
Build an
organization
hackers hate
Proactive security culture in practice


Build an
organization
hackers hate
Proactive security culture in practice

Chris Dale

- CHO, Principal and Co-Founder at River Security
- Principal Instructor at SANS
- Previously CISO

"I show how criminals break in, and help throw them back out."

GCIH Certified Incident Handler
GPEN Certified Penetration Tester
GSLC Security Leadership
GIAC Mobile Device Security Analyst
GDAT Defending Advanced Adversaries

GCTI Cyber Threat Intelligence
GCFA Certified Forensic Analyst
GXIH Experienced Incident Handler
GXPT Experienced Penetration Tester
GSP Security Professional

Era	1980 Identify	1990 Protect	2000 Detect	2010 Respond	2020 Recover
Core Challenges	What do we buy to support business	Viruses, server side attacks, insecure configs	Too many logs and alerts. Client-side attacks	Assume breach, privilege sprawl, lack of best practices	Ransomware, DDOS, wipers
Solutions	Asset management, system management tools	Antivirus, firewalls, secure configs	IDS, IPS, SIEM	Incident Response & Tools (EDR, SOAR)	Distributed, Immutable, Ephermal systems
Security Team Composition & Focus	None	Special interest / Vulnerability management	Security operations / Threat management	Dedicated business unit / security department	Large diversity of roles. Security champions, dev/sec/ops, PII responsible, …

Source: dietriad.com & Sounil Yu

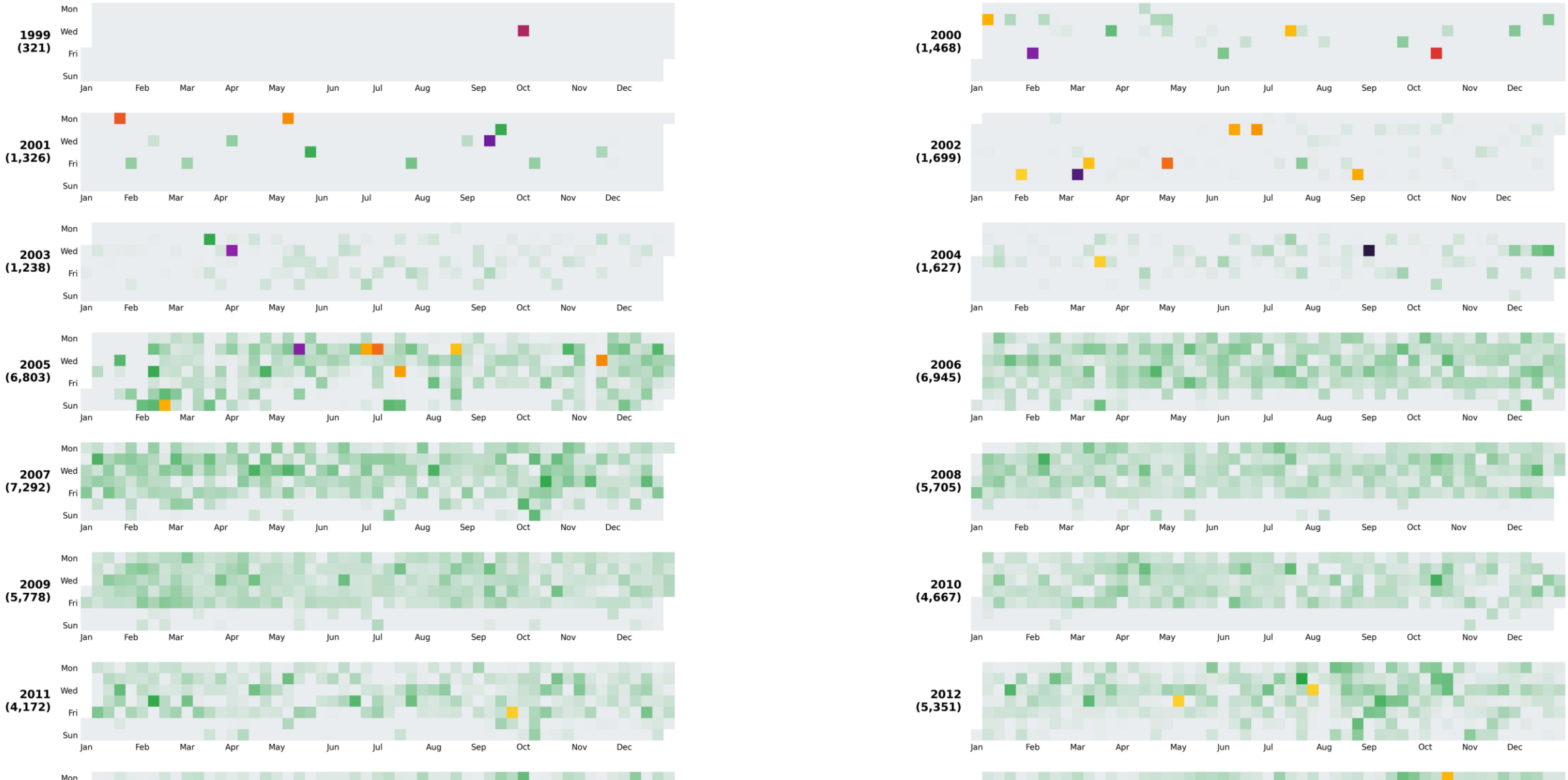

THIS IS
FINE

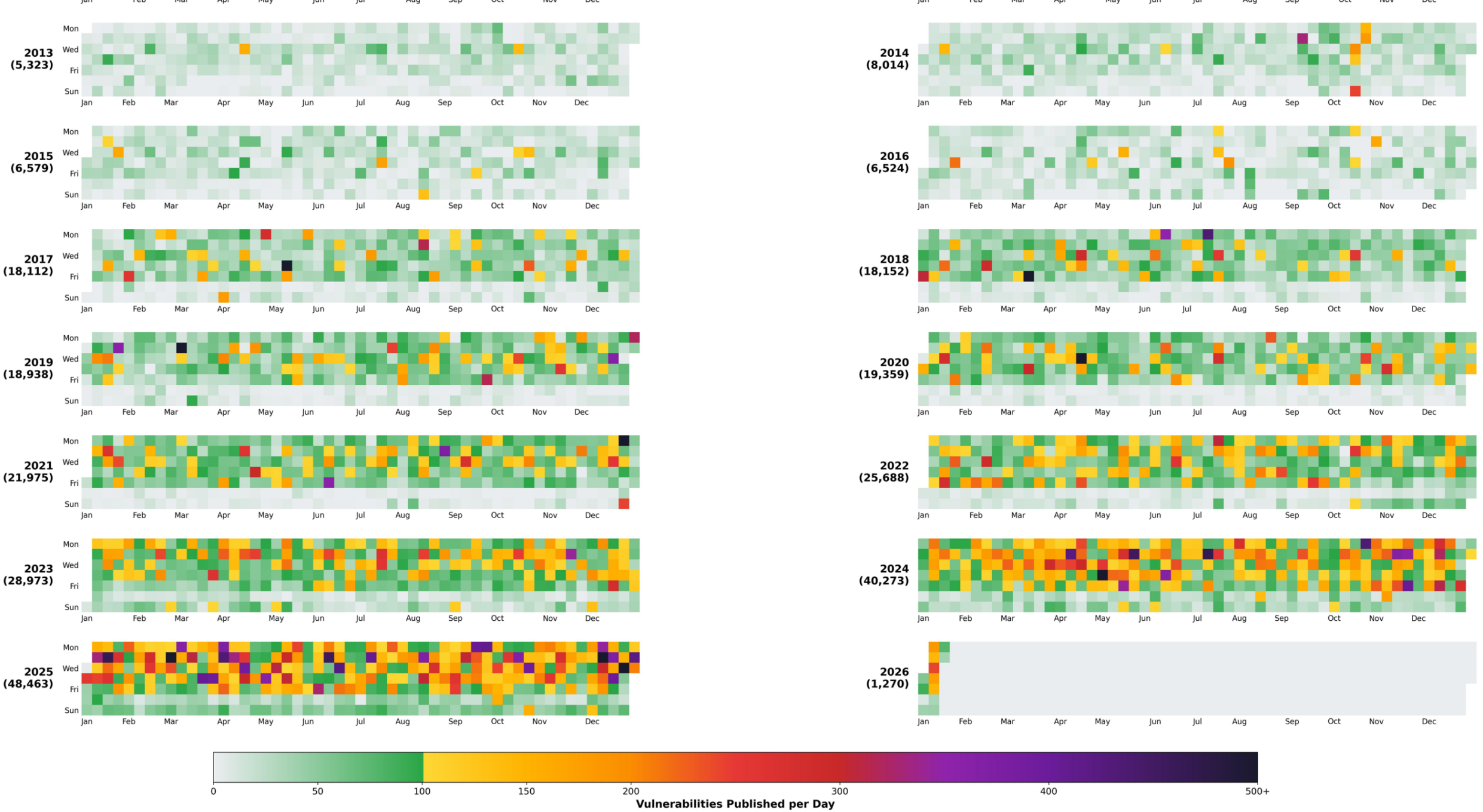
Security in the AI era

	2026 AI
Core Challenges	AI Hacking, eCrime monetization, saturated bug bounty, speed
Solutions	Bugcapolypse, AI assisted defense, attack surface reduction, patch management
Security Team Composition & Focus	Chief AI Officer, AI champions

Vulnerability Publications by Day (1999-2026)

