Securaa Prerequisites For SIA, SOAR, TIP & CSAM

Contact Information: support@securaa.io

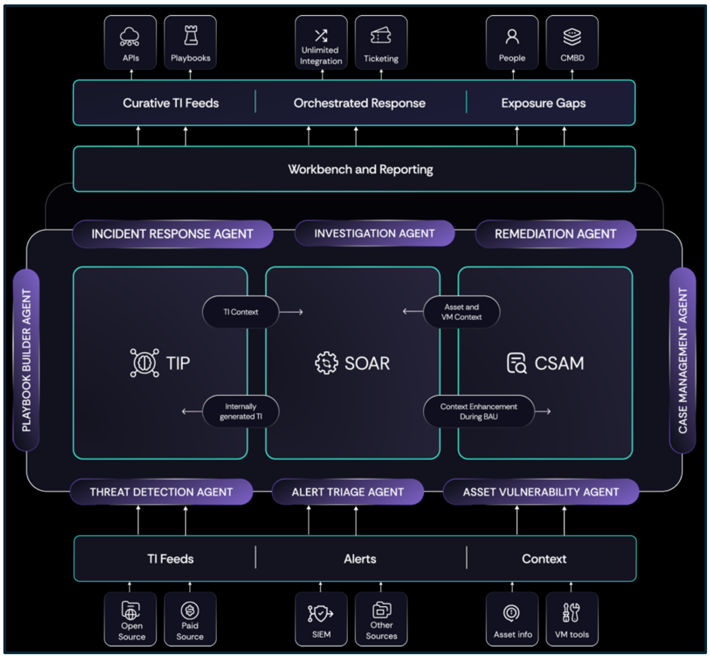
432,6th Main, Vijay Nagar, Mysore, 1st Stage KA 570017 IN

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 playbooks to improve SOC’s ability to shrink the triage and response time.

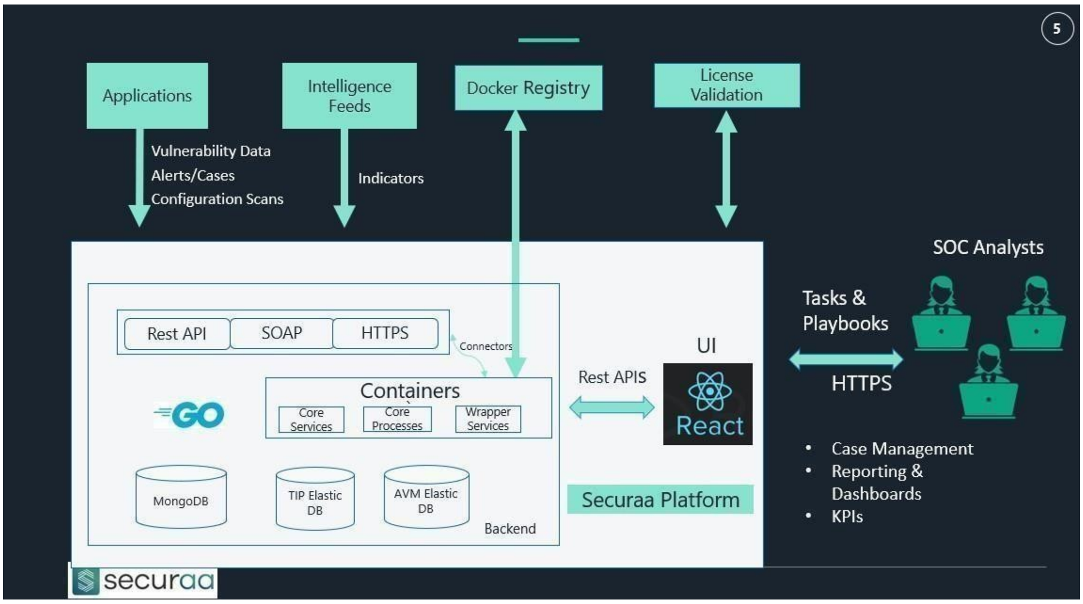


Product Components

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

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

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



Prerequisites

Prerequisites for SOAR Deployment

Securaa needs the following for a successful deployment:

- Internet connectivity to Securaa Servers to download the latest software versions and Docker images
- Administrative privileges on the operations system platform
- SSH Connectivity tools like Putty to connect with Securaa platforms
- Browser software like Chrome to access Securaa's web interface.

