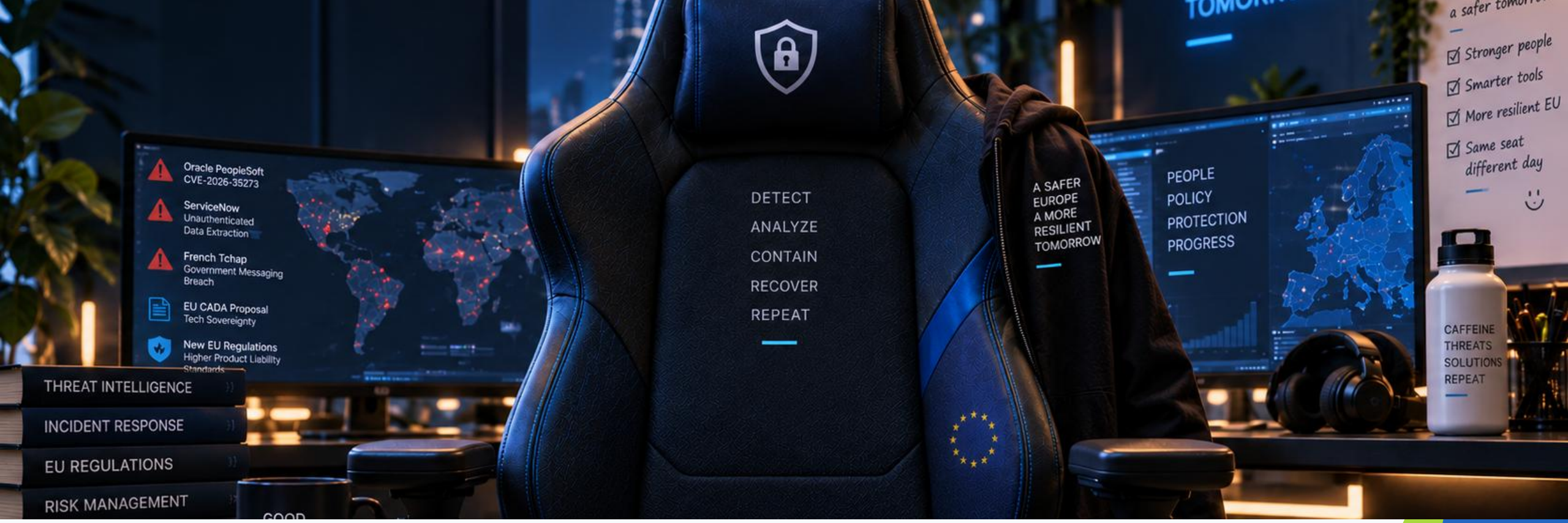


John ILIADIS
IT Infrastructure Director, TEIRESIAS S.A.
Audit Chair, ISC2 Hellenic Chapter

Same Seat, Different Day

Enterprise CyberDefense: a Groundhog Day Cycle

At a glance

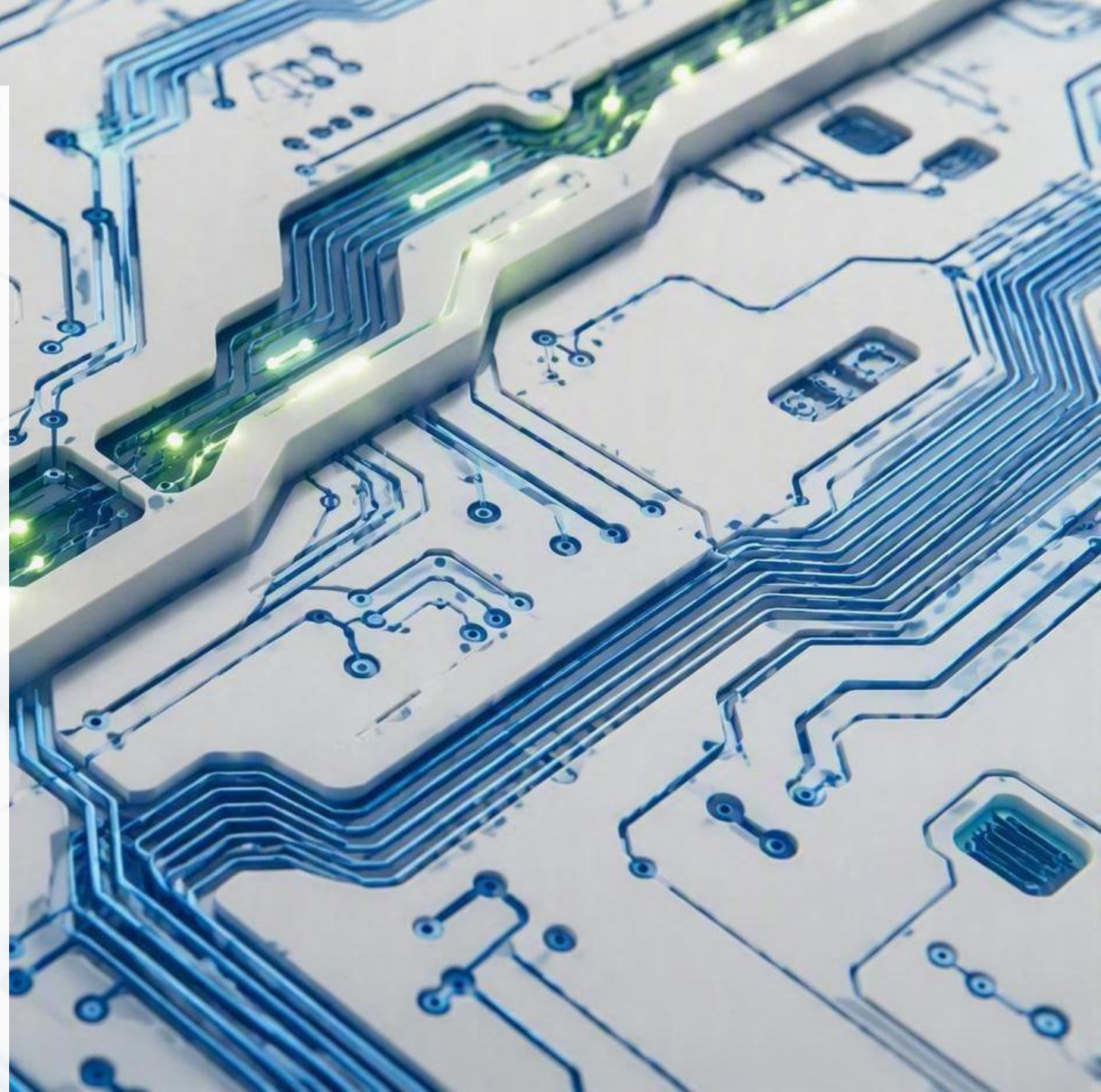
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark

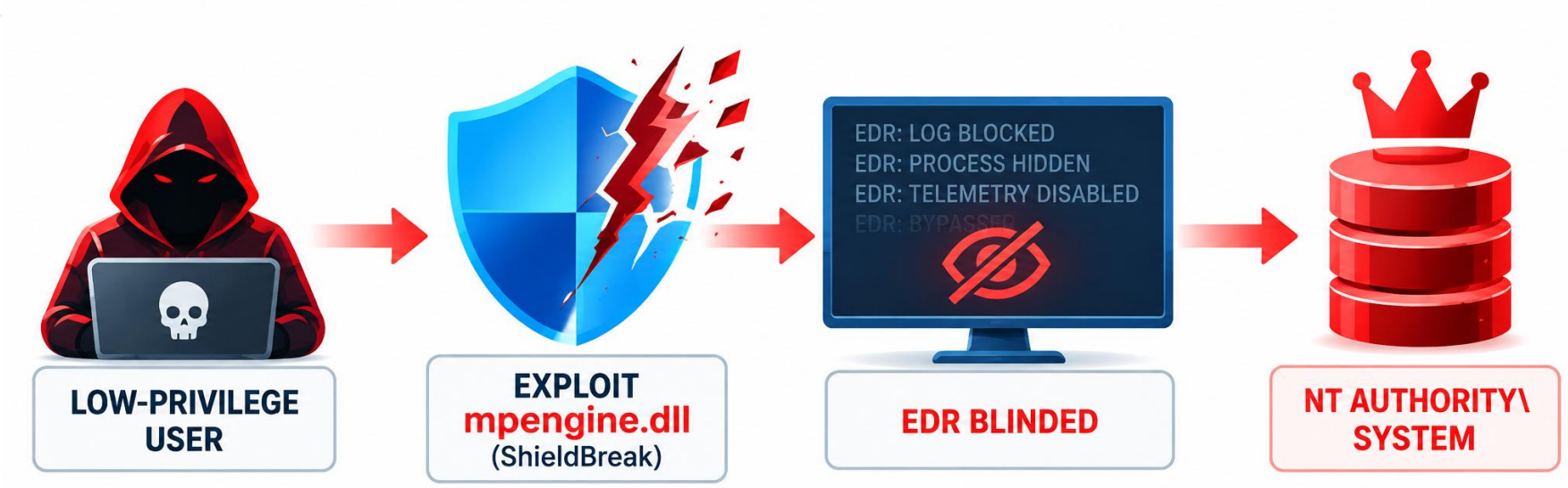


What Groundhog Day?



MONDAY, 10:14AM

Endpoint Controls: Exploited to Blind Us



PILLAR 1

ShieldBreak — CVE-2026-69414

A local elevation-of-privilege flaw in Microsoft Defender's Malware Protection Engine can move a low-privilege attacker to SYSTEM.

