Beyond Container CVE Analysis: A GitOps-Based Attestation and Sandbox Framework for Container Supply Chains

IEEE SEEDA-CECNSM CONFERENCE 2025
19-21 September | Patras, Greece
IEEE Computational Intelligence Society

E. SYRMOS*, P. RADOGLOU-GRAMMATIKIS, E. KATSAROS, J. SEKHAR BANERJEE, A. KAZAKLI, K. PANITSIDIS, V. VITSAS AND P. SARIGIANNIDIS

**K3Y LABS, ESYRMOS@K3Y.BG*

P2CODE

Under P2CODE

K3Y Ltd

E. Syrmos
P. Radoglou-Grammatikis
E. Katsaros
A. Kazakli

International Hellenic University

V. Vitsas

University of Western Macedonia

K. Panitsidis
P. Radoglou-Grammatikis
J. S. Banerjee
P. Sarigiannidis

This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101093069 (P2CODE)

Introduction & Related Work

Introduction

Software Containers Industry:

- **87%** of enterprises adopted Kubernetes of, with **66%** using it in prod [1]
- **$16.32 billion** by 2030, outpacing security practices [2]

Security Issues in Software Containers :

- **604+ CVE** per container image on average [3]
- **87%** of container images running in production have high-severity CVEs [4]

Related Work

Why Existing Solutions Fall Short ?

S.1 - Static CVE Scanners (*Trivy, Clair, Grype*):

- Detect 95-99% overlap on known CVEs
- Miss Runtime threats, zero-day exploits, behavioral anomalies

S.2 - SBOM/SLSA Compliance Frameworks :

- *Limited adoption due to a visibility gap in the supply chain*
- Implementation barriers due to complex implementations and unclear communications of primary challenges [5]

S.3 - Hardened Base Images :

- Reduce the known vulnerability area and dependencies

SLSA = Supply Chain Levels for Software Artifacts

SBOM = Software Bill of Material

This Paper's Research Scope

DevSecOps Framework

Introduce a Framework for proactive docker container images analysis

Static & Runtime

Combine static & runtime analysis of Docker container images of unknown individual contributors

Standard Compliant

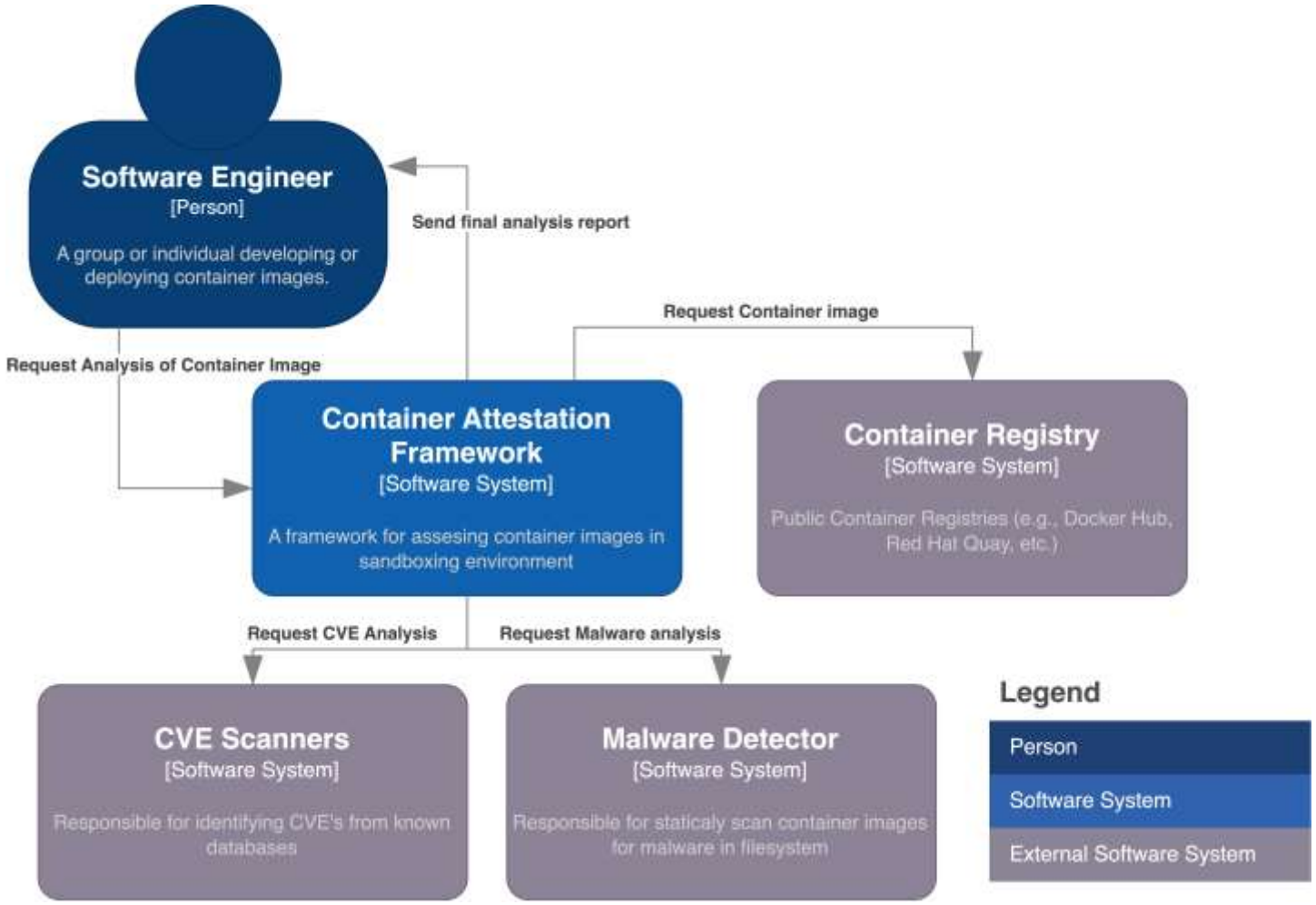
Structure and evaluate static CVE reports & runtime behavioral analysis into STIX format

