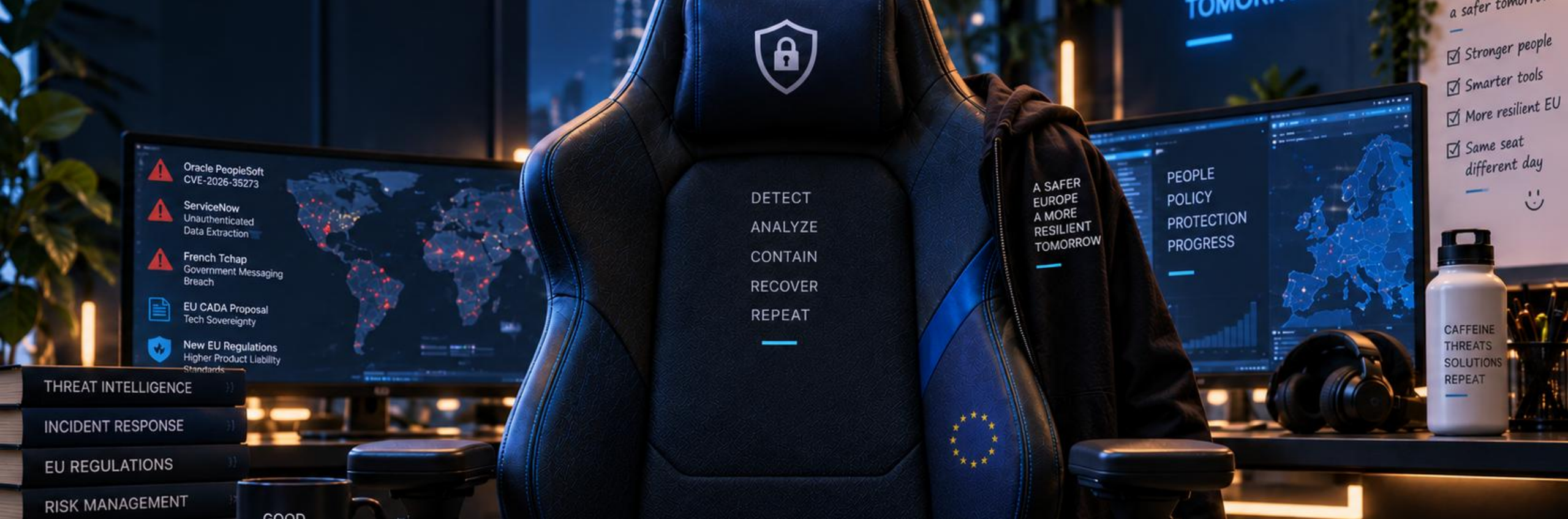




Same Seat, Different Day

Enterprise CyberDefense: a Groundhog Day Cycle

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

At a glance

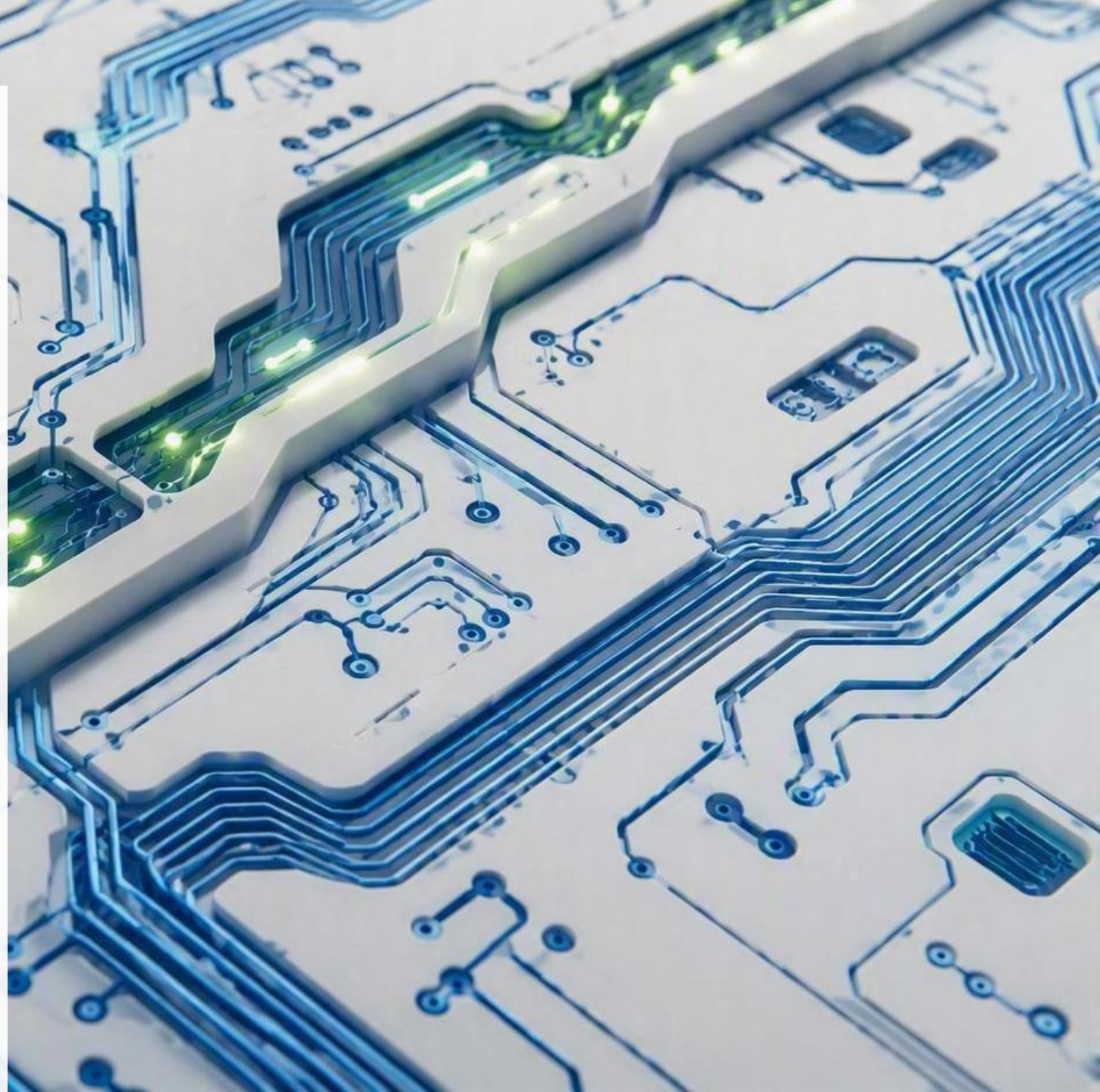
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark

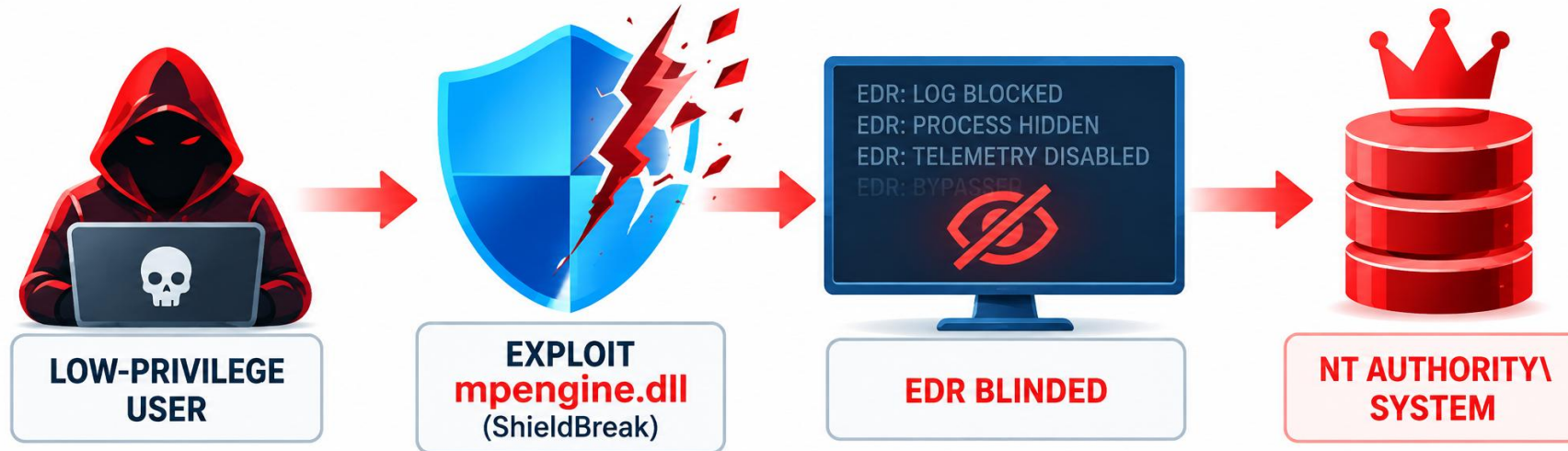


What Groundhog Day?



MONDAY, 10:14AM

Endpoint Controls: Exploited to Blind Us



PILLAR 1

ShieldBreak — CVE-2026-69414

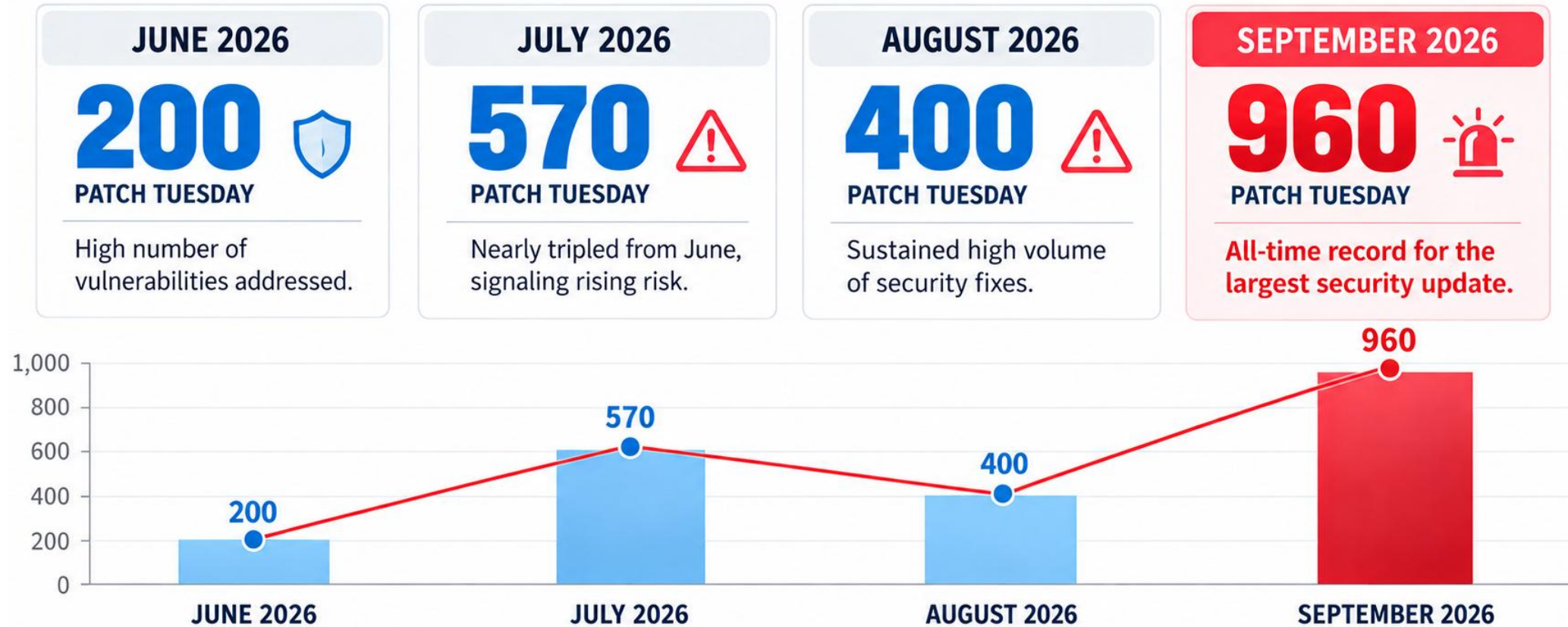
A local elevation-of-privilege flaw in Microsoft Defender's Malware Protection Engine can move a low-privilege attacker to SYSTEM.