Total: 322,035 vulnerabilities | Peak: 3,123 in a single day

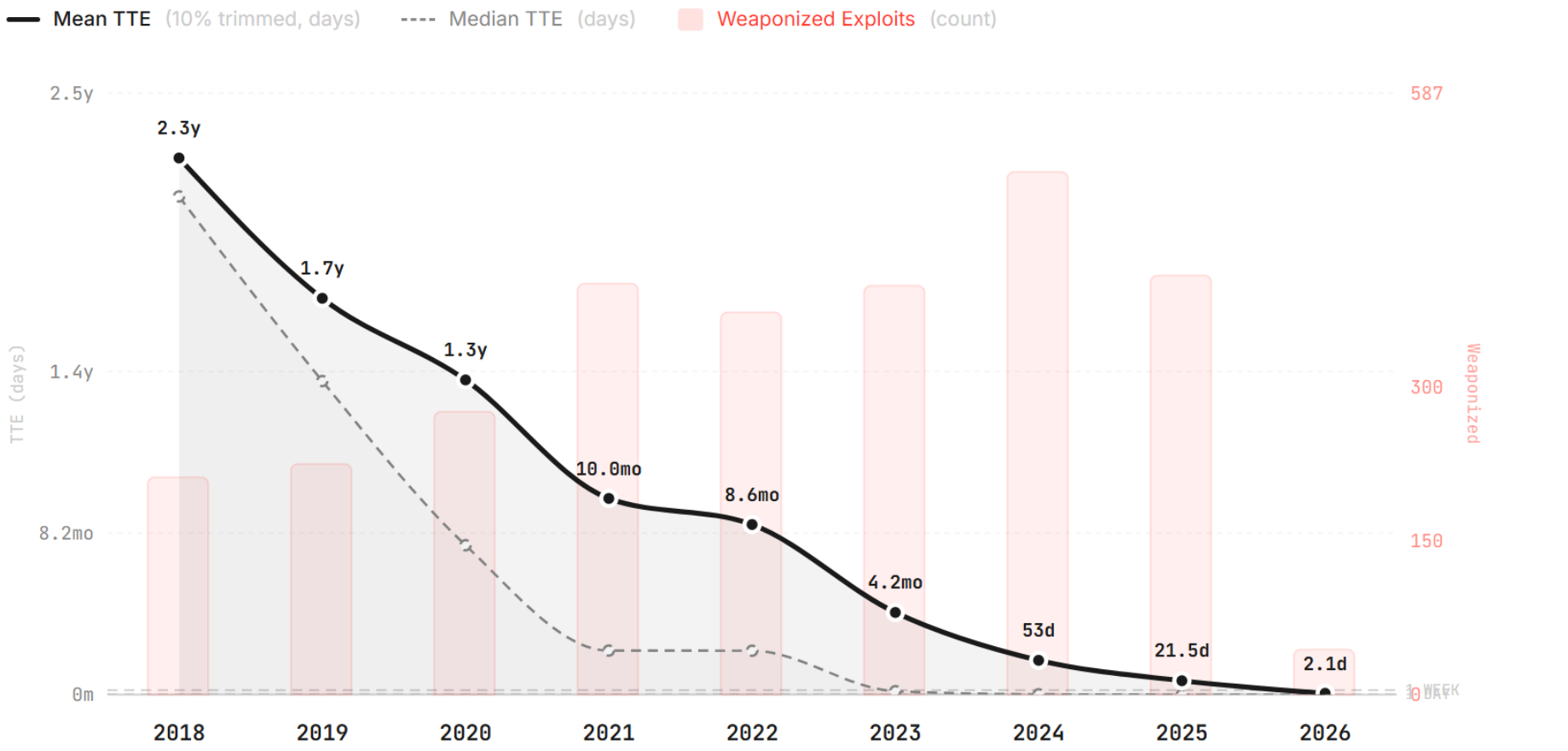




Source: https://www.reddit.com/r/dataisbeautiful/comments/1qbvbs1/oc_cybersecurity_vulnerabilities_discovered_by/

From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.



Based on 3,500+ confirmed-exploited CVEs (CISA KEV + VulnCheck KEV, with VulnCheck XDB timestamps for early-year CVEs) zerodayclock.com

Source: zerodayclock.com

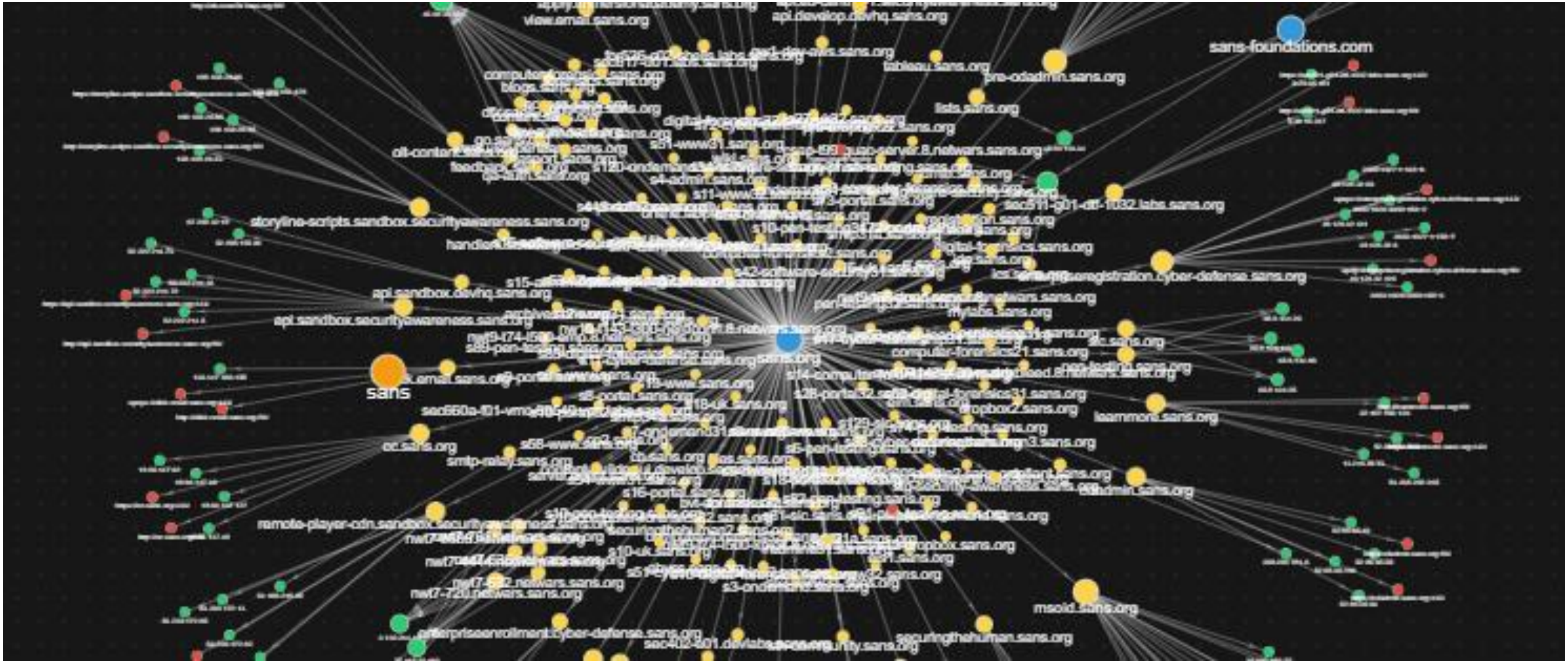
Proactiveness: assume breach, win anyway

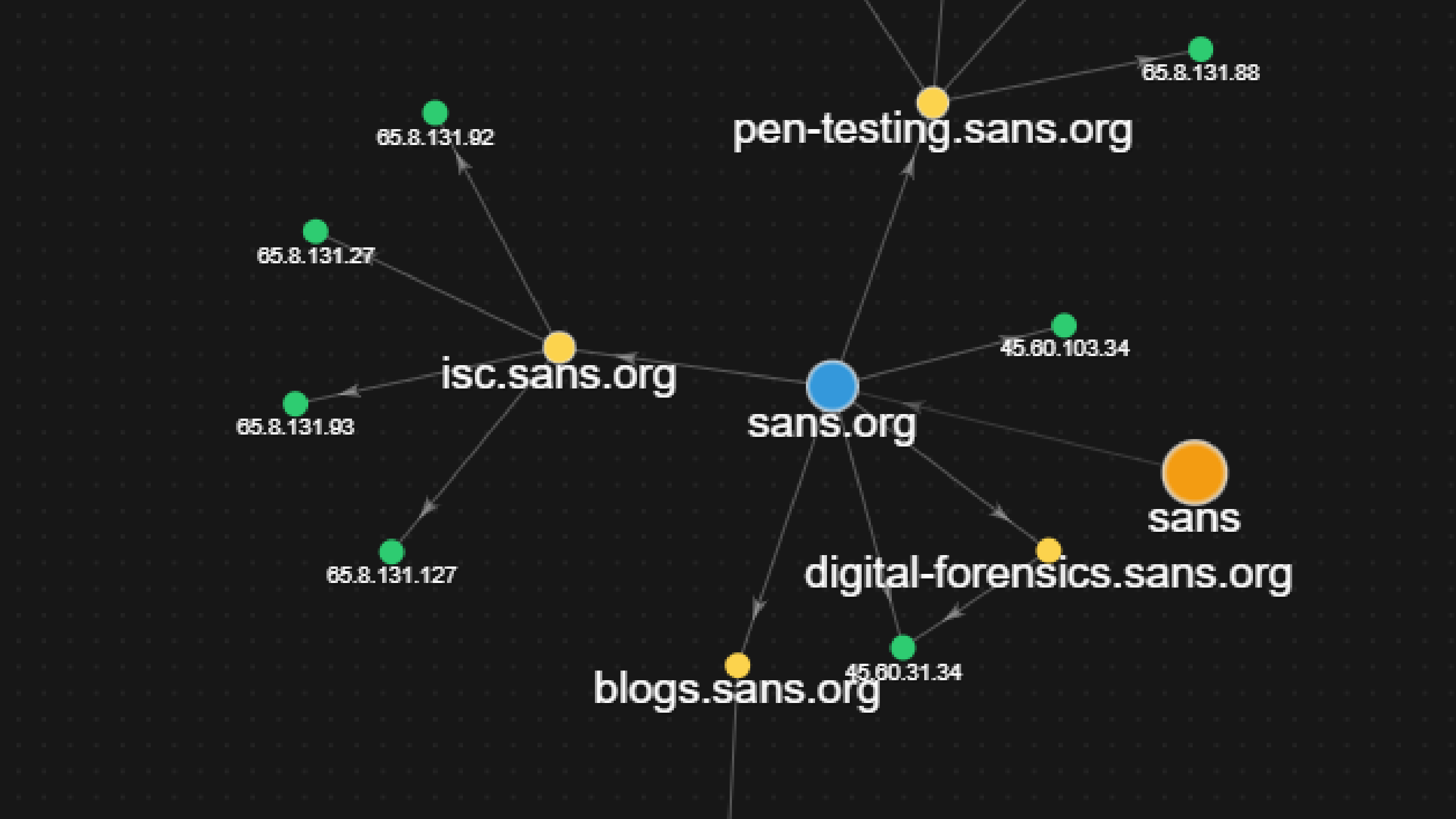
- A mindset and a behaviour
- Hunt for problems before they hunt you
- Act *before* the incident, not after

Assume breach. Hunt for it before it finds you, and engineer so you win anyway.

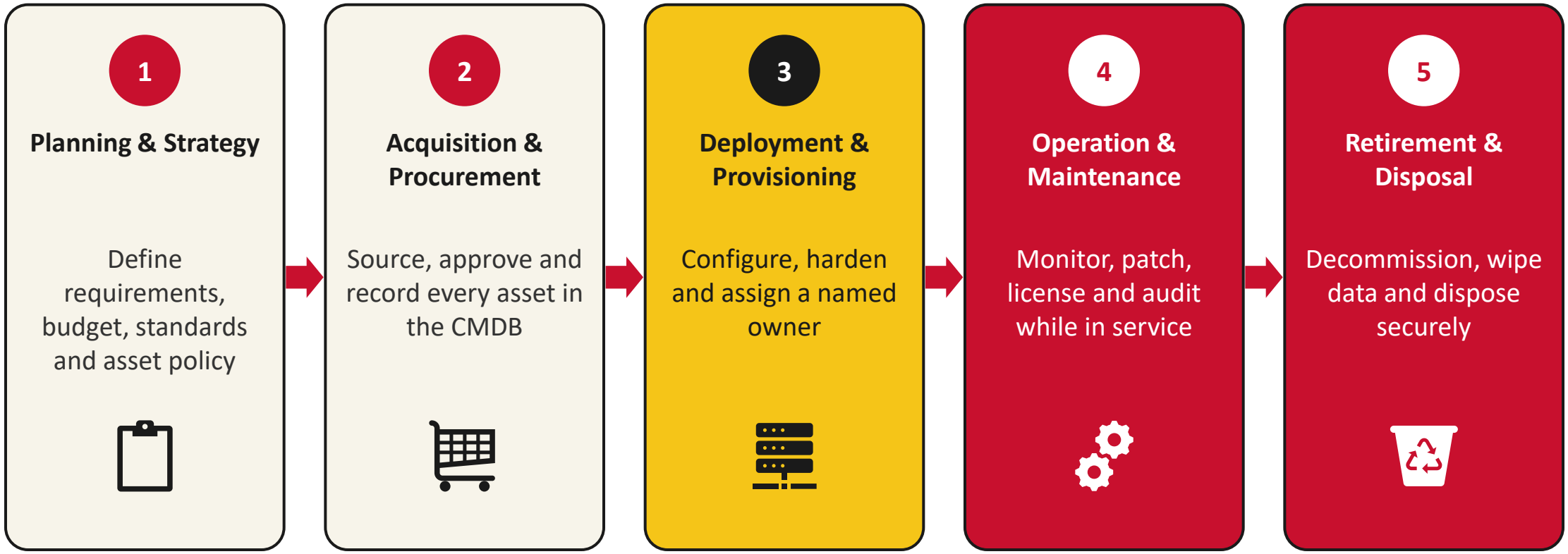
REDUCE YOUR ATTACK SURFACE!