Extendable

Kubernetes-ready via *admission controller* in production pipelines

Proposed Architecture

Framework Architecture

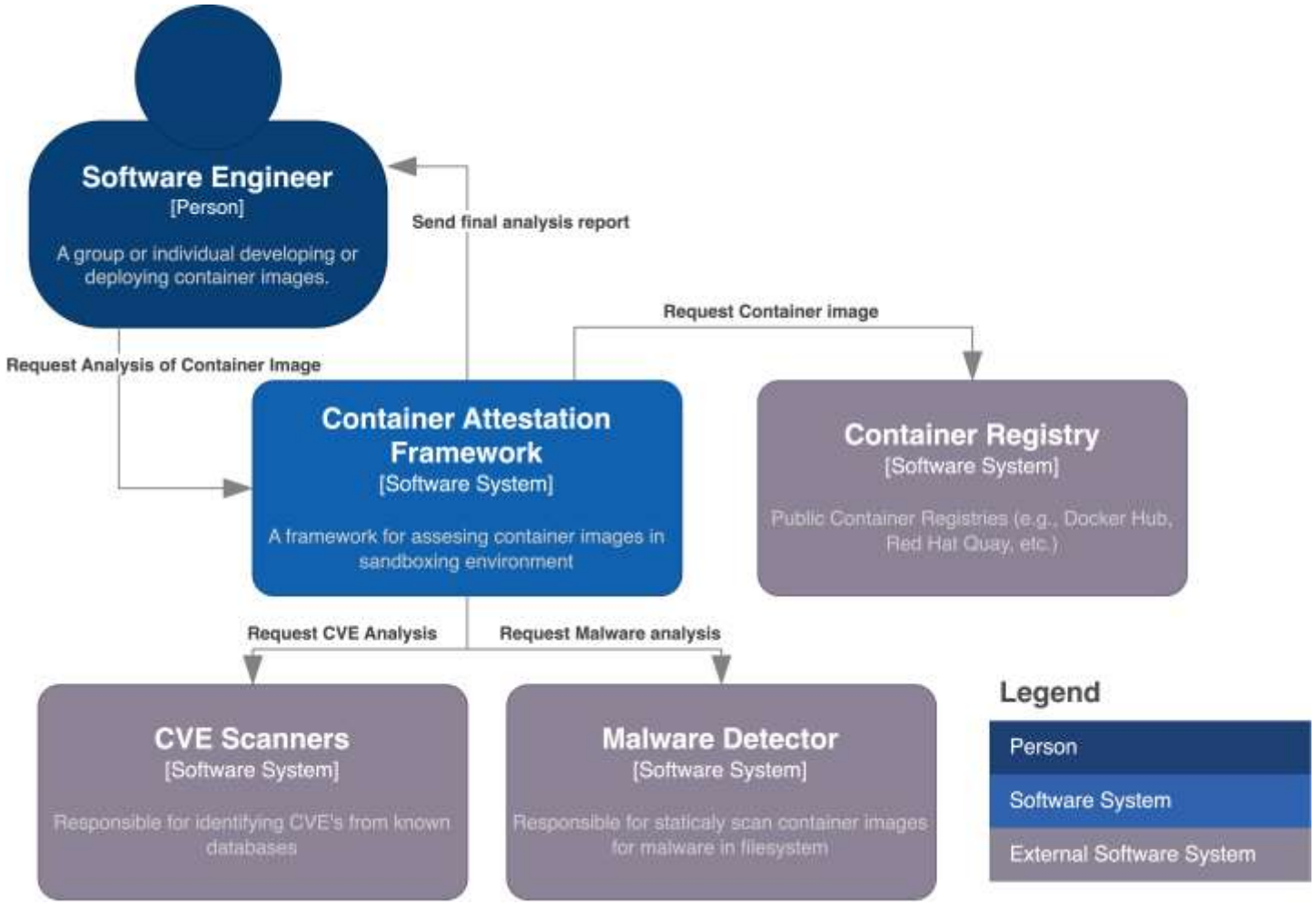


Abstraction levels via C4 model

1 Context-Level

Complexity + Interaction

Framework Architecture



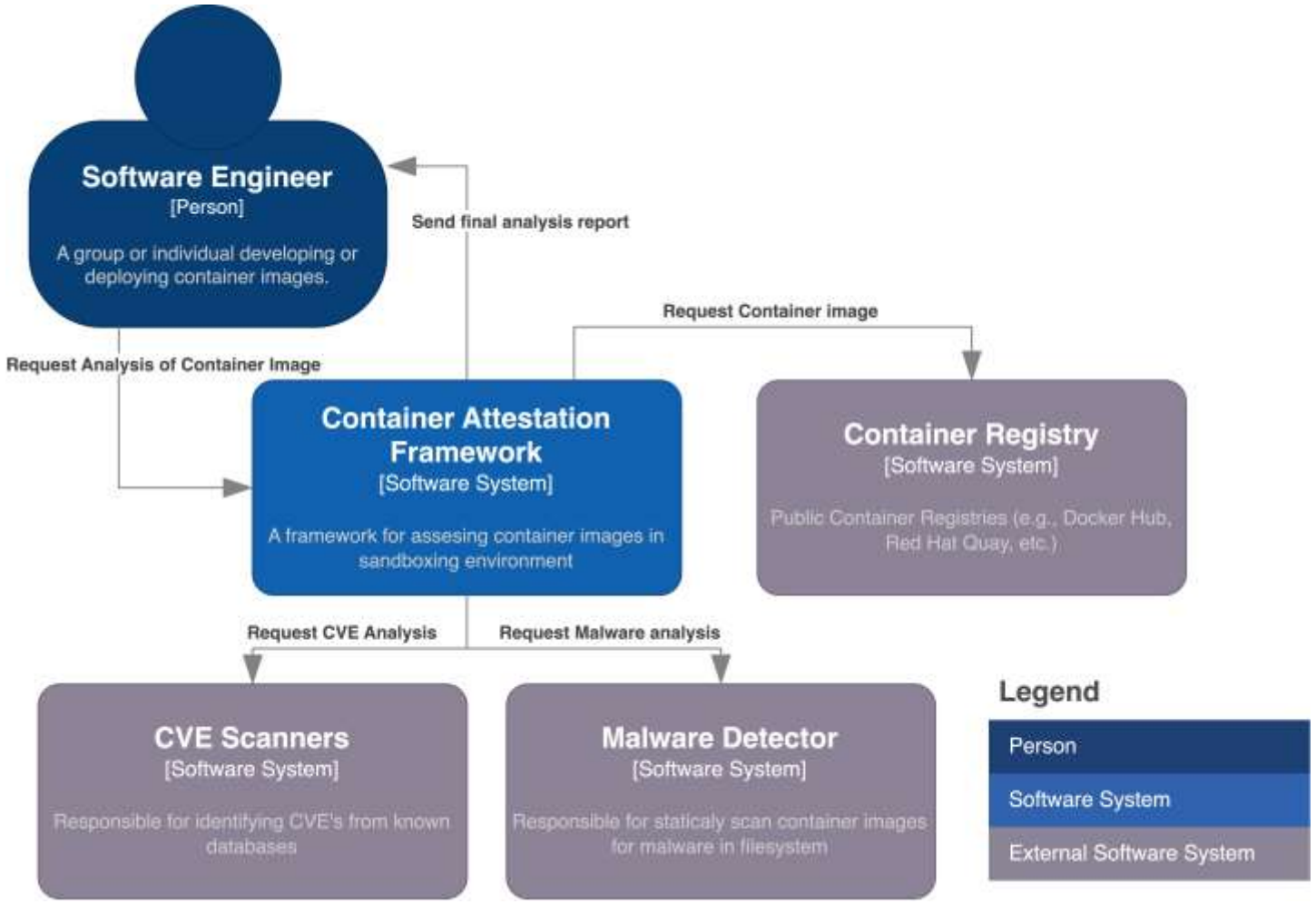
Abstraction levels via C4 model

1 Context-Level

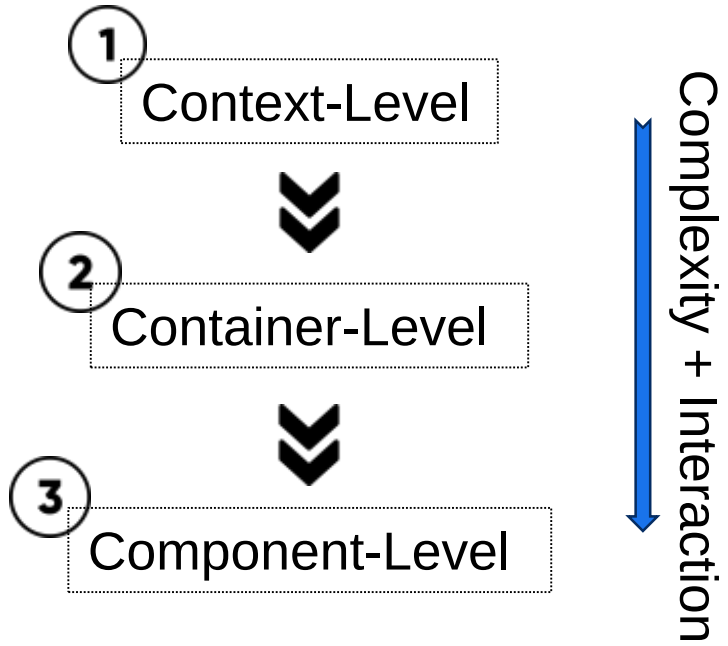
2 Container-Level

Complexity + Interaction

Framework Architecture

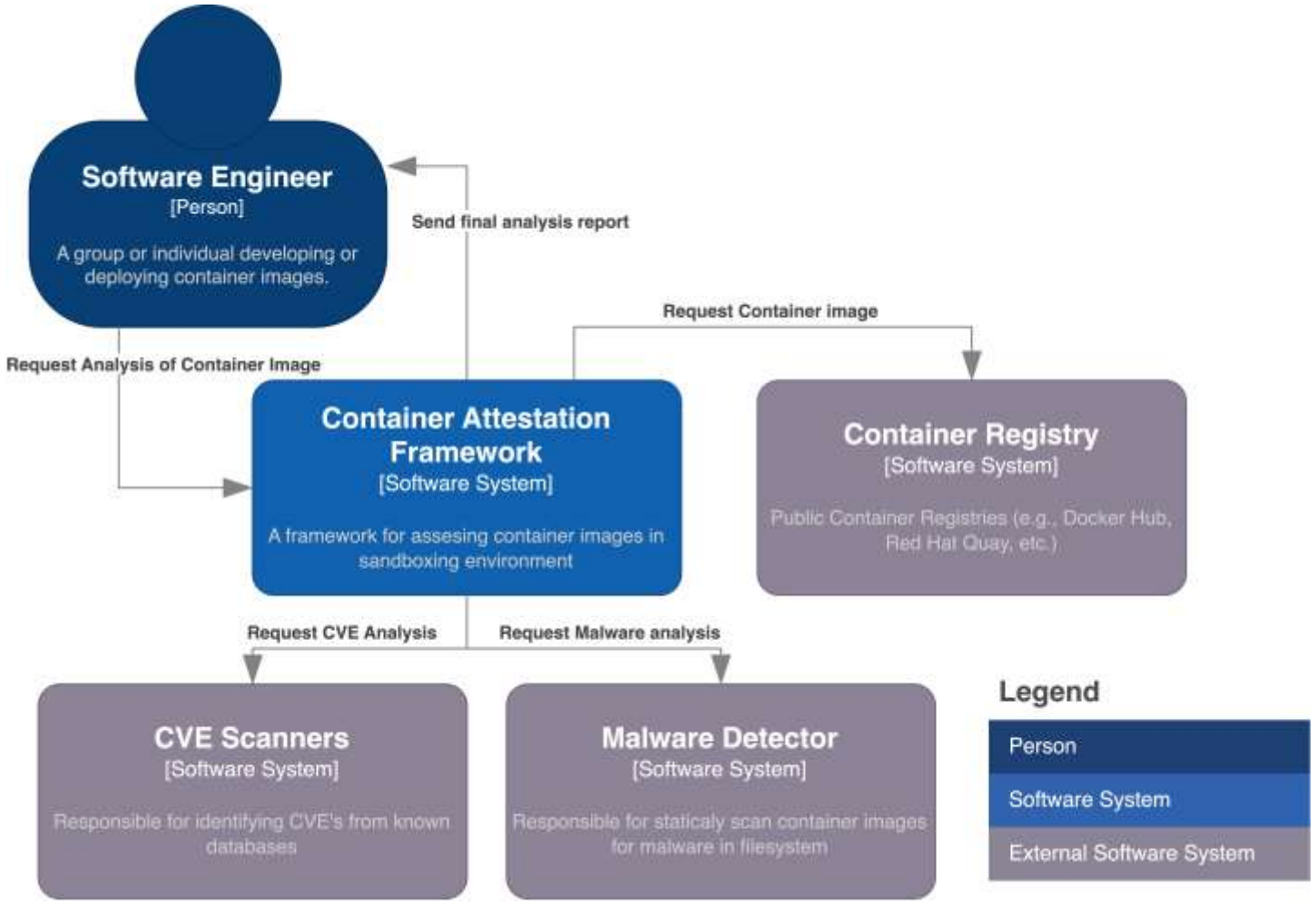