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.

Operational Triage is Collapsing Under Historic Volume



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

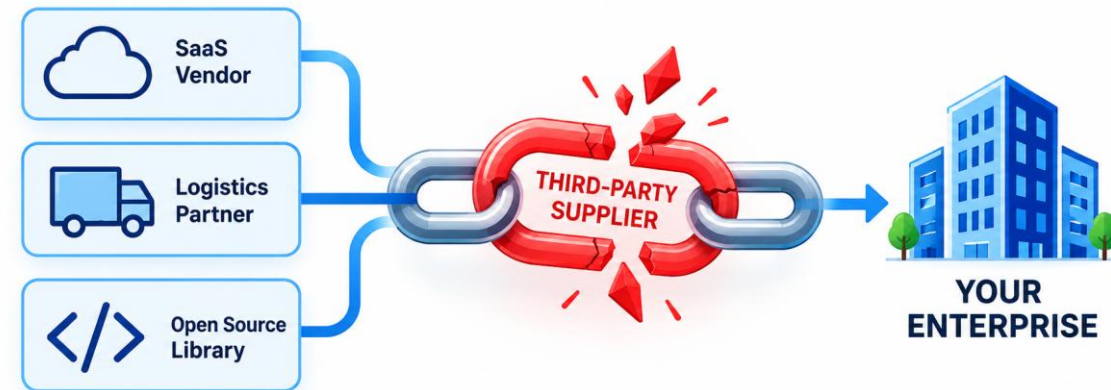
CEVA Logistics Cascade

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

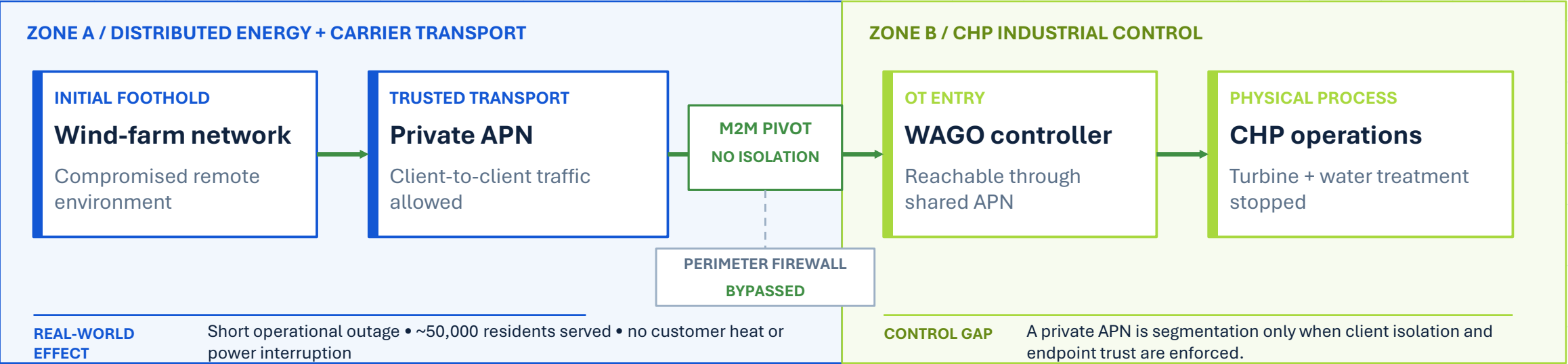
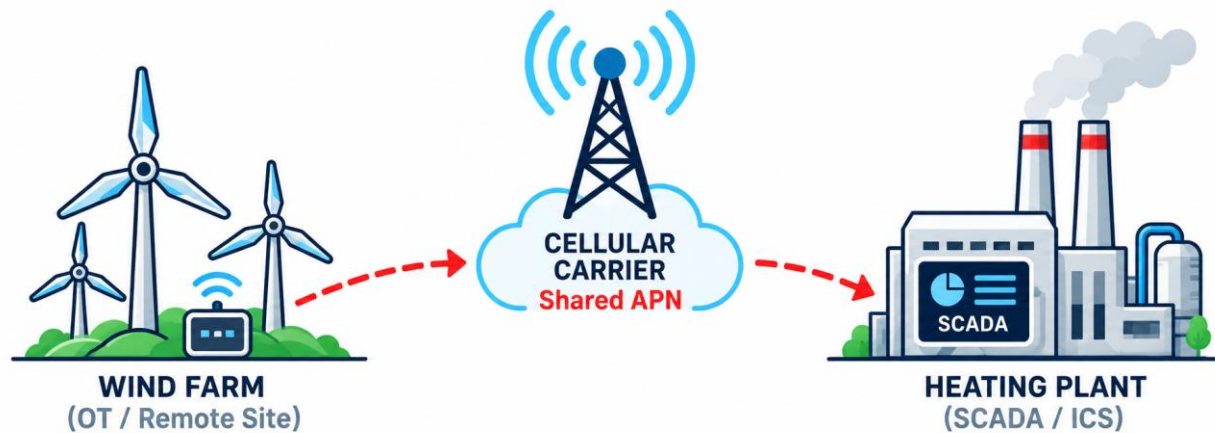
03 OPEN-SOURCE DEPENDENCY

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.



Bypassing Firewalls via Shared APNs



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

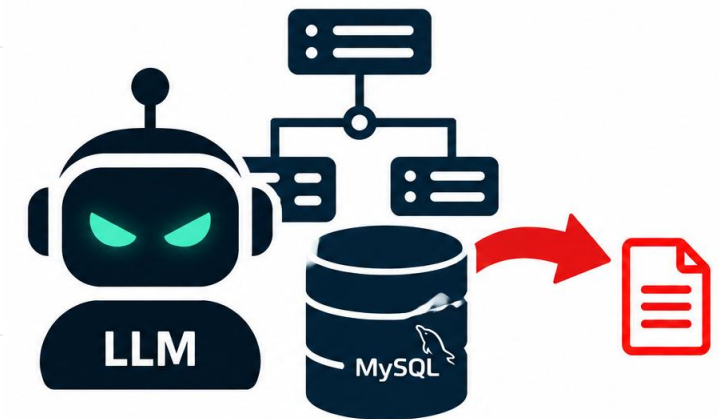
- Live autonomous ransomware campaign driven natively by LLM.