Source: riversecurity.eu/active-focus




65.8.131.88
pen-testing.sans.org
65.8.131.92
65.8.131.27
isc.sans.org
45.60.103.34
65.8.131.93
sans.org
sans
65.8.131.127
digital-forensics.sans.org
45.60.31.34
blogs.sans.org

Asset Mgmt Lifecycle



Servers as Pets

Named Individually

Manually cared for

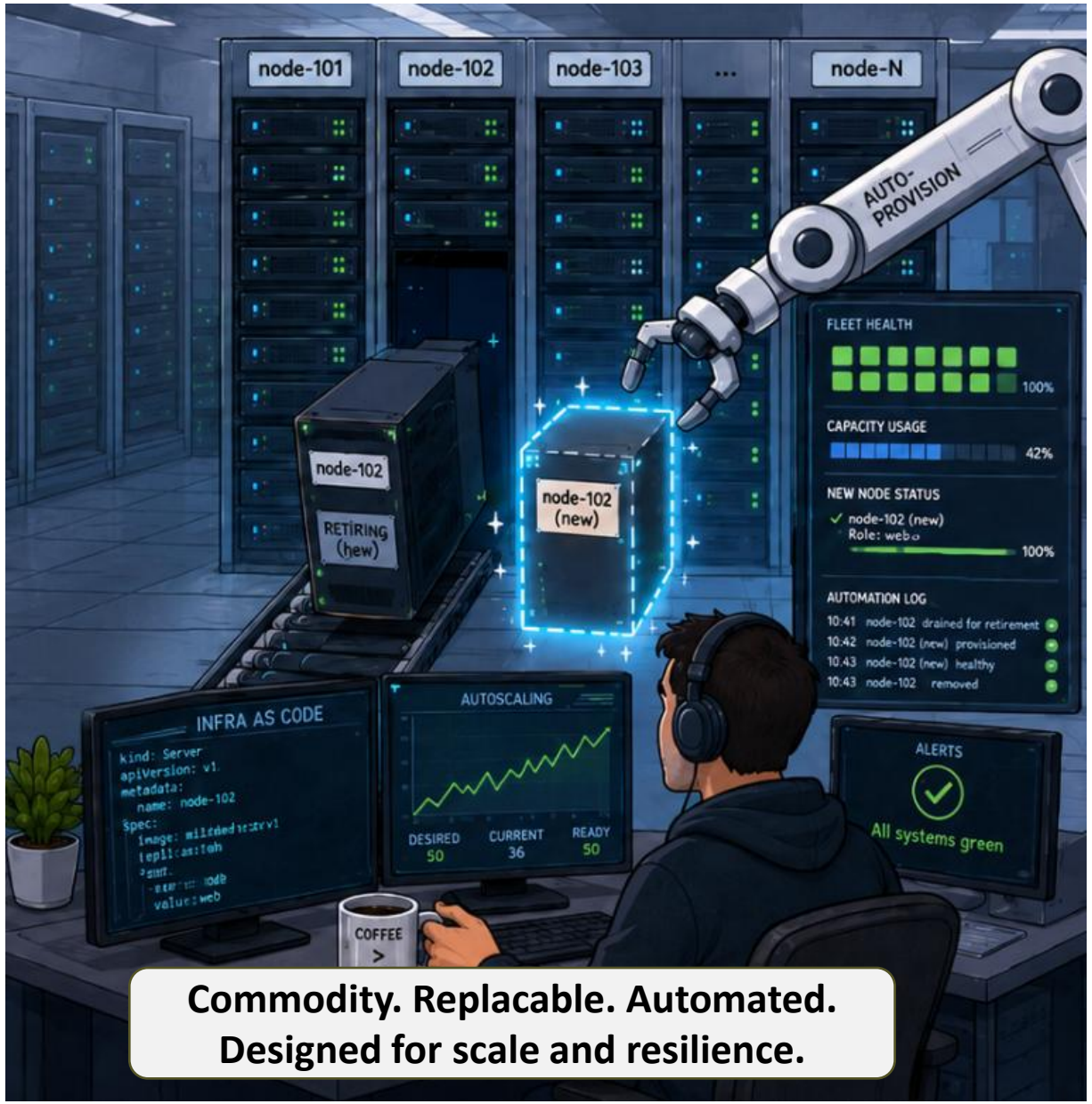
Hard to replace

Special snowflakes

Unique. Loved. Hand-maintained.
Hard (and risky) to replace.