Abstraction levels via C4 model



Context-Level

Context-Level



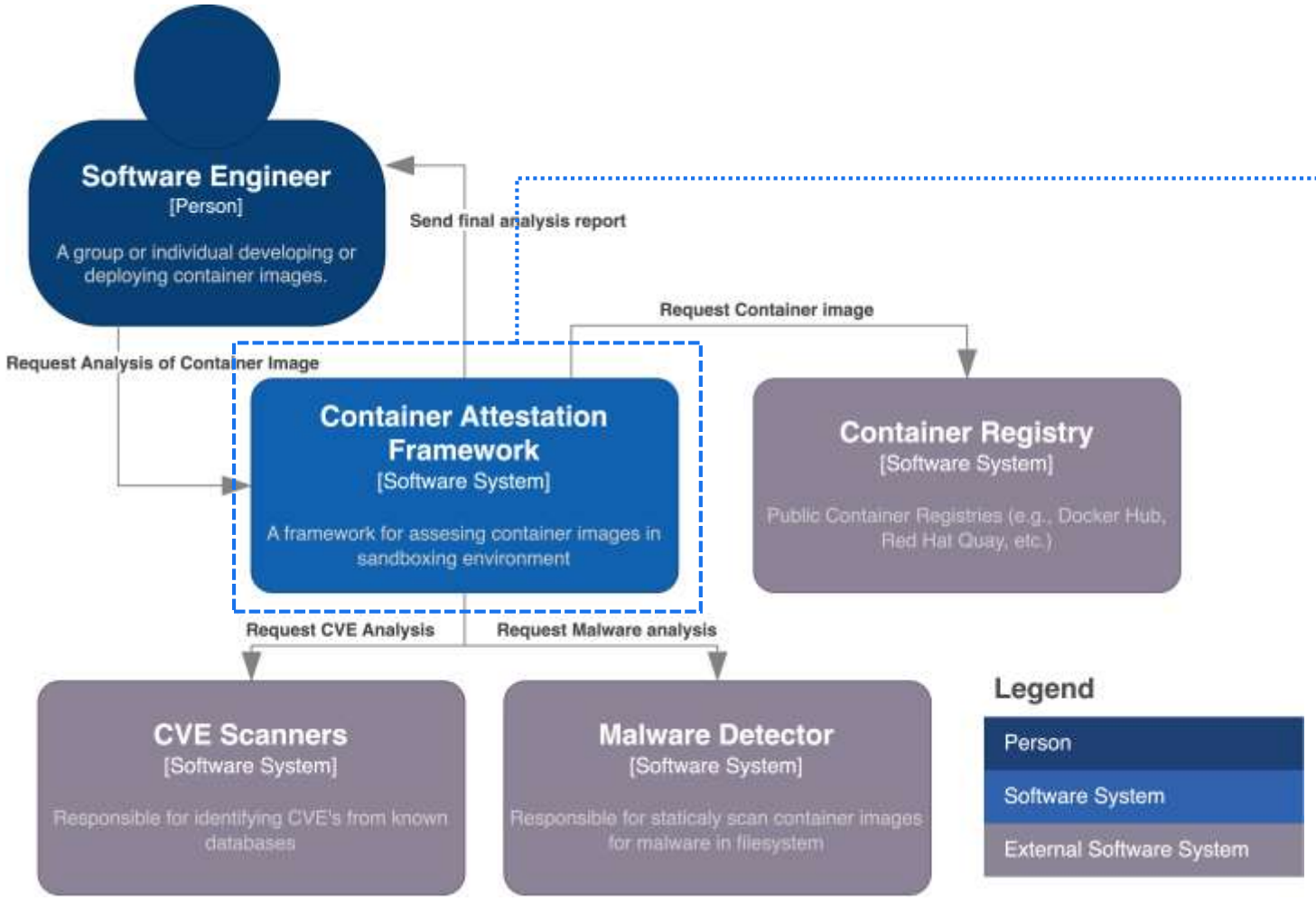
Software System

- ❑ Container Attestation Framework

External Software Systems

- ❑ Container Registry
- ❑ CVE Scanners
- ❑ Malware Detector

Context-Level



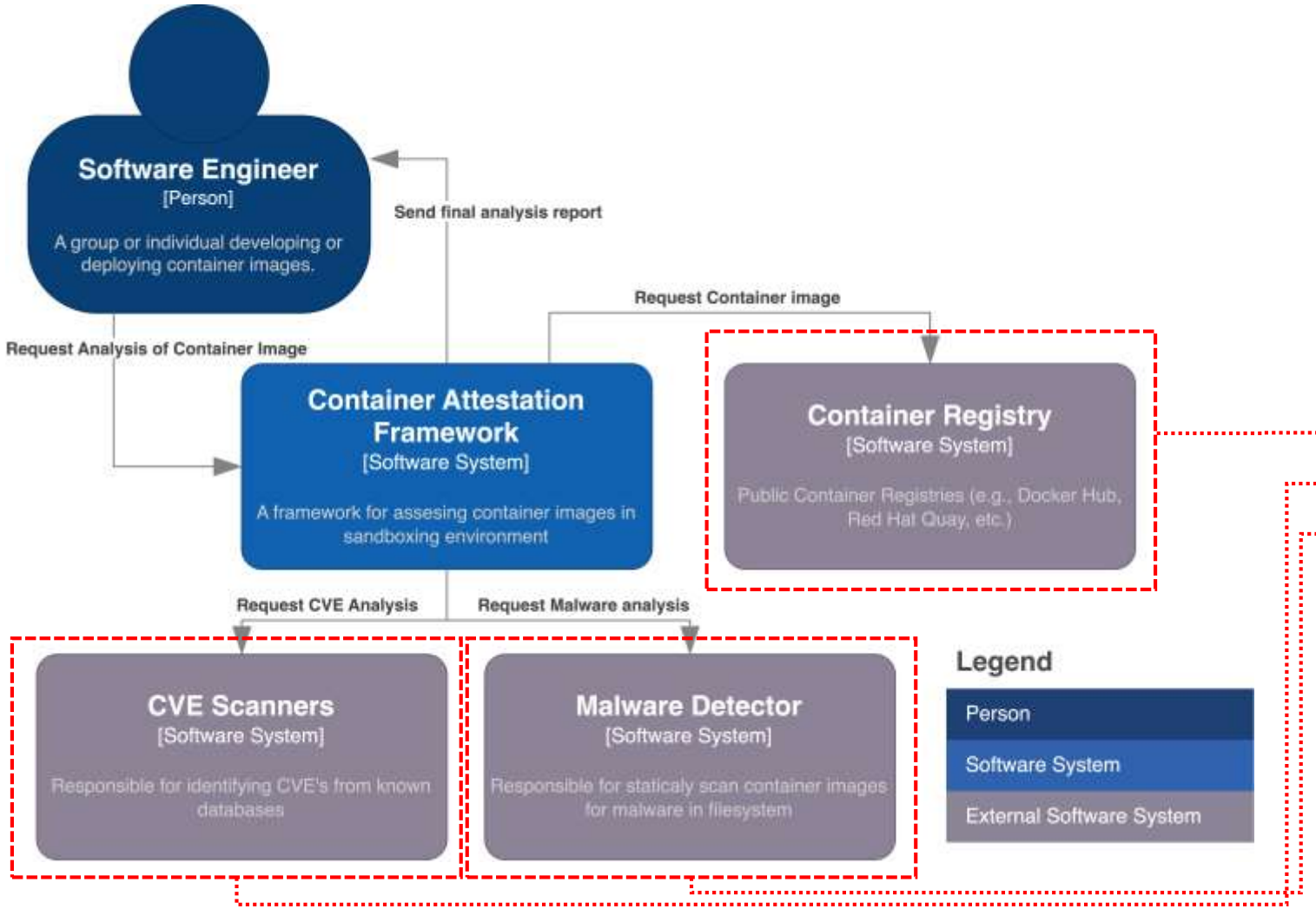
Software System

- ❑ Container Attestation Framework

External Software Systems

- ❑ Container Registry
- ❑ CVE Scanners
- ❑ Malware Detector

Context-Level



Software System