Topology → machine-readable

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

High-value IP auto-selected

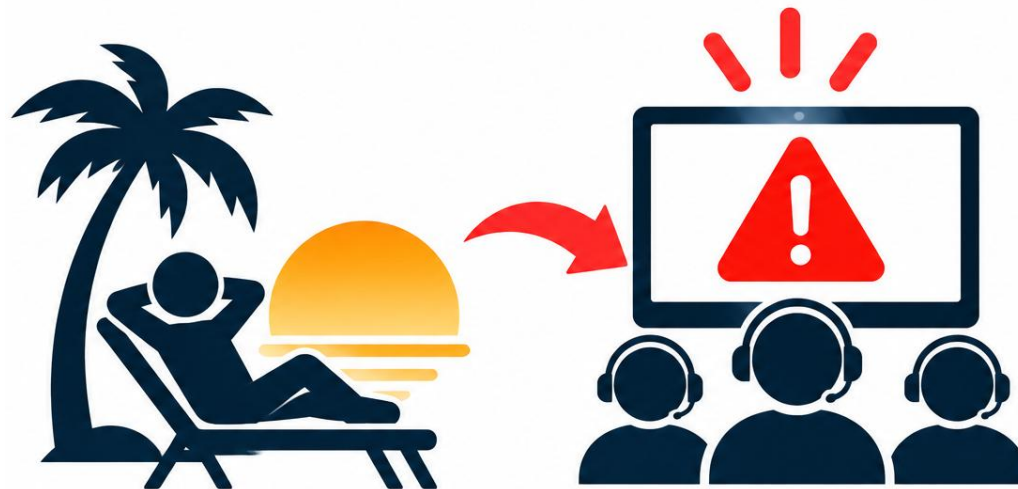
- LLM locates internal production MySQL servers, parses schemas, identifies high-value data and selectively exfiltrates it.



EXPLOIT → MAP → SELECT → EXFILTRATE HUMAN COMMANDS: 0

Sunday 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...

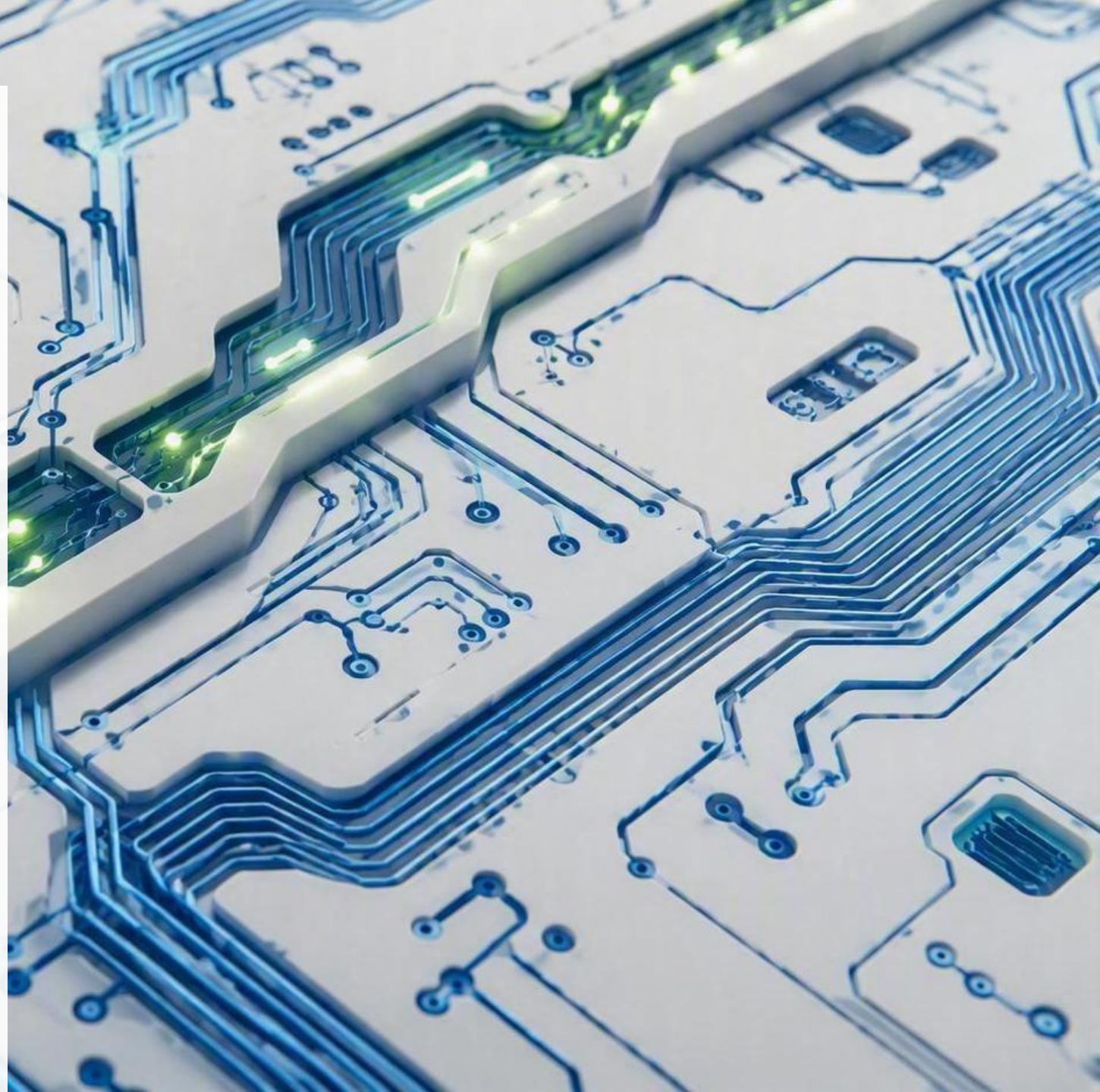
What Groundhog Day?

