

CARTINT

AI-Native Automotive Threat Intelligence and Compliance
Acceleration

ANALYST WORKLOAD

-87%

COMPLIANCE ACCELERATION

-79%

THREAT THROUGHPUT

8x

Reducing analyst workload by 87% and accelerating compliance by 79%.

- whoami



Rolando Doromal, Jr.
Auto Threat Researcher
VicOne

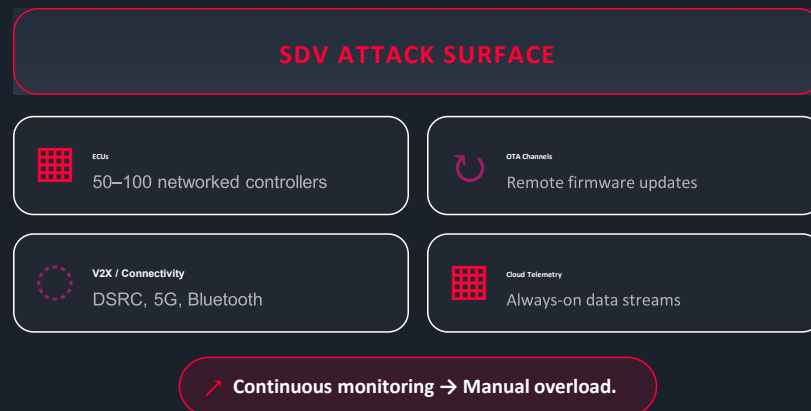


Reuel Magistrado
Auto Threat Researcher
VicOne

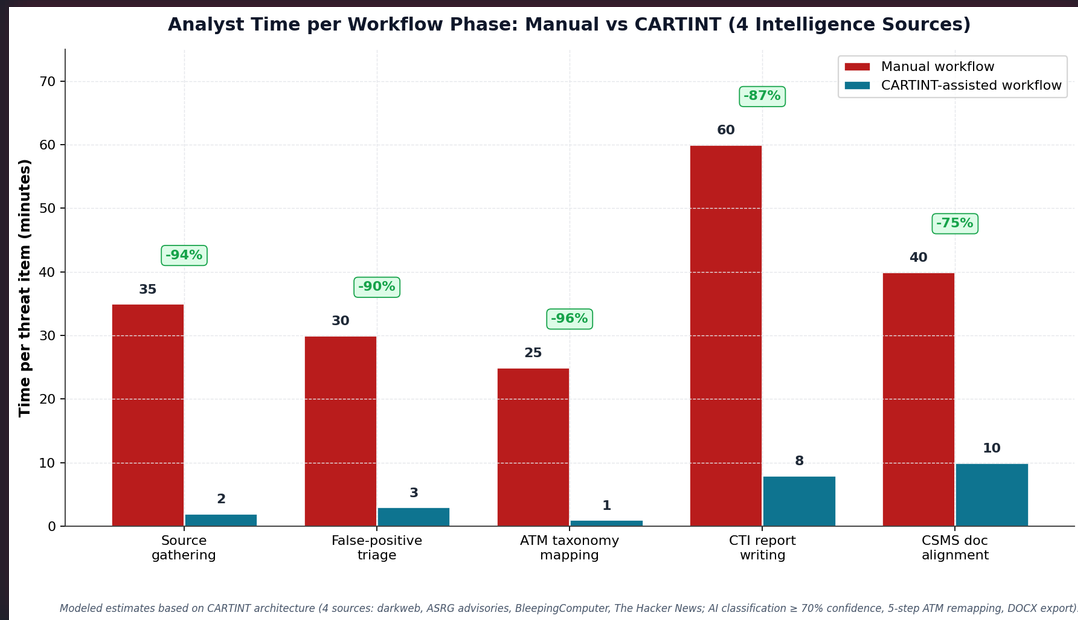
Automotive cybersecurity now demands **AI-Native intelligence**, not **intelligence**, not manual analysis.

Modern vehicles are software-defined systems. A single platform now carries dozens of networked ECUs, persistent OTA update channels, cloud telemetry links, and V2X interfaces — collapsing the once-isolated vehicle into a continuously connected attack surface that evolves with every firmware push.