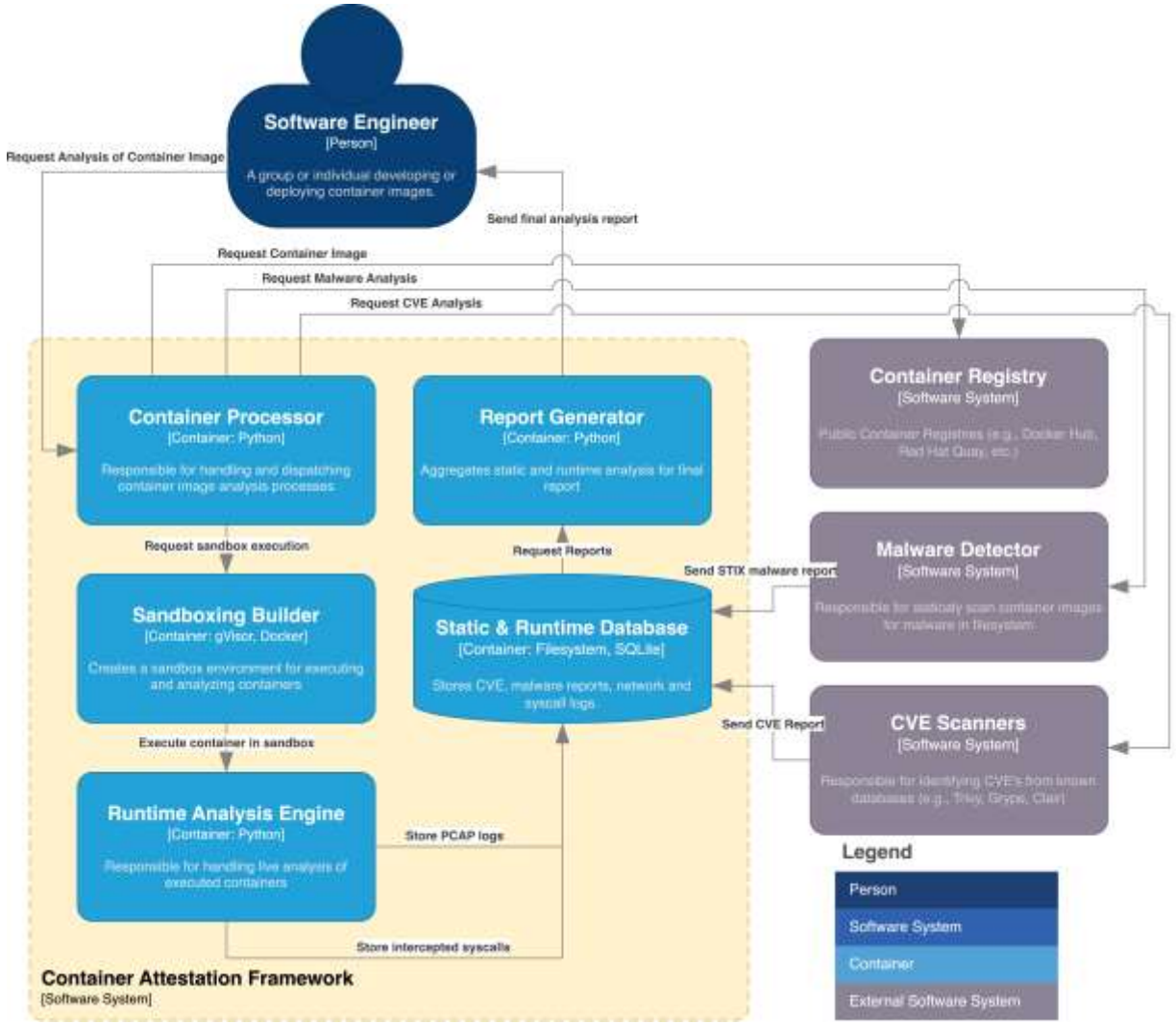
- ❑ Container Attestation Framework

External Software Systems

- ❑ Container Registry
- ❑ CVE Scanners
- ❑ Malware Detector

Container-Level

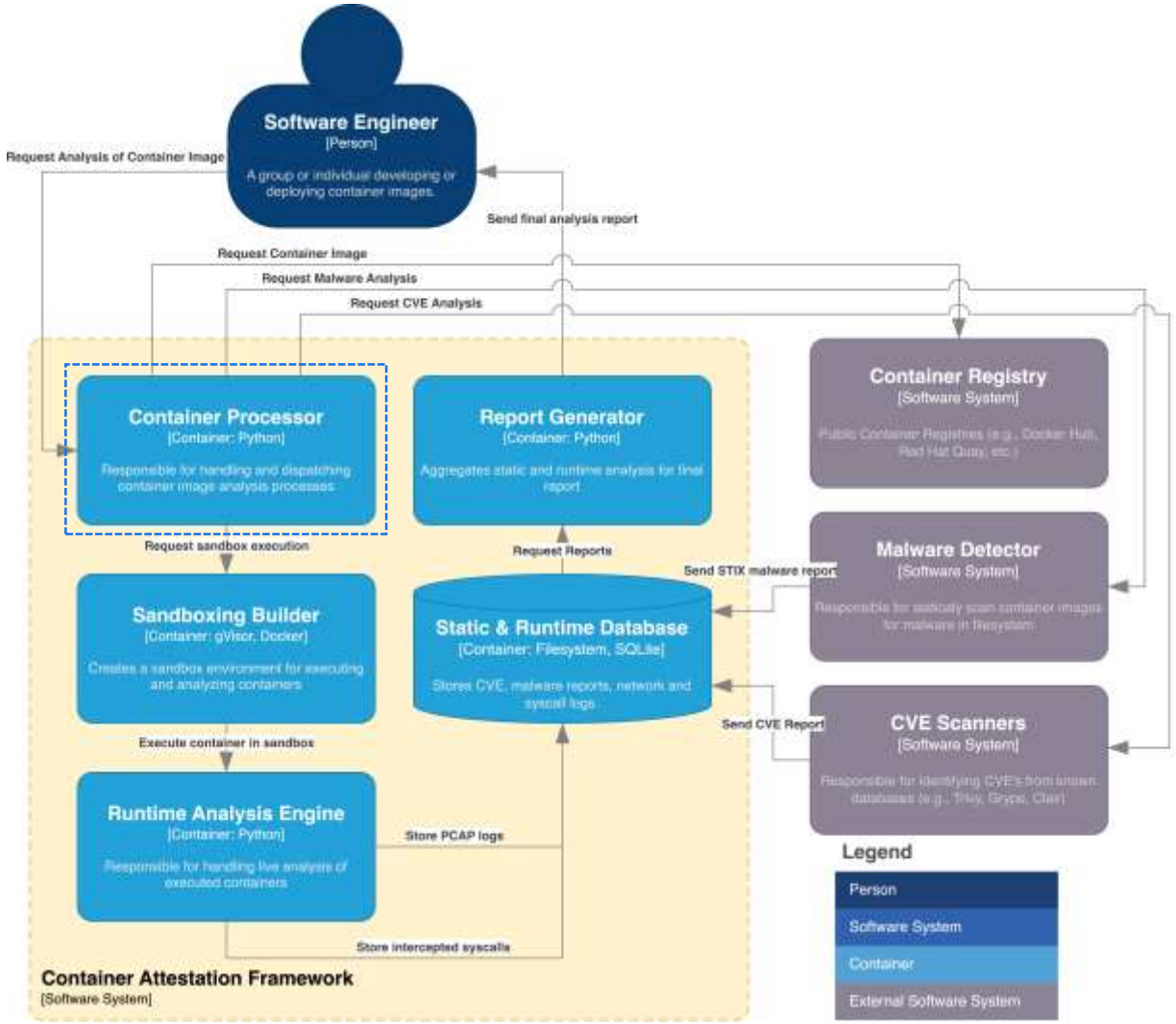
Container-Level



Container Attestation Framework

- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ❑ Report Generator

Container-Level



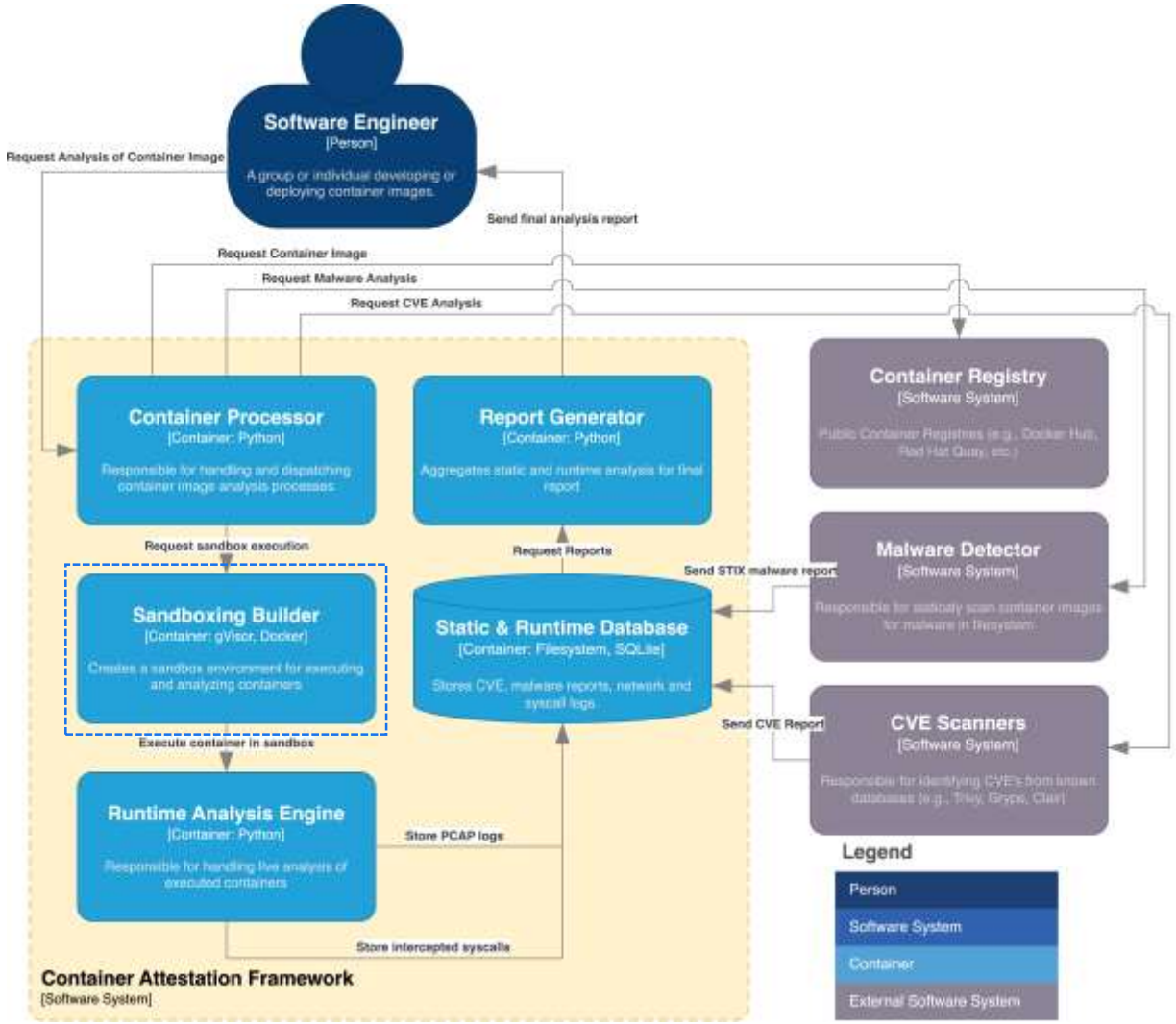
Container Attestation Framework

- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ❑ Report Generator

