INTELLIGENCE — LAYER 3

L3 The Intelligence Layer

WHERE TRUSTED ENTITIES BECOME JUDGMENT

L3 is where Converge360 turns trusted entities into judgment. Foundation says **who and what** exists; Intelligence decides what to think about it. Three engines apply three kinds of reasoning — does this **matter**, is it **known-bad**, and what is **actually happening** — assembling the answer into correlated, timeline-ordered incidents that Operations can act on.

WHERE L3 SITS

- L5 Experience
- L4 Operations
- **L3 Intelligence**
- L2 Foundation
- L1 Ingestion & Discovery

COMPONENTS
3
Rule Engine, Threat Intelligence & Correlation Engine.

CONSUMES
Entities + events + feeds
Foundation entities, events and threat feeds.

PRODUCES
Correlated incidents
Timeline-ordered incidents, not raw alerts.

FEEDS INTO
↑ L4
Operations executes the response.

Three engines, one verdict

05
Rule Engine
WHETHER IT MATTERS
Applies detection & policy logic to entities and events — producing rule hits and classifications.

06
Threat Intelligence
WHETHER IT'S KNOWN-BAD
Adds external context — enriched IOCs and adversary intel against the wider threat landscape.

07
Correlation Engine
WHAT'S HAPPENING
Stitches rule hits, threat context and entities into coherent, timeline-ordered incidents.

Why intelligence matters

Raw entities don't defend anything on their own — something has to decide what they mean. Without judgment, every team drowns in undifferentiated signal: real attacks buried beside routine noise, the same incident reported five different ways. Intelligence is where that noise becomes a **verdict**. It scores what matters, flags what's known-bad, and stitches scattered signals into a single coherent story — so the layers above act on **incidents, not alerts**.

From signal to verdict
Detection and policy logic decide what actually deserves attention.

Context from the outside world
External threat intel says whether something is already known-bad.

One story, not many alerts
Scattered signals are stitched into single, timeline-ordered incidents.

COMPONENT 05 · INTELLIGENCE

Rule Engine

Decides whether something matters

Rule Engine decides **whether something matters** — applying detection and policy logic to the entities and events flowing up from Foundation.

Not every event deserves a human's attention. Rule Engine is where that triage happens. It applies detection logic and organizational policy to Foundation entities and the events attached to them, evaluating each against the conditions that define risk in your environment. What it finds, it labels: rule hits that mark something worth looking at, and classifications that say what kind of thing it is. Those judgments become the structured raw material the Correlation Engine later assembles into incidents.

KEY CAPABILITIES

Detection logic
Evaluates entities and events against the conditions that signal risk.

Policy enforcement
Applies your organization's rules and standards consistently, every time.

Classification
Labels what each hit is, so downstream layers can reason about it.

Rule hits at scale
Produces structured findings across the full entity set, continuously.

WHAT IT EVALUATES

DETECTION & POLICY

- **Policy violations**
- **Threshold breaches**
- **Misconfigurations**
- **Behavioral signals**
- **Compliance checks**
- **Known patterns**

The platform's first filter

Rule Engine separates the events that warrant attention from the constant background hum — so **nothing important is lost** and **nothing trivial is escalated**.

← CONSUMES

- Foundation entities from L2
- Events attached to those entities

→ PRODUCES

- Rule hits & classifications
- Structured findings for the Correlation Engine

COMPONENT 06 · INTELLIGENCE

Threat Intelligence

Decides whether something is known-bad

Threat Intelligence decides **whether something is known-bad** — bringing the outside world's knowledge to bear on your entities.

Some threats you can only recognize if you know what's happening beyond your walls. Threat Intelligence adds that external context. It consumes Foundation entities alongside external threat feeds, enriching indicators of compromise and matching your environment against the wider threat landscape — known adversaries, malicious infrastructure, active campaigns. The output is enriched IOCs and threat context: the knowledge of whether something the platform sees is already understood to be dangerous.

KEY CAPABILITIES

IOC enrichment
Augments indicators with reputation, context and confidence.

Adversary intel
Maps activity against known threat actors and active campaigns.

Feed aggregation
Consolidates many external threat feeds into one coherent view.

Known-bad matching
Flags entities and events that match the wider threat landscape.

WHAT IT DRAWS ON

EXTERNAL CONTEXT

- **IOC feeds**
- **Reputation data**
- **Adversary / TTP intel**
- **Malware signatures**
- **Campaign tracking**
- **Vulnerability intel**

Inside meets outside

Rule Engine asks whether something matches **your rules**; Threat Intelligence asks whether **the rest of the world** already considers it dangerous — judging from the inside and the outside at once.