Regulators have responded. UN ECE R155 §7.4.2 and ISO/SAE 21434 Clause 9 both mandate continuous monitoring of cyber threats against vehicles in the field, plus structured reporting into the CSMS evidence pack. Yet most pack. Yet most VSOC teams still execute that obligation through manual, fragmented workflows — spreadsheets, browser tabs, and copy-paste into audit audit templates.



Manual CTI workflows consume **190 minutes** per threat item — and cap throughput at **~2.5 items / analyst / day**.



Per-phase reduction with CARTINT

1. Source gathering **-94%**
2. False-positive triage **-90%**
3. ATM taxonomy mapping **-96%**
4. CTI report writing **-87%**
5. CSMS documentation **-75%**

📉 **Total: 190 min → 24 min per item (-87%)**

Figure 3-1. Analyst time per workflow phase — manual vs CARTINT-assisted (minutes per threat item). Modeled estimates.

How can automotive teams automate
automate threat relevance, ATM
mapping, and CTI reporting at scale —
— *without increasing analyst headcount
headcount or manual workload?*

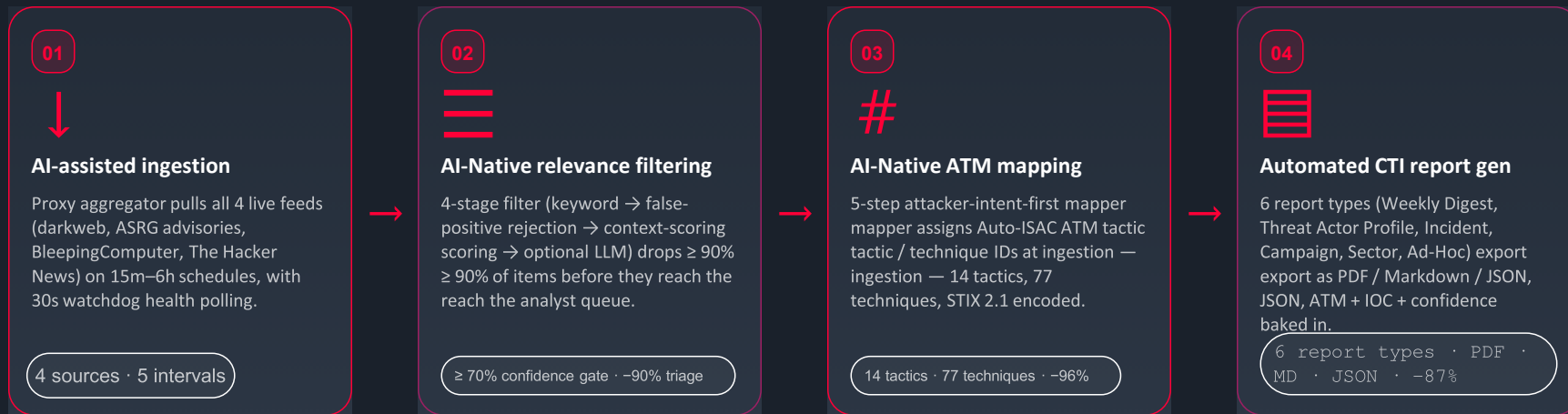
THE CHALLENGE

The obligation under R155 §7.4.2 and ISO 21434 Clause 9 is continuous — but the operating budget for VSOC teams is not. Scaling monitoring cannot mean scaling headcount.



CARTINT delivers **AI-Native automation** across ingestion, filtering, mapping, and reporting.

A single pipeline replaces four previously manual, disconnected sub-tasks. Every stage is AI-assisted; every output is structured for the Auto-ISAC ATM (STIX 2.1) and ready for CSMS documentation.



Every stage **compounds**: each downstream step depends on the upstream output. Removing any one stage collapses the chain.

AI-Native filtering eliminates **90%** of false positives — and collapses triage time from **30 minutes to 3.**

4-STAGE RELEVANCE PIPELINE

01



Keyword pre-filter

Automotive vocabulary (OEM names, ECU types, CAN/OTA protocols) rejects obvious non-matches.



02



False-positive rejection

Heuristic rules drop duplicates, marketing marketing noise, and non-automotive CVEs.



03



Context scoring

ML classifier scores automotive relevance 0–100%.



04



Optional LLM review

Edge cases routed to LLM for final judgment; $\geq 70\%$ confidence required to advance.

