024 were exploited

PROBLEM 2

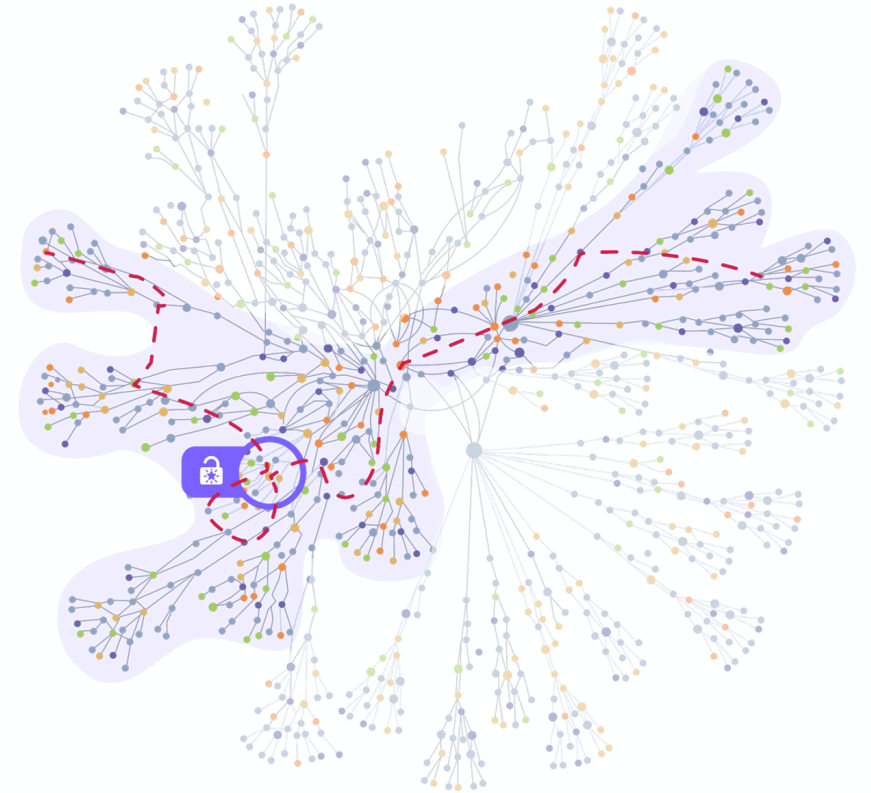
ONLY EXPLOITING A FRACTION OF EXPOSURE

Manual pentesting can't meet real-world scale and speed.