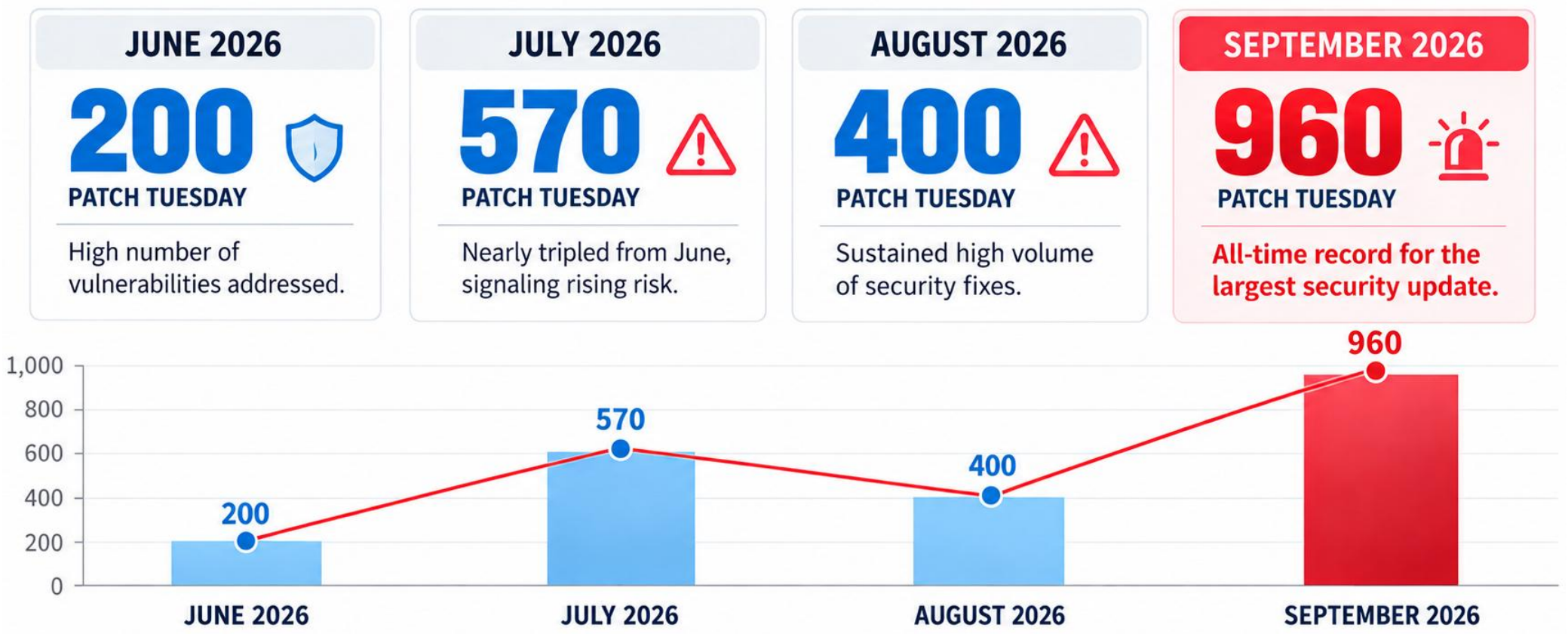
PILLAR 2

Signed-Driver Trust Abuse

GodDamn ransomware used the malicious Microsoft-signed PoisonX driver to disable endpoint defenses. Fox Tempest separately showed how fraudulent signing can industrialize the same trust-chain weakness.

TUESDAY, 09:23PM

Operational Triage is Collapsing Under Historic Volume



Sources: https://www.bleepingcomputer.com/tag/patch-tuesday/

WEDNESDAY, 4:11pm

Perimeter Nullified When Suppliers Failed

01 THIRD-PARTY HR SaaS

TinyPulse / Nintendo of America

Attackers compromised TinyPulse, the employee-survey service used inside Nintendo of America. Survey content compromised.

02 FULFILLMENT PARTNER

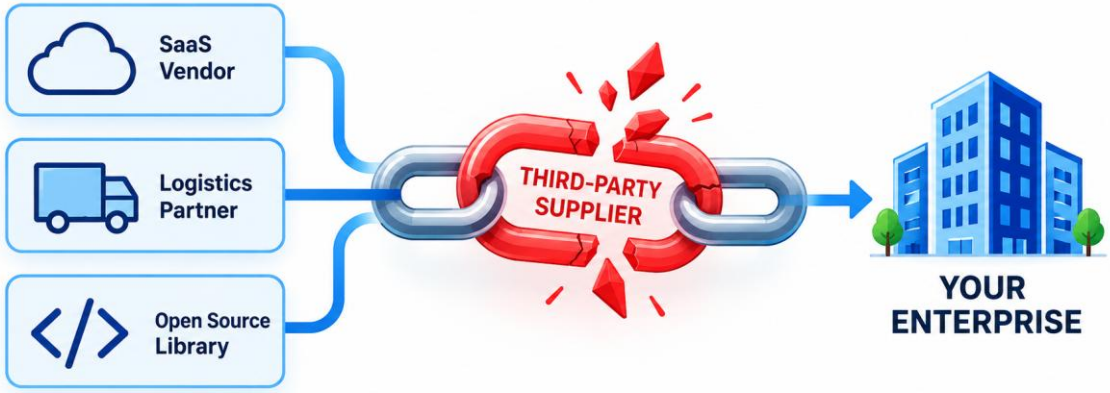
CEVA Logistics Cascade

A cyber intrusion disrupted contract-logistics operations across eight European warehouses. Delivery data flowed outward to downstream customers.

03 OPEN-SOURCE DEPENDENCY

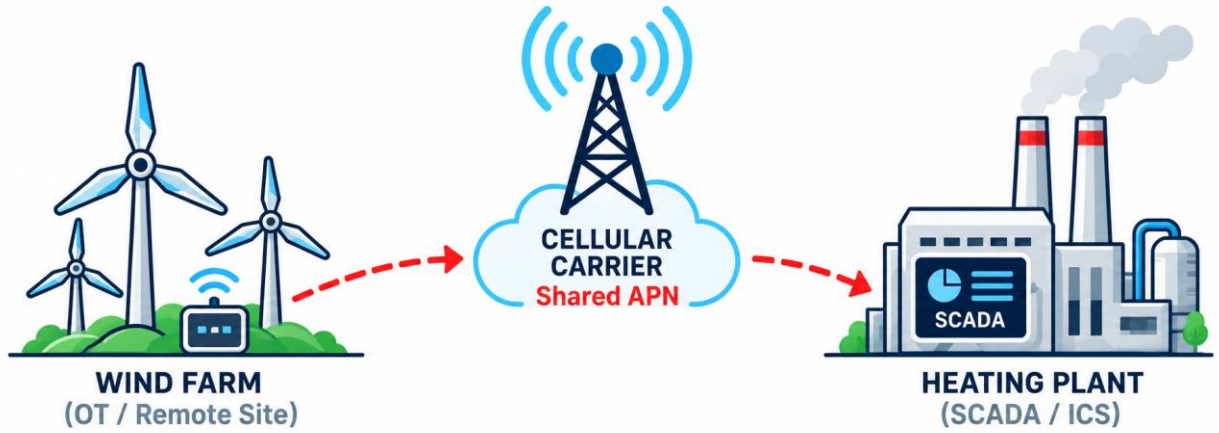
ChainDrop npm Poisoning

A compromised maintainer token pushed malicious code into Keyv and Cacheable; legitimate release workflows published it with valid provenance. A credential stealer harvested various secrets.