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...

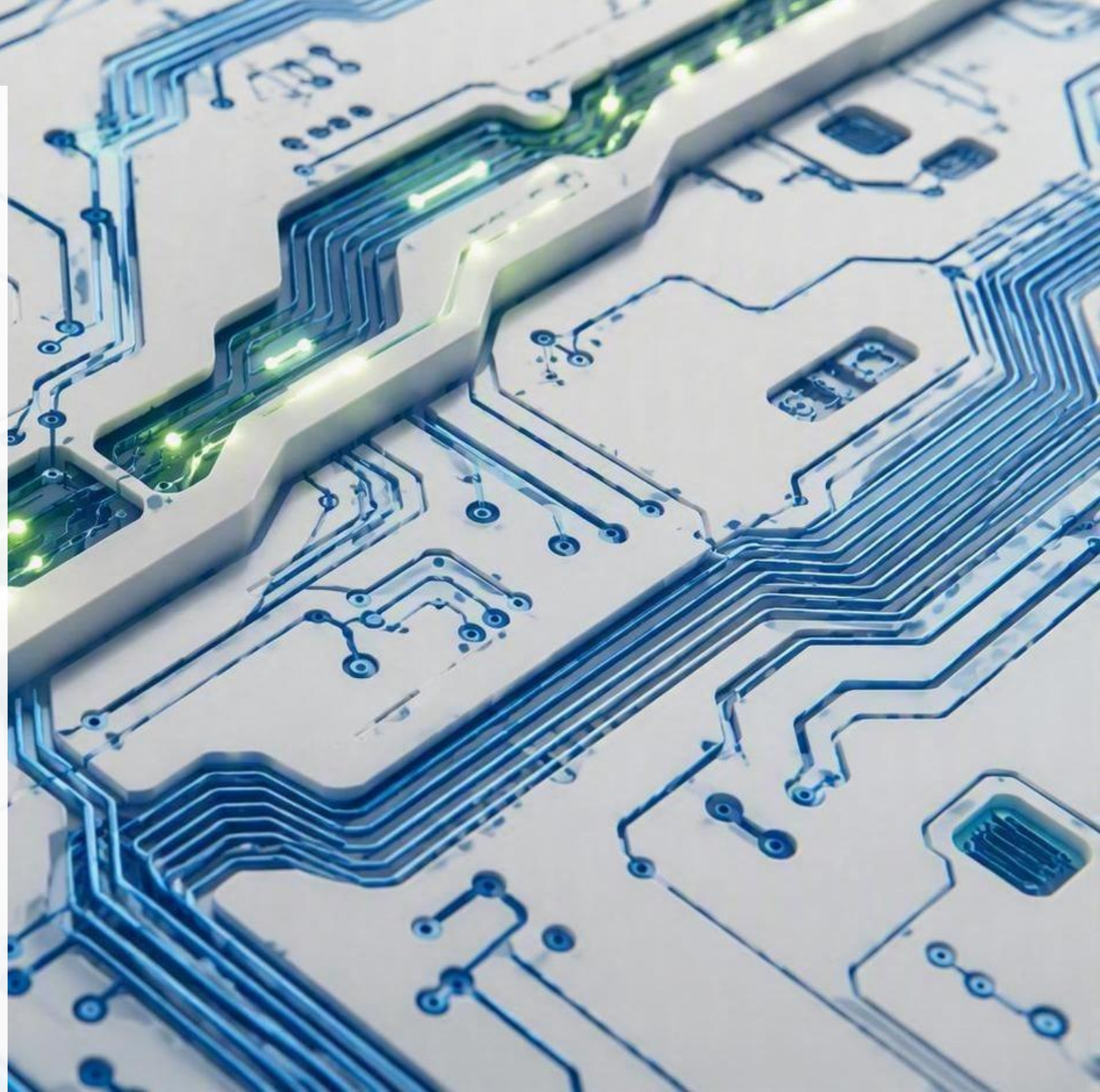
What Groundhog Day?

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...