- ⚠ Snapshot in time
- ⚠ Narrow test scope
- ⚠ Unknown pentester skill

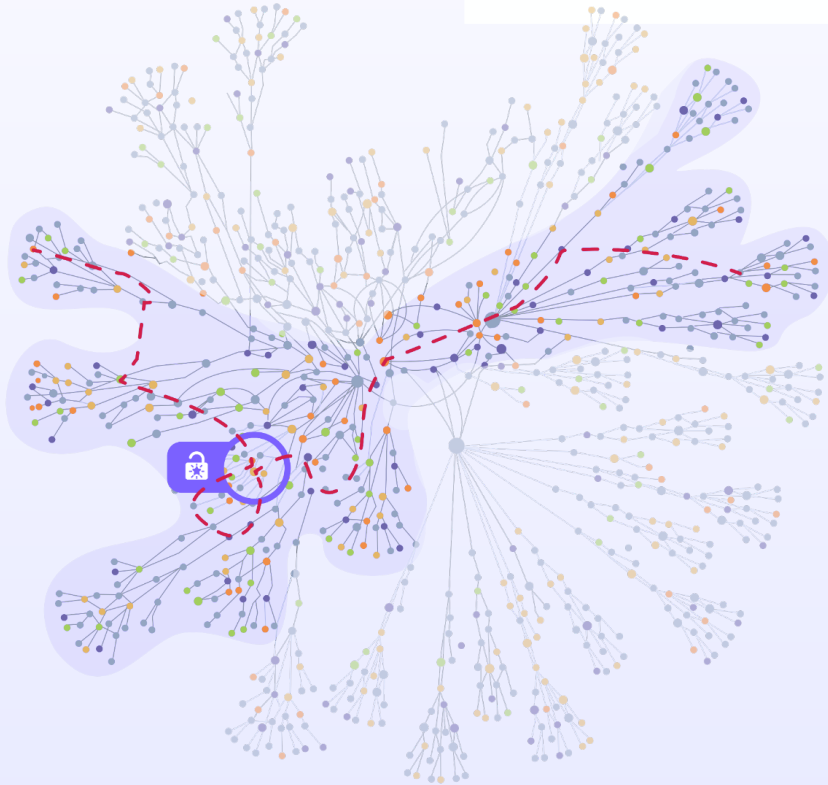
<5%

Typical environment coverage with manual pentesting



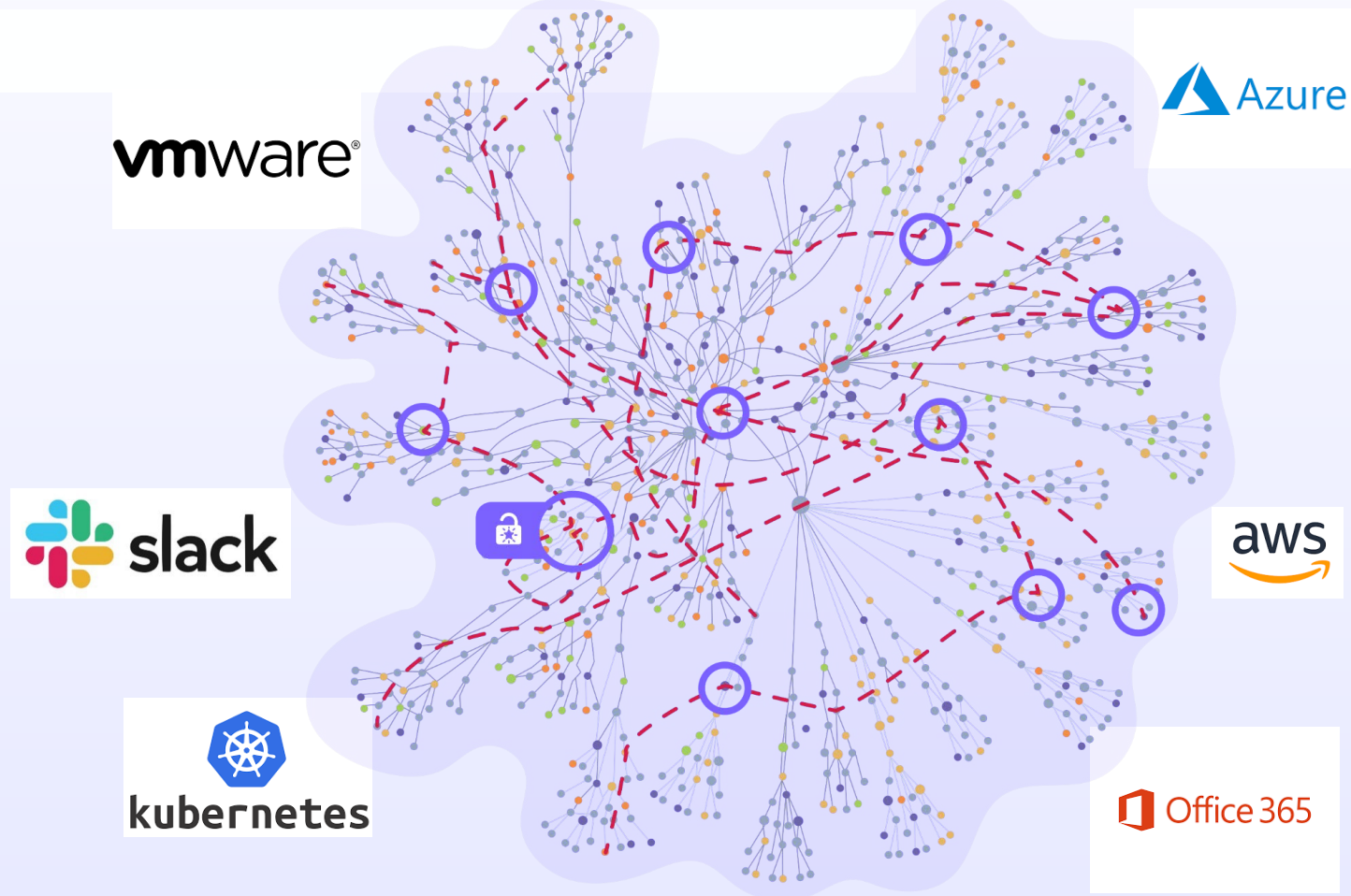
Speed, Scale, Thoroughness

Traditional Pentest



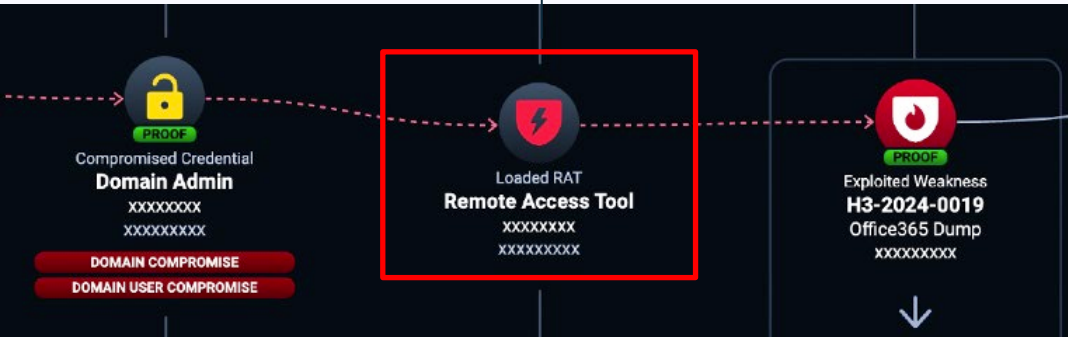
Vs.

Horizon3 NodeZero Pentest



EDR will save us all...

RAT is an in-memory implant for post-exploitation



- **How? 97%** of the time, RAT was implanted via compromised credential
- **“Prevent OS Credential Dumping”** on EDR’s is usually disabled by default
- **Key point:** verify the configuration of your security tools!!

