methodino®

Cybersecurity Risk, continuously computed

Computed Security Intelligence –

Context your SIEM can’t generate.

Authors Erik Witte, Jeffrey Nelissen, Andre Sibov

Date April 29th, 2026

Executive Overview

Most SOCs believe they operate at maturity Level 4. In practice, they operate at Level 2 — with a Level 4 price tag. The reason is not a failure of tooling or intent. It is a failure of data. And unverified data is not just an operational problem. It is an uncomputed risk.

Events are dropped silently. Assets are miscounted. IP addresses contain typos. The result: your SOC draws conclusions from a fraction of the data that actually exists — and your cybersecurity risk exposure is larger than any dashboard shows.

Computed Security Intelligence (CSI) is the intelligence layer that fixes this. Built on the Methodino Data Quality and Semantic Chain Engine, CSI validates every data source before your SOC acts on it — and continuously translates what your infrastructure is doing into quantified, defensible cybersecurity risk.

Risk you can measure. Compliance you can prove. Both, continuously computed.

1. Invisible Data Is Uncomputed Risk

A single typo in an IP address. An open-source SIEM that silently drops events. An asset list last validated months ago. These are not edge cases. They are the norm in enterprise SOC environments.

The consequence is not just incomplete detection. It is uncomputed risk. Every event your SOC cannot see is a risk exposure that cannot be measured, cannot be quantified, and cannot be reported to the board. You are not managing cybersecurity risk. You are managing the fraction of it that happens to be visible.

What we see in the field:

- One IP address typo → 900% difference in visible data
- 11 assets found vs. 16 actual — a 45% blind spot
- 1,600 events visible vs. 148,000 actual
- Active SOC: 22 events visible vs. our 52; 6 IPs vs. our 12
- Elastic Search silently discards events — proven at production scale

You cannot compute the risk you cannot see.

2. The Before / After Picture

Metric	Without CSI	With CSI
Assets discovered	11 found	16 found (+45%)
Events visible	1,600	148,000 (+9,150%)
IP connections	6 connections	12 connections
Data quality	Assumed complete	Validated at 99%+
SOC maturity	Self-rated: 4	Verified: Level 5 – 6
Cybersecurity risk	Partially visible	Continuously computed

3. Why Existing Tools Cannot Solve This

SIEM platforms are built to detect threats, not to validate the data they operate on. Your Splunk or Sentinel deployment surfaces what it receives. If sources are misconfigured, if feeds are partial, if asset data is stale — the SIEM has no mechanism to tell you. It works with what it is given. And what it is given is incomplete.

Category	What it does well	What it cannot do
SIEM (Splunk, Sentinel, Elastic)	Real-time event detection, alerting, correlation	Validate that the data it receives is complete or accurate
GRC / Compliance tools	Control frameworks, workflow, audit coordination	Connect to live SOC data; validate operational state
CMDB / Asset management	Record-keeping, configuration items	Detect when records diverge from actual infrastructure
Managed SOC / MSSP	24/7 monitoring, triage, incident response	Guarantee data completeness before analysts act on it

No existing security platform validates that the data it operates on is complete. Computed Security Intelligence is that validation layer — and the risk computation layer that sits above it.

4. Computed Security Intelligence: The Architecture

CSI operates in four integrated functions:

Data Quality Engine — every source, every feed, every asset is validated before conclusions are drawn. Silently dropped events are detected. Misconfigured sources are flagged. Typos in critical identifiers are corrected. (Trust Core Foundation)

Semantic Chain View — end-to-end visibility across IT, OT, and network layers. Relationships between assets, events, and identities are mapped semantically — revealing chain-level context that raw event data cannot. (Trust Core Foundation)

Cybersecurity Risk Computation — validated event data is translated into quantified risk exposure via FAIR-based methodology. Cyber events become financial risk figures — defensible to the CRO and board. (Computed Security Intelligence)

Continuous Compliance Overlay — NIS2, ISO 27001, and DORA compliance are continuously validated — not periodically assessed. Evidence is generated automatically, not manually assembled. (Module: Computed Compliance Automation)

5. The SOC Maturity Ladder – Where CSI Applies

Level	Name	Core Capability	With Computed Security Intelligence
1	Initial	Ad hoc monitoring, business hours only	—
2	Managed	24/7 coverage. Basic SIEM. First playbooks	—
3	Defined	Standardized processes. Threat hunting. MITRE ATT&CK mapped	DQ gaps first identified here
4	Optimized	Automated response. AI-assisted detection. Full MITRE coverage	Continuous DQ closes the blind spot at L4
5	Innovative	Predictive AI/ML-native SOC. Follow-the-sun. Nation-state threat hunting	Verifies what L5 assumes: complete data
6	Assured	All L5 capabilities + 99%+ data accuracy continuously guaranteed	Defined and delivered by Methodino

Level 6 does not yet exist in the market. Methodino defines it.

