Securaa Prerequisites For SOAR

Contact Information
support@securaa.io

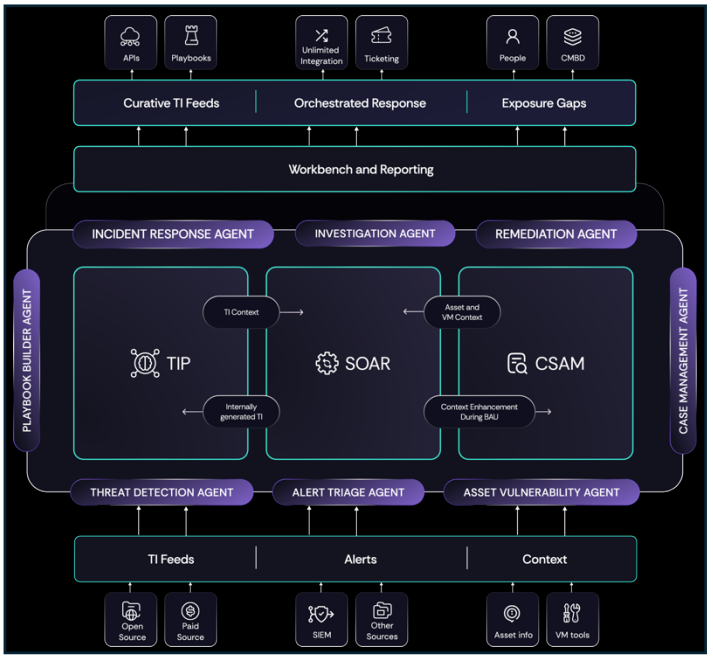
432,6th Main, Vijay Nagar, Mysore, 1st Stage KA 570017 IN

Table of Contents

Securaa Platform Overview

Securaa brings together the benefits of a mature threat intelligence platform (TIP), proactive cyber security asset management (CSAM), and reliable security orchestration,automation, and response (SOAR) under a single umbrella.

- Threat Intelligence feeds for SOC teams to be predictive while enabling effective management of protective and detective security controls
- Unified compliance posture across assets to proactively manage the organization’s vulnerability posture and security controls coverage gaps.
- Out of box API integrations and pre-configured playbooksto improve SOC’s ability to shrink the triage and responsetime.

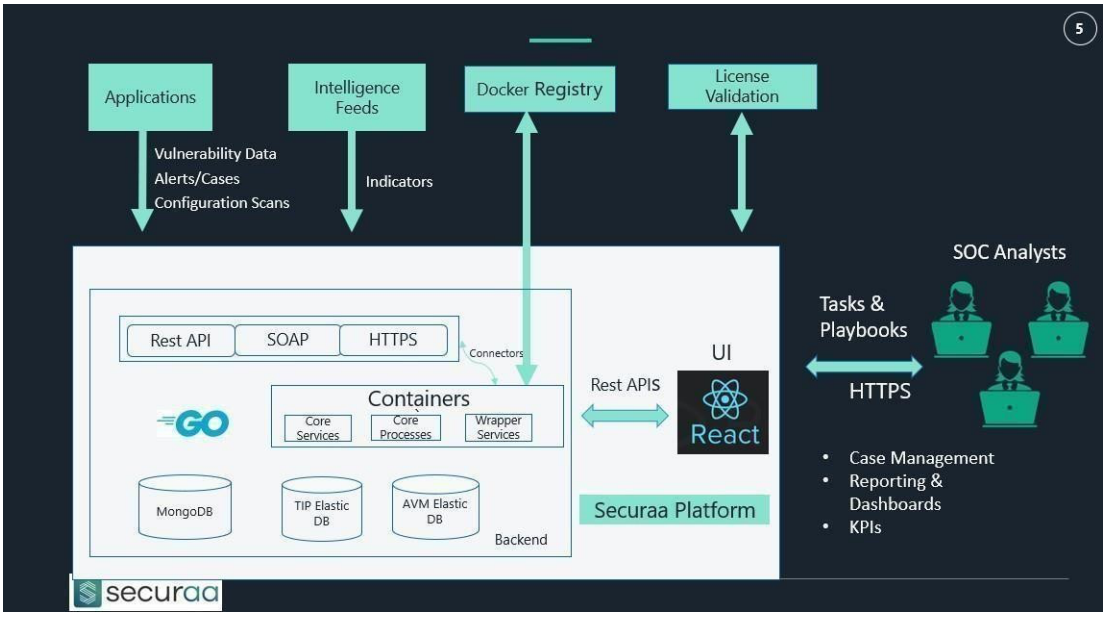


Product Components

Securaa comprises of the following components as shown inthe architecture diagram below:

- Application Server (Developed in react)
- Databases (Mongo dB and Elastic)
- Intelligence feeds (Only with a TIP License) to use theThreat Intelligence Platform.
- Docker Registry: To pull the latest images from Securaaservers for installation.
- Licensing Server: To validate the license

The product is accessible through a web interface for analystsand other users.



Prerequisites

Prerequisites for SOAR Deployment

Securaa needs the following for a successful deployment:

- Internet connectivity to Securaa Servers to download thelatest software versions and Docker images
- Administrative privileges on the operations system platform
- SSH Connectivity tools like Putty to connect with Securaaplatforms
- Browser software like Chrome to access Securaa's webinterface.
- The machine CPU should support AVX to validate below command can be used:
  - **lscpu | grep avx** (this command will show if AVX is supported or not)

Operating system requirements

Securaa can be deployed on the following operating systems and must meet the minimum hardware requirements.

Operating System	Supported Version
RHEL	9.x
Ubuntu	20.04x, 22.04x

Hardware Requirements Enterprise/Standalone Setup (Proof of concept):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers MINIMUM	MULTI VM (3 servers) MINIMUM
CPU	8 CPU cores	6 CPU cores	8 CPU cores
Memory	16 GB RAM	8 GB RAM	16 GB RAM
Storage	250 GB SSD	250 GB SSD	250 GB SSD

Hardware Requirements MSSP (Proof of concept):

COMPONENT	SINGLE VM MINIMUM	MULTI VM (2 servers) MINIMUM	MUTI VM (3 servers) MINIMUM	REMOTE INTEGRATION SERVER
CPU	8 CPU	4 CPU	4 CPU	8 CPU
Memory	16 GB RAM	8 GB RAM	4 GB RAM	4 GB RAM
Storage	250 GB SSD	150 GB SSD	100 GB SSD	100 GB SSD

Network Connectivity Requirements

The following URLs need to be whitelisted before installation. Securaa downloads the latest software version, Docker images,and other dependencies from these URLs:

- https://s3.us-east-2.amazonaws.com/
- https://665853670667.dkr.ecr.us-east-2.amazonaws.com/
- https://release.securaa.io:9002
- https://production.cloudflare.docker.com
- https:// registry-1.docker.io
- https:// auth.docker.io
- https:// ecr.us-east-2.amazonaws.com
- prod-us-east-2-starport-layer-bucket.s3.us-east-2.amazonaws.com

The following ports need to be whitelisted.

1. 443 – Web access
2. 8000 – Web socket

Prerequisites Before Installation

wget should be pre-installed.

Note: Internet Access is mandatory for Securaa Installation only.