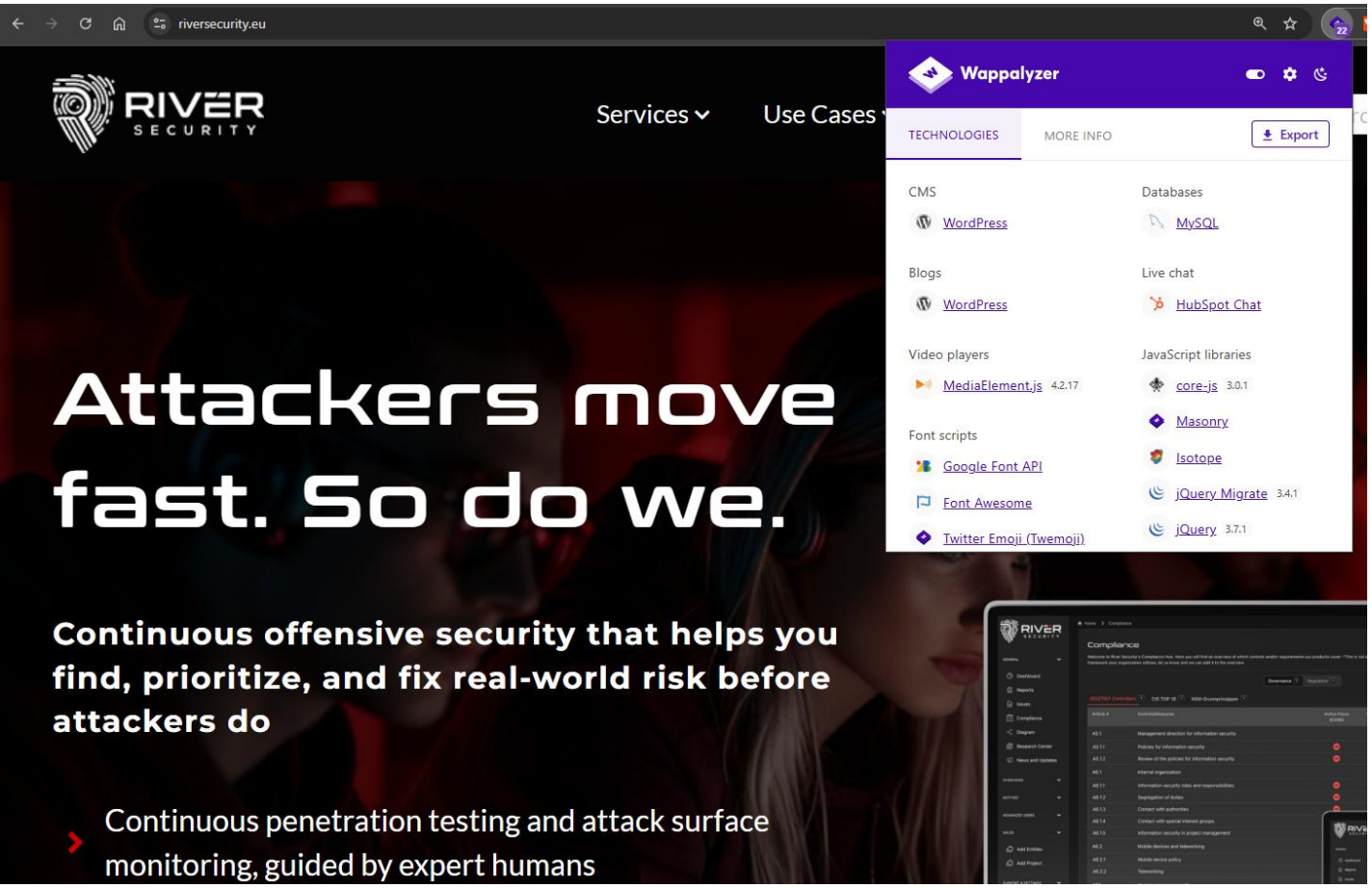
Servers as Cattle

- **Standardized**
- **Automated**
- **Easily replaced**
- **Scale-out fleet**



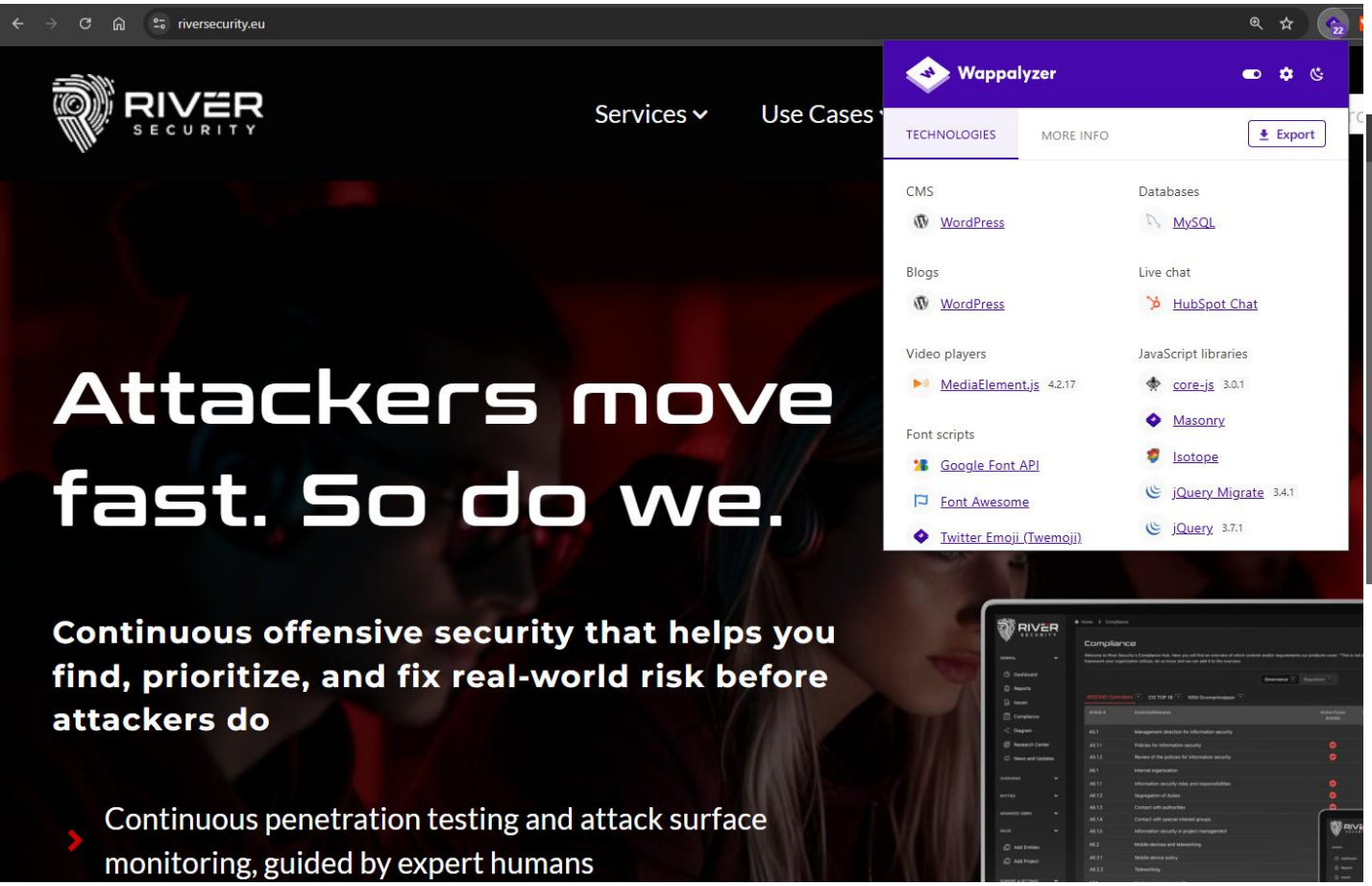
Commodity. Replacable. Automated.
Designed for scale and resilience.

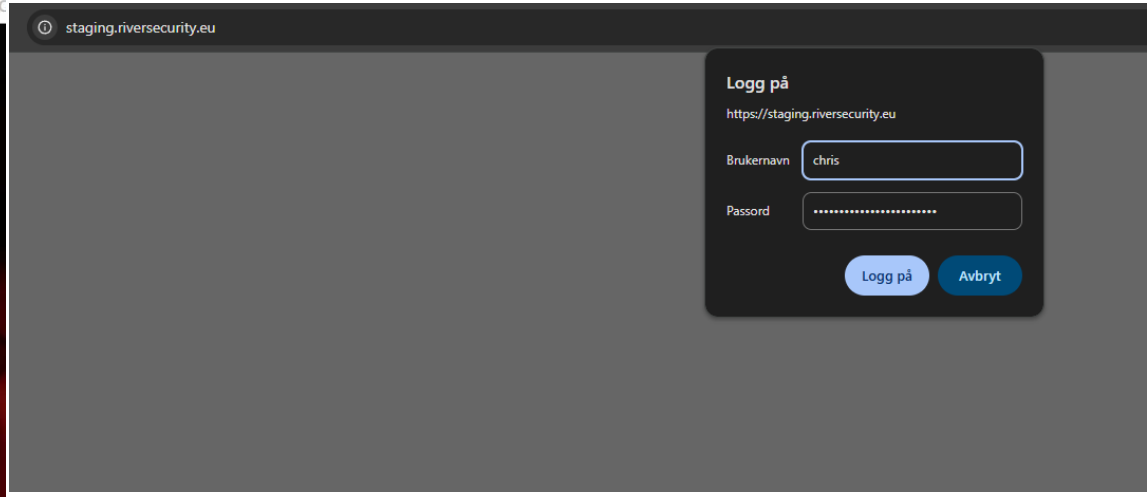
Example: One of the best defenses , is to not have anything to attack



Somebody hacks my frontpage?
Potential critical consequences

Example: One of the best defenses , is to not have anything to attack





Win the game by not playing it!

riversecurity.eu

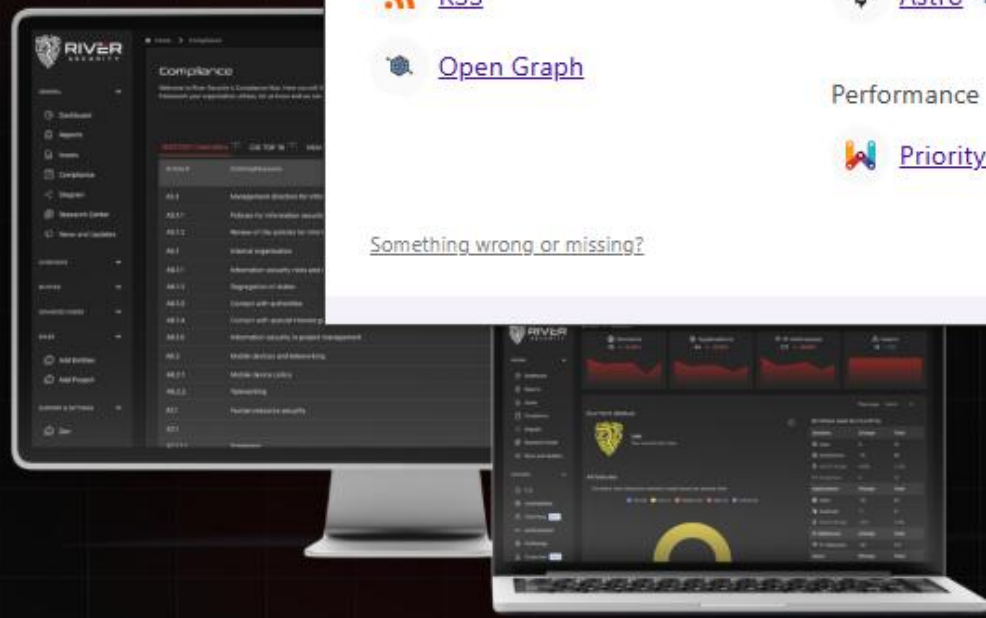
RIVER SECURITY

Services Use Cases About Us

ADVANCED PERSISTENT TESTING

Attackers move fast. We help you move faster.

Continuous, expert-led security testing that finds and validates the risks most likely to affect your business—before attackers do.



Wappalyzer

TECHNOLOGIES MORE INFO

Analytics
Leadfeeder

CDN
Cloudfl

JavaScript frameworks
Astro 7.1.5

Payment proc
Stripe

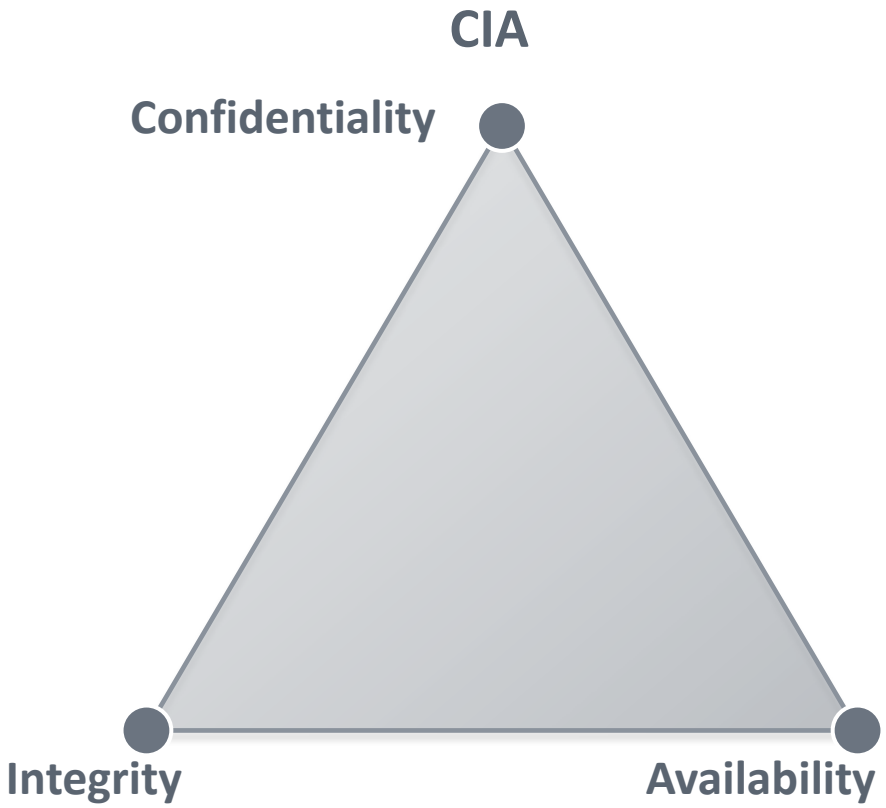
Miscellaneous
RSS
Open Graph

Static site ge
Astro

Performance
Priority

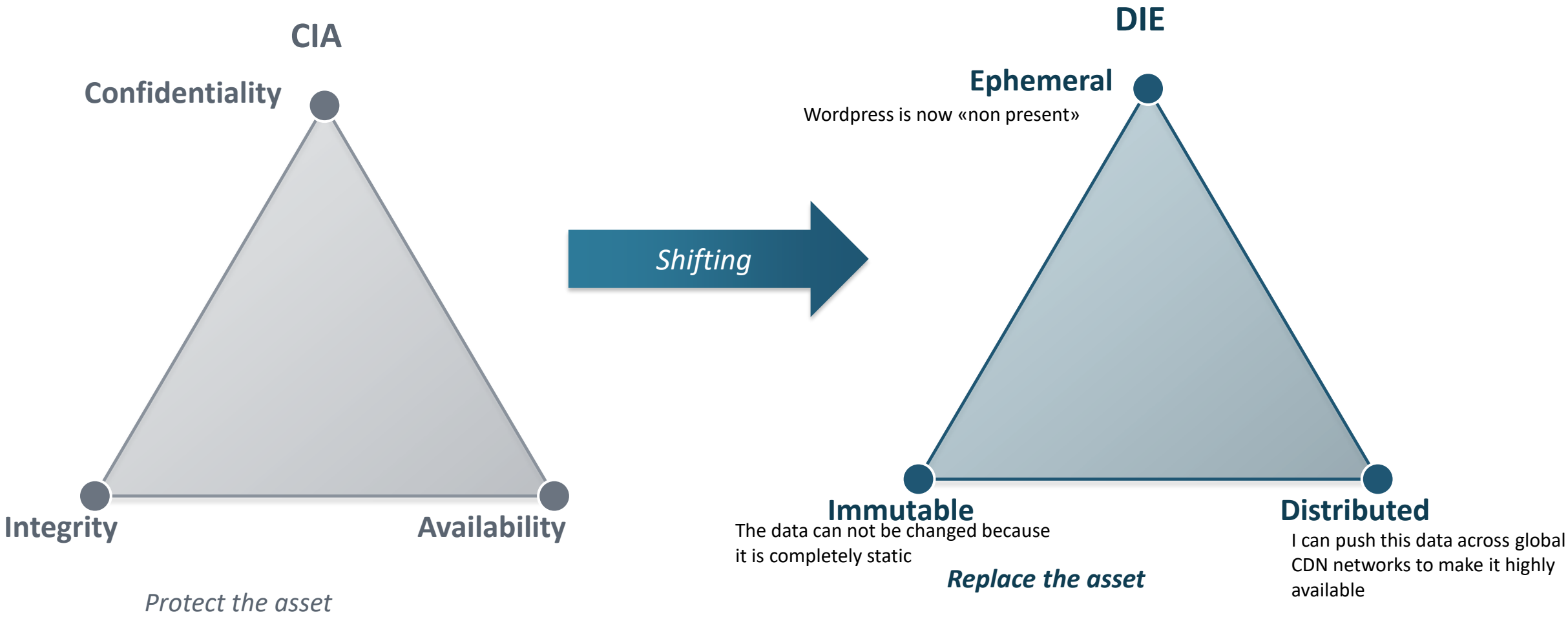
Something wrong or missing?

