

CORNCON 12:
THE 12 CHAOS MONKEYS OF CYBER
CornCon Cybersecurity Conference
Davenport, IA • October 1-3, 2026



AI-Augmented Vulnerability Research: Risk, Opportunity, Governance

Sebastiaan Gybels

SVP Cyber Security
Northern Trust



THE PERSON TELLING THIS STORY

Hi, I'm Sebastiaan Gybels.

Federal Reserve	Big 4 Audit
Cyber-risk	2 x CISO

Scan to connect on LinkedIn

20+ years building, auditing, regulating, and leading cyber risk..

I've signed the report.

I've also watched it go stale.

9:14 a.m. – Critical Vulnerability Published



THREAT INTEL · LIVE FEED

CVE-2026-3117 — unauthenticated · remote · code execution

Halcyon Edge Gateway · internet-facing · CVSS 9.8

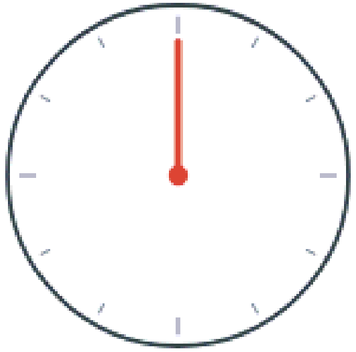
YOU'VE MET THIS BEFORE Log4Shell · MOVEit · Citrix Bleed

hours
from disclosure to mass exploitation

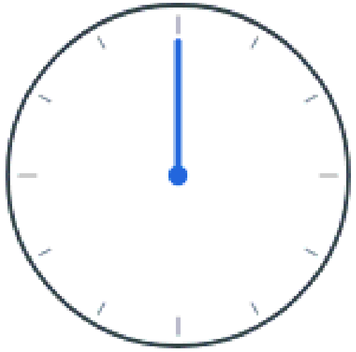
~1 in 3
breaches trace to a known, unpatched vulnerability

Disclaimer: This is an Illustrative scenario.

THE WHOLE TALK IS ONE RACE



THE GAP BETWEEN THEM



ATTACKER

Exploits in minutes

THE ATTACKER'S CLOCK

DEFENDER

Responds in hours / days

YOUR CLOCK

How fast can you decide — and prove it?

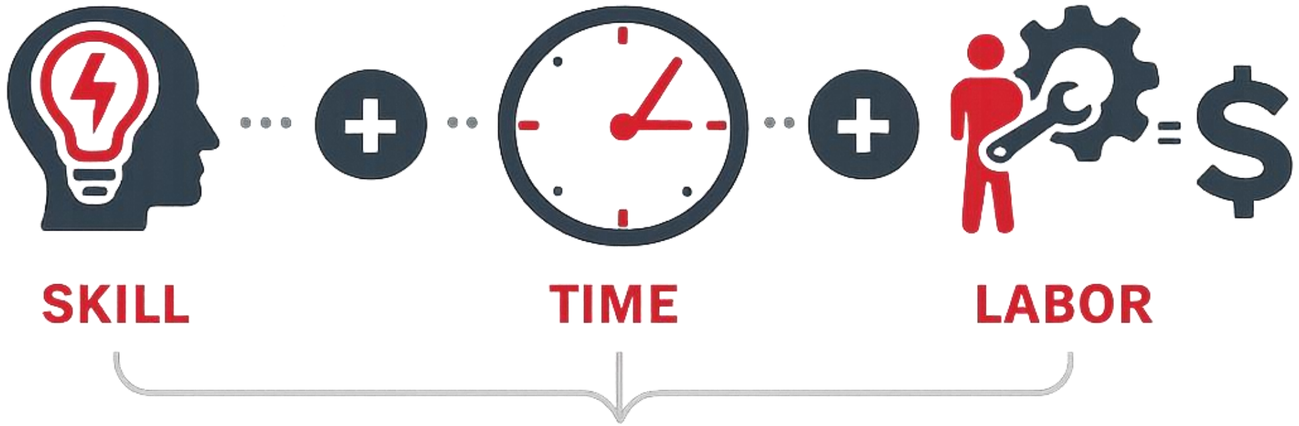
THE REAL QUESTION

What does AI now cost?

Not the power of the model — the price of an attack.