THURSDAY, 04:42PM

Bypassing Firewalls via Shared APNs



ZONE A / DISTRIBUTED ENERGY + CARRIER TRANSPORT

INITIAL FOOTHOLD

Wind-farm network

Compromised remote environment

TRUSTED TRANSPORT

Private APN

Client-to-client traffic allowed

M2M PIVOT

NO ISOLATION

PERIMETER FIREWALL

BYPASSED

ZONE B / CHP INDUSTRIAL CONTROL

OT ENTRY

WAGO controller

Reachable through shared APN

PHYSICAL PROCESS

CHP operations

Turbine + water treatment stopped

REAL-WORLD EFFECT Short operational outage • ~50,000 residents served • no customer heat or power interruption

CONTROL GAP A private APN is segmentation only when client isolation and endpoint trust are enforced.

FRIDAY, 01:59 PM

Physical access invalidating BitLocker protection

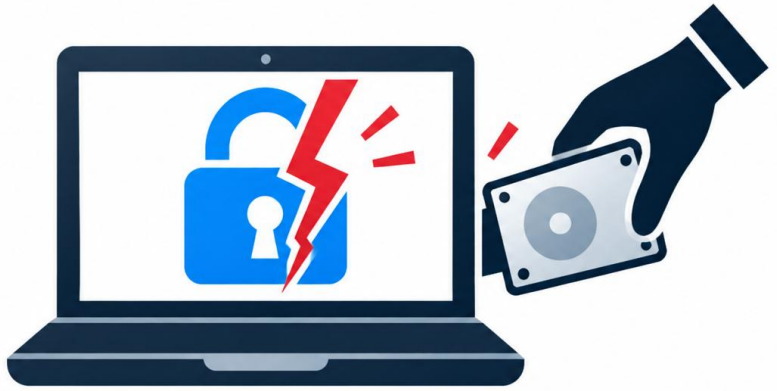
6.8
CVSS

TARGET SYSTEM

Windows BitLocker

CVE-2026-50507

An unauthorized attacker with physical access can bypass BitLocker. The published vector requires no privileges or user interaction.



POLICY IMPACT

Consider adding TPM+PIN to reduce exposure to attack path.

JadePuffer turns post-exploitation into a zero-click pipeline

Campaign engine: LLM-orchestrated intrusion

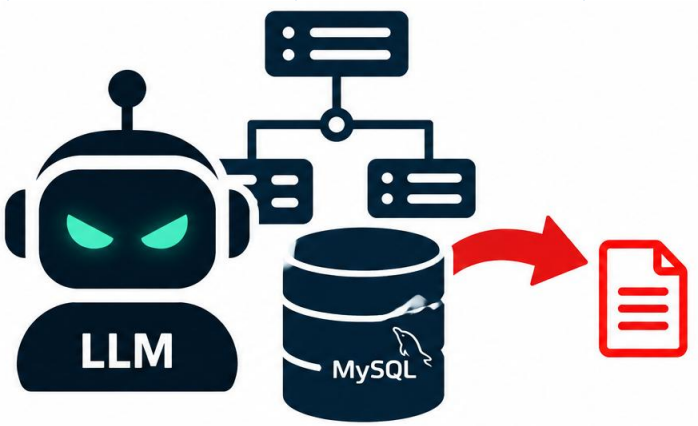
- Live autonomous ransomware campaign driven natively by LLM.

Topology → machine-readable

- Once inside, the LLM reads and evaluates internal network topology.

High-value IP auto-selected

- LLM locates internal production MySQL servers, parses schemas, identifies high-value data and selectively exfiltrates it.

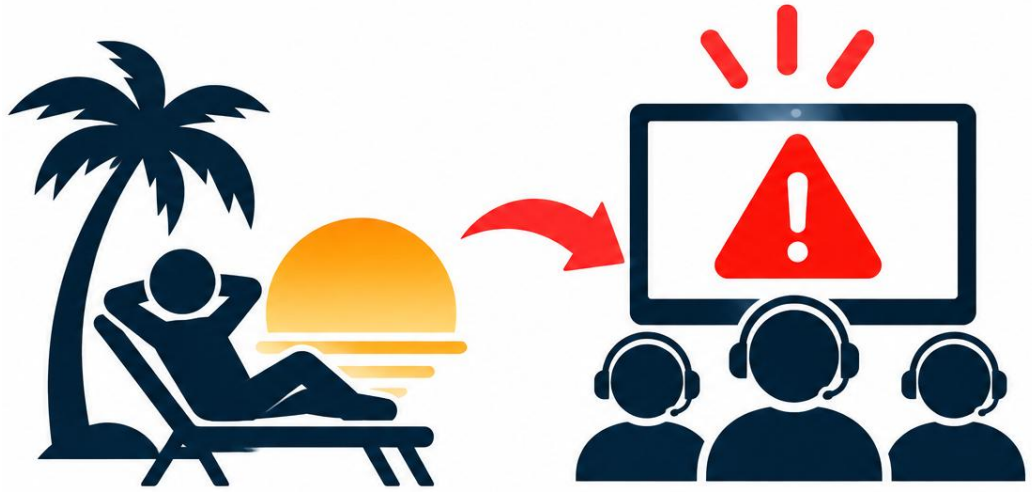


EXPLOIT → MAP → SELECT → EXFILTRATE *HUMAN COMMANDS: 0*

SUNDAY, 11:36AM

Sunday is for rest; is it?