Proactiveness is a Shift from CIA



Protect the asset

Proactiveness is a Shift from CIA to DIE



Read more: https://dietriad.com/

Home > Overviews > Technology

river security as | Clear Filter

Technology Overview

This dashboard provides an overview of technologies identified across your attack surface.

Technologies are detected through multiple automated artifacts and correlated to assets and entities.

Select a technology to explore where and how it appears in your environment.

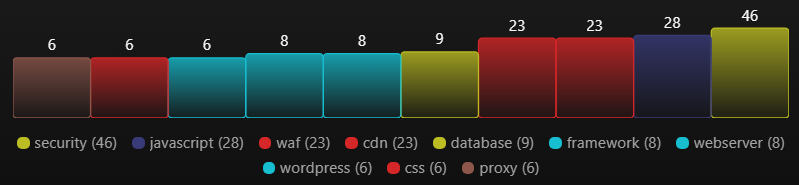
Technologies idenfied

141

mediaelement.js (3)
max mega menu (3)
Show 33 more

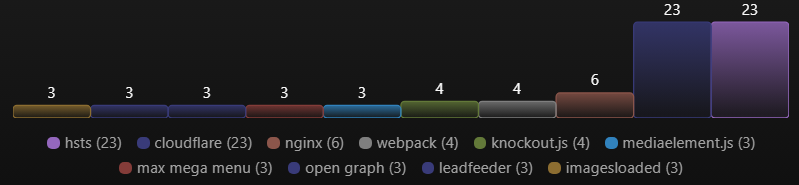
Top10 - Tags

163



Top 10 - Technologies

75



Technologies

187

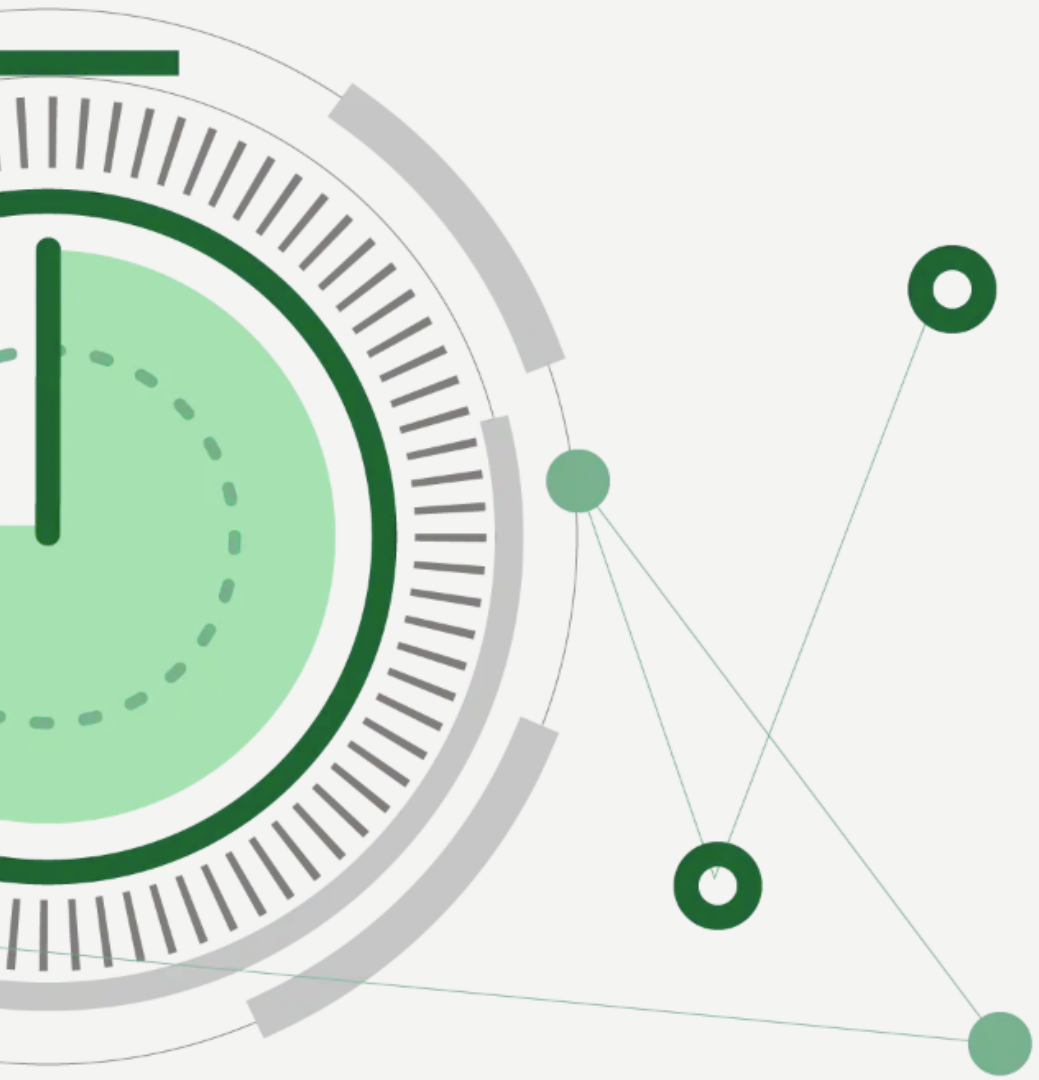
of breaches now start with software vulnerabilities, beating stolen passwords as the top way attackers get in. Hackers are shifting their focus from tricking people to exploiting systems.

of all breaches now involve ransomware, but payouts are shrinking. Even as ransom amounts decrease, businesses are frequently choosing not to pay.

different attack techniques are now being bolstered by generative AI. Threat actors are using AI to work faster at every stage—from spotting security gaps to writing malware.

higher click rates make mobile devices the new favorite target. We've gotten better at spotting phishing emails, so attackers are moving to our pockets. Whether it's a fake text or a scam call, people are often more likely to fall for a mobile threat than a traditional email.

Source: https://www.verizon.com/business/resources/reports/dbir/



Attackers have an unfair advantage

Attackers scan the entire internet for vulnerabilities within 45 minutes. Meanwhile, enterprises take an average of 3+ weeks to find and fix them.

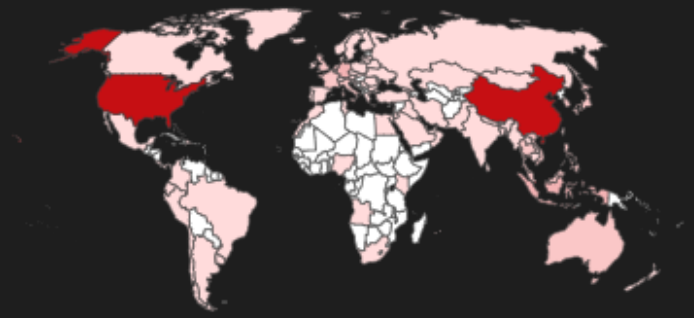
They’re actively looking for weaknesses. Are you?

Watch the webinar →

TOTAL RESULTS

614,650

TOP COUNTRIES



China	398,625
United States	82,429
Singapore	41,686
Hong Kong	13,456
Germany	8,142

More...

View Report | Download Results | Historical Trend

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB.

Bad Request

65.197.215.52
tts-ext.qualcomm.com
vip-mwssweb-xwebprodiis.qualcomm.com
QUALCOMM
United States, Las Vegas

SSL Certificate

Issued By:
|- Common Name:
Sectigo Public Server Authentication CA OV R36
|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
vip-mwssweb-xwebprodiis.qualcomm.com
|- Organization:
QUALCOMM INCORPORATED