FOR THIRTY YEARS, AN ATTACK HAD A PRICE

9:14 · still Tuesday



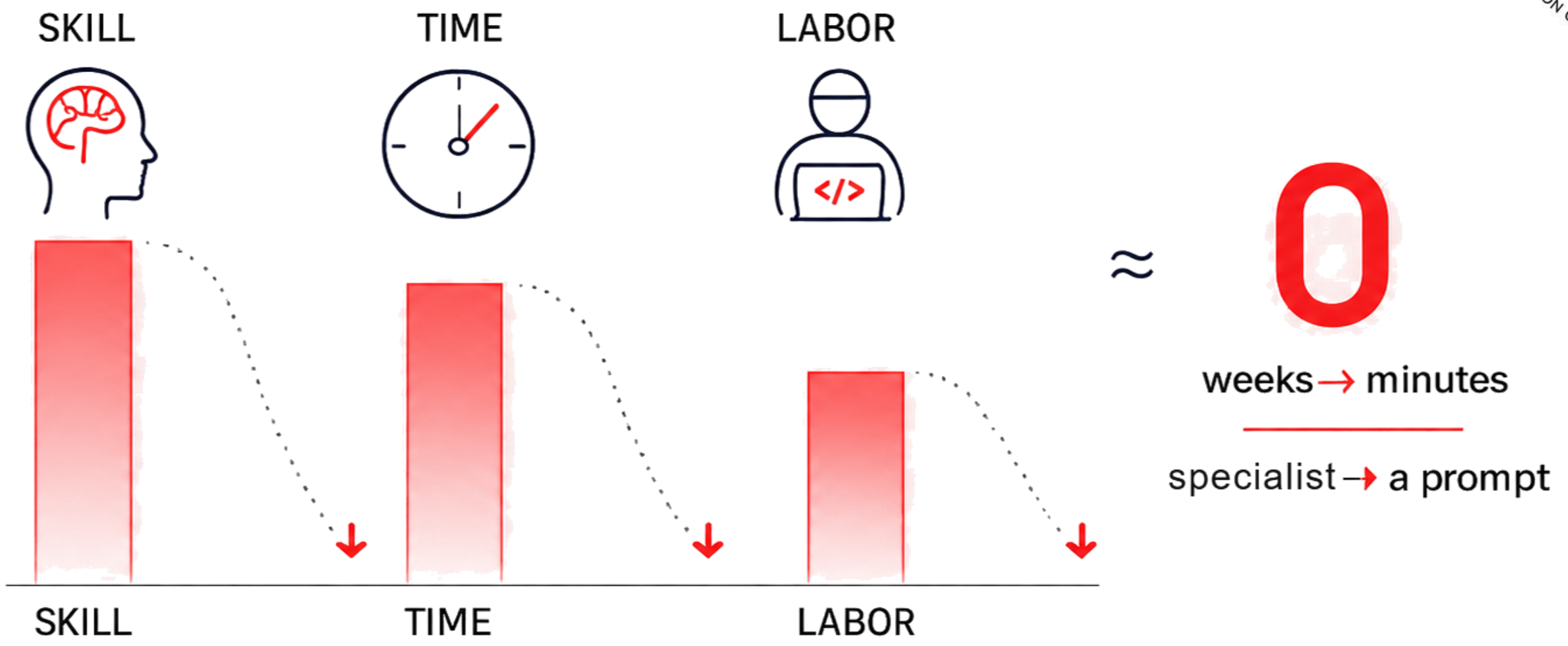
— the tax that kept everyone out.

WHAT ONE EXPLOIT USED TO COST

Weeks of a specialist's time.

A scarce, expensive human — per target.

AI MADE THE TAX COLLAPSE



THE COST TO ATTACK COLLAPSED FROM WEEKS OF EXPERTISE TO MINUTES OF AUTOMATION.

Obscurity was never protection.



It was a subsidy.

Attackers now enumerate the entire internet continuously — every exposed Confluence, Ivanti and edge appliance.
Being small was never the same as being hidden.

WE BRACED FOR THE WRONG ATTACKER

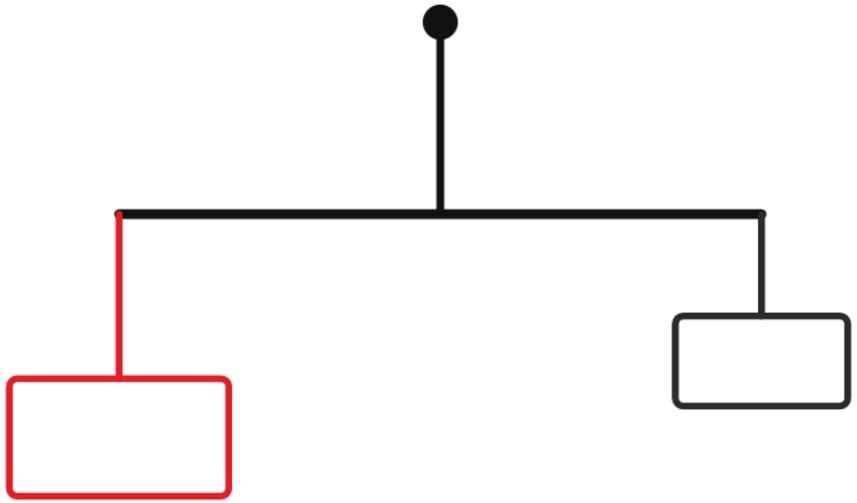
9:14 · still Tuesday

~~SMARTER~~ → **CHEAPER**

From potentially 100 targets to 100,000 targets

Cheaper means **more**, and more arrives **faster**. Your threat model shifts from **sophistication** to **scale & speed**.