→ ATM MAPPER · NEXT STAGE

-90%

TRIAGE TIME REDUCTION
30 min → 3 min per item

 $\geq 70\%$

CONFIDENCE THRESHOLD
Architectural constant (C3)

4

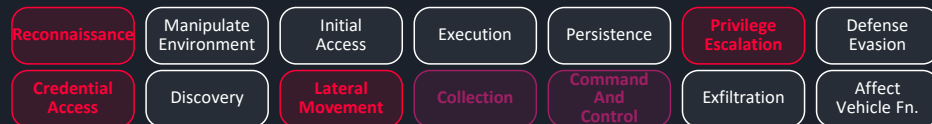
FILTER STAGES
keyword → FP → context → LLM

~6%

ANALYST TIME ON FP (POST-AI)
Ponemon: was 27% pre-AI (B4)

A 5-step **attacker-intent-first** mapper cuts taxonomy mapping time by **96%** — and produces automotive-native intelligence artifacts at ingestion.

AUTO-ISAC AUTOMOTIVE THREAT MATRIX · 14 TACTICS · 77 TECHNIQUES



● CARTINT mapping focus (4) ● Purple-tagged (2) ● Other tactics (8)

STIX 2.1 encoded · 7,024 objects · 384 KB bundle

5-STEP ATTACKER-INTENT-FIRST MAPPER

- 01 Extract IOCs & context from the ingested item.
- 02 Identify attacker intent — what the adversary wants to achieve.
- 03 Map intent → candidate ATM tactics (1..N).
- 04 Drill into techniques (77) using item context.
- 05 Assign confidence + emit STIX 2.1 artifact for CSMS.

25 min → 1 min per item · **-96%** mapping time

Mapping to ATM at ingestion — not MITRE ATT&CK Enterprise — is what makes the downstream report generation and CSMS alignment automatable. There is no translation layer between the intelligence artifact and the automotive practitioner.

Automated report generation cuts writing time by **87%** — and exports directly as **PDF · Markdown · JSON** for CSMS integration.

SIX REPORT TYPES · AUTO-DRAFTED

Weekly Digest

Roll-up of accepted threats in the past 7 days for VSOC leadership review.

WEEKLY

Threat Actor Profile

Consolidated profile of a tracked actor with mapped ATM tactics and historical IOCs.

ACTOR

Incident Report

Time-ordered incident narrative with timeline, IOCs, and CSMS-ready evidence pack.

INCIDENT

Campaign Analysis

Cross-incident pattern analysis linking campaigns across sources and time windows.

CAMPAIGN

Sector Assessment

Automotive-sector trend view across OEMs, ECU families, and threat categories.

SECTOR

Ad-Hoc

Analyst-defined template; AI streams a draft from selected items + ATM context.

AD-HOC

THREE EXPORT FORMATS · CSMS-READY

PDF

MARKDOWN

JSON

cartint_incident_report_2026-07-08.pdf

CARTINT · Incident Report

Tactic	Technique	Confidence	IOC
Initial Access	T1659	0.86	hash:...a3f9
Lateral Movement	T1485	0.91	ip:10.0.4.12

STIX 2.1 aligned · ATM 14/77 · Confidence ≥ 70%

PDF

Audit-ready CSMS evidence packs
packs · regulator submission.

MARKDOWN

Analyst review & wiki / ticketing
integration.

JSON

STIX 2.1 native · ISAC / TAXII
programmatic sharing.

60 min → 8 min per report

-87% writing time

AI-Native automation flips analyst focus from **86% operational** to **75% strategic**.

BEFORE CARTINT

Five operational categories consume the week — hunting gets ~14%.

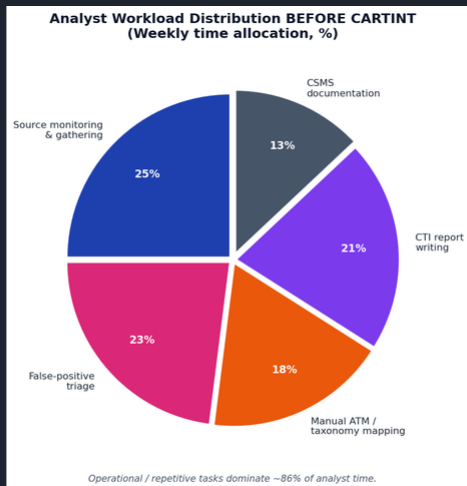


Figure 4-1. Analyst workload distribution BEFORE CARTINT — operational categories dominate ~86% of weekly time.

