Resilmesh
securing cyber infrastructures

From Components to Platform: Ensuring Resilmesh Works End-to-End

Modern cybersecurity systems are increasingly designed as modular ecosystems rather than monolithic tools. Detection engines, intelligence services, data aggregation layers, and mitigation mechanisms coexist within the same environment. However, their real value only emerges when they operate as a coordinated and validated platform.

Resilmesh adopts a structured, plane-based architecture to organize its cybersecurity capabilities. Each plane has a defined role, but the strength of the system lies in how these layers interact, exchange information, and support coherent end-to-end workflows, from data collection to automated mitigation.

Transforming architectural design into reliable operational behavior is therefore a key step in evolving from a collection of components to a fully integrated cybersecurity platform.

A Plane-Based Architecture with Complementary Responsibilities

Resilmesh is organized into four primary planes, each contributing to cyber situational awareness and operational resilience.

Aggregation and Collaboration Plane

This plane acts as the system's data pre-processing and interoperability backbone. Components such as Vector, NATS, SLP Enrichment and the MISP Client enable:

- Telemetry collection and transformation
- Message brokering across distributed components
- Indicator enrichment and normalization
- Secure intelligence exchange

By ensuring that heterogeneous data sources are aggregated, normalized and forwarded correctly, this plane enables reliable upstream analysis.

However, connectivity alone is not sufficient. The integrity, consistency and timing of inter-component exchanges must be validated to ensure that downstream processes receive structured and actionable information.

Threat Awareness Plane

The Threat Awareness Plane focuses on real-time monitoring, anomaly detection and intelligence correlation. It incorporates components such as:

- Wazuh (SIEM capabilities)
- AI Correlation (AIC)
- AI-Based Detector (AIBD)
- Federated Learning Anomaly Detector (FLAD)
- Robust Cyber Threat Intelligence (RCTI) including IoB and MISP Server
- Threat Hunting and Forensics (THF)

This plane transforms processed telemetry into security-relevant insights. Detection outputs are propagated through structured channels so they can be contextualized and acted upon.
For the platform to function end-to-end, outputs generated here must remain consistent with the data models and expectations of the upper planes. Validation ensures that alerts are not only generated, but correctly interpreted and consumed by the rest of the system.

Situation Assessment Plane

Detection alone does not provide situational awareness. The Situation Assessment Plane evaluates risks in context, correlating asset information, service dependencies and network status.

It includes components such as:

- CASM (Cyber Asset Attack Surface Management)
- CSA (Critical Service Awareness)
- ISIM (Infrastructure and Service Information Model)
- NSE (Network Status Evaluation)
- NDR (Network Detection and Response)
- SACD (Situation and Network Awareness Consolidated Dashboard)

This plane consolidates technical findings into systemic understanding. It enables visualization of infrastructure relationships, risk aggregation and projection, and contextual interpretation of security events.

The quality of this contextual layer depends directly on the reliability of upstream data flows. Any inconsistency in aggregation or detection may propagate into incomplete situational views. Ensuring consistency across planes is therefore critical to maintaining coherent awareness.

Security Operations Plane

The Security Operations Plane closes the loop by orchestrating mitigation and response. It includes:

- Mitigation Manager (MM)
- Playbooks Tool (PT)
- Workflow Orchestrator (WO)

This plane translates detection and assessment outputs into structured Courses of Action. Based on situational data, mitigation workflows can be selected and executed through predefined playbooks and orchestration mechanisms.

The integration between detection, assessment and mitigation is essential. Alerts must be correctly contextualized before triggering response workflows. Likewise, mitigation outcomes must feed back into the system to preserve situational consistency.
This closed feedback loop transforms Resilmesh from a monitoring solution into a coordinated security platform.

Ensuring Inter-Plane Interaction Works in Practice

While the architectural separation of planes provides clarity and scalability, operational effectiveness depends on validated inter-plane interaction.

End-to-end behavior requires:

- Reliable propagation of telemetry and alerts.
- Consistent data models between enrichment, detection and assessment.
- Verified dependencies between detection outputs and mitigation workflows.
- Predictable behavior under realistic operational constraints.

System-level validation focuses on confirming that the full chain, from aggregation to automated response, behaves coherently. Rather than validating components in isolation, the emphasis is on ensuring that information flows remain intact and meaningful across the entire architecture.

Deployment Automation as an Enabler of Platform Integrity

Beyond architectural interaction, operational readiness also depends on reproducible and reliable deployment.

Resilmesh introduces structured deployment automation mechanisms, including:

- Plane-based modular repository organization.
- Cascading Docker Compose execution.
- Environment-specific deployment profiles (Domain, IT Domain, IoT Domain).
- Centralized orchestration scripts.
- Infrastructure-as-Code provisioning through Terraform for cloud environments.

This approach significantly reduces manual configuration effort and deployment time, while improving repeatability and minimizing human error. Automation plays a critical role in ensuring that the platform behaves consistently across environments. By aligning repository structure with the architectural planes and enabling controlled, environment-aware deployments, Resilmesh strengthens both integration coherence and operational stability.

Zero-touch provisioning and scripted configuration further reduce the probability of misconfiguration, supporting reliable end-to-end functionality.

From Architecture to Operational Confidence

Resilmesh demonstrates how a modular, plane-based cybersecurity architecture can evolve into a unified and deployable platform. Its value lies not only in advanced detection, intelligence or visualization capabilities, but in:

- Coordinated inter-plane interaction
- Structured validation of data flows
- Automated and reproducible deployment
- Integration of detection, assessment and mitigation into a continuous loop

By ensuring that components operate coherently across aggregation, threat awareness, situational assessment and security operations, Resilmesh moves beyond isolated innovation and toward practical, operational cyber situational awareness.

The transformation from components to platform is achieved not merely through architectural design, but through validated interaction, controlled orchestration and automation-driven consistency.

Follow Resilmesh on Social Media:

Funded by the European Union