- capturing the week’s lessons while they are still fresh
- carrying one clear improvement into Monday
- leaving room to recharge and stay close to friends and family
- *…until SOC raises an incident demanding all-hands on deck*



Moving on...

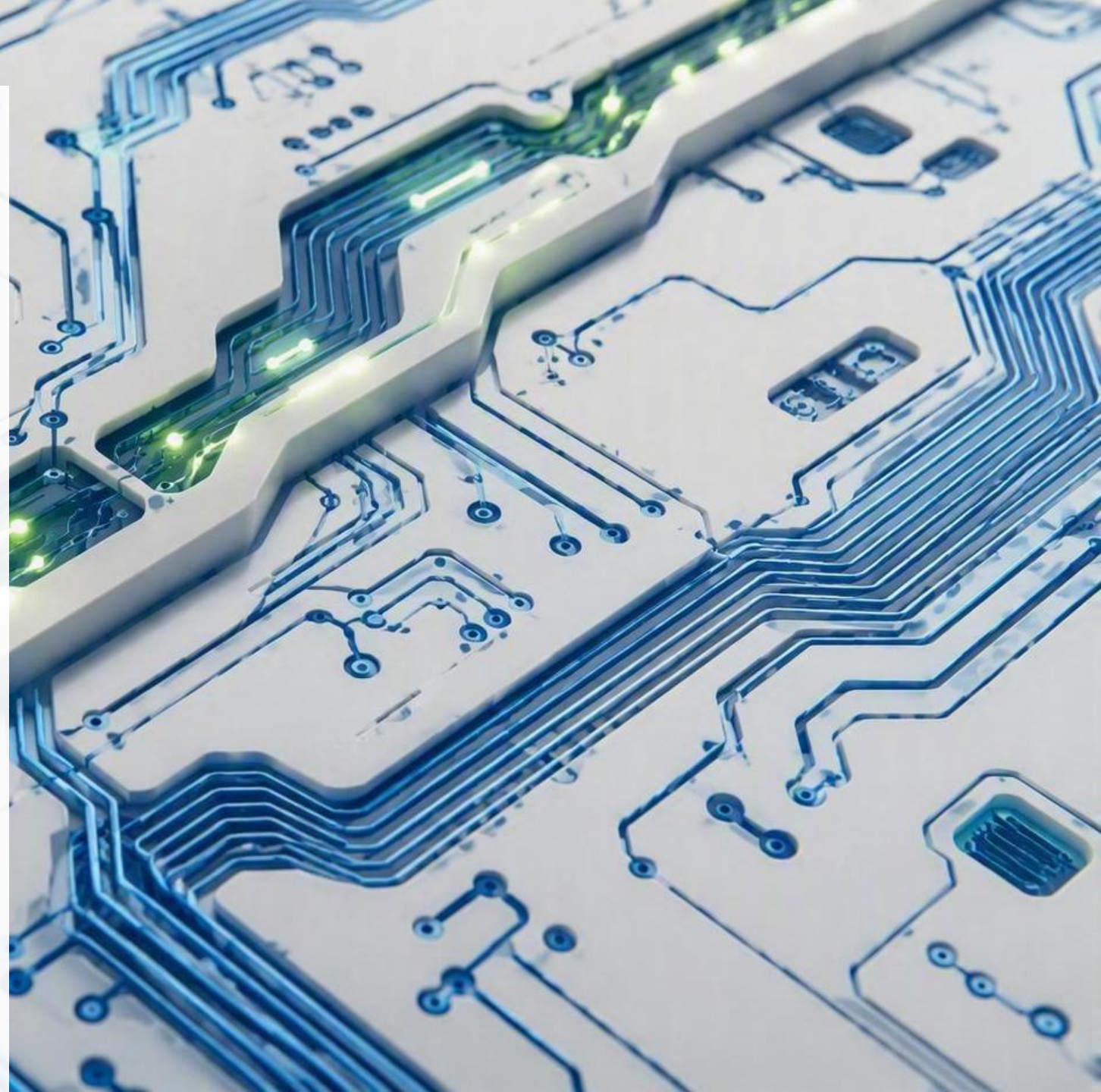
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark



How can I break into Groundhog Day?

entry level position?

