WHITEPAPER

Computed Security Intelligence

Why your SOC draws conclusions from a fraction of the data that actually exists — and what to do about it.

Methodino · methodino.ai
Version 1.0 · 2026 · Confidential — Not for distribution

Executive Summary

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. 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.

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 closes the gap between what your infrastructure is doing and what your SOC believes it is doing.

900%	148K	99%+	Level 6
more data from a single DQ fix	events vs. 1,600 actually visible	data accuracy (ref: Ministry of Justice)	Assured SOC — defined by Methodino

01 The Uncomfortable Truth About Your SOC Data

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. And their consequences are severe.

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

Why this matters:

Your SOC can only respond to threats it can see. Incomplete data means incomplete detection. The threats you miss are not theoretical — they are live, in your environment, invisible to your current tooling.

- 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 are not at maturity Level 4. You are at Level 2 — with a Level 4 price tag.

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 (+100%)**
Data quality	Assumed complete	**Validated at 99%+**
SOC maturity	Self-rated: 4	**Verified: Level 5–6**

Numbers derived from a single Methodino deployment. Client environment: production enterprise SOC with active Splunk SIEM.

02 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 simply works with what it is given.

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. CSI is that validation layer.

03 Computed Security Intelligence: The Architecture

CSI is not a replacement for your SIEM. It is the layer that makes your SIEM truthful. It 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.

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.

Continuous Compliance Overlay

NIS2, ISO 27001, and DORA compliance are continuously validated — not periodically assessed. Evidence is generated automatically, not manually assembled.

Maturity Verification

We show you where you actually are, not where you believe you are. Self-assessed maturity claims are tested against the verified data state.

04 The SOC Maturity Ladder — Where CSI Applies

CSI does not operate at a single maturity level. It is relevant from Level 3 onward — and definitively resolves the data reliability question at Level 4 and above.

Level	Name	Core Capability	Role of CSI
1	Initial	Ad hoc monitoring, business hours only.	—
2	Managed	24/7 coverage. Basic SIEM. First playbooks.	—
3	Defined	Standardised processes. Threat hunting. MITRE ATT&CK mapped.	DQ gaps first identified here.
4	Optimised	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.

05 Proof at Scale: Ministry of Justice, Netherlands

The Dutch Ministry of Justice (Justitiële Informatiedienst — JIO) is one of the most complex IT/OT environments in Dutch government: 28 firewalls across three vendors, seven contradictory data sources, and audit cycles consuming six weeks per cycle. CSI was deployed across this environment. The results were auditor-validated.

99%+	33×	2 days	€1.6M+
data accuracy — auditor-validated	faster issue resolution	audit prep (was 6 weeks)	annual savings documented

What was deployed:

- 2,116 firewall policy issues resolved in 6 weeks
- 4 frameworks live simultaneously: ISO 27001, NIST, NIS2, BIO2
- 50% automation of change impact analysis
- Seven previously contradictory data sources unified
- Audit preparation reduced from 6 weeks to 2 days

What this means for your SOC:

The same DQ Engine and Semantic Chain Engine that delivered these results at JIO is the same engine that powers CSI in your environment. The platform is not adapted for each deployment — the intelligence is structural.

> *"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**

06 Business Case

The financial case for CSI rests on four quantifiable drivers: reduced audit labour, faster issue resolution, lower compliance overhead, and improved risk posture. The JIO deployment provides the reference baseline.

Cost Driver	Current State	With CSI
Audit preparation labour	6 weeks × 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	**33× faster**
Data accuracy	Self-assessed	**99%+ continuously validated**
Total documented ROI (JIO)	—	**€1.6M+ annual savings**

Reference figures derived from the JIO deployment and validated by JIO's own auditors. FAIR-based risk figures computed using the Methodino QUANT module.

07 Engagement Model

CSI is available in three engagement configurations, depending on your current SOC maturity, existing tooling, and desired level of operational involvement.

Service Tier	Scope	Investment
Intelligence Layer Add-on	Deploy the Methodino DQ Engine on top of your existing Splunk environment.	**From €150K/year**
SOC Intelligence Upgrade	Work alongside your existing MSP or internal SOC. You keep operations; Methodino brings the intelligence.	**From €350K/year**
Full Elite SOC Service	Methodino manages Splunk Enterprise Security end-to-end, with full DQ assurance and compliance automation.	**€500K – €2M/year**
Elite SOC + Compliance Automation	Full Elite SOC Service combined with continuous multi-framework compliance.	**From €2M/year**

All configurations include the Methodino DQ Engine, Semantic Chain View, and a structured on-boarding process. The Free SOC Data Quality Audit is the standard entry point.

08 Next Step

The gap between what your SOC sees and what is actually there is measurable. We measure it in 2–4 weeks, at no cost, with no obligation. The audit result is yours regardless of what you decide next.

Start with a 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. No commitment. Just proof.

Contact: Roy Hoogland, CRO — roy.hoogland@methodino.ai
Web: methodino.ai

Computed Security Intelligence is a product of Methodino (Shield ICT B.V.). Registered under KVK 62505300. methodino.ai