# LOGFORCE: Architectural Overview of SEB and SynA

LOGFORCE R&D Team

May 9, 2025

## Abstract

This document presents a comprehensive architectural overview of SEB (Synthetic Endpoint Brain) and SynA (Synthetic Analyst), two foundational components of the LOGFORCE cybersecurity platform. Through modular endpoint instrumentation and centralized explainable AI, LOGFORCE delivers real-time, autonomous threat investigation and response.

## 1 LOGFORCE Framework Overview

LOGFORCE is an autonomous cybersecurity system built around two synergistic components:

**SEB (Synthetic Endpoint Brain)**: A modular, lightweight agent that resides on endpoints to monitor behavior, capture system telemetry, and execute investigations.

**SynA (Synthetic Analyst)**: A centralized AI engine that orchestrates investigations, interprets findings, and continuously improves through user feedback and telemetry.

Together, SEB and SynA enable autonomous, explainable, and adaptive endpoint protection.

## 2 SEB – Synthetic Endpoint Brain

### Role

SEB is deployed directly on endpoints and acts as a localized analyst. It is highly modular and lightweight, with collectors that ingest behavior and exporters that deliver findings.

### Architecture

- **Collectors**: Modular plugins that monitor system activities such as DNS queries, process creation, and file access.

- **Exporters**: Send output data to external systems like HTTP endpoints (webhook) or cloud storage (e.g., GCS).
- **Core**: Handles configuration parsing, unified event schema, and dynamic CLI integration.

### Execution Modes

**Standalone**: Acts as a local telemetry collector and investigator. **Connected**: Integrates with LOGFORCE backend and SynA to support AI-driven tasks, feedback loops, and investigation lifecycle management.

## 3 SynA – Synthetic Analyst

### Role

SynA is the centralized intelligence engine behind LOGFORCE. It coordinates investigations, enriches findings, and evolves its models based on feedback from users and endpoint agents.

### Capabilities

- Accepts data from SEB and other sources.
- Tasks SEB with verification steps (e.g., binary signature checks, user validation).
- Provides explainable conclusions (XAI) to guide further actions.
- Stores knowledge in LMMDB (Lighting), including results, errors, and natural language feedback.

### Model Evolution and Knowledge Tokenization

To incentivize community participation and reward validated contributions to detection logic, LOGFORCE introduces a novel tokenized feedback mechanism, powered by the **Sophia NFT framework**.

- Each verified improvement or analytical suggestion, once adopted by SynA, is minted as a **non-fungible token (NFT)**.
- These NFTs are uniquely linked to the investigative or heuristic logic they represent and include metadata such as contributor identity, model lineage, and deployment frequency.
- NFT holders acquire a **traceable ownership stake** in the decision logic of the model, enabling a decentralized and incentivized contribution model.

- The Sophia framework introduces an optional **crypto-token economy** where model usage metrics could translate to micro-royalty payouts to NFT holders.

This system transforms model evolution into a community-owned process, ensuring high-quality detection logic is fairly recognized and cryptographically attributed.

## 4 SynA + SEB Interaction Workflow

1. **Detection**: LC or DataDriver triggers an alert.
2. **Deployment**: SEB is launched to investigate the affected endpoint.
3. **Tasking**: SynA requests specific checks (e.g., network, user identity, file access).
4. **Execution**: SEB executes commands and returns structured responses.
5. **Feedback**: Failures and explanations are returned in natural language.
6. **Learning**: SynA uses outcomes to enhance the model and adjust future interactions.

## 5 Advantages

- Lightweight and self-contained endpoint investigations.
- No adapters or overhead—SEB runs, logs, and exits.
- Logs are directly actionable in LC/DataDriver platforms.
- Rich model training via continuous, contextual feedback.
- Fully autonomous, reducing human-in-the-loop overhead.

# 6 System Diagram

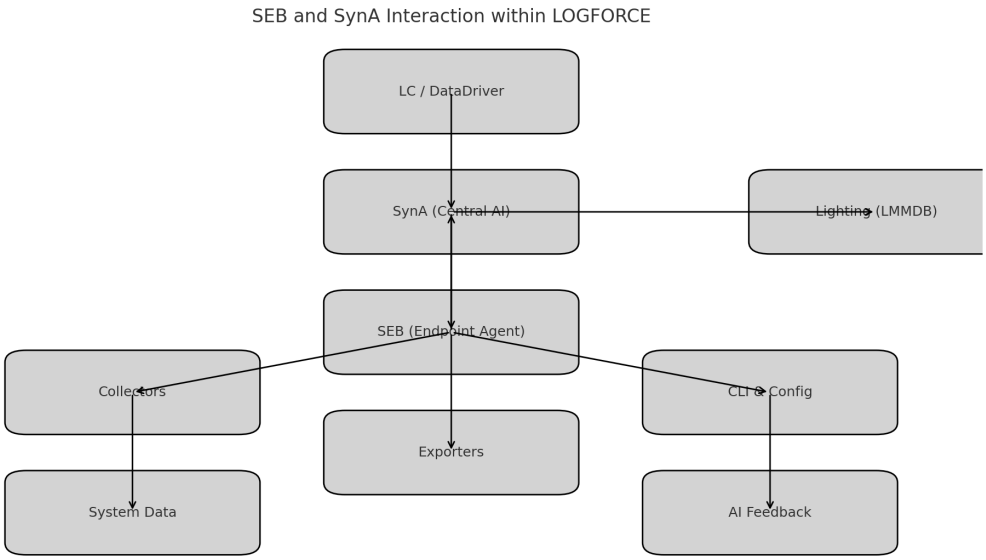


Figure 1: Interaction between SEB and SynA within the LOGFORCE architecture.

# 7 Conclusion

LOGFORCE represents the next generation of cybersecurity platforms—autonomous, explainable, and agile. SEB and SynA work together seamlessly to ensure threats are not only detected but fully understood and acted upon, all without burdening analysts with excessive alerts or manual steps.