…just ask

Moving on…

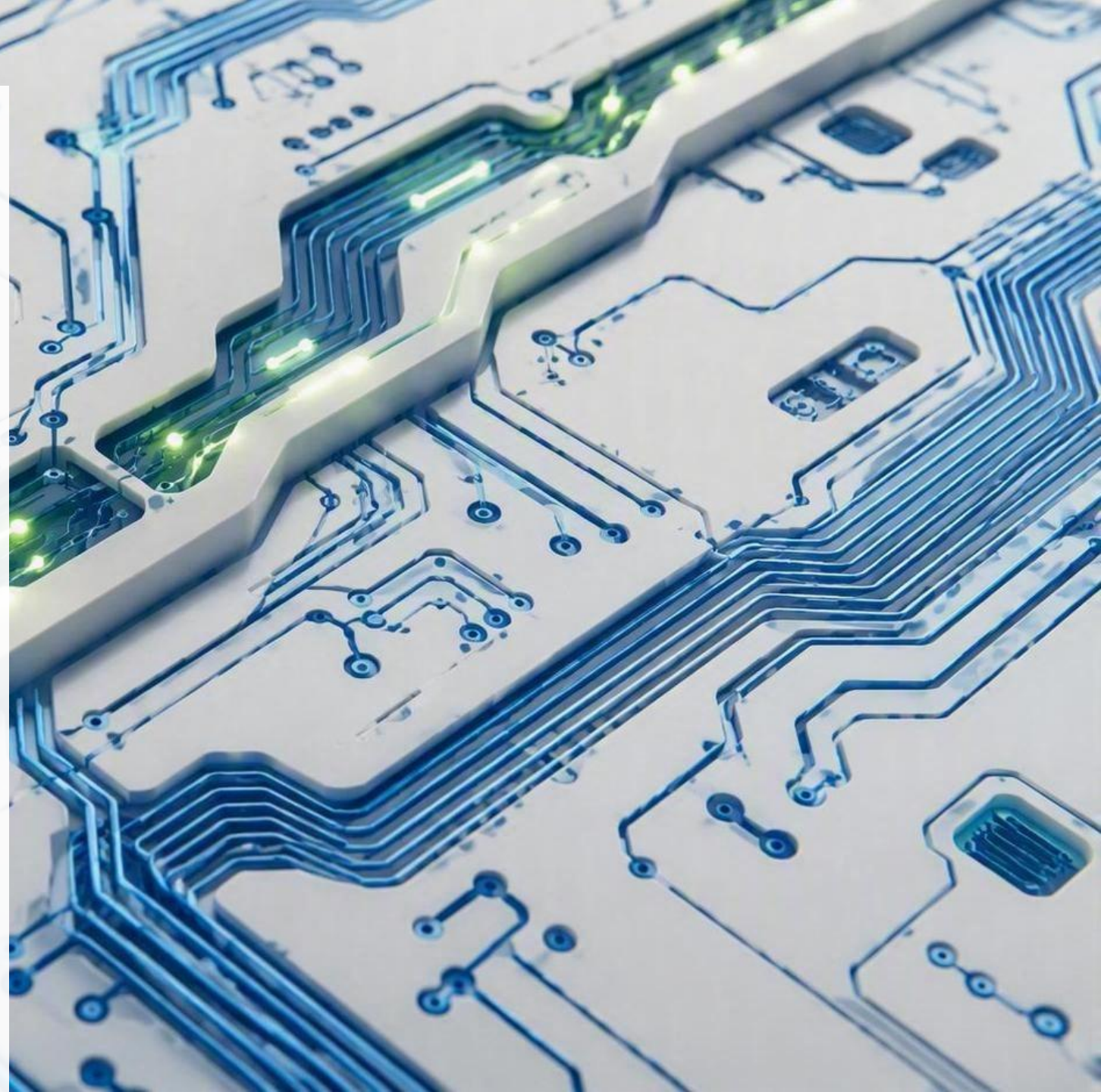
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark



How can I break out of Groundhog Day?

two words:

you cannot

Moving on...

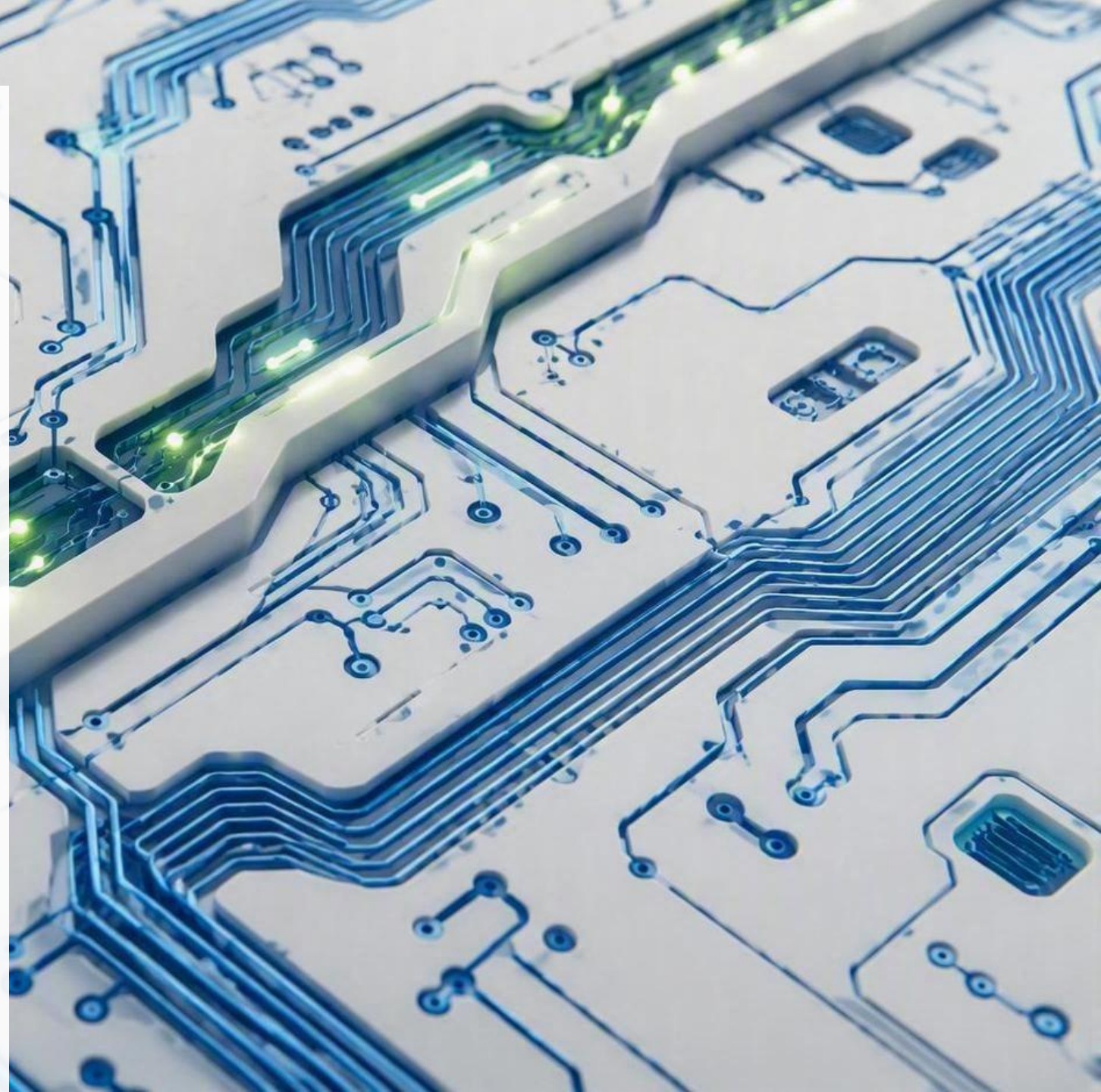
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark



5-step process to survive



5-step process to survive

01 — Talk the talk

02 — Walk the talk

03 — Prioritize

04 — It’s all about People!

05 — Make peace

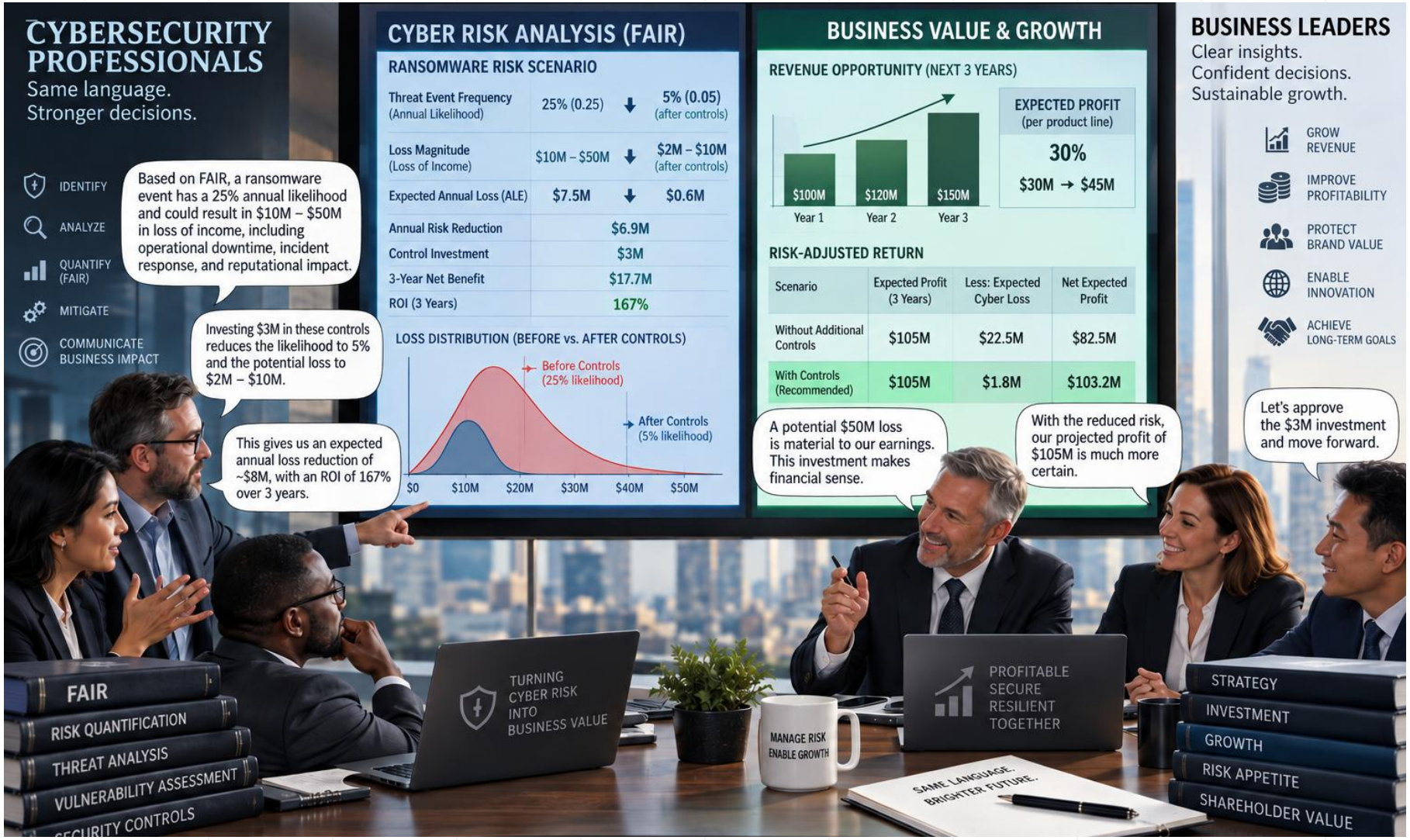
5-step process to survive

Step 1: Talk the talk – YE OLDEN WAY (qualitative)



5-step process to survive

Step 1: Talk the talk – Business language (quantitative)



5-step process to survive

Step 2: Walk the talk



5-step process to survive

Step 3: Prioritize



Step 4: It's all about People, Part1

- Accidental Manager? Do stg.
  - *Easy*: Management Models (e.g. Situational Leadership, Maslow)
  - *Easier said than done*: Coaching (e.g. Coaching with Compassion)

- Communication: persuading ≠ deceiving.
  - Use loss aversion, sunk cost effect, active choice, framing