BE HONEST ABOUT WHAT IT IS



ACCELERATION

NOVELTY

9:31 · same Tuesday

A force multiplier. Not magic.

The cost collapse cuts **both** directions — the defender gets the same leverage:

Triage & dedupe	days → **minutes**
Reachability	manual → **automatic**
Patch validation	a sprint → **an hour**

WHAT CHANGES MONDAY
Put AI on the defender’s side of the same ledger — start with triage.

ORGANIZATIONAL FRICTION CREATES DECISION LATENCY

The traditional model was rational for a periodic world. Today, it can't keep up.

TRADITIONAL MORNING: THE DECISION TAKES 30–90 DAYS

01	02	03	04
TICKET	30-DAY SLA	CHANGE WINDOW	QUARTERLY REVIEW
Day 0	+30 days	Next monthly	+90 days
Vulnerability identified and logged	Queued for assessment within SLA	Wait for approved change window	Reviewed in quarterly risk cycle

WHY IT EXISTED
Batching change around regulatory reporting and change windows kept core banking stable.

WHY IT CREATES FRICTION TODAY
The attacker's window is hours; the sanctioned cycle is months.

DECISION LATENCY: 30–90 DAYS
Risk accumulates while we wait.

AI-AUGMENTED MODEL: THE DECISION TAKES MINUTES TO HOURS

THREAT INTEL	ASSET INVENTORY	OWNERSHIP	ENGINEERING QUEUE	APP SECURITY	RISK REVIEW	CAB / APPROVAL	DEPLOYMENT
Minutes	Minutes	Minutes	Hours	Hours	Hours	Hours	Minutes–Hours
Continuous intel and exploit signals	Real-time asset and exposure context	Automated ownership and criticality	Risk-ranked backlog and automated workflows	Automated analysis and remediation recommendations	Continuous risk scoring and acceptance	Digital approvals and policy as code	Automated deployment and validation

WHAT MAKES THIS POSSIBLE
Connected data • Connected processes • Governed automation

WHAT CHANGES MONDAY
Instrument the handoffs. Measure decision latency — not just patch SLA.

DECISION LATENCY: MINUTES TO HOURS
We decide faster. We reduce risk faster.

THE ATTACKER'S WINDOW
Exploit ready in hours.
Automated. Relentless. Global.

THE GAP IS DECISION LATENCY
Every day we wait increases exposure.
Every minute we save reduces risk.

OUR OPPORTUNITY
Remove friction. Connect the dots.
Make faster, governed decisions.

A HUMAN CANNOT CONTINUOUSLY UNDERSTAND CYBER RISK

The scale, speed, and interconnectedness exceed human cognitive capacity. Our past practices were rational responses to that reality.

THE PROBLEM: BEYOND HUMAN CAPACITY

Modern environments generate more signals, change faster, and interconnect more systems than any human can continuously comprehend.

43,000+
NEW CVEs / YEAR
~120 new vulnerabilities every day

200M+
VULNERABILITIES
across open source, third-party, and code

12M+
ASSETS & SYSTEMS
hybrid, multi-cloud, on-prem, and edge

1 ANALYST
HUMAN LIMIT
attention, time, and cognitive overload

Humans are excellent at focus.
Cyber risk requires continuous, real-time, enterprise-scale comprehension.

RESULT: WE RELY ON SAMPLES, NOT REALITY
Snapshots. Estimates. Committees.
Good intentions — partial visibility — slow decisions.

WHY OUR PAST PRACTICES WERE RATIONAL

Every habit we built solved a real problem in a different era.
They optimized stability when change was slow and information was scarce.

DOCUMENTS over discovery
"We need complete, accurate information before we act."
Rational because information was hard to collect. Collect first, decide later.

SCORES over context
"We need a consistent way to compare and prioritize."
Rational because context was limited. Normalize risk so we can rank it.

COMMITTEES over velocity
"We need alignment and shared accountability."
Rational because decisions were infrequent and high impact.

PERIODIC REVIEWS over continuous
"We review regularly to stay in control of change."
Rational because change was slow. Batch the changes, reduce disruption.