AFTER CARTINT

Strategic share rises to ~75% — hunting, validation, tuning, advisory.

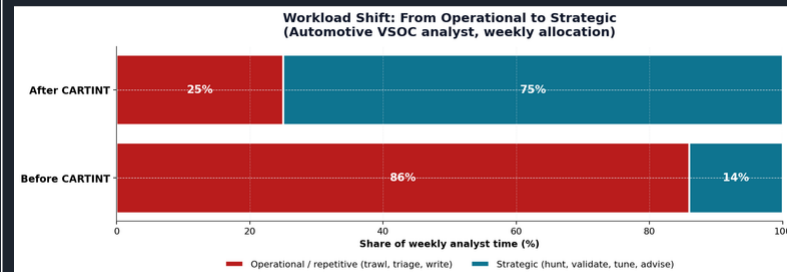


Figure 4-2. Workload shift — operational vs strategic share, before vs after CARTINT.

OPERATIONAL

86% → 25%

STRATEGIC

14% → 75%

BURNOUT DRIVER

Repetitive ingest → Hunting

CARTINT accelerates CSMS workflows by **79%** on average — across six regulatory phases.

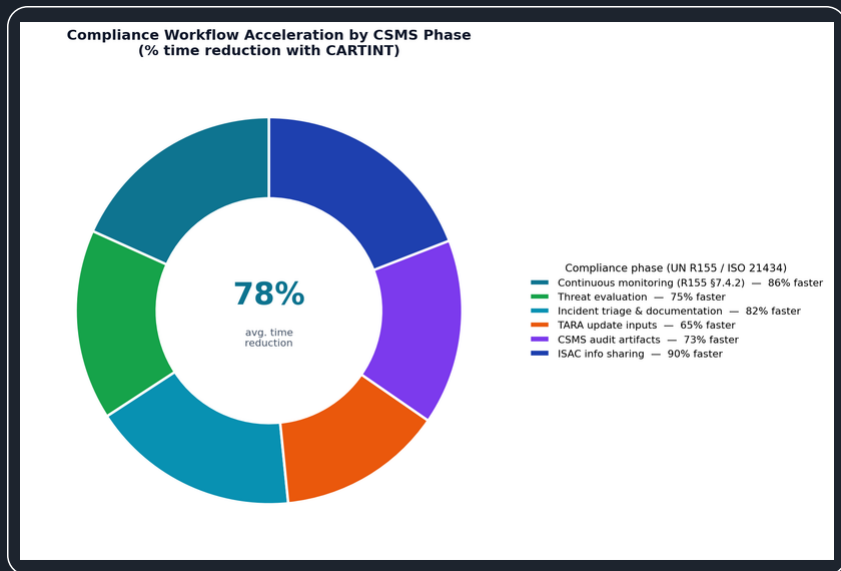
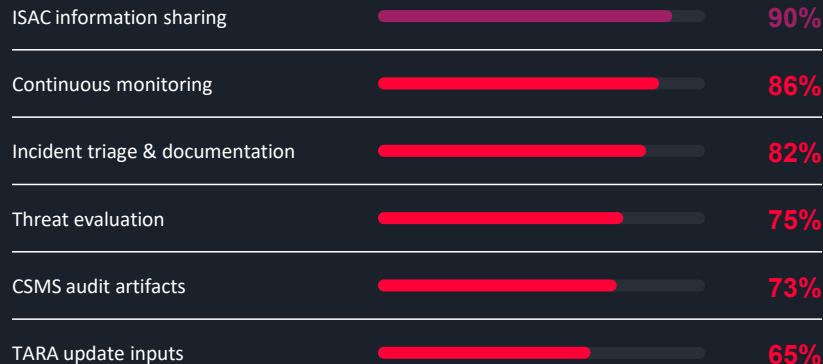


Figure 4-3. Compliance workflow acceleration by CSMS phase — % time reduction with CARTINT. Average: 79%.

PER-PHASE ACCELERATION



AVERAGE

79%

TARA acceleration is capped at 65% because CARTINT shortens input-gathering but not the human risk-assessment step.