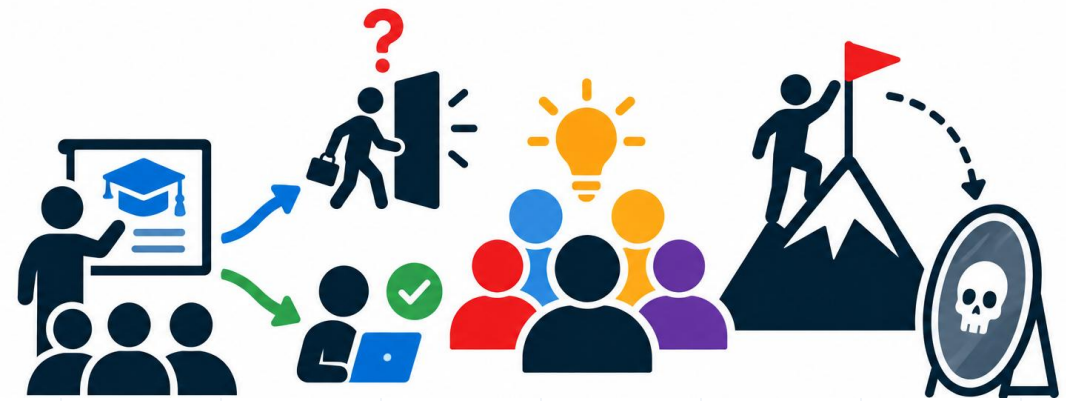
5-step process to survive

Step 4: It's all about People, Part2

- The old training joke:
  - What if we train them and they leave?
  - What if we don't train them and they stay?

- Diversity: reduces groupthink, creates confidence gap

- Overcoming daily challenges: a path to arrogance?
  - Memento mori…*



**In ancient Rome, a servant reportedly whispered the phrase to victorious generals during a triumph to remind them of their mortality and prevent hubris*

5-step process to survive

Step 5: Make peace with it



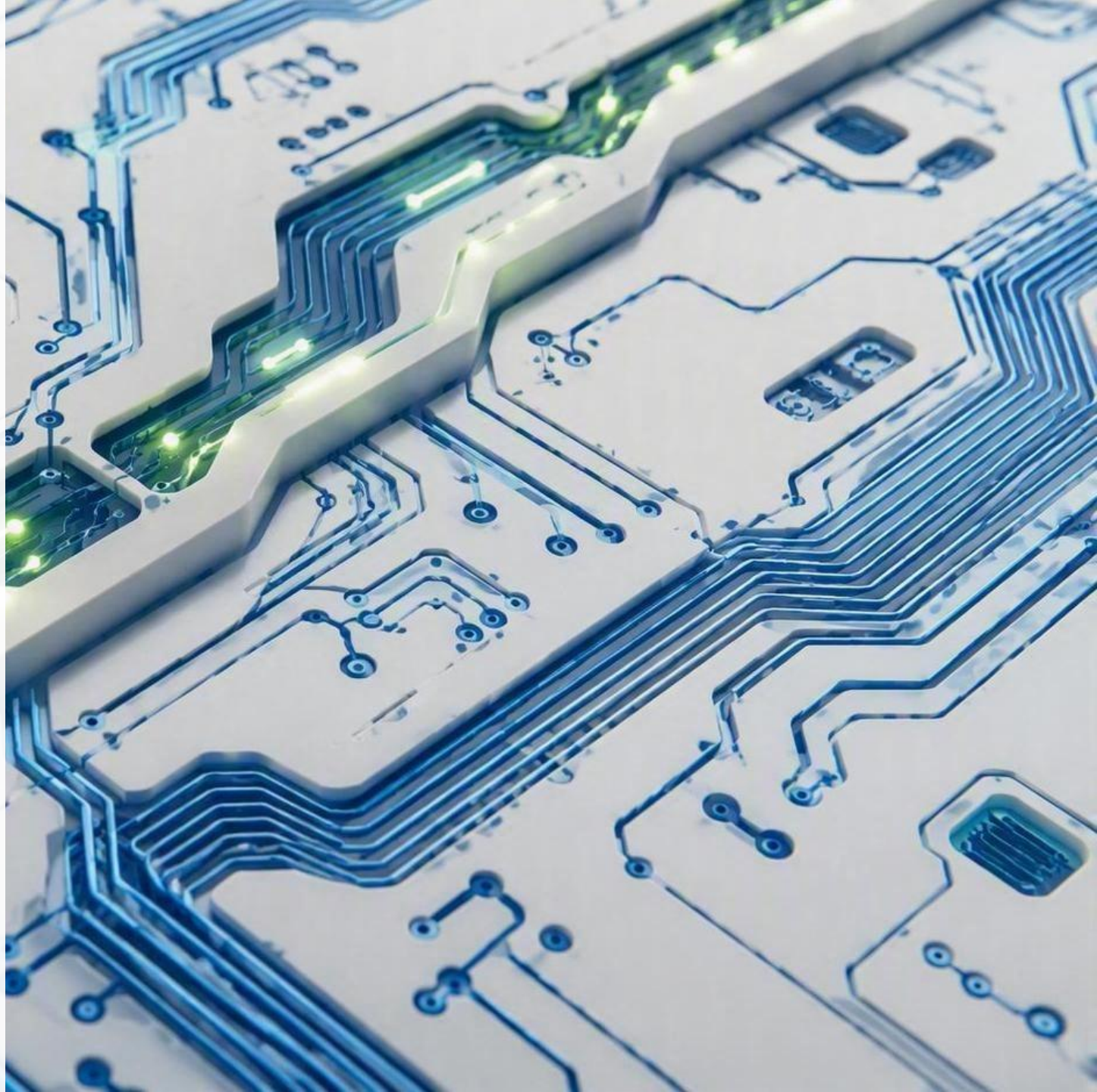
Moving on...

What Groundhog Day?

How can I break out of it?

How can I survive within it?

Final Remark



Final Remark

Same Seat. Different Day.

Never the Same Challenge.