They were not wrong. They were right — for the world we had.
The world changed. **Our operating model must evolve.**

HUMAN LIMITS + RATIONAL HABITS = DECISION LATENCY

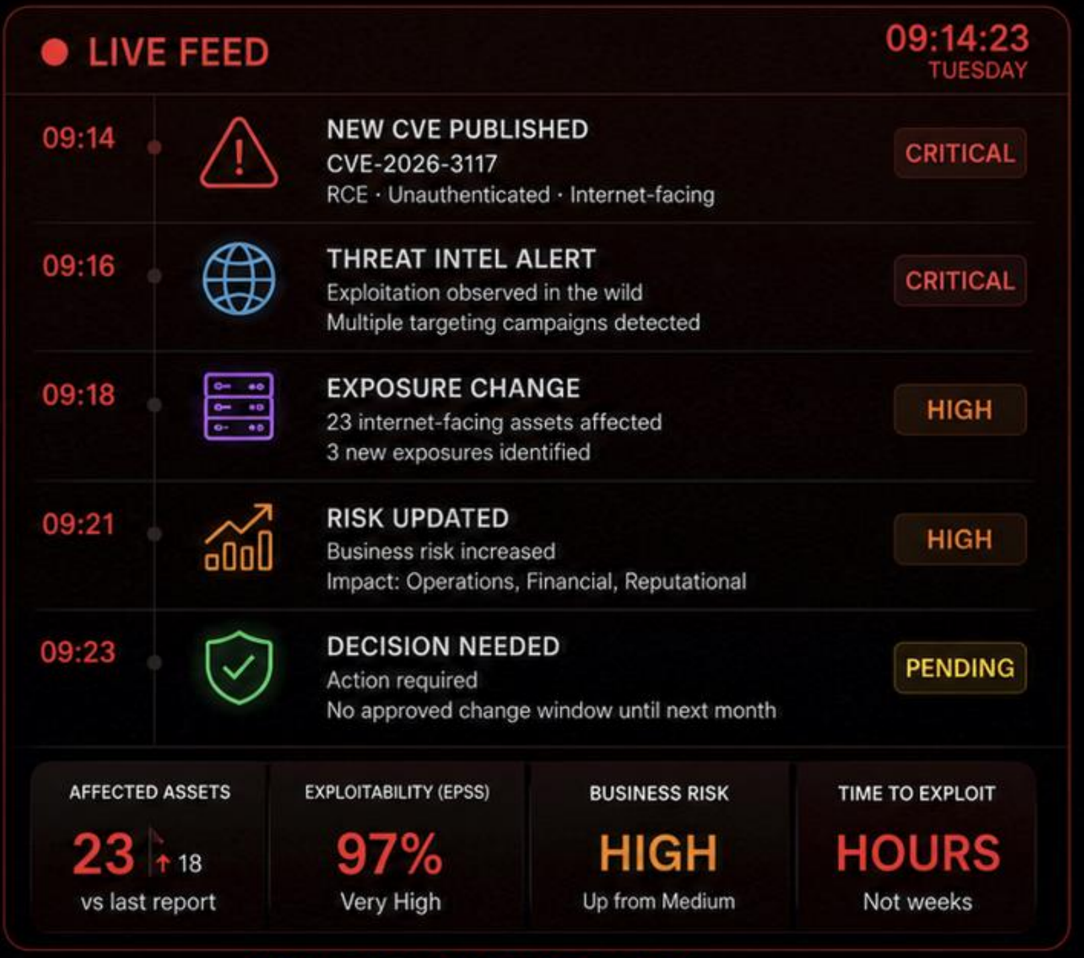
The past optimized for stability. The future demands continuous understanding and speed.

THE CHALLENGE:
Bridge the gap between what's possible and what we can decide.

A PHOTOGRAPH.

The risk picture—as of last quarter.
Meanwhile, today: the estate has already changed.

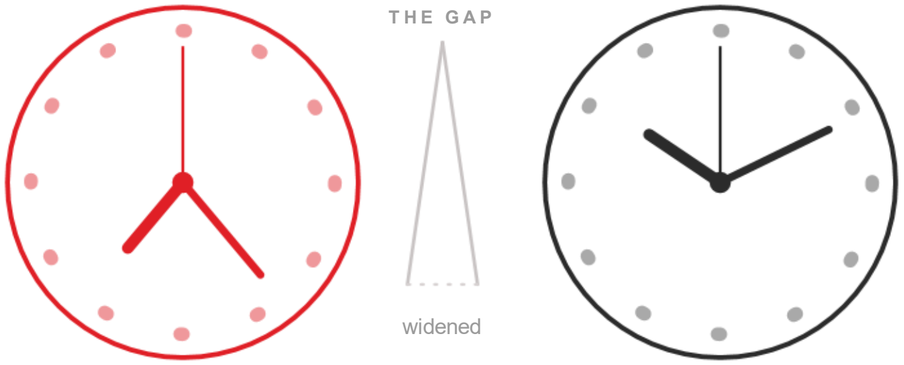




A PHOTOGRAPH
Yesterday's truth. Accurate—for a moment.