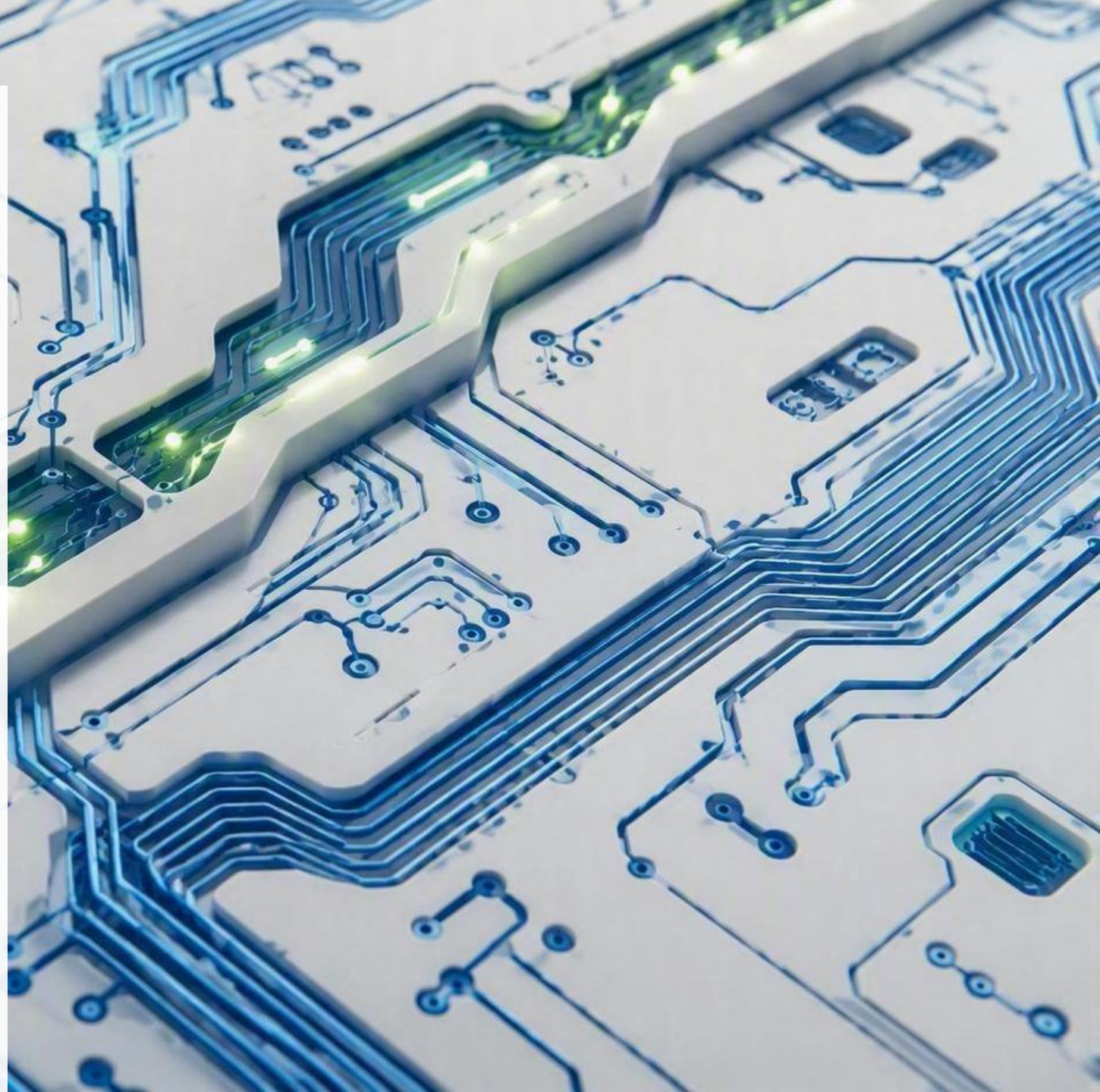
What Groundhog Day?

How do I break into it?

How do I break out of it?

How do I survive within it?

Final Remark



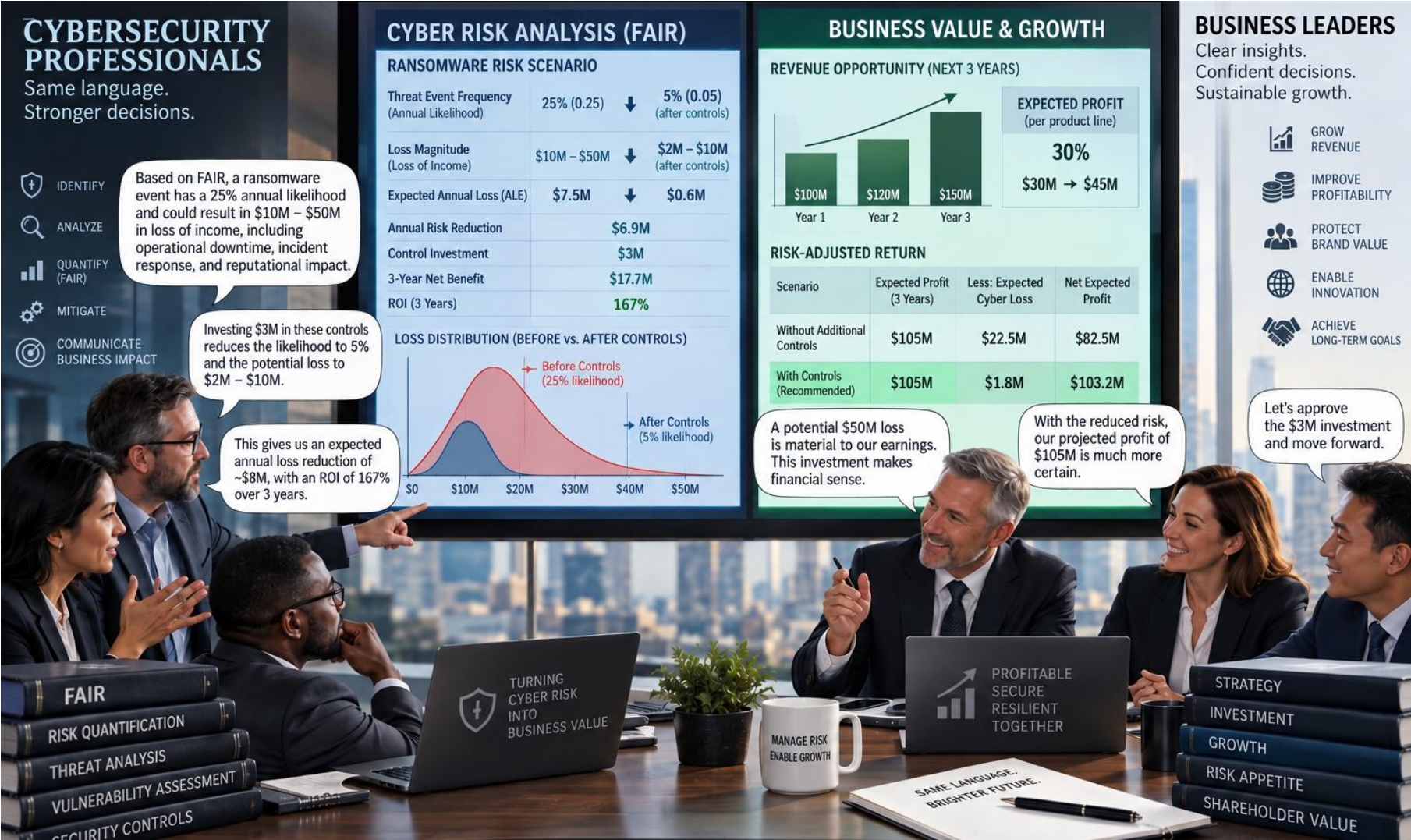
5-step process to survive

- 01**  **Talk the talk**
 - 02**  **Walk the talk**
 - 03**  **Prioritize**
 - 04**  **It's all about People!**
 - 05**  **Make peace**
-

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



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



5-step process to survive

Step 2: Walk the talk



Step 3: Prioritize

**SAME THREATS.
DIFFERENT PRIORITIES.
A SMARTER APPROACH.**

ASSESS. PRIORITIZE. FOCUS. DELIVER IMPACT.