← CONSUMES

- Foundation entities from L2
- External threat intelligence feeds

→ PRODUCES

- Enriched IOCs & threat context
- Known-bad signals for the Correlation Engine

COMPONENT 07 · INTELLIGENCE

Correlation Engine

Decides what is actually happening

Correlation Engine decides **what is actually happening** — stitching rule hits, threat context and entities into coherent, timeline-ordered incidents.

A single attack scatters itself across dozens of signals: a rule hit here, a known-bad indicator there, three entities that only matter once you see them together. Correlation Engine is where those fragments become a story. It consumes the rule hits from Rule Engine, the threat context from Threat Intelligence and the canonical entities from Foundation, then links related signals across time and connection into single, coherent incidents — each one timeline-ordered, so responders see not just that something happened, but the sequence of how it unfolded.

KEY CAPABILITIES

Signal stitching
Links related rule hits, indicators and entities into one incident.

Timeline assembly
Orders events chronologically so the story reads end to end.

Entity correlation
Connects the who and what across otherwise separate signals.

Incident creation
Produces coherent incidents ready for Operations to act on.

WHAT IT ASSEMBLES

INTO INCIDENTS

- **Related rule hits**
- **Threat indicators**
- **Linked entities**
- **Event sequences**
- **Attack timelines**
- **Coherent incidents**

Where the three engines meet

Rule Engine says **what matters**, Threat Intelligence says **what's known-bad** — and Correlation Engine brings both together with the entities to answer the only question that triggers a response: **what is actually happening?**

← CONSUMES

- Rule hits + threat context
- Canonical entities from Foundation

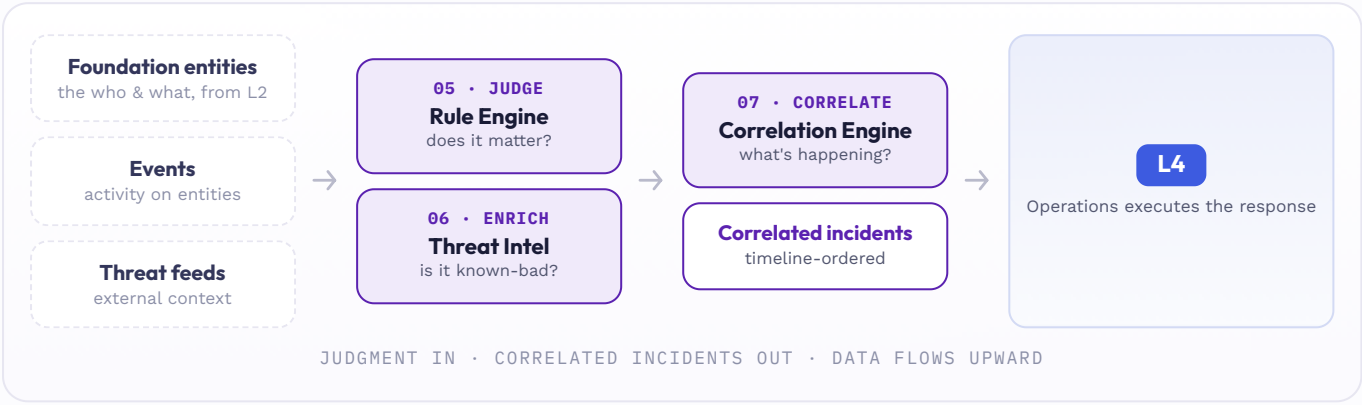
→ PRODUCES

- Correlated, timeline-ordered incidents
- Incidents & timelines for L4 Operations

HOW L3 WORKS AS ONE LAYER

Three engines. One verdict.

Rule Engine decides what matters, Threat Intelligence decides what's known-bad, and Correlation Engine brings both together with the entities beneath them. The result is the layer's whole purpose: not more alerts, but coherent, timeline-ordered incidents — the single, trustworthy answer to "what is actually happening" that Operations needs before it acts.



CROSS-CUTTING · AGENTIC AI / LLM FABRIC

Judgment is exactly where reasoning helps most.

The agentic fabric threads through all five layers, including this one. At L3 it helps **weigh ambiguous signals**, **draft the rationale behind each rule hit**, correlate across feeds faster than a human could, and **propose the incident narrative** — so analysts review conclusions instead of assembling them.

COMPONENT	CONSUMES	PRODUCES	DOWNSTREAM
Rule Engine	Foundation entities + events	Rule hits, classifications	→ L4
Threat Intelligence	Foundation entities + threat feeds	Enriched IOCs, threat context	→ L4
Correlation Engine	Rule hits + threat context + entities	Correlated incidents, timelines	→ L4

Incidents, not alerts

Scattered signals become coherent, timeline-ordered incidents.

Inside and outside context

Your policy and the world's threat intel judge every signal together.

Ready to act on

Operations receives verdicts to respond to, not noise to triage.

Intelligence turns trusted entities into a verdict — what matters, what's known-bad, and what is actually happening.