CONTINUOUS REALITY
The world keeps changing—minute by minute.

THE GAP WIDENED WHILE WE STOOD STILL



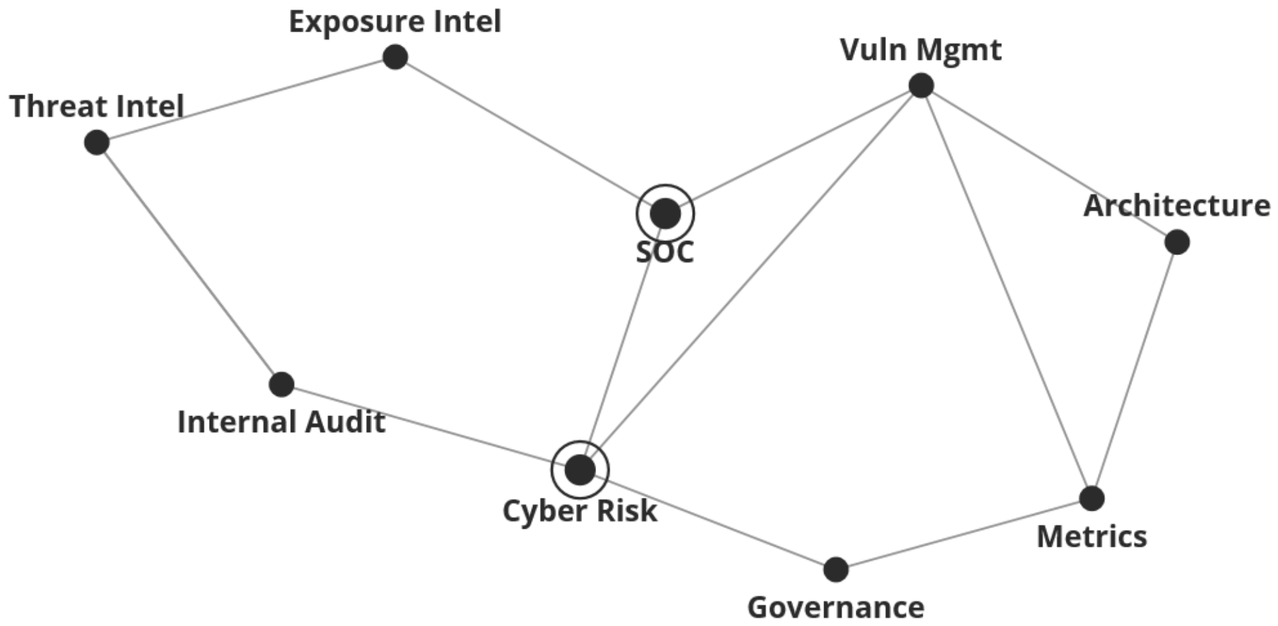
We weren’t wrong.

The ground moved.

Tell the board plainly: our controls didn’t fail —

our **cycle time** did.

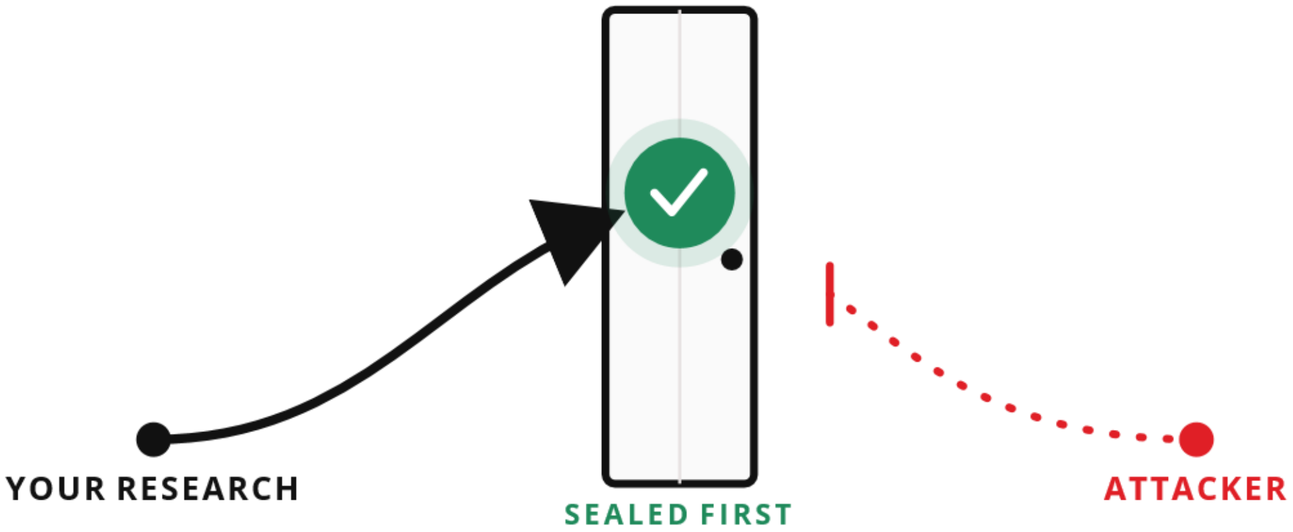
9:58



Ten periodic functions → one continuous organism.