Business Risks



Weaknesses



Impacts



Credentials



Compromised Hosts



Threat Actors

exploit

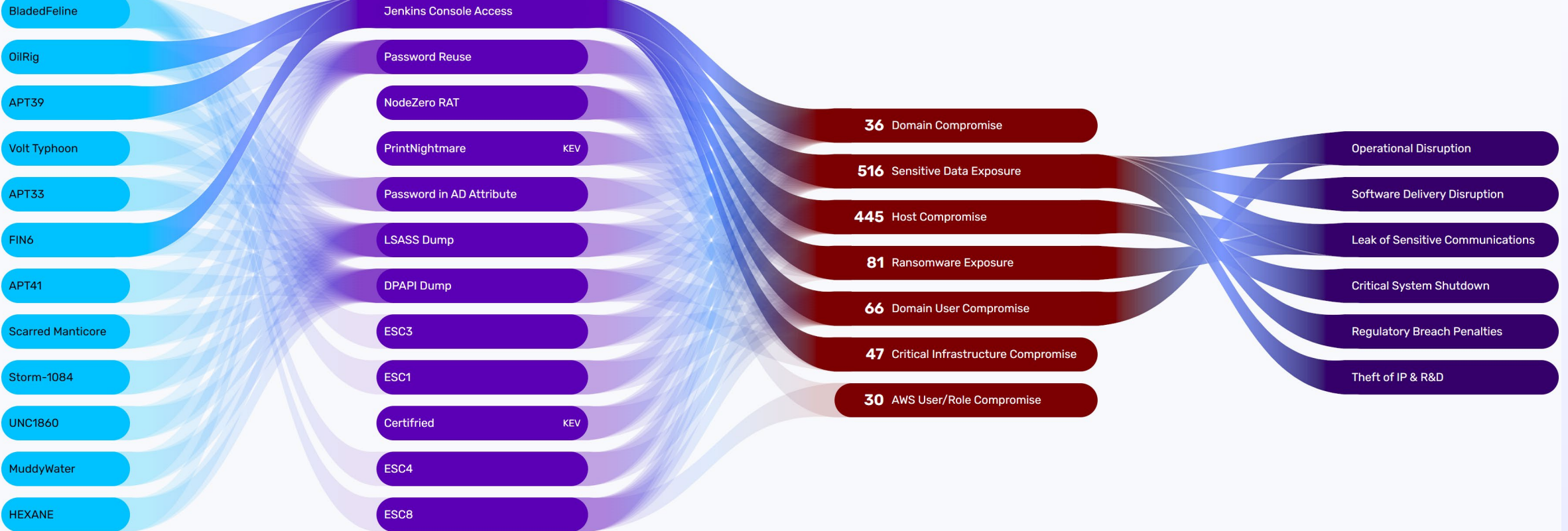
Weaknesses

to achieve

Impacts

resulting in

Business Risks

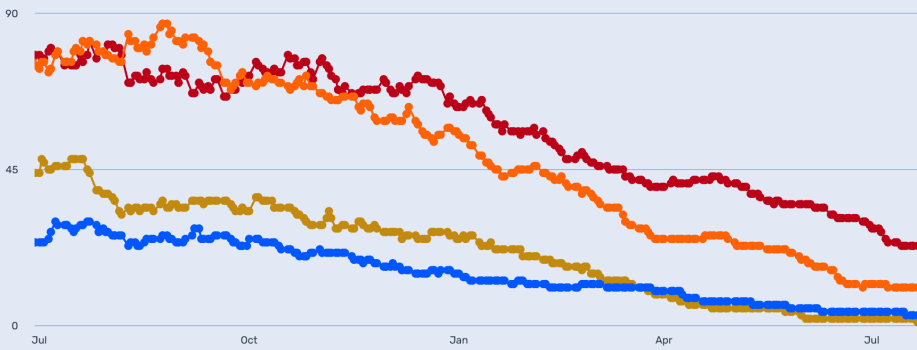


- Trends over Time
- Remediation Summary
- Pentest Campaigns
- Systemic Issues

Open Weaknesses Over Time

Trends in identified weaknesses and vulnerabilities over a selected time period.

By Severity 

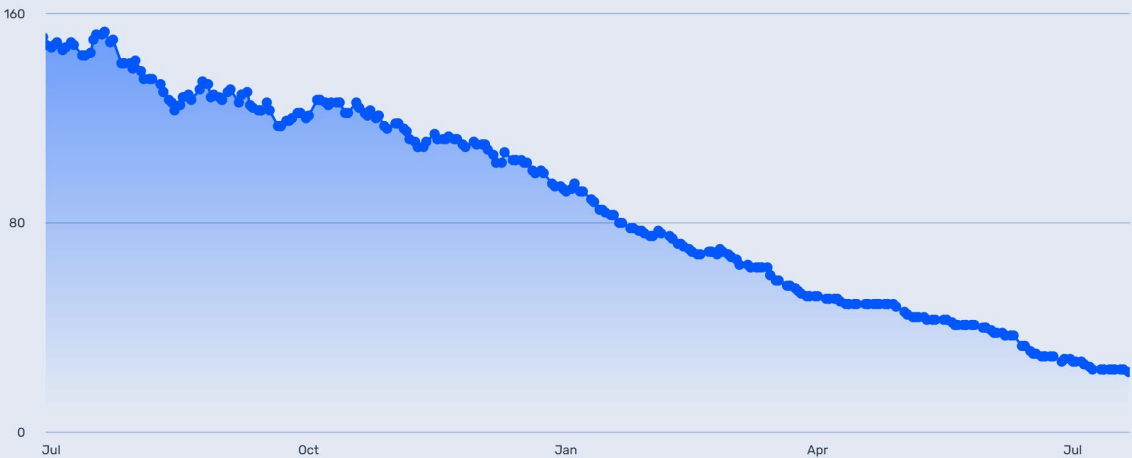


Toggle to View:  Critical  High  Medium  Low  Info

Critical 23 ↓ 68 %
High 11 ↓ 85 %
Medium 1 ↓ 98 %
Low 3 ↓ 89 %
Info 4

Attack Paths Over Time

Trends in identified attack paths discovered by NodeZero over a selected time period.