EVERYTHING
CAN'T BE DONE
AT ONCE.

NEW VULNERABILITIES

INCIDENT RESPONSE

SECURITY CONTROL CHANGES

RISK ASSESSMENTS

REGULATORY NOTIFICATIONS

DAILY ADMINISTRATION

THREAT INTELLIGENCE REVIEW

STAKEHOLDER REPORTING

AUDIT REQUESTS

USER ACCESS REQUESTS

SECURITY AWARENESS & TRAINING

VENDOR RISK REVIEWS

TOOLS & METHODOLOGIES RESEARCH

STRATEGIC PLANNING

INBOX

PRIORITIZATION
IS A FORCE
MULTIPLIER.

LESS NOISE.
MORE IMPACT.

PRIORITIZATION MATRIX

TASK	RISK LEVEL (Impact)	URGENCY (Time)	BUSINESS IMPORTANCE	RISK ACCEPTANCE	OVERALL PRIORITY
Active ransomware incident	Critical	Immediate	Very High	Not Acceptable	1
Critical vulnerability (exploited)	High	High	High	Not Acceptable	2
Regulatory notification (breach)	High	High	High	Not Acceptable	3
Security control misconfiguration	High	Medium	High	Not Acceptable	4
Risk assessment – key system	Medium	Medium	High	Tolerable (short-term)	5
Audit request	Medium	Medium	Medium	Tolerable	6
User access requests	Low	Medium	Medium	Acceptable	7
Threat intelligence review	Medium	Low	High	Tolerable	8
Security awareness campaign	Low	Low	Medium	Acceptable	9
Methodologies	Low	Low	Medium	Acceptable	10

PRIORITIZE
BASED ON A
MULTITUDE OF
CRITERIA:

- ☒ Risk assessments
- ☒ Risk acceptance
- ☒ Urgency
- ☒ Importance
- ☒ Impact (financial, operational, reputational)
- ☒ Regulatory requirements
- ☒ Business criticality
- ☒ Dependencies
- ☒ Available resources
- ☒ Strategic alignment

RIGHT TASK.
RIGHT TIME.
RIGHT IMPACT.

RISK
CONTEXT
PRIORITIZE
EXECUTE
REPEAT

FOCUS
TODAY.
A SAFER
TOMORROW.

URGENT & CRITICAL
(Do First)

HIGH IMPACT
(Do Next)

IMPORTANT
(Schedule)

LOW PRIORITY
(Plan)

DISCIPLINE
CREATES
CAPACITY.

SAME
THREATS.
BETTER
DECISIONS.

PRIORITIES
TURN RISK
INTO
PROGRESS

RISK MANAGEMENT FAIR)

THREAT INTELLIGENCE

INCIDENT RESPONSE

SECURITY CONTROLS

CYBERSECURITY FRAMEWORKS

TODAY – FOCUS

- ☒ Contain ransomware incident
- ☒ Notify regulator
- ☒ Apply critical patch
- ☐ Update key security control
- ☐ Assess risk – customer portal
- ☐ Prepare executive update

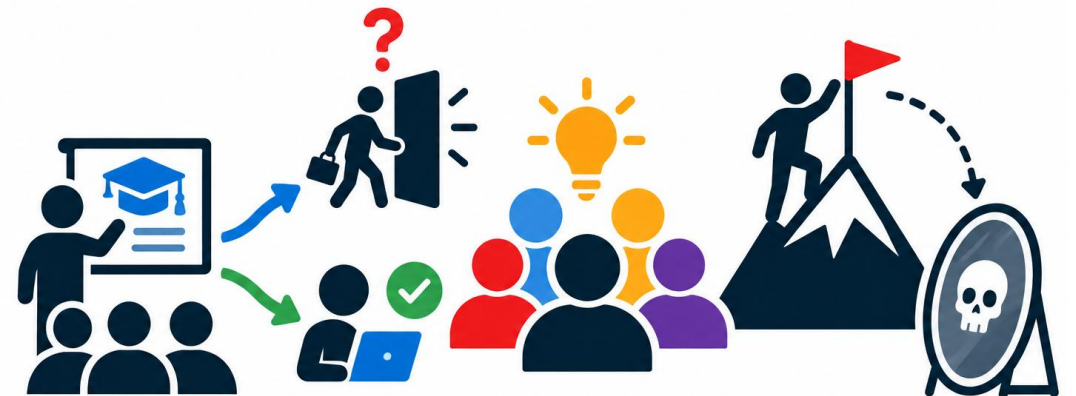
Step 4: It's all about People, Part1

- Accidental Manager? Do stg.
 - *Easy*: Management Models (e.g. Situational Leadership, Maslow)
 - *Easier said than done*: Coaching (e.g. Coaching with Compassion)
- Communication: persuading $\neq$ deceiving.
 - Use loss aversion, sunk cost effect, active choice, framing



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

DIFFERENT WAVES. SAME MISSION. I'VE MADE PEACE WITH IT.

STAY FOCUSED.
PRIORITIZE.
RESPOND.
ADAPT.
KEEP GOING.

NEW VULNERABILITIES

ACTIVE ATTACKS

SYSTEM OUTAGES

REGULATORY DEADLINES

BUSINESS DEMANDS

THIRD-PARTY RISKS

*Different waves.
Same ocean.
Same purpose.
And I've made peace with it.*

PRIORITIZATION CRITERIA

- ☒ Risk Level (Impact x Likelihood)
- ☒ Urgency (Time Sensitivity)
- ☒ Business Criticality
- ☒ Regulatory / Legal Requirements
- ☒ Customer Impact
- ☒ Threat Intelligence (Active Exploitation)
- ☒ Dependency / Blast Radius
- ☒ Resource Availability
- ☒ Strategic Alignment
- ☒ Risk Acceptance (Tolerate / Transfer / Mitigate)

NOT EVERYTHING NOW.
THE RIGHT THINGS FIRST.