Same teams, same people — rewired from a calendar to a nervous system.

THE DEFENDER REACHED IT FIRST



It found the door first.

Your own research found the next Halcyon Edge flaw first — **closed before any public PoC existed**.



Speed without a brain is a seizure.

Autonomous action with no governance = an outage, an audit finding, or a breach **you caused yourself**.

The risk register is dead.

Long live risk intelligence.

— A promotion, not a demolition — a **continuous, evidence-driven, explainable** view of risk.

SNAPSHOT vs. STREAM

From static risk registers that capture a moment
to risk intelligence that reflects reality as it changes.

RISK REGISTER (SNAPSHOT)

Point-in-time view

BOARD RISK REPORT

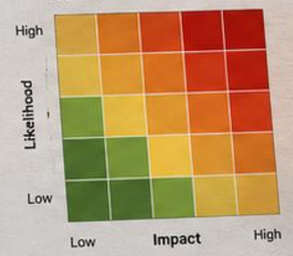
Enterprise Risk Register

APPROVED
March 31, 2026

Assessment Date: March 31, 2026

TOP CYBER RISKS	INHERENT RISK
1 Third-Party Risk	HIGH
2 Vulnerability Management	MEDIUM
3 Privileged Access	MEDIUM
4 Data Protection	LOW
5 Security Awareness	LOW

RISK HEAT MAP



Notes: Risks assessed based on information available at the time of reporting.

Approved by Risk Committee

Report Owner: CRO Office

Captured on March 31, 2026
09:00 AM

REALITY
KEEPS MOVING

RISK INTELLIGENCE (STREAM)

Continuous, real-time view

CRITICAL RISKS	ACTIVE THREATS	EXPOSED ASSETS	RISK TREND
23 +7	12 +3	389 +24	Improving
vs last 24h	vs last 24h	vs last 24h	vs last 7d

LIVE RISK EVENTS — Last updated: 09:23:47 AM

09:23	Critical vulnerability exploited in the wild CVE-2026-3117 – Internet-facing asset impacted	CRITICAL
09:21	New asset discovered on internet 23 assets now exposed	HIGH
09:18	Threat intelligence: Active exploitation confirmed Multiple targeting campaigns detected	CRITICAL
09:16	Configuration drift detected High-risk change in production environment	HIGH
09:14	New CVE published CVE-2026-3117 – RCE – CVSS 9.8	CRITICAL

RISK OVER TIME (REAL-TIME)



Continuously updated
09:23 AM

A snapshot informs. A stream empowers.



Stale the moment it’s signed.

The board report ages as the ink dries.

~3,300

new CVEs published between signing and the next board meeting.

WHAT CHANGES MONDAY

Give the board a **live link**, not a signed PDF.

AI doesn’t make the register wrong.

It removes the limit it was built to work around.

The limit was human: sample, document, score, decide-by-committee. Lift it, and all four dissolve.

RISK MOVES TO THE CENTRE

A living model that ingests signal continuously and renders the register as one of its outputs.

SENSE — SIGNAL PLANES

Threat Intelligence
known-exploited · PoC feeds

Exposure Management
continuous attack-surface scan

Asset Context
ownership · reachability · criticality

Business Context
revenue · service · obligation

DECIDE — REASONING CORE

Decision Intelligence

continuous · evidence-driven · explainable

Risk register rendered output

Board view live link

GOVERN

Human Approval
accountable decision-maker within pre-authorized bounds

ACT

Automation
bounded response · patch · isolate · ticket

CONTINUOUS LEARNING every decision retrains the model

WHAT CHANGES MONDAY

Stop maintaining the register **as the source of truth** ; make it a rendered view of the live model.



THE PIECES ARE ALREADY YOURS

You already own almost every capability.

Threat Intelligence ✓	Exposure Management ✓	Asset Inventory ✓	CMDB ✓
SIEM ✓	EDR ✓	Vulnerability Mgmt ✓	Risk Register ✓
Automation ✓	Governance ✓	Business Context ✓	Operating as one system?

Mature. And disconnected.

All **11 of 11** capabilities owned — they just don't yet operate as one connected decision system.

What changes Monday: map what you already own to one decision flow before buying anything new.

Integrate, don't procure.

A TUESDAY MORNING INSIDE

the AI-augmented security organization

CVE-2026-3117. Same 9:14. Now watch the org respond.