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 26 Aug 2026 16:05:40 GMT
Cneonction: close
Content-Length: 334
```

NetScaler AAA

2026 GLOBAL THREAT REPORT

YEAR OF THE EVASIVE ADVERSARY

The average eCrime breakout time fell to **29 minutes** in 2025, a 65% increase in speed from the prior year. The fastest breakout took just **27 seconds**. In one intrusion, data exfiltration began within four minutes of initial access. The window to detect, decide, and respond has narrowed dramatically.

By the Numbers: M-Trends 2026

The metrics in this year's report highlight how adversaries are shifting their approaches to bypass modern security controls:

- **Global Median Dwell Time:** Global median dwell time rose to 14 days from 11 days. This shift likely reflects growing sophistication, particularly in evading defenses. When looking specifically at the high quantity of cyber espionage and North Korean IT worker incidents, the median dwell time for both categories was 122 days.
- **Initial Infection Vectors:** Exploits remained the most common initial infection vector for the sixth consecutive year, accounting for 32% of intrusions. However, highly interactive voice phishing saw a significant surge to 11%, becoming the second-most commonly observed vector.
- **Detection by Source:** Organizations are improving their internal visibility. Across all 2025 investigations, 52% of the time organizations first detected evidence of malicious activity internally, an increase from 43% in 2024.
- **Targeted Industries:** The full scope of incidents affected more than 16 industry verticals, with the high tech sector (17%) outpacing the financial sector (14.6%) as the most frequently targeted industry, shifting the financial sector out of the top spot it held in 2024 and 2023.

Source: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026

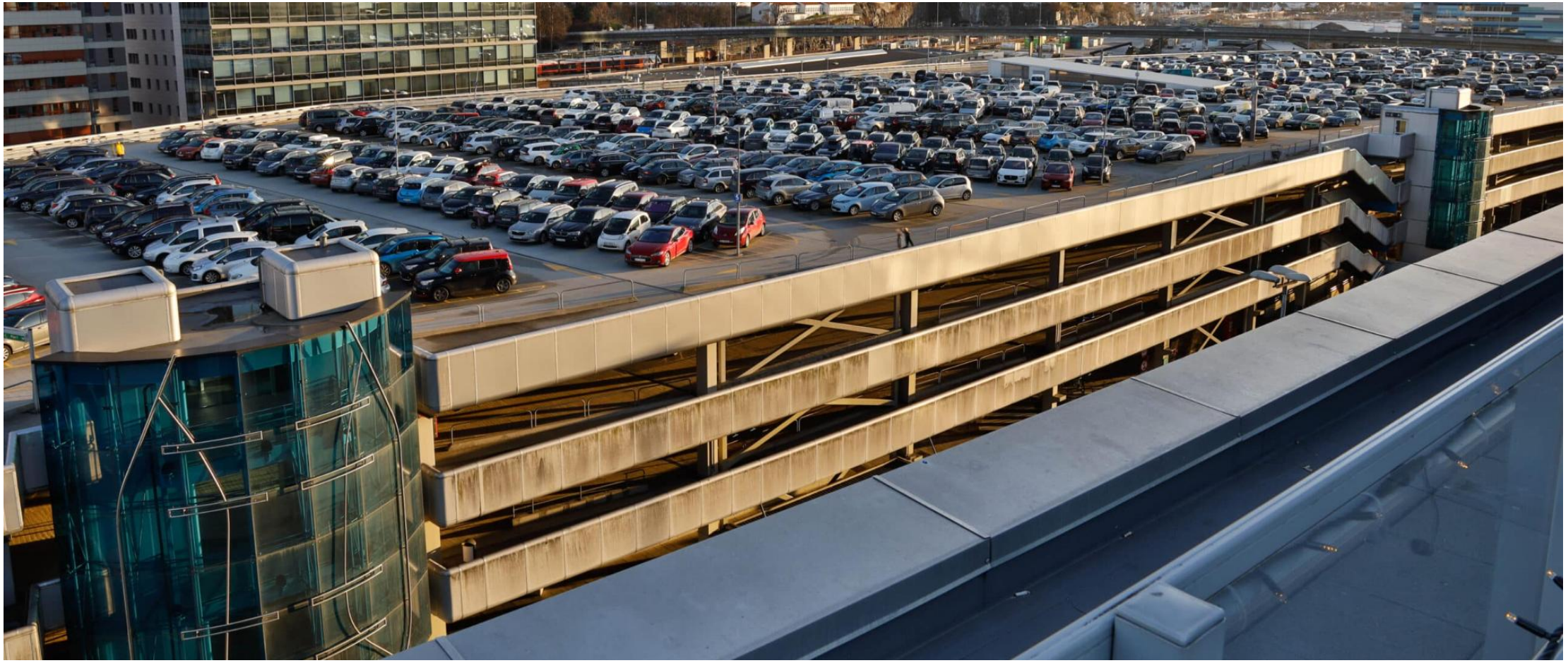
Defenders

VS

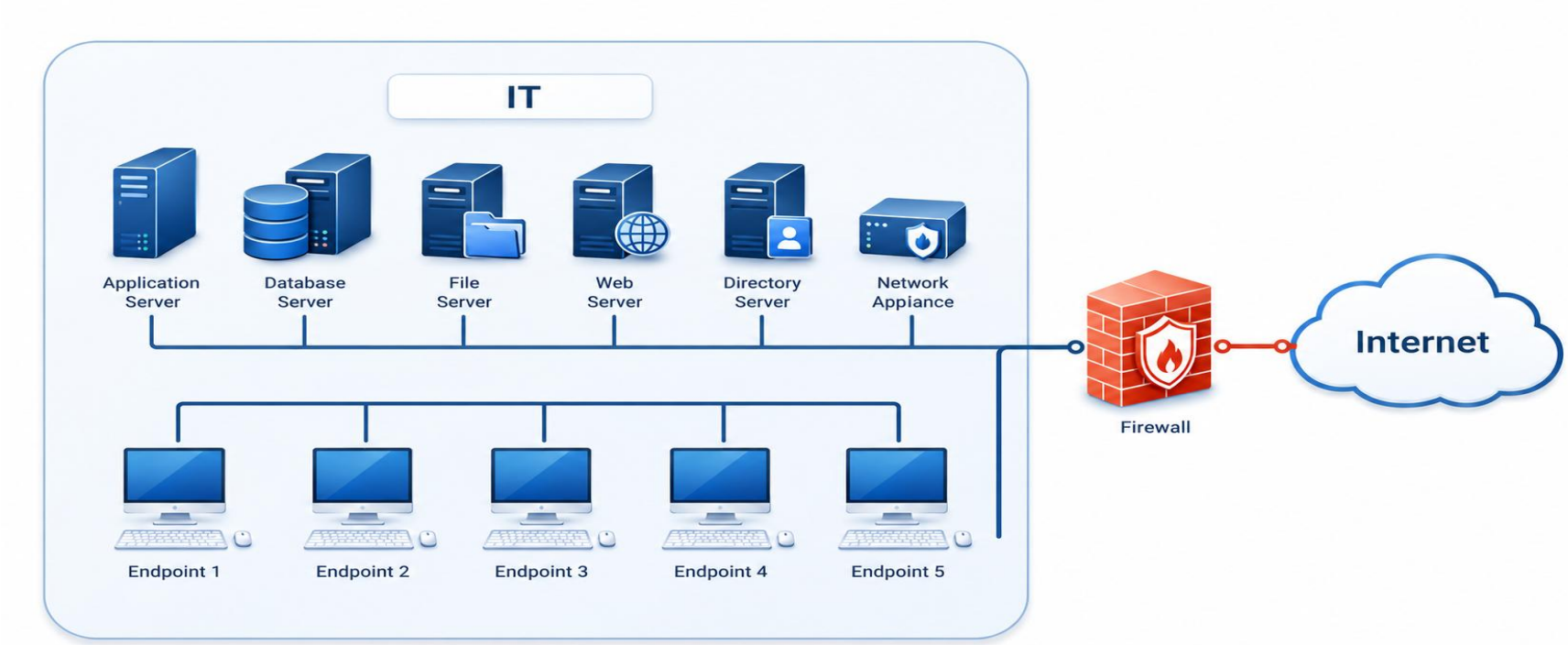
Attackers

Defender architecture

Make it harder for attackers

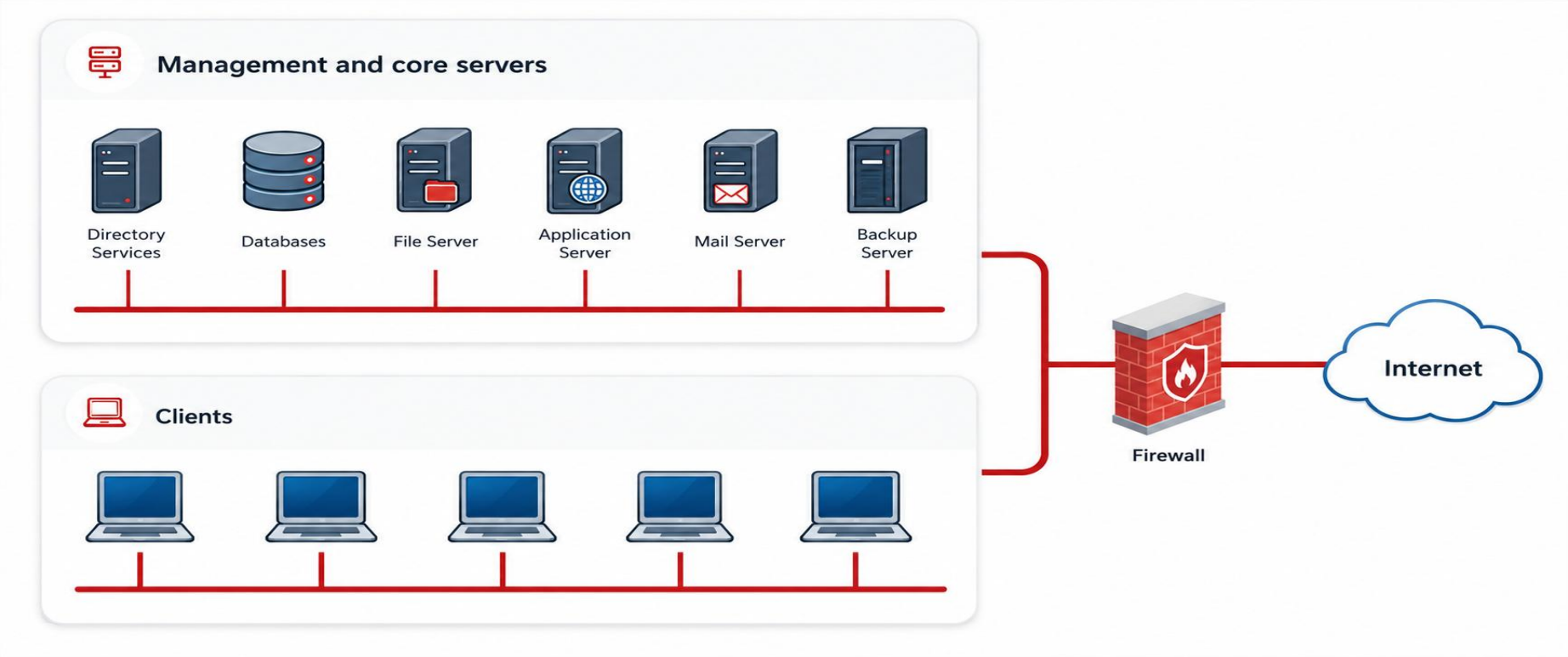


Network architecture: sad, but common



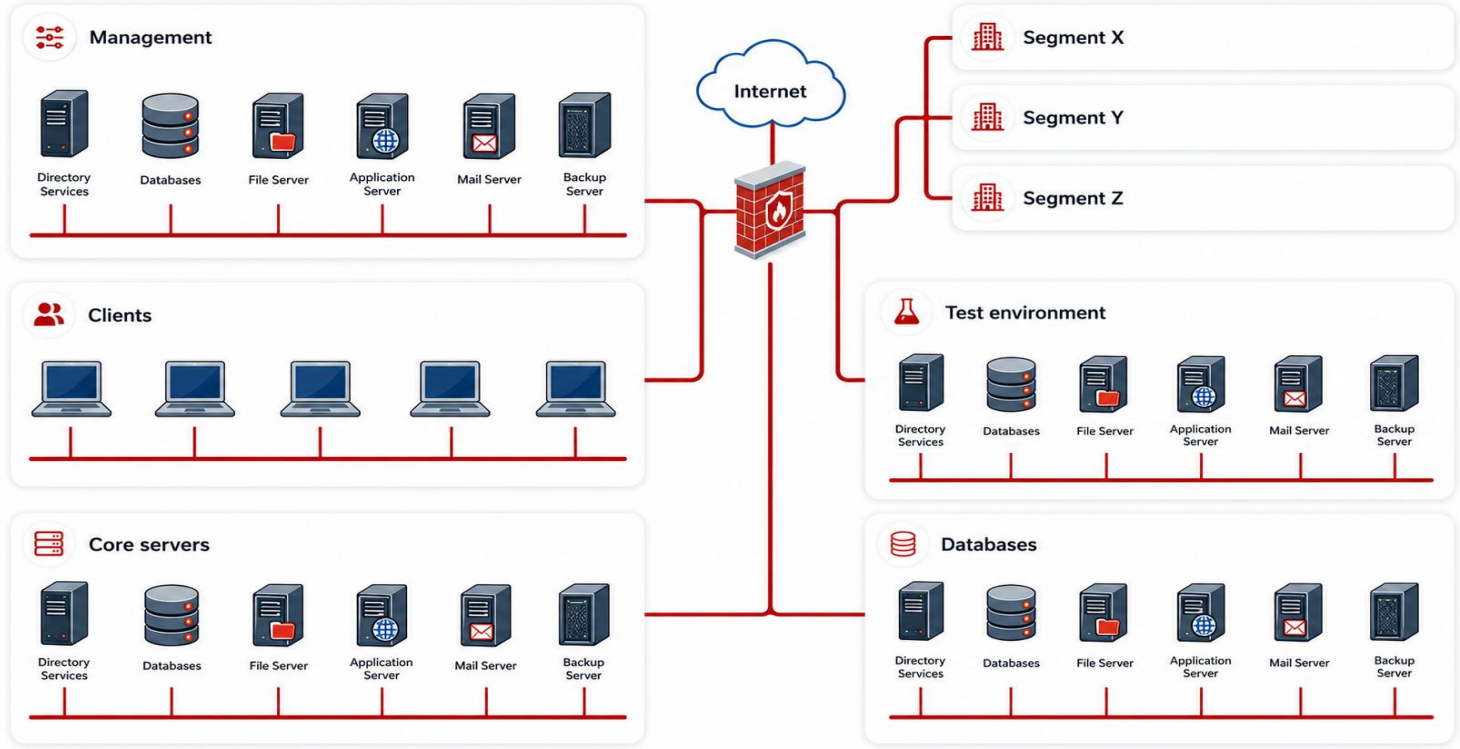
Flat network. IT, users, and the internet share one trust zone. One phish away from full compromise.

Network architecture: also quite common