Open Attack Paths 23 ↓ 84 %
Critical Infrastructure Compromise 7 ↓ 75 %
BusinessEmailCompromise 6 ↓ 63 %
Ransomware Exposure 3 ↓ 86 %
Sensitive Data Exposure 3 ↓ 90 %



HORIZON3

NodeZero[®] WebApp Pentesting



Horizon3.ai Is Building a WebApp Pentest



True black -box test with authentication support, designed to run continuously

No code access required.

Multi-role, session-aware testing that mirrors attacker behavior and runs as often as the customer needs.



Safe to run in production against external -facing apps or in the CI/CD

Guardrails, safe execution tiers, and deterministic behavior allow the same test to operate safely in live environments or shift-left in the pipeline.



Unified and integrated with NodeZero's External + Internal + Cloud engines for attack chaining

One offensive engine across WebApps, external exposure, internal paths, identities, and cloud—finally showing how attackers move through the whole environment.



NodeZero's Offensive Engine Has Advantages



Production - Safe Testing

- Safely executes exploit chains in real customer environments



Real Exploitability Proof

- Proof-based engine catches what DAST/ SAST/ Consultants miss
- Every finding backed by **replayable artifacts** (GIFs, logs, requests)



Multi - Step Attacks

- BAC → endpoint accessed → SSRF → image fetched → IAM profile revealed → cloud tokens stolen → ... → full control



Preprod + Prod Validation

- Pivots and chains across External + Internal + WebApps (both public-facing and internal) testing in one full spectrum loop



Continuous Testing

- Repeated scheduled tests catch the latest exploitable vulnerabilities



NodeZero Has Depth & Speed Where It Matters

NodeZero focuses on the top CWEs (e.g. OWASP Top 10) enterprises need.