See CARTINT's **AI-Native pipeline** in action — from ingestion to ATM mapping to CTI export.

localhost:3000 · cartint dashboard

Dashboard

Intel

ATM Matrix

Reports

Sources

AI CONFIDENCE ≥ 70% 4 SOURCES ACTIVE

CAN-bus injection exploit listed on dark-web forum

BLEEPINGCOMPUTER T0007 · Credential Access

Tesla infotainment bypass sold on Telegram channel

ASRG T0012 · Network Injection

BMW procedure object leak via misconfigured S3 bucket

AUTO-ISAC T0002 · Lateral Movement

OTA update signing-key compromise rumor surfaced

RECORDED FUTURE T0014 · Supply Chain

GNSS spoofing kit targeting ADAS, repo on GitHub

BLEEPINGCOMPUTER T0008 · Position Spoofing

ATM MATRIX · LIVE OVERLAY

P00		P03	
	P10		P13
		P20	

12 cells 3 red · 2 purple

Watchdog: 30s poll OK WebSocket: connected Last scrape: 47s ago

CARTINT v0.9 · BUILD 2026.07

1 INGEST

Watch a new dark-web listing hit the feed via WebSocket.

2 MAP

AI classifier scores relevance; ATM mapper assigns T0007 / T0012 within ~1s.

3 EXPORT

Analyst clicks Export → PDF / Markdown / JSON Incident Report lands in CSMS folder, 8 min later.

AI-Native automation reduces analyst time by **87%** and accelerates compliance by **79%**.

PER-ITEM HANDLING TIME

190 → 24 min

↘ -87%

Source + triage + ATM + report + CSMS — five phases compressed into validation.

THROUGHPUT MULTIPLIER

8×

2.5 → 20 items / analyst / day

480 productive minutes / 24 min per item, vs 190 min manual.

WORKLOAD MIX

86% → 25%

operational share · strategic rises 14 → 75%

Hunting, validation, tuning, advisory — the role regulators expect.

COMPLIANCE ACCELERATION

79%

average across 6 CSMS phases

ISAC sharing 90% · continuous monitoring 86% · TARA inputs 65% (capped by human judgment).

✦ **CARTINT transforms** VSOC operations from manual fragmentation to structured, compliant efficiency.

Next steps to validate and extend AI-Native performance — from modeled estimates to **audit-grade evidence**.

ID	Priority	Recommendation	Expected Impact	Validation
R-1	P0	Run a controlled time-and-motion study in 2–3 pilot VSOs (manual vs CARTINT) over 4 weeks.	Converts modeled estimates into auditable evidence for R155 / 21434 audits.	Compare per-item handling time; publish precision/recall.
R-2	P1	Add a TARA-hook integration that ingests accepted CARTINT threats as TARA input candidates (ISO/SAE 21434 Clause 15).	Lifts the lowest-acceleration phase (65%) toward 80%+.	Pilot with 1 OEM TARA template; measure input-gathering time.
R-3	P1	Ship the planned STIX/TAXII export and validate against Auto-ISAC ingestion.	Locks in the 90% ISAC-sharing acceleration; removes re-keying.	Round-trip test: export → ISAC → re-import.
R-4	P1	Publish precision / recall baselines for the AI classifier against a curated automotive CVE dataset.	Quantifies the false-positive gate's real-world performance.	Use Tesla (ATM-P0001..P0005) and BMW procedure objects as ground truth.
R-5	P2	Package an air-gapped deployment mode (local Ollama, no external API) for OEM restricted environments.	Removes the procurement / data-residency blocker for Tier-1 deployments.	Benchmark Ollama Llama3.2 vs Z.AI on classification accuracy.

Sequencing: R-1 first (validates every downstream business case); R-2 + R-3 in parallel (close the two largest compliance gaps); R-4 gates production rollout; R-5 unlocks Tier-1 OEM.

AI-Native automation is the future of automotive cyber threat intelligence.

CARTINT demonstrates how AI can transform compliance and threat monitoring from manual burden to strategic advantage. It is open-source. It is open-source, automotive-native, and ready for industry validation.

VICONE

*“Driving Automotive Cybersecurity Forward.”
Forward.”*

OPEN-SOURCE REPO

github.com/reuelmagistrado/cartint ↗

EVIDENCE

Analyst Workload Report · Evidence Traceability Supplement