Two zones, one firewall. Inside each segment everything still trusts everything. Lateral movement is trivial.

Architecture: closer to where we need to be



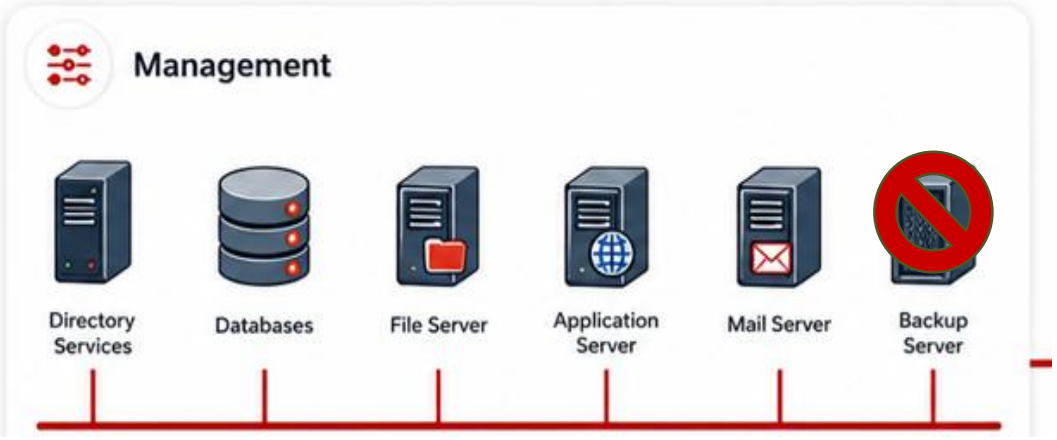
Segmented by function and blast radius. One compromised host is one segment, not the whole estate.

Backups and Data

- **Plan for the worst**
  Assume breach; rehearse the recovery, not just the response.

- **Back up off-site and offline**
  Air-gapped, immutable copies are what survive ransomware.

- **Delete or isolate stale data**
  What's not on the network can't be stolen, archive or remove what you don't need.



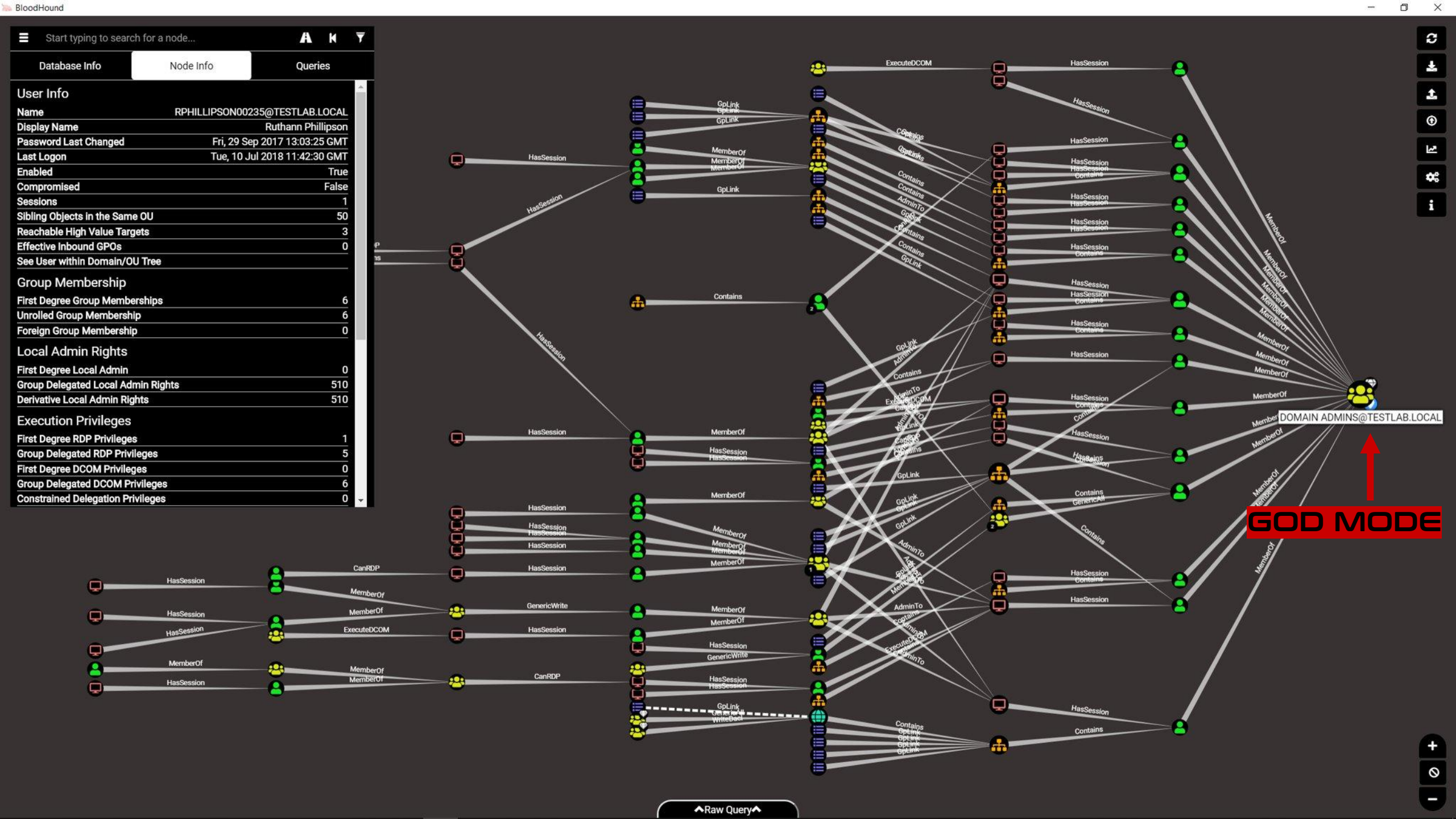
AN ORGANIZATION ATTACKERS HATE...

The one with POLP...?

Principle of Least Privileges

In River Security there are two admins for Azure AD,
and it is neither the CTO nor the CHO (me) main accounts.

Hacker with admin vs not


BloodHound
Start typing to search for a node...
Database Info
Node Info
Queries
User Info
Name RPHILLIPSON00235@TESTLAB.LOCAL
Display Name Ruthann Phillipson
Password Last Changed Fri, 29 Sep 2017 13:03:25 GMT
Last Logon Tue, 10 Jul 2018 11:42:30 GMT
Enabled True
Compromised False
Sessions 1
Sibling Objects in the Same OU 50
Reachable High Value Targets 3
Effective Inbound GPOs 0
See User within Domain/OU Tree
Group Membership
First Degree Group Memberships 6
Unrolled Group Membership 6
Foreign Group Membership 0
Local Admin Rights
First Degree Local Admin 0
Group Delegated Local Admin Rights 510
Derivative Local Admin Rights 510
Execution Privileges
First Degree RDP Privileges 1
Group Delegated RDP Privileges 5
First Degree DCOM Privileges 0
Group Delegated DCOM Privileges 6
Constrained Delegation Privileges 0
DOMAIN ADMINS@TESTLAB.LOCAL
GOD MODE
Raw Query

The 1-10-60 Rule

1 MINUTE

DETECT

Spot the alert

10 MINUTES

INVESTIGATE

Triage and understand

60 MINUTES

REMEDIATE

Contain and recover

Great Detection is Hard

Detection signal is often low-fidelity, which leads to...

- False positives drown out real signal
- Saturated SOC analysts - alerts are ignored
- Blindspots in coverage that attackers exploit

What if we could turn the tables on the attackers?

Taking Back The Advantage

Attackers need to be lucky once. Defenders need to be lucky every time.

Flip the tables on the attacker!

1

Attacker breaks in