Operation

Dispatching container image analysis

Container-Level



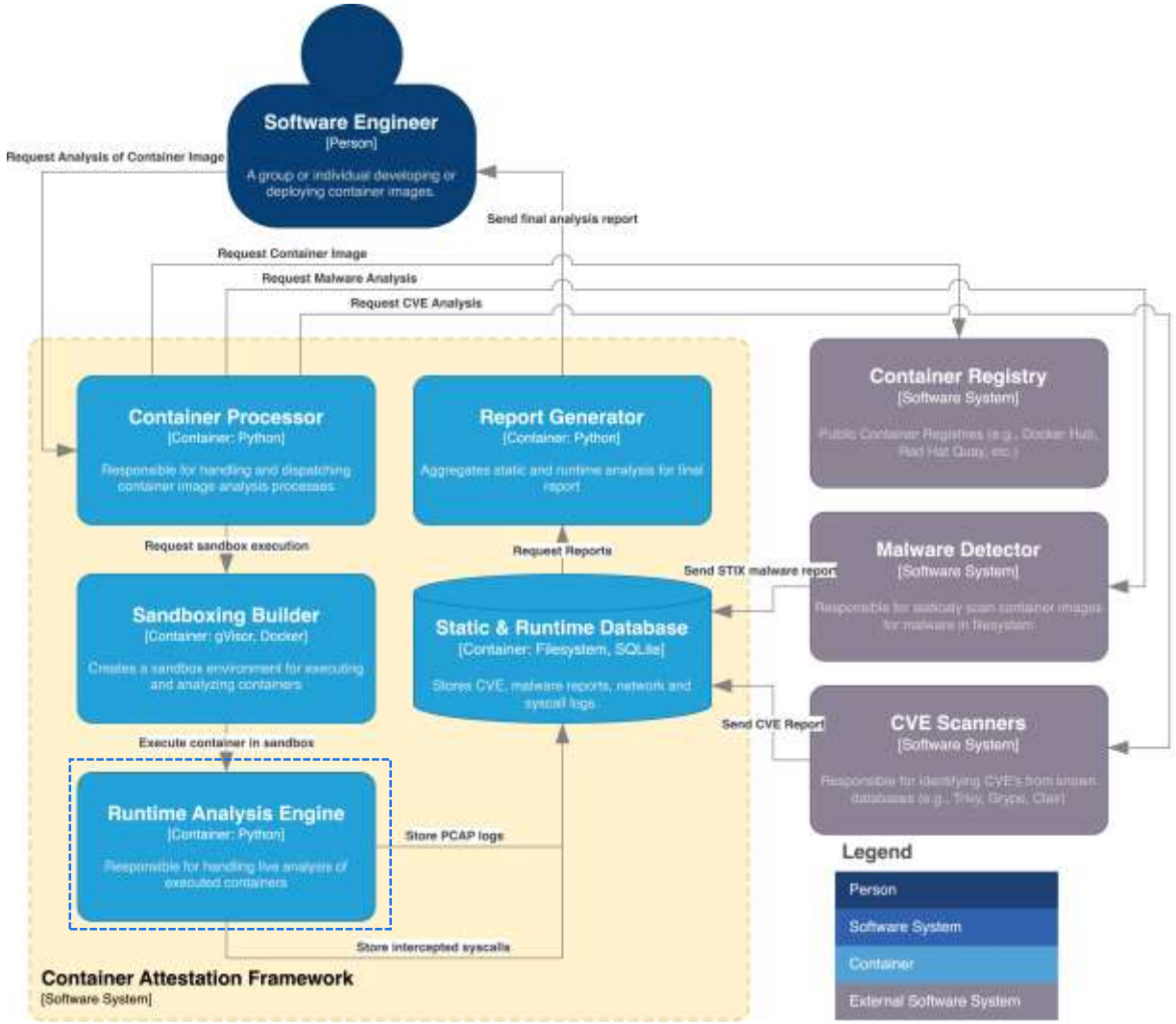
Container Attestation Framework

- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ❑ Report Generator

Operation

Create a sandboxing environment for analysis

Container-Level



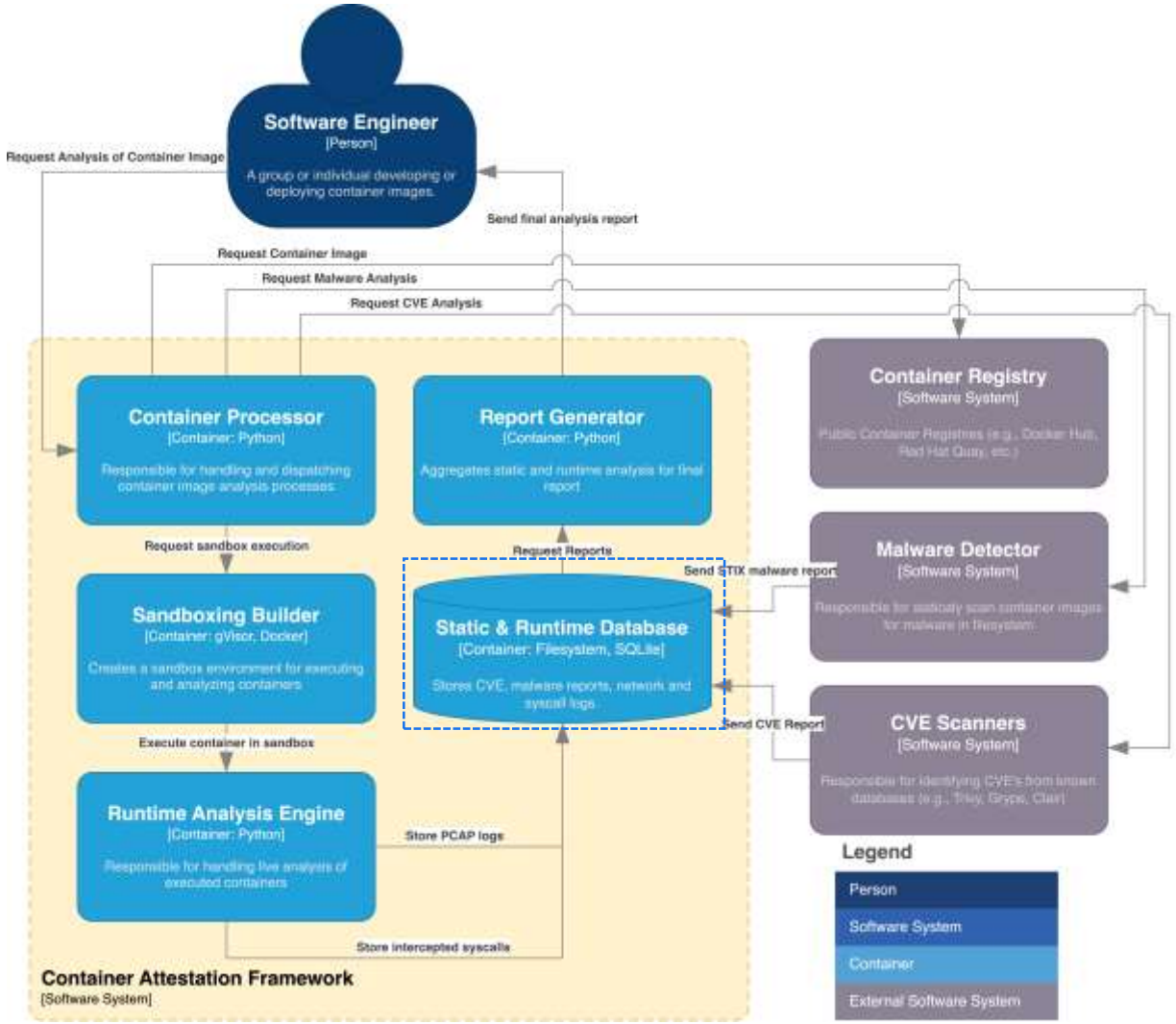
Container Attestation Framework

- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ❑ Report Generator

Operation