Broken Access Control

XSS

Injection

Misconfigurations

Authentication failures

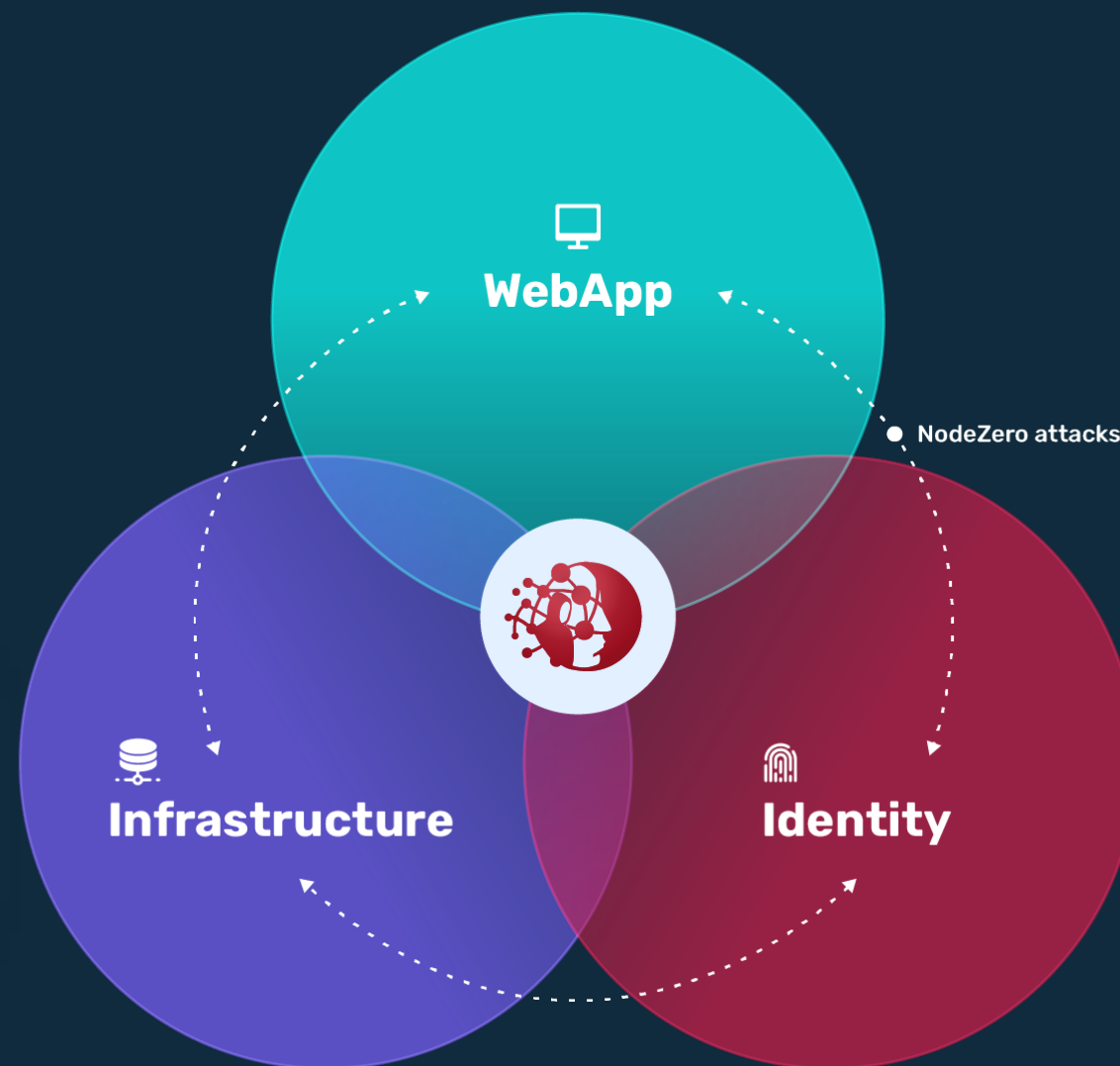
Insecure design

NodeZero also includes a set of features that will provide completeness and coverage for testing cases:

- **Authenticated Testing:** Multi-role, session-aware testing that mirrors real attacker behavior.
- **Route Discovery + Mapping:** Automatic identification of pages, routes, and actions with visual traceability.
- **Production - Safe Execution Modes:** Light assessment → full exploit modes with guardrails.
- **Replayable, Proof - Based Artifacts:** Screenshots, GIFs, logs, and endpoint traces.
- **Internal + External Testing:** Immediate value whether customers start from internal or external.