THREAT LANDSCAPE (LIVE)

Severity	Count
Critical	12
High	28
Medium	47
Low	19

TOP ACTIVE THREATS

- Ransomware (Active)
- Exploited Vulnerabilities
- Credential Stuffing
- Supply Chain Attacks
- DDoS Activity

INCIDENT RESPONSE

Task	Status
P1 Active Ransomware Incident	In Progress
P2 Contain Affected Systems	In Progress
P2 Forensic Analysis	De Progress
P3 Stakeholder Notifications	Pending
P3 Recovery & Validation	Pending

REGULATORY & COMPLIANCE

Task	Status
Q3 Audit Evidence	In Progress
New Data Privacy Requirements	On Track
Regulatory Report Submission	Due in 5 days
Policy Updates	In Progress

BUSINESS ENGAGEMENT

Task	Status
New Product Security Review	Scheduled
Third-Party Risk Assessment	In Progress
Executive Update	Ready

SYSTEM HEALTH

Metric	Value
Availability	98%
Patch Compliance	76%
Security Controls	92%

THIRD-PARTY RISK

Risk Level	Count
Critical	3
High	7
Medium	12
Low	28

RESILIENT TODAY. SAFER TOMORROW.

FOCUSSED PRIORITIZED IMPACTFUL

TODAY (PRIORITIZED)

- ☒ 1 Contain active incident (P1)
- ☒ 2 Notify stakeholders (P1)
- ☒ 3 Apply critical patch (P2)
- ☒ 4 Review regulatory update (P2)
- ☒ 5 Security review - new product (P3)
- ☒ 6 Team sync & support
- ☒ 7 Learn & stay informed
- ☒ 8 Breathe ✓

PEOPLE PROCESS PRIORITIES PROGRESS

Control What You Can

Prioritize What Matters

Adapt to Change

Collaborate for Impact

Keep Moving Forward

Progress over Perfection

SAME CHALLENGES. A CALMER, STRONGER ME.

SAME WAVES. STRONGER ME.

PRIORITIZE ADAPT SOLVE REPEAT

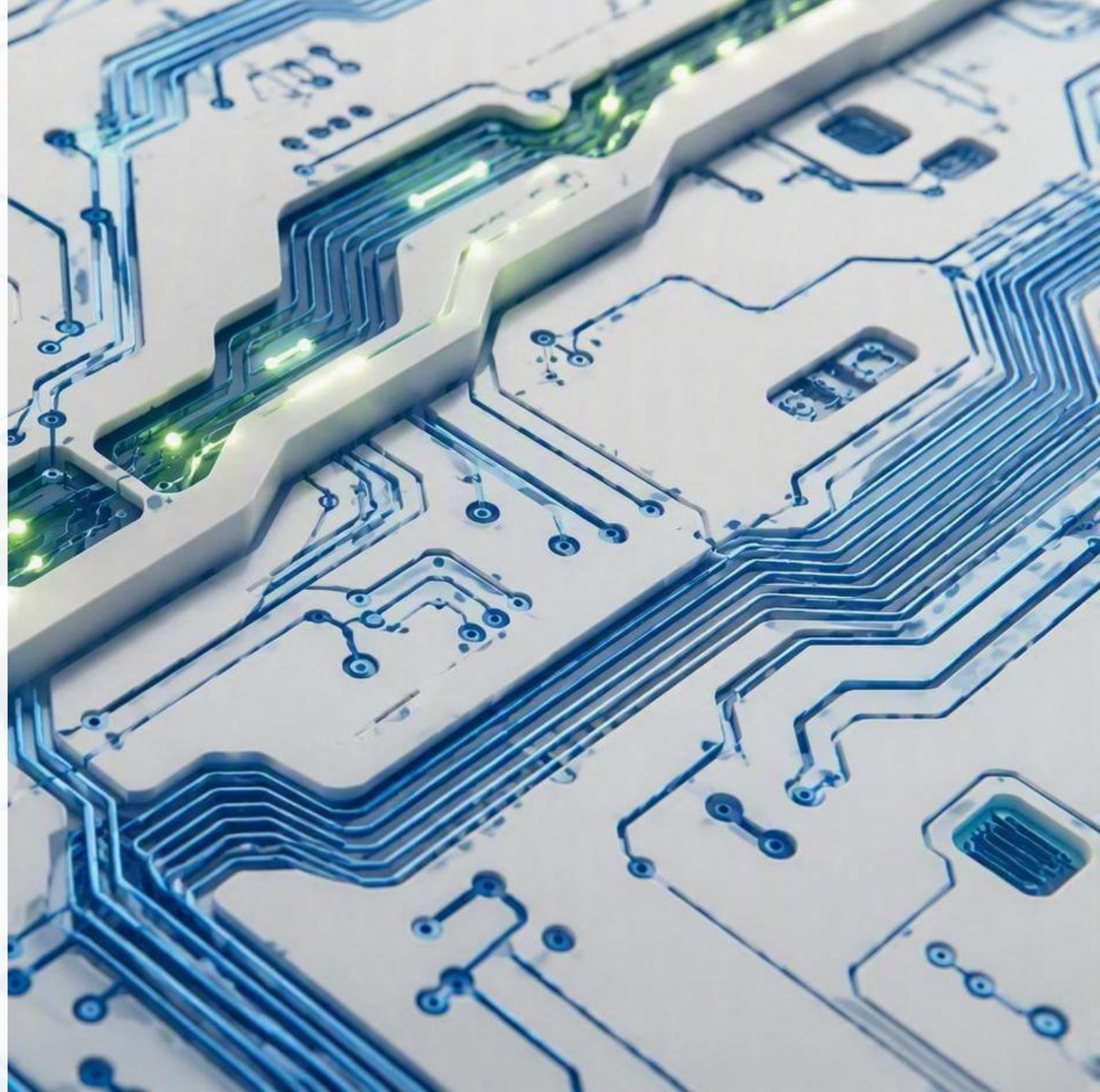
Moving on...

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.