Execution and monitoring of the sandboxing environment

Container-Level



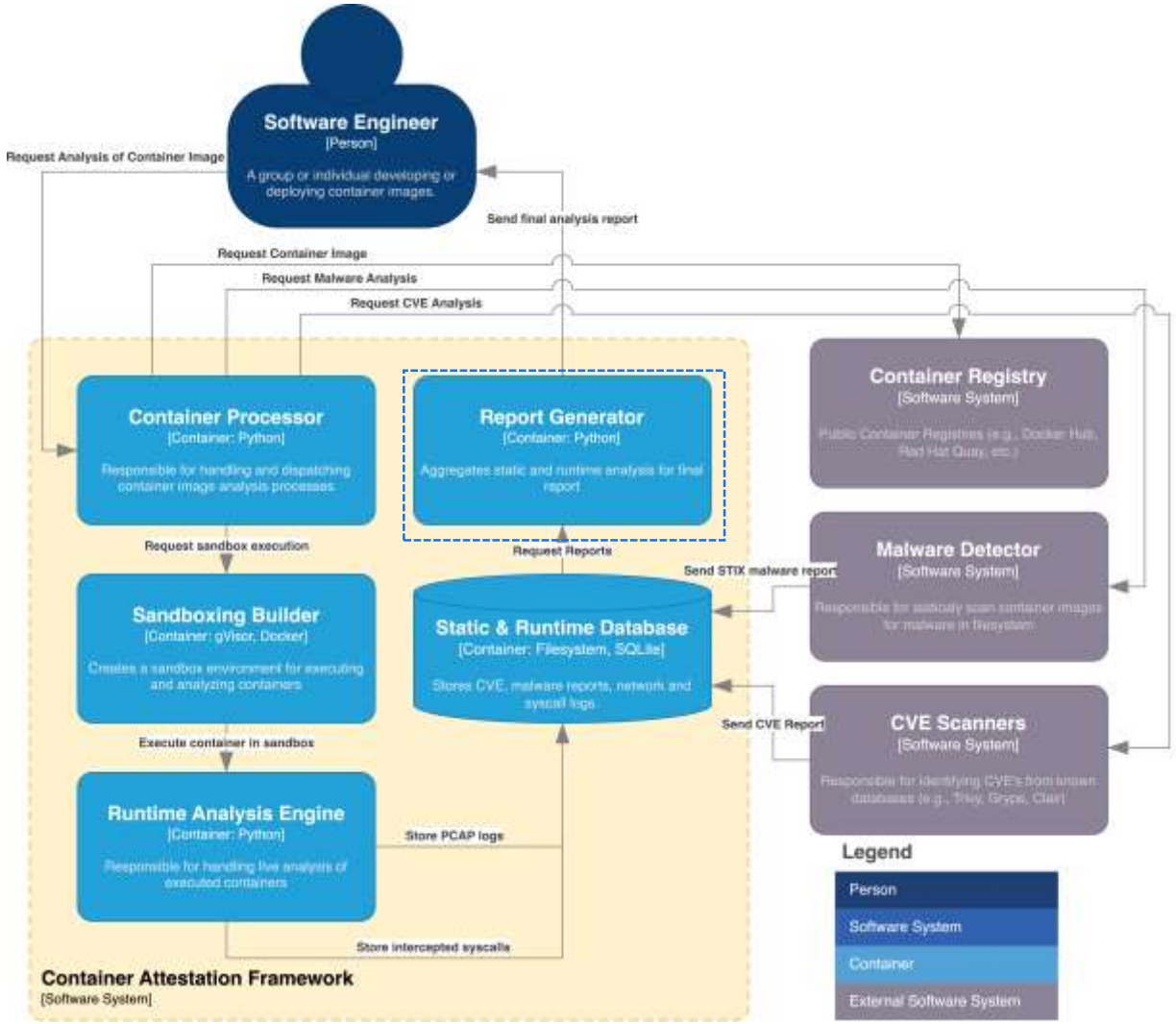
Container Attestation Framework

- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ❑ Report Generator

Operation

Store CVE reports and sandboxing metadata (network & syscalls)

Container-Level



Container Attestation Framework

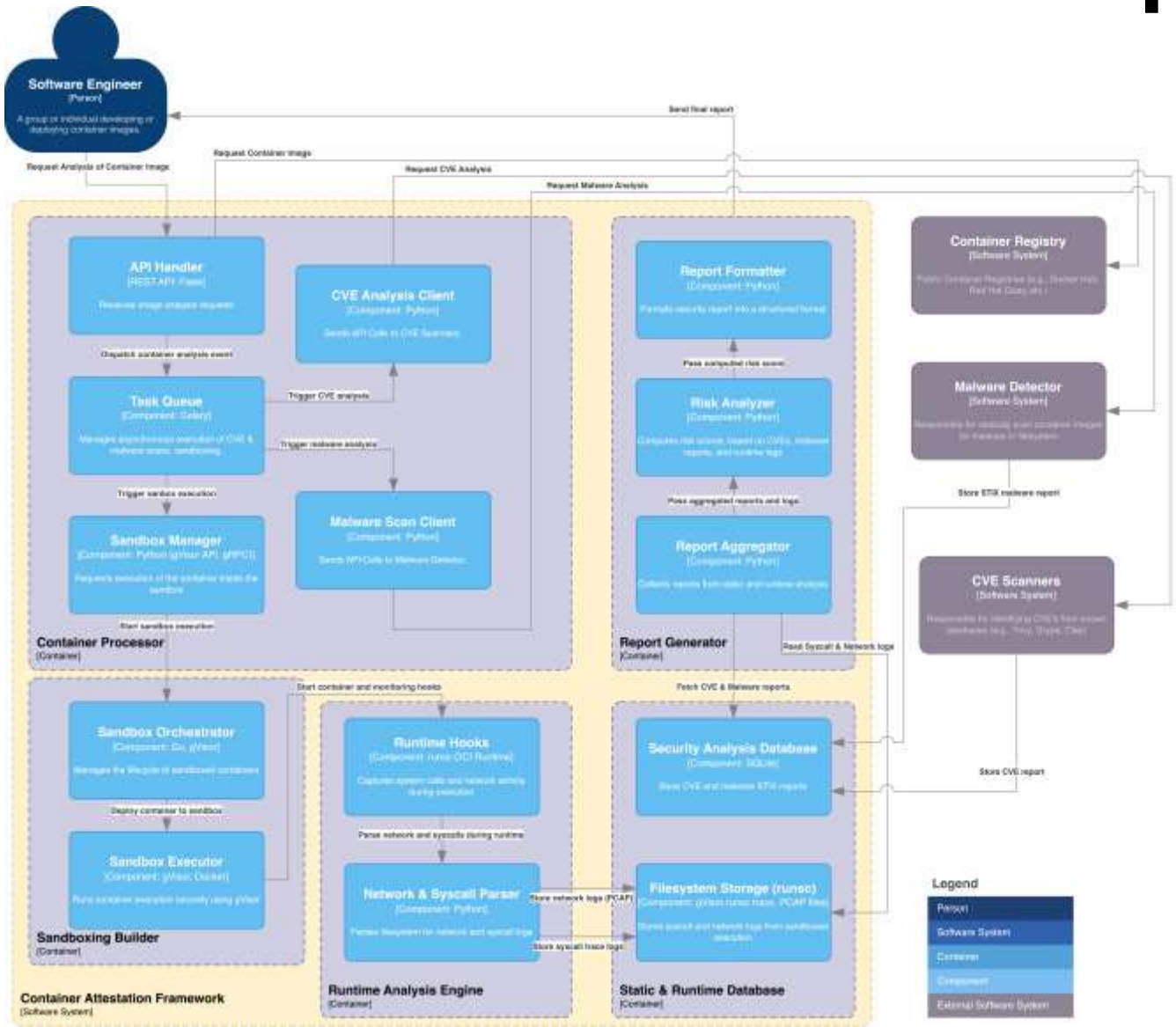
- ❑ Container Processor
- ❑ Sandboxing Builder
- ❑ Runtime Analysis Engine
- ❑ Static & Runtime Database
- ➡ ❑ Report Generator