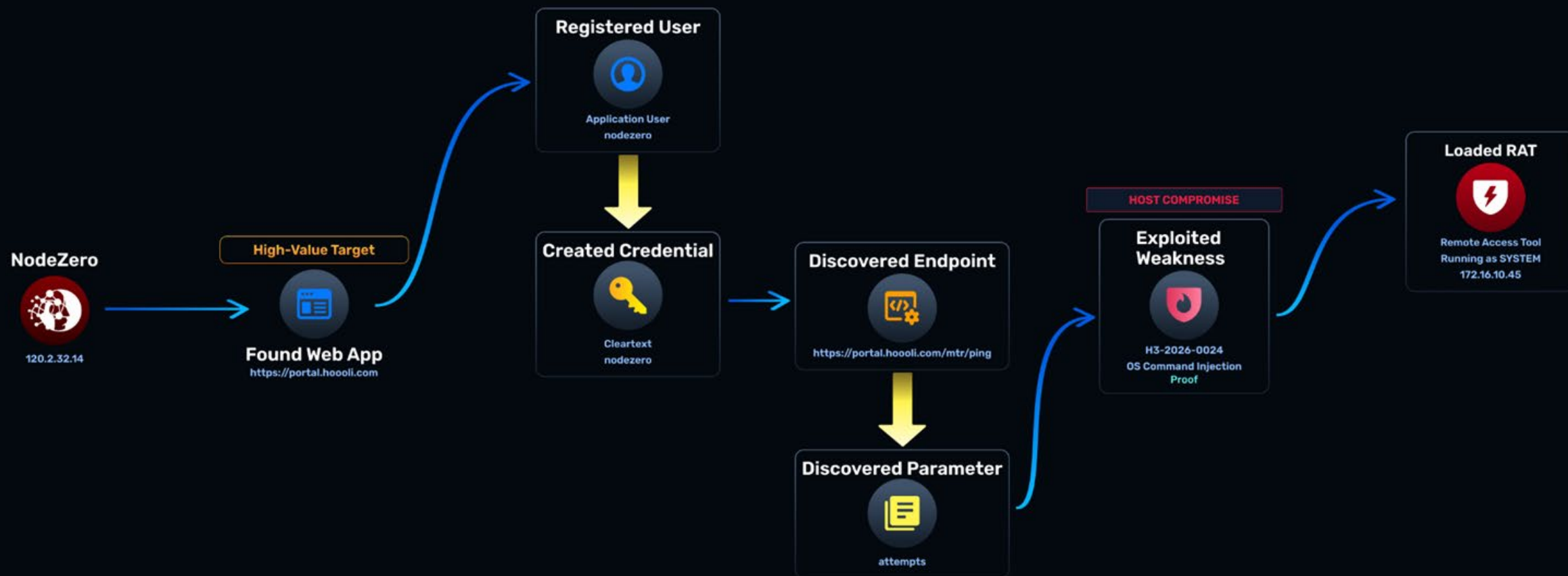
Our Vision

- Hackers and APTs chain compromise with apps, infra, IAM
- Coupling AI with safety and automation is key



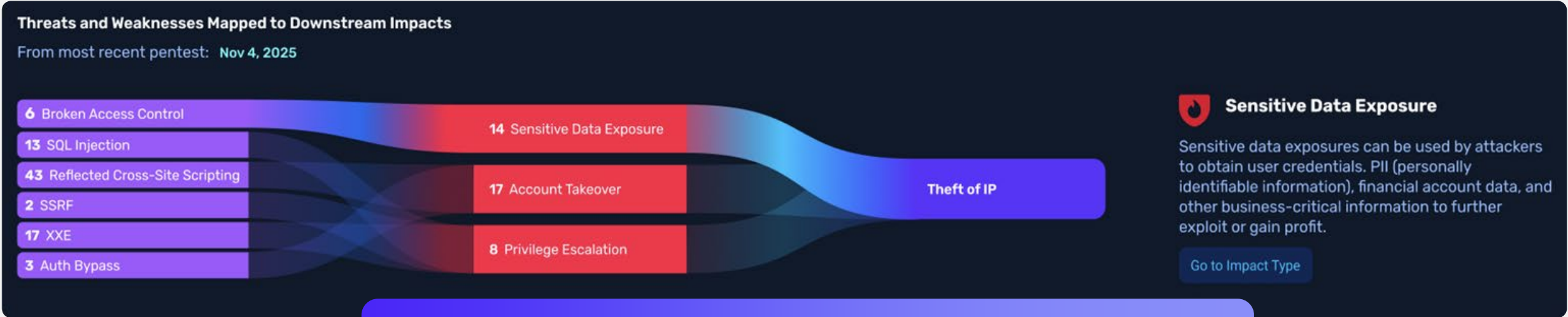
NodeZero is the only AI-Powered platform that autonomously attacks WebApps, Infrastructure, and Identities.

Sample Use Case: Pivot Inside From WebApp





Sample Use Case: Pilfer Sensitive Data



NodeZero WebApp Pentesting Shows Consequence
& Business Risks —not just OWASP Top 10



Sample Use Case: Run At Scale With Perspectives



As a CIO or CISO, establishing the right cadence is crucial

“It’s Pentest Wednesday”...

Did you:

1. Log us?
2. Alert on us?
3. Stop us?
4. Why not?





Our Vision

The only AI-powered platform that autonomously attacks infrastructure, identity, and web apps.

PROACTIVE SECURITY PLATFORM

We built the world's best and most experienced AI hacker, conducting over 250K production-safe tests.