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
OEL	8.10

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

COMPONENT	SINGLE VM MINIMUM
CPU	8 CPU cores
Memory	16 GB RAM
Storage	250 GB SSD

Hardware Requirements Enterprise/Standalone Setup (PRODUCTION):

COMPONENT	SINGLE VM MINIMUM	REMOTE INTEGRATION SERVER
CPU	32 CPU cores	8 CPU
Memory	64 GB RAM	4 GB RAM
Storage	1 TB SSD	100 GB SSD

Hardware Requirements MSSP (Proof of concept):

COMPONENT	SINGLE VM MINIMUM	REMOTE INTEGRATION SERVER
CPU	8 CPU	8 CPU
Memory	16 GB RAM	4 GB RAM
Storage	250 GB SSD	100 GB SSD

Hardware Requirements MSSP (PRODUCTION):

COMPONENT	SINGLE VM MINIMUM	REMOTE INTEGRATION SERVER
CPU	32 CPU	8 CPU
Memory	64 GB RAM	16 GB RAM
Storage	1 TB SDD	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

Prerequisites Before Installation

wget should be pre-installed.

Note: Internet Access is mandatory for Securaa Installation only.

Prerequisites for TIP Deployment

Securaa TIP needs the following for a successful deployment

- Connectivity to Securaa Servers to download the latest software versions and docker images and connectivity to open-source feed URLs to get the latest feeds (URLs mentioned in network requirements).
- Port 7000,443 should be open in the TIP machine to establish connectivity with SOAR.
- Administrative privileges on the operations system platform.
- SSH Connectivity tools like Putty to connect with Securaa TIP machine.
- Browser software like Chrome to access the Securaa web interface.

Operating system requirements

Securaa TIP 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
OEL	8.10

Hardware Requirements

MSSP POC (Proof of concept):

COMPONENT	Specification
CPU	4 CPU
Memory	16 GB RAM
Storage	300 GB SSD [~ 20 Million Records]

MSSP (PRODUCTION):

COMPONENT	Specification
CPU	8 CPU
Memory	32 GB RAM
Storage	500 GB SSD [~ 30 Million Records]

Note : More storage needs to be added if records exceed 30 million.

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://repo.securaa.io/

Open-source feed URLs to be whitelisted in the firewall:

- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/7777%20Botnet%20IPs.txt
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report- from-ADEO/refs/heads/master/Indicators%20of%20Compromise-FileNames.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Ares%20RAT%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/AsyncRAT%20IPs.txt
- https://raw.githubusercontent.com/Azure/Azure-

Sentinel/master/Sample%20Data/Feeds/Log4j_IOC_List.csv

- https://faf.bambenekconsulting.com/feeds/dga-feed-high.gz
- https://faf.bambenekconsulting.com/feeds/maldomainml/malware-master.txt
- https://faf.bambenekconsulting.com/feeds/maldomainml/phishing-master.txt
- https://www.binarydefense.com/banlist.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/BitRAT%20IPs.txt
- https://www.blocklist.de/downloads/export-ips_ssh.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Browser%20Exploitation%20Framework%20(BeEF)%2 0IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Brute%20Ratel%20C4%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/BurpSuite%20IPs.txt
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report- from-ADEO/refs/heads/master/Indicators%20of%20Compromise-C2Address.txt
- https://hole.cert.pl/domains/domains.txt
- https://cinsscore.com/list/ci-badguys.txt
- https://www.cisa.gov/sites/default/files/publications/AA19-024A_IOCs.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Caldera%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Cobalt%20Strike%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Collector%20Stealer%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Covenant%20C2%20IPs.txt
- https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/refs/heads/m aster/phishing-domains-ACTIVE.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/DarkComet%20Trojan%20IPs.txt
- https://dataplane.org/proto41.txt

- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/DcRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Deimos%20C2%20IPs.txt
- https://www.dshield.org/ipsascii.html
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Patriot%20Stealer%20IPs.txt
- https://cdn.ellio.tech/community-feed
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/dan-pollock-someonewhocares-org.txt
- https://raw.githubusercontent.com/ktsaou/blocklist-ipsets/master/firehol_level1.netset
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Gh0st%20RAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/GoPhish%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Gozi%20Trojan%20IPs.txt
- https://content.govdelivery.com/attachments/USDHSCIKR/2020/03/23/file_attachm ents/1408126/ACSC%20Advisory%20-%202020-
- 005%20-%20Indicators%20of%20Compromise%20-%20COVID-19%20malicious%20activity.csv
- https://blocklist.greensnow.co/greensnow.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hachcat%20IPs.txt
- https://raw.githubusercontent.com/mitchellkrogza/The-Big-List-of-Hacked-Malware- Web-Sites/refs/heads/master/.dev-tools/_strip_domains/domains.tmp
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hak5%20Cloud%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Havoc%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hookbot%20IPs.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/1.txt

- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/2.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/3.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/5.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/6.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/7.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/8.txt
- https://raw.githubusercontent.com/ktsaou/blocklist-ipsets/master/firehol_level1.netset
- https://lolbas-project.github.io/api/lolbas.csv
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report- from-ADEO/refs/heads/master/Indicators%20of%20Compromise-MD5Hashes.txt
- https://malsilo.gitlab.io/feeds/dumps/url_list.txt
- https://malshare.com/daily/malshare.current.all.txt
- https://bazaar.abuse.ch/export/txt/md5/recent/
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Metasploit%20Framework%20C2%20IPs.txt
- https://mirai.security.gives/data/ip_list.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/MobSF%20IPs.txt
- http://multiproxy.org/txt_anon/proxy.txt
- https://myip.ms/files/blacklist/general/latest_blacklist.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Mythic%20C2%20IPs.txt
- https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/cold- steel/NCSC-MAR-Cold-Steel-indicators.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NanoCore%20RAT%20Trojan%20I

Ps.txt

- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NetBus%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NimPlant%20C2%20IPs.txt
- https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/notrack-malware.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Orcus%20RAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/projecthoneypot.org-aa.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Oyster%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/PANDA%20C2%20IPs.txt
- https://raw.githubusercontent.com/pan-unit42/iocs/master/diamondfox/diamondfox_panels.txt
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/adaway.txt
- https://raw.githubusercontent.com/ph00lt0/blocklist/refs/heads/master/domains.tx t
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/kadhosts.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Poseidon%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Posh%20C2%20IPs.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/ipsum.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Pupy%20RAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Quasar%20RAT%20IPs.txt
- https://api.recordedfuture.com/v2/ip/risklist?format=csv%2Fsplunk
- https://api.recordedfuture.com/v2/domain/risklist?format=csv%2Fsplunk

- https://api.recordedfuture.com/v2/hash/risklist?format=csv%2Fsplunk
- https://api.recordedfuture.com/v2/url/risklist?format=csv%2Fsplunk
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/RedGuard%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Remcos%20Pro%20RAT%20Trojan%20IPs.txt
- https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
- https://isc.sans.edu/api/threatlist
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report- from-ADEO/refs/heads/master/Indicators%20of%20Compromise-SHA1Hashes.txt
- https://socprime.com/wp-content/uploads/WannaCry_IOCs_public-sources-and- VT.csv
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/easyprivacy.txt
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/nocoin.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/ShadowPad%20IPs.txt
- https://raw.githubusercontent.com/brakmic/Sinkholes/master/Sinkholes_List.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Sliver%20C2%20IPs.txt
- https://www.spamhaus.org/drop/drop.txt
- https://www.spamhaus.org/drop/edrop.txt
- https://www.spamhaus.org/drop/dropv6.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/SpiceRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/SpyAgent%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Supershell%20C2%20IPs.txt
- https://www.blocklist.de/downloads/export-ips_all.txt
- https://raw.githubusercontent.com/botherder/targetedthreats/