Operation

Construct a STIX report with CVE and runtime analysis information

Component-Level

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

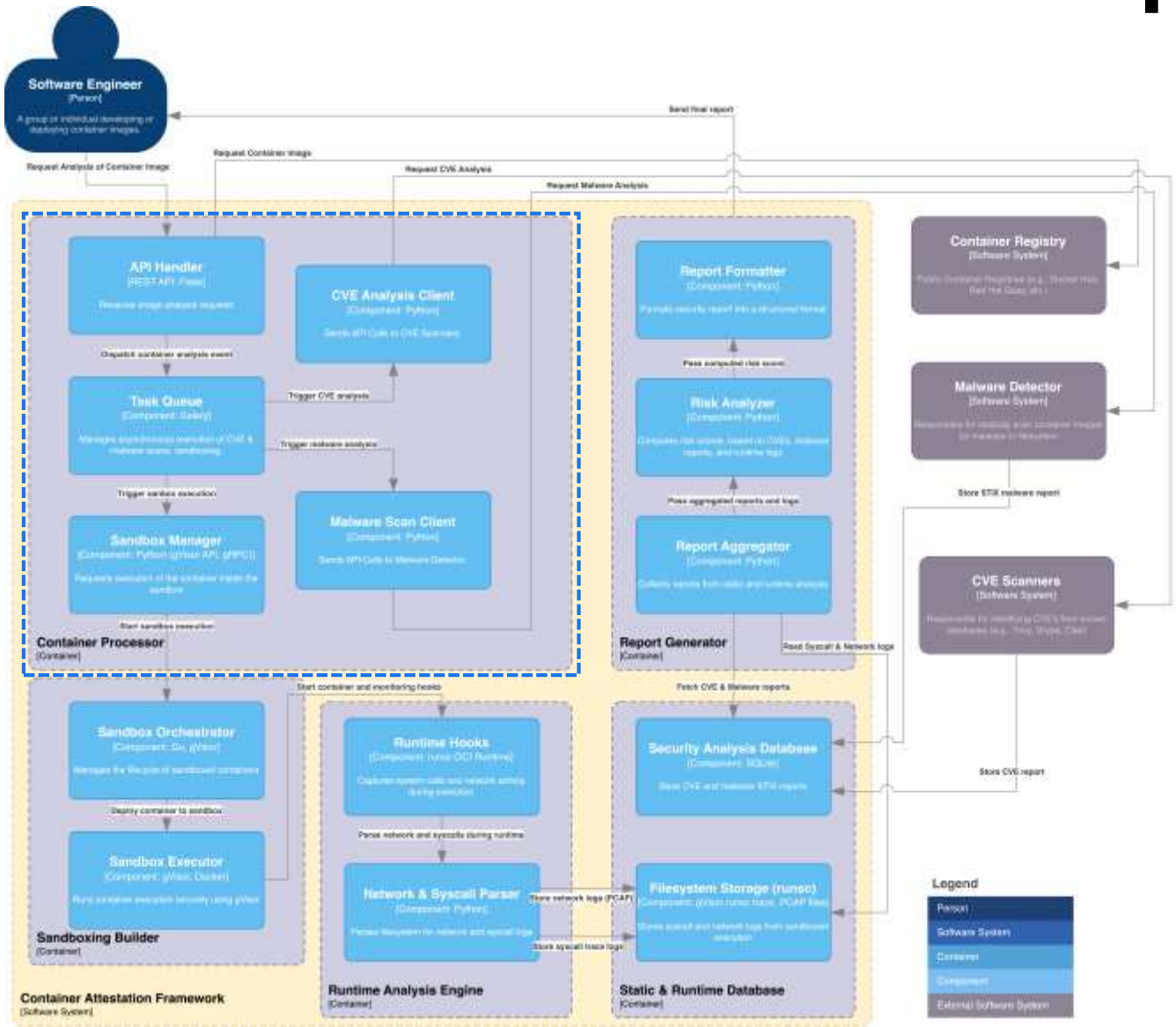
Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

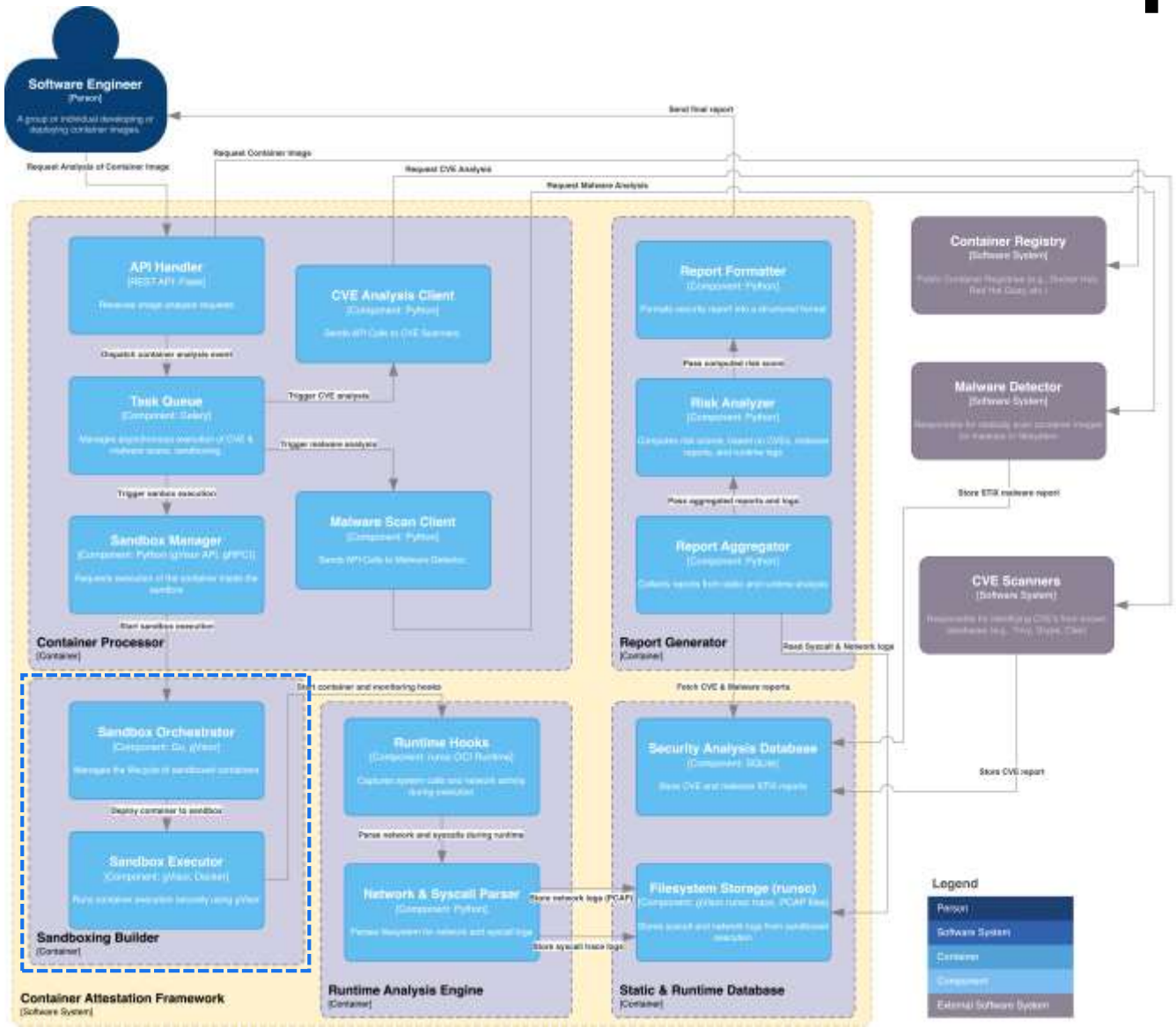
Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

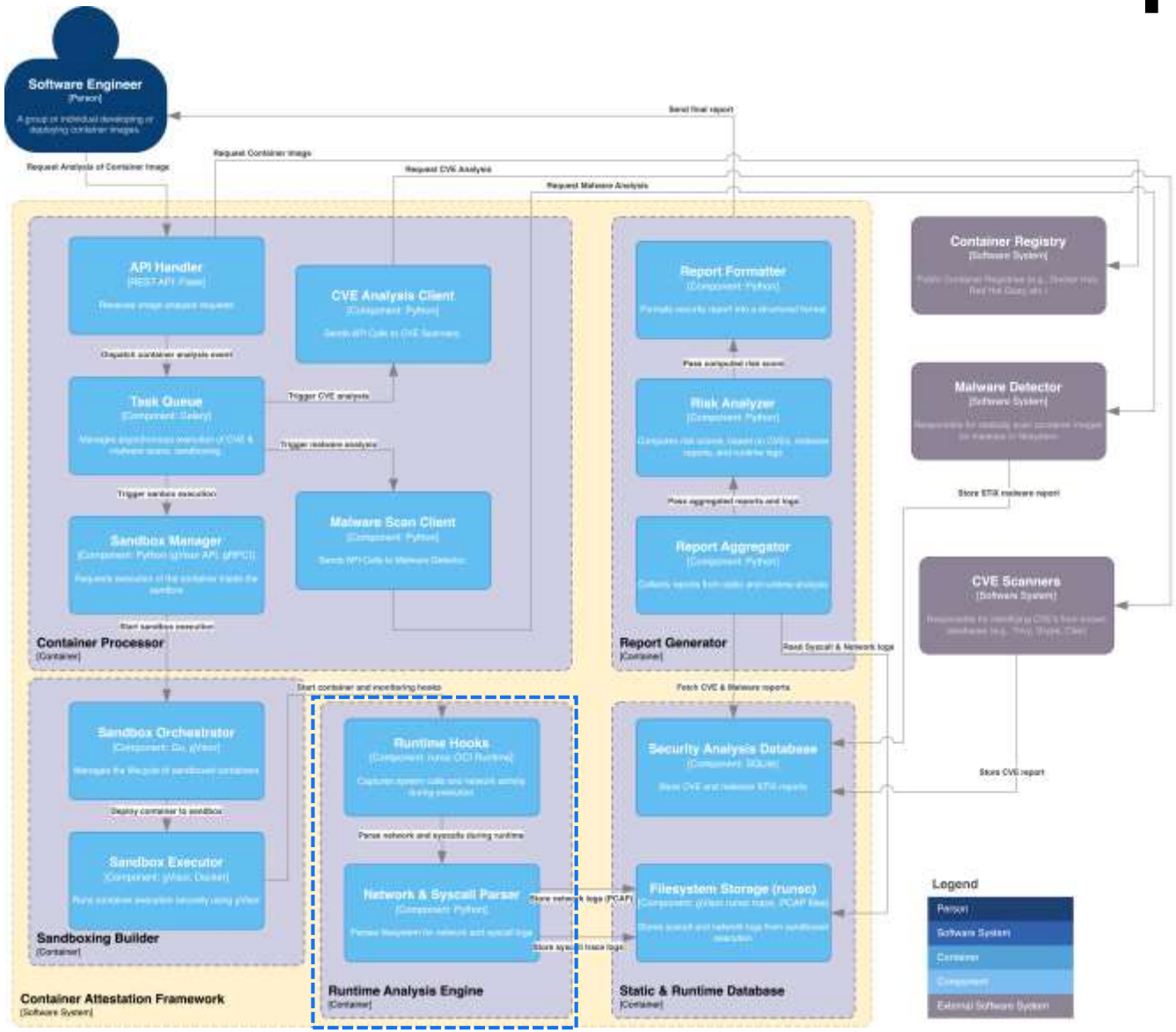
Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