6. Proof at Scale: Ministry of Justice, Netherlands

The Dutch Ministry of Justice deployed CSI across one of the most complex IT/OT environments in Dutch government. Results were validated by JIO's own auditors.

99%+ data accuracy — auditor-validated; **33×** faster issue resolution; **2 days** audit preparation — was 6 weeks; **€1.6M+** annual savings documented; **2,116** firewall policy issues resolved in 6 weeks; **4** frameworks live simultaneously: ISO 27001, NIST, NIS2, BIO2

"We had seven data sources that contradicted each other. Our data accuracy was 40%. Audit preparation took six weeks — and we still found gaps during the assessment."
Department Head, Infrastructure, Platforms & Workplace, Ministry of Justice, Netherlands

The same DQ Engine and Semantic Chain Engine that delivered these results is the same engine that powers Computed Security Intelligence in your environment

7. What This Means by Role

For the CISO Real-time visibility into control execution status across your full attack surface. Cybersecurity risk expressed in financial terms — not as a maturity score, but as a quantified exposure figure. Evidence continuously generated, not manually assembled before every audit.

For the SOC Lead Know where you actually are on the maturity ladder, not where you believe you are. Every data source validated before your analysts act on it. False positives reduced. True risk surfaced.

For the CRO Cybersecurity risk quantified in the same financial language as enterprise risk. FAIR-based figures that connect your security posture to your risk register — and your board conversation.

For the Board One number. One picture. Cybersecurity risk that is computed, not estimated — and defensible to any regulator, insurer, or counterparty that asks.

Computed Security Intelligence answers the question every CISO needs answered in real time: where are we vulnerable right now?

8. Business Case

Cost Driver	Current State	With CSI
Audit preparation labour	6 weeks x team cost	2 days – saving **~€520k**/year
Risk exposure reduction	Unquantified / assumed	**€8.1M** reduction (FAIR-validated)
Compliance operational overhead	13% of IT budget	Up to **80%** reduction
Issue resolution speed	baseline	**33x** faster
Data accuracy	Self-assessed	**99%+** continuously validated
Total documented ROI	--	**€1.6M+** annual savings (ref: JIO)

9. Engagement Model

Intelligence Layer Add-on — deploy the Methodino DQ Engine on top of your existing Splunk environment. Immediate visibility uplift. No SOC transition required. From €150K/year.

SOC Intelligence Upgrade — work alongside your existing MSP or internal SOC. You keep operations; Methodino brings the computed intelligence. From €350K/year.

Full Elite SOC Service — Methodino manages Splunk Enterprise Security end-to-end, with full DQ assurance, risk computation, and compliance automation. €500K–€2M/year.

Elite SOC + Compliance Automation — full Elite SOC Service combined with continuous multi-framework compliance. From €2M/year.

Next step: Free SOC Data Quality Audit

In 2–4 weeks, we show you the gap between what your SOC currently sees and what is actually there — and what that gap means in quantified risk exposure. No commitment. Just proof.

About Methodino

Methodino builds Computed Risk Intelligence infrastructure — the semantic foundation that computes compliance, financial risk, and AI governance continuously from live system behaviour.

Computed Governance covers three questions: Are we compliant? What is our financial exposure? Are we in control of AI behaviour? Computed Security Intelligence answers a fourth: Where are we vulnerable right now?

Operating beneath GRC, SIEM, and security tools, Methodino connects fragmented data sources into one computed truth. Risk you can measure. Compliance you can prove. Both, continuously.

Proven at the Dutch Ministry of Justice. Deployed across government, financial services, and critical infrastructure.

Contact

methodino.ai – info@methodino.ai

Roy Hoogland, CRO – roy.hoogland@methodino.ai

Your next step

The leaders who act now
will define the governance standards for the AI era.

Those who wait risk being defined by them.

Start computing your risk.

Book an Executive Briefing

methodino®