→ PROACTIVE OFFENSE

Autonomous Offensive Security : Attack your environment to real, find exploitable weaknesses before adversaries do.

→ PRECISION DEFENSE

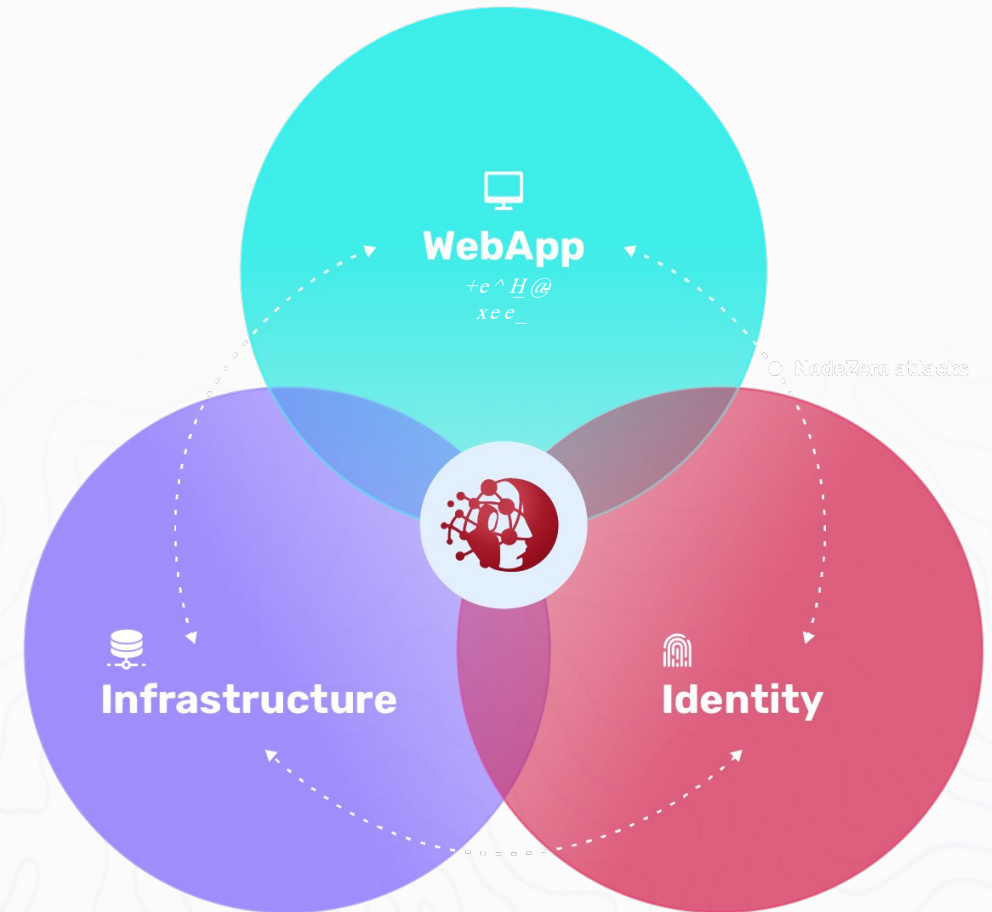
Offense informs Defense : Capture how controls behave, generate tuning recommendations, verify remediation.

→ NODEZERO WEB APP PENTESTING

Check the Front Door : Web app pentesting to map every app route to find real, exploitable vulnerabilities.

→ AGENTIC RED & BLUE TEAMS ^{te 1^ q}

Autonomously take actions based on what NodeZero discovers.





“

The future of cyber warfare will run
at machine speed — algorithm vs.
algorithm — with humans by exception.”



Snehal Antani

CEO and Co-Founder Horizon3

Thank You!

Jens.Egger@horizon3.ai

www.horizon3.ai
www.linkedin.com/company/horizon3ai
x.com/Horizon3ai
youtube.com/@horizon3ai

Schedule a demo

[https://horizon3.ai/contact](https://horizon3.ai/contact-us/schedule-demo/) -
[us/schedule -demo/](https://horizon3.ai/contact-us/schedule-demo/)