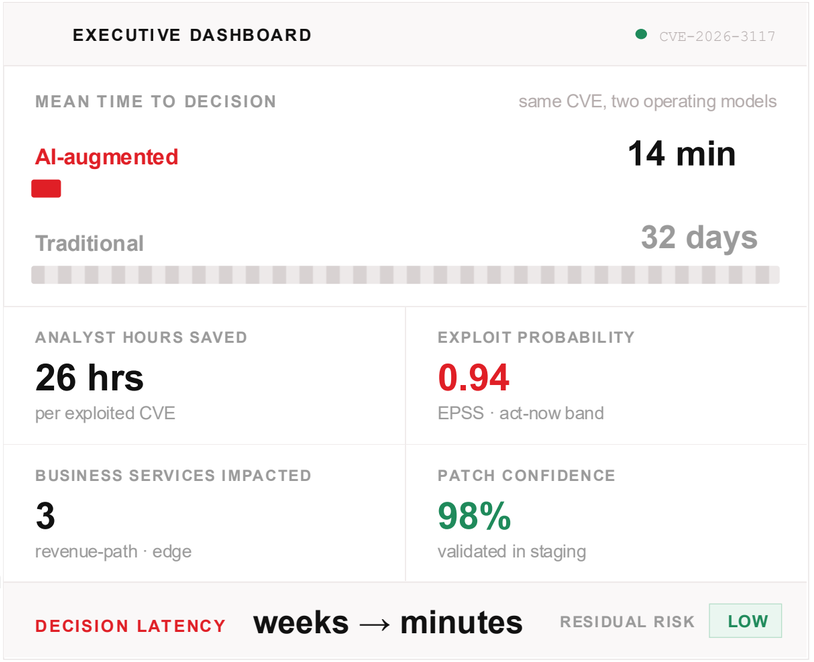
Follow Maya, the on-call vulnerability lead.



9:14

FROM DISCLOSURE TO ACTING — IN MINUTES

09:14	DISCLOSURE	CVE-2026-3117 hits the feed
09:16	THREAT INTEL	exploited-in-wild confirmed
09:18	EXPOSURE	edge-gw-04 · internet-facing
09:21	RISK	live re-score · business-critical
09:23	DECISION	recommended: emergency patch
09:28	ACTION	containment live · patch follows under pre-auth



9:28

A human decides.