Or the attacker is already on the inside as a trusted insider.

2

Reconnaissance commences

Attacker looks for ways towards god mode

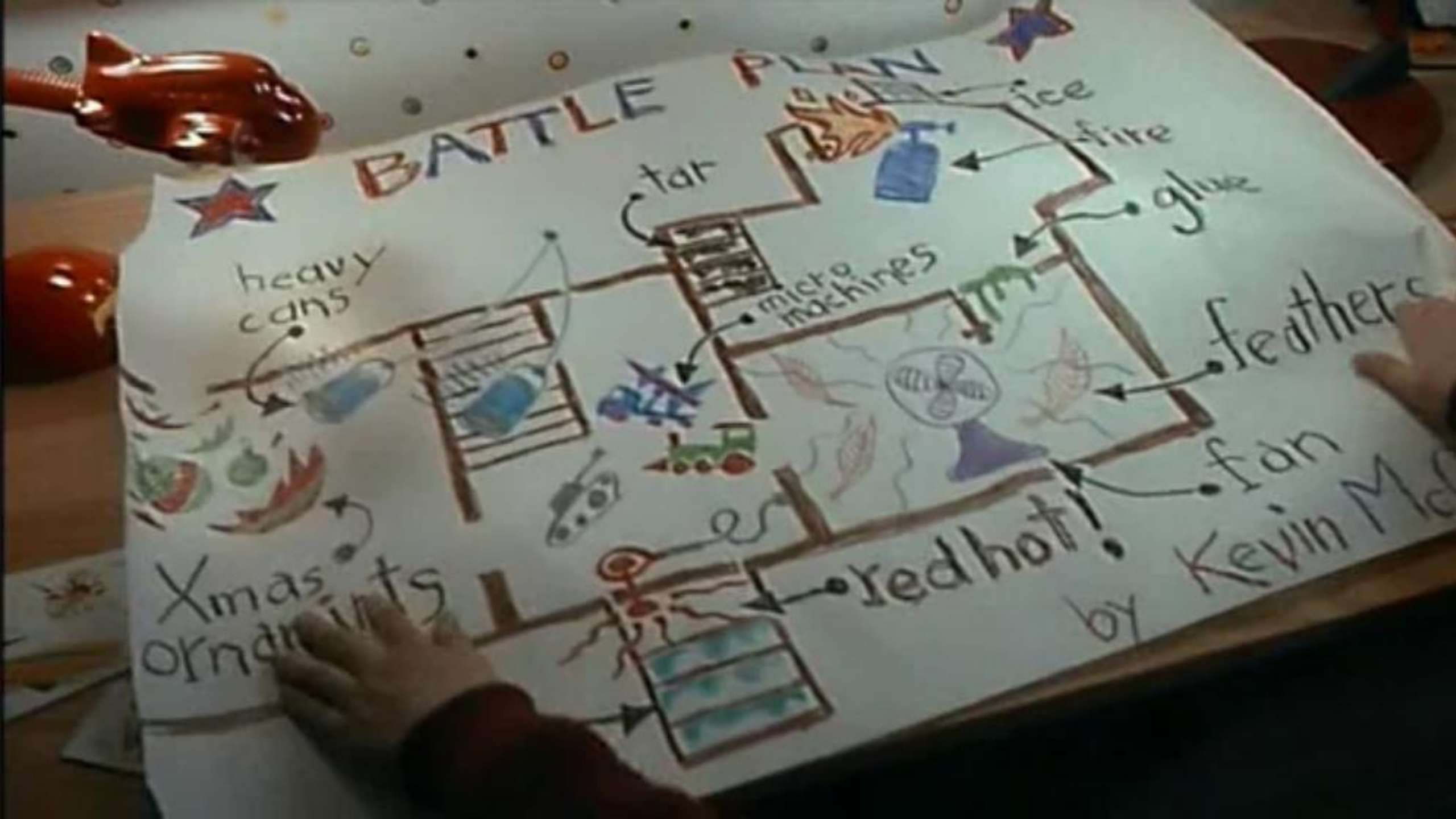
3

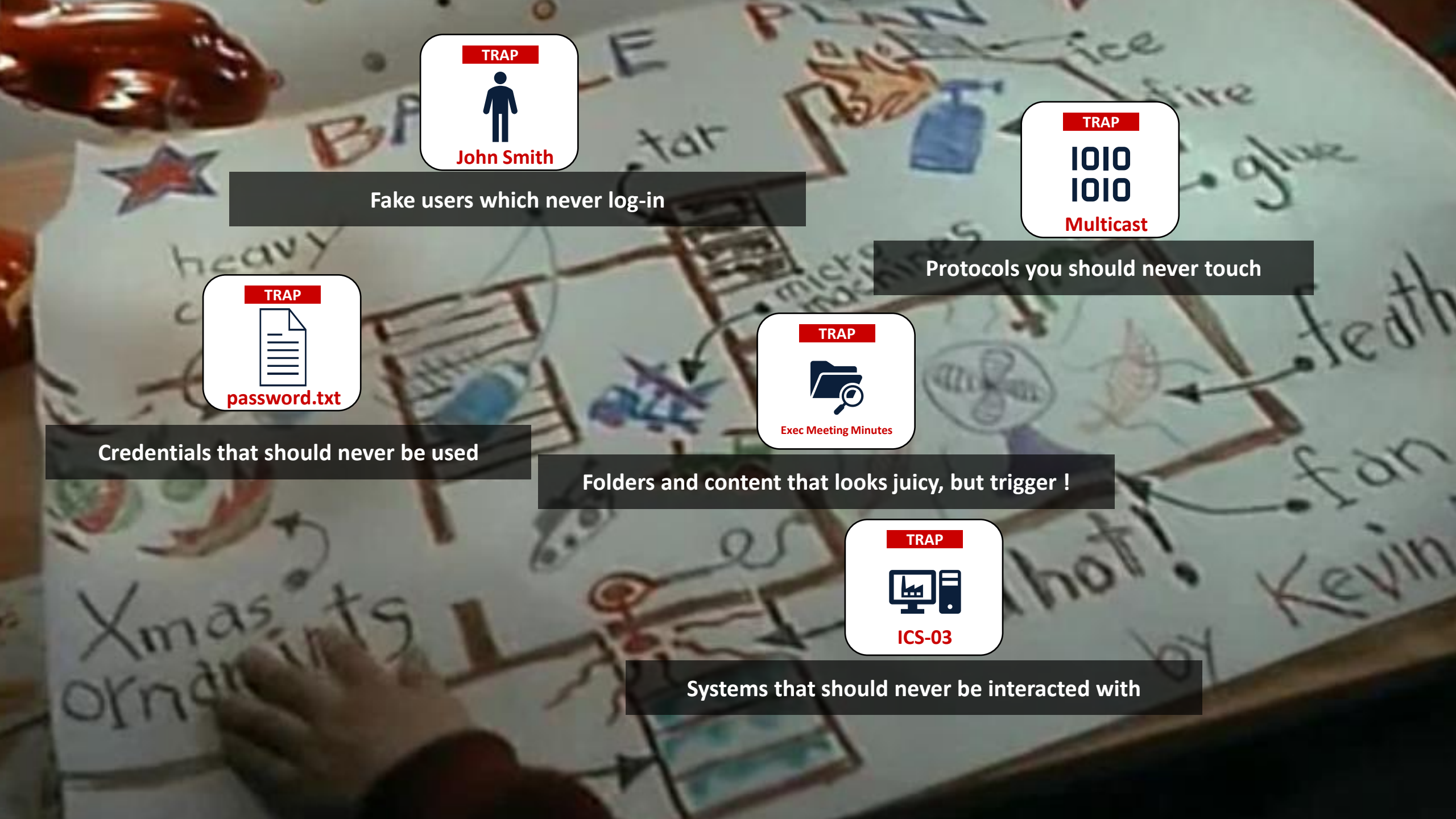
The bait is taken

The attacker is instantly revealed.

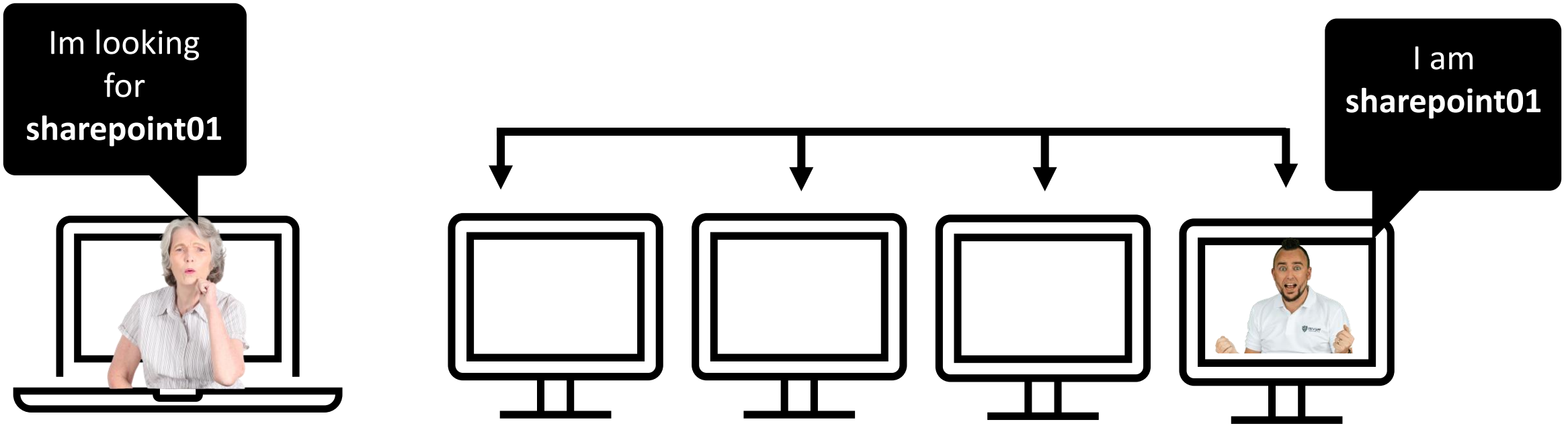
Each trigger is a high-fidelity alert, signal without noise.


This is my house. I have to defend it.


BATTLE PLAN
ice
fire
tar
glue
heavy cans
micro machines
feathers
fan
redhot!
Xmas ornaments
by Kevin M


TRAP
John Smith
Fake users which never log-in
TRAP
1010
1010
Multicast
Protocols you should never touch
TRAP
password.txt
Credentials that should never be used
TRAP
Exec Meeting Minutes
Folders and content that looks juicy, but trigger !
TRAP
ICS-03
Systems that should never be interacted with

Example: Tricking Attackers



LLMNR is a protocol enabled when DNS doesn't have answers

Fighting Agentic AI

Source: https://tracebit.com/blog/context-bombs-stopping-ai-attackers-in-their-tracks

Success rates in simulated tests

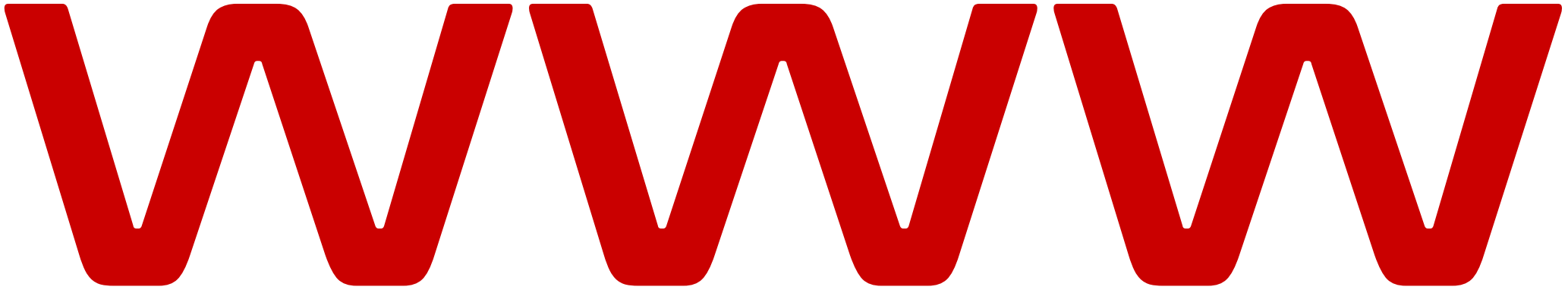
57% → 5%

Chance of an AI agent gaining full administrator access once context bombs are planted

93% → 0%

Top-tier models such as Opus 4.8 saw their success rate collapse to zero

Employees understand the internet



Everyone on the internet is out to get you!

WE'RE JUST A "PING" AWAY

Hackers
Criminals
Governments
Fraudsters

Cheaters
Murderers
Mafia
Sex-offenders

Drug-lords
Terrorists
Scammers
Trolls

Team River Security @ Hacker Space 2022

Provider in the Continuous Offensive Security Space

- Attack Surface Management
- Continuous Penetration Testing
- And a touch of Incident Response

- 25 employees
- 6 years in business
- 50+ public customer testimonials
- 18+ customer cases

Team River Security @ Hacker Space 2026
Temperature -25 Celsius

Provider in the Continuous Offensive Security Space

- Attack Surface Management
- Continuous Penetration Testing
- And a touch of Incident Response

- 25 employees
- 6 years in business
- 50+ public customer testimonials
- 18+ customer cases

Q & A

Got questions? Let's talk at our booth

Connect with me
linkedin.com/in/chrisad/

Follow River Security
linkedin.com/company/river-security/

Continuous Security
riversecurity.eu

RIVER SECURITY

Thank you!