

Compellio Launches New Solution to Enable Verifiable Data in Cybersecurity and Threat Intelligence Exchange



Compellio, a pioneer in bridging decentralised and centralised trust infrastructures, announces the launch of its plug-and-play solution designed to bring cryptographically verifiable data and auditable workflows to cybersecurity operations and Cyber Threat Intelligence (CTI) exchanges.

The open-source, self-hostable component allows Security Operations Centers (SOCs), Managed Security Service Providers (MSSPs), Small and Medium Enterprises (SMEs), and DevSecOps teams to generate non-repudiable proof of threat detections without exposing sensitive operational context or internal infrastructure blueprints.

Solving the Zero-Trust Dilemma in Modern Incident Response

As regulatory frameworks such as NIS2 take effect and contractual incident response SLAs tighten, organizations face an urgent dilemma: **how to prove exactly when a threat signal was detected without handing external parties raw telemetry that could leak internal IP addresses, asset topologies, or proprietary data.**

Manual sanitisation or redaction of standard STIX/TAXII threat feeds often destroys precision timestamps and cryptographic integrity, rendering logs unverifiable to third-party auditors,

insurance providers, or cross-sector intel exchanges.

Compellio's new solution eliminates this trade-off through a seamless three-step pipeline:

1. **Ingest:** Native TAXII endpoints ingest standardised STIX threat payloads directly inside the customer's secure boundary.
2. **Abstract:** The engine converts payloads into Tokenized Asset Records (TARs), preserving cryptographically hashed fingerprints and time metadata while stripping out internal operational context.
3. **Anchor:** Using the Compellio Registry API, TARs are automatically anchored to public or private blockchain networks, creating a permanent, tamper-proof record of detection.

Expanding Horizons: Key Application Areas

While the underlying engine is rooted in core threat intelligence, its ability to anchor verifiable telemetry without revealing sensitive state makes it a critical building block across three major technology frontiers:

- **Cyber Threat Intelligence & Trusted Sharing:** Cross-organisational CTI sharing has historically stalled due to mutual distrust and fear of data leaks. Compellio's new solution enables MSSPs, SOCs, and enterprises to share verified detection signals across public or private networks. Because authenticated Registry API endpoints guard against data poisoning and guarantee non-repudiable timestamps, organisations can discover global threat trends collectively, with zero exposure of internal assets.
- **Agentic & AI-Based Operations in Software Supply Chains:** As autonomous AI agents take over software compilation, DevSecOps pipelines, and threat mitigation routines, human oversight can become a bottleneck. By piping agentic workflow signals into the engine, every automated decision, dependency inspection, and code-integrity alert is automatically converted into a TAR and anchored on-chain, creating an unalterable audit trail of AI agent actions for human supervisors and regulators.
- **Dual-Use Applications for Critical Systems:** Infrastructure operating in defense, aerospace, energy, and dual-use technological domains requires extreme security guarantees. The localised abstraction layer allows critical infrastructure operators to emit verifiable compliance proofs to external oversight bodies without ever exposing classified operational parameters or mission-critical system state.

*« Security teams should never be forced to choose between defending operational privacy and demonstrating verifiable accountability, » said **Denis Avrilionis, CEO of Compellio**. « With our new solution, we are providing a lightweight, plug-and-play trust layer that integrates into existing*

security stack workflows, enabling instant verification of detection timelines while keeping raw telemetry strictly within the enterprise boundary. »

Proven at the CyberSuite Hackathon

The capabilities of Compellio's new solution are being showcased during hands-on testing scenarios at the [CyberSuite Hackathon](#). Event participants use standard TAXII producers to simulate threat signals, verifying the end-to-end STIX-to-TAR translation, queue persistence across restarts, and live webhook callbacks from the Registry API to confirm non-repudiable on-chain detection timestamps.

By connecting standard security pipelines directly into immutable ledgers, Compellio is helping set a new standard for transparent, privacy-preserving cybersecurity operations.

Availability

The new Compellio solution is [available as an open-source, containerised component](#) ready for cloud, on-premises, or air-gapped deployments. Organisations can integrate the solution directly via the Compellio Registry API.