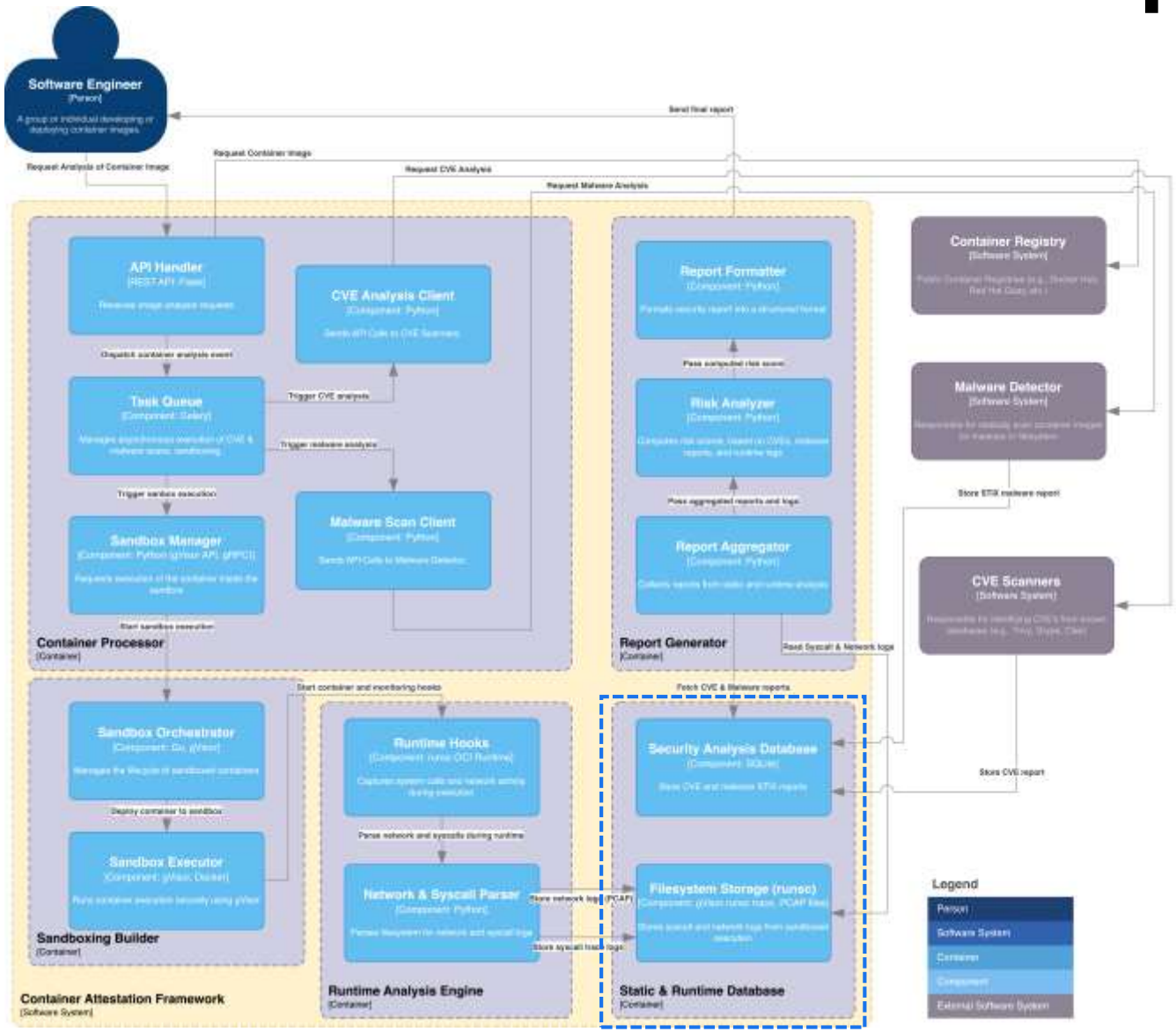
Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

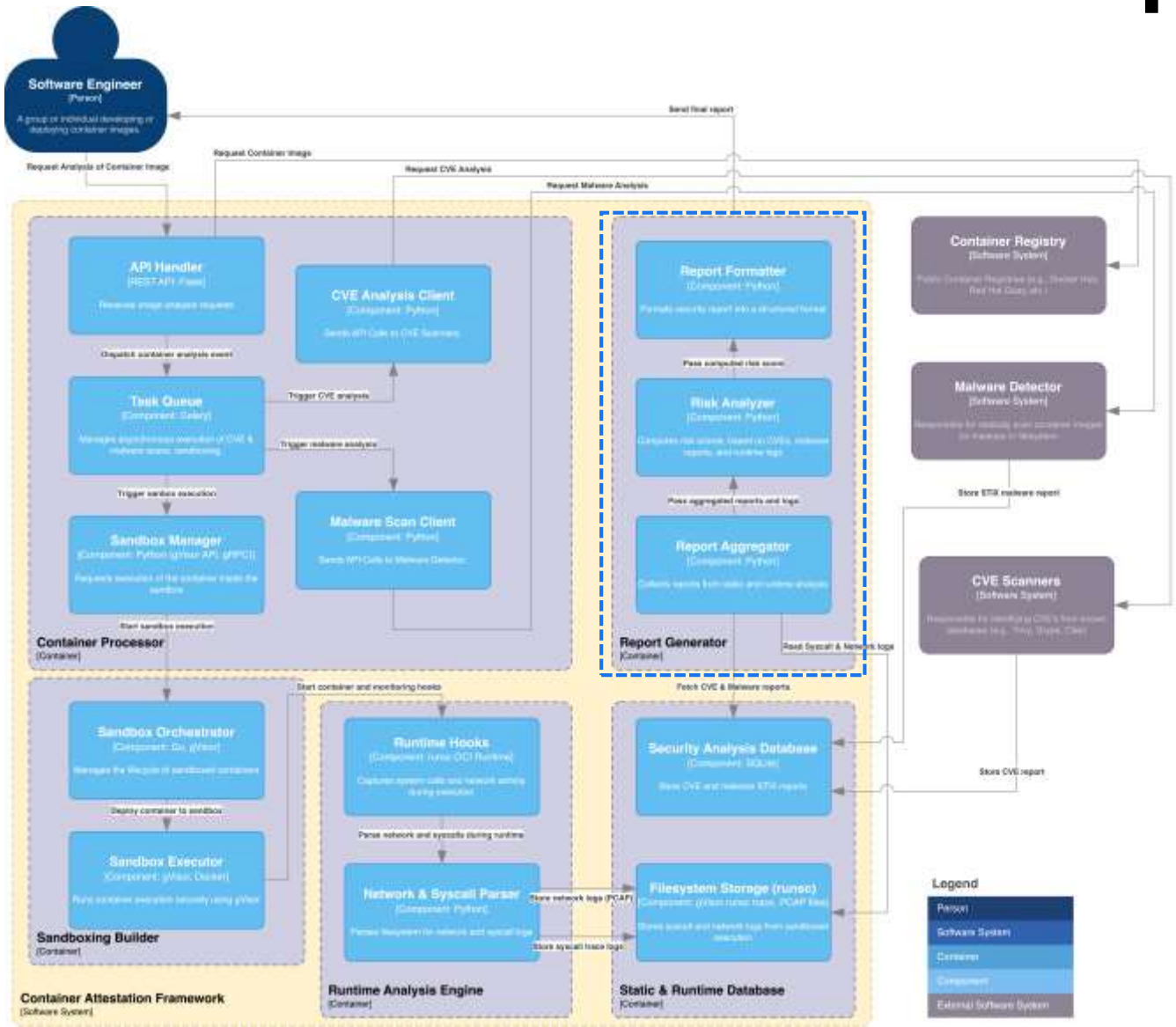
Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Component-Level



Container Processor

- ❑ API Handler
- ❑ Task Queue
- ❑ CVE Analysis Client
- ❑ Malware Scan Client
- ❑ Sandbox Manager

Sandboxing Builder

- ❑ Sandbox Orchestrator
- ❑ Sandbox Executor

Runtime Analysis Engine

- ❑ Runtime Hooks
- ❑ Network & Syscall Parser

Report Generator

- ❑ Report Aggregator
- ❑ Risk Analyzer
- ❑ Report Formatter

Static & Runtime Database

- ❑ Filesystem Storage (runsc)
- ❑ Security Analysis Database

Conclusion & Future Work

Conclusion

- Introduced first GitOps-native framework combining CVE scanning with runtime behavioral analysis
- Demonstrated architecture supporting compliance standards while addressing SBOM/SLSA coverage gaps
- Proposed a practical solution for organizations delaying deployments due to container security concerns

Future Work

- Production deployment validation and performance benchmarking
- ML-based anomaly detection for behavioral patterns
- Extended ecosystem integration and automated policy enforcement

Appendix & Refs

Appendix & Refs

[1]: https://edgedelta.com/company/blog/kubernetes-adoption-statistics
[2]: https://www.mordorintelligence.com/industry-reports/docker-container-market
[3]: https://www.helpnetsecurity.com/2024/12/11/containers-security-concerns/
[4]: https://www.darkreading.com/vulnerabilities-threats/87-of-container-images-in-production-have-critical-or-high-severity-vulnerabilities
[5]: https://arxiv.org/abs/2409.05014