9:14

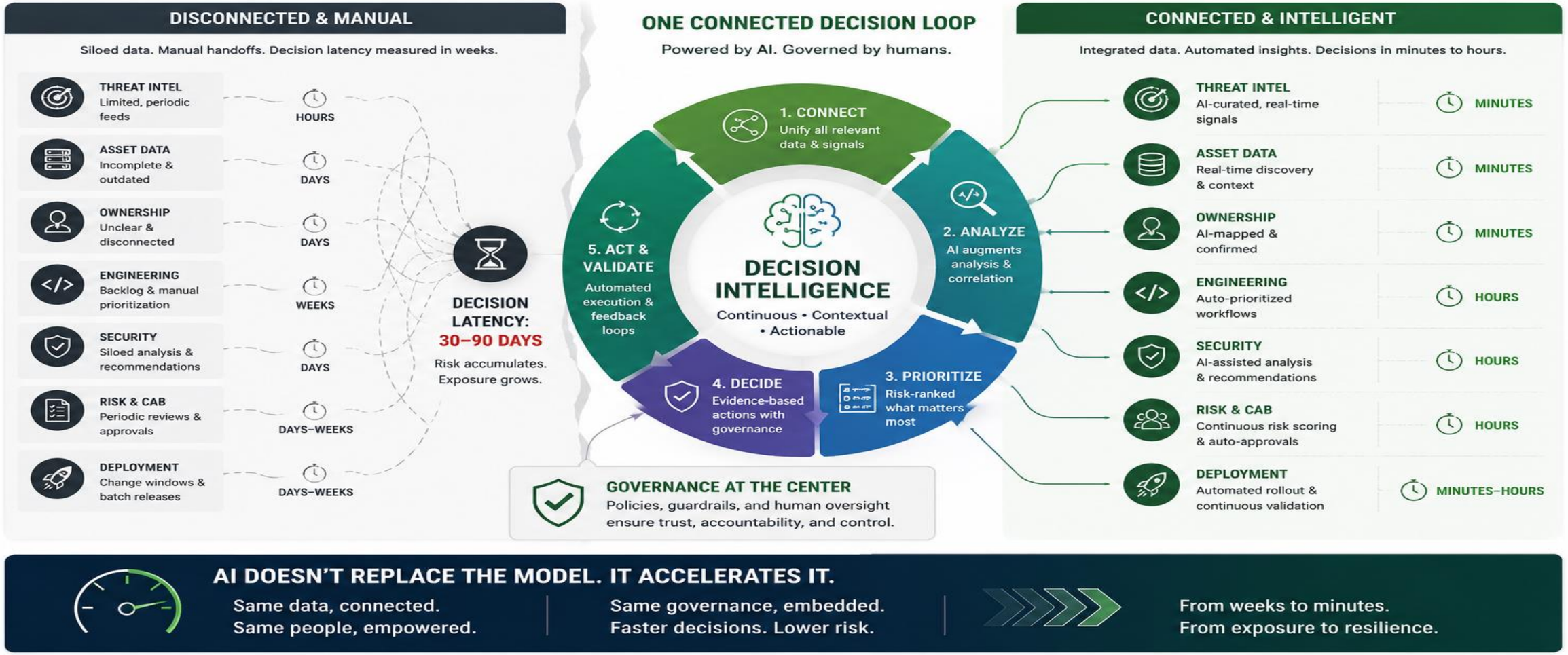
9:18

9:23



AI AMPLIFIES THE OPERATING MODEL

The model creates the value. AI accelerates both sides. Governance keeps it trustworthy.



AI DOESN'T REPLACE THE MODEL. IT ACCELERATES IT.

Same data, connected.
Same people, empowered.

Same governance, embedded.
Faster decisions. Lower risk.

From weeks to minutes.
From exposure to resilience.

Not a product you install.

A way an organization runs.

You don’t **buy** this — you **operate** it. An operating model with an owner and a metric, not a line item.

Technology isn’t the bottleneck — **disconnected data, processes & decisions** are.

Connected data	Connected processes	Connected decisions	Governed automation	Continuous learning



THE CLOCK THAT DECIDES WHO WINS



EXPLOIT

ready in hours

MEAN TIME TO DECISION

14 min

this morning · target < 60 min



DECISION

the gap = **decision latency**

~~**Not how fast you patch.**~~

How fast you decide.

Measure it Monday: **credible signal → authorized decision**. Baseline this quarter.

GOVERNED VELOCITY

Speed and governance aren’t enemies — three things braid them into one line:

SPEED

ACCOUNTABILITY

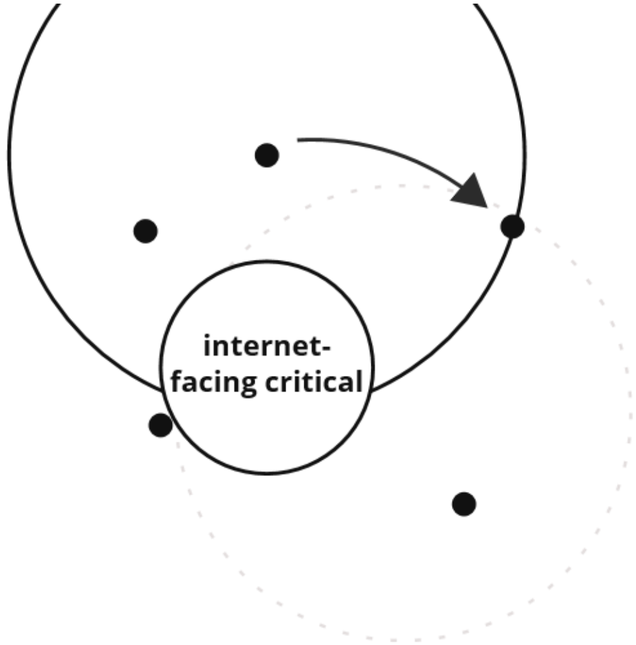


1 **Pre-authorized bounds** blast radius capped · rollback ready

2 **An accountable decision-maker**

3 **An examiner-ready decision record**

Fast. And accountable.



Build it one loop at a time.

Start with the internet-facing critical — the next CVE-2026-3117.

TARGET **decision latency < 1 hour in a quarter**

DAYS 0–30 — exit: 1 loop live

Wire one loop

Internet-facing critical · owner: VM lead + Security Eng · don't wait for a clean CMDB — the loop repairs asset data as it runs

→

DAYS 30–60 — exit: MTTD baselined

Baseline & prove

Measure MTTD; first governed auto-action · owner: Cyber Risk + SOC

→

DAYS 60–90 — exit: MTTD < 1 hr

Expand

Second asset class; board-KPI on decision latency · owner: CISO



EXPLOIT — STILL RUNNING



DECISION — STOPPED, IN BOUNDS

Move fast. And prove it.

They decided how to decide.

THIS MORNING **9:14 → 9:28 · 14 minutes** | THE OLD WAY ~~30–90 days~~

#CORNCON

2026 CORNCON CYBERSECURITY CONFERENCE



Thank You!



Connect on LinkedIn

Sebastiaan Gybels

SVP Cyber Security, Northern Trust

Staying secure in an increasingly complex and chaotic world