master/targetedthre ats.csv

- https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
- https://www.dan.me.uk/torlist/
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/UnamWebPanel%20IPs.txt
- https://urlabuse.com/public/data/malware_url.txt
- https://urlabuse.com/public/data/phishing_url.txt
- https://dataplane.org/vncrfb.txt
- http://vxvault.net/URL_List.php
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/VenomRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Villain%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Viper%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Vshell%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/XMRig%20Monero%20Cryptominer%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/XtremeRAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/ZeroAccess%20Trojan%20IPs.txt
- https://zerodot1.deteque.com/main/ipfeeds/mining/ZeroDot1sMinerIPsLATESTv6.tx t
- https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
- https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
- https://urlhaus.abuse.ch/downloads/csv_online/
- https://otx.alienvault.com/api/v1/pulses/subscribed?limit=50
- https://lists.blocklist.de/lists/apache.txt
- https://lists.blocklist.de/lists/bots.txt
- https://lists.blocklist.de/lists/bruteforcelogin.txt
- https://lists.blocklist.de/lists/ftp.txt
- https://lists.blocklist.de/lists/imap.txt
- https://lists.blocklist.de/lists/mail.txt

- https://lists.blocklist.de/lists/sip.txt
- https://lists.blocklist.de/lists/ssh.txt
- https://lists.blocklist.de/lists/strongips.txt
- https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
- https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt
- http://danger.rulez.sk/projects/bruteforceblocker/blist.php
- http://rules.emergingthreats.net/blockrules/compromised-ips.txt
- https://v.firebog.net/hosts/Prigent-Malware.txt
- https://3.12.164.173/events/restSearch
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/njRAT%20Trojan%20IPs.txt
- https://openphish.com/feed.txt
- https://osint.digitalside.it/Threat-Intel/lists/latesturls.txt
- https://osint.digitalside.it/Threat-Intel/lists/latestips.txt
- https://osint.digitalside.it/Threat-Intel/lists/latestdomains.txt
- https://phishing.army/download/phishing_army_blocklist_extended.txt
- https://home.nuug.no/~peter/pop3gropers.txt
- https://sblam.com/blacklist.txt
- https://secneurx.app/API/v1/getfeeds
- http://tracker.viriback.com/dump.php
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/akamai.com-aa.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/sekio-aa.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/sekio-aa.txt
- https://raw.githubusercontent.com/mitchellkrogza/phishing/refs/heads/main/IP- addr.in-addr.arpa
- https://raw.githubusercontent.com/tsirolnik/spam-domains-list/master/spamdomains.txt

Prerequisites for CSAM Deployment

Securaa CSAM needs the following for a successful deployment:

- Connectivity to Securaa servers is required to download the latest software versions and Docker images. After establishing the connection, the application must be configured in the Application tab within the CSAM application. This configuration enables data fetching from cloud platforms, including AWS, Azure, and GCP, as well as on-premises infrastructure tools such as Nessus, QRadar, and Symantec.
- Port 8229 should be open in the CSAM machine to establish connectivity with SOAR.
- Administrative privileges on the operations system platform.
- SSH Connectivity tools like Putty to connect with Securaa CSAM machine.
- Browser software like Chrome to access the Securaa web interface.

Operating system requirements

Securaa CSAM 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

POC (Proof of concept):

COMPONENT	**Specification**
CPU	4 CPU
Memory	16 GB RAM
Storage	300 GB SSD

MSSP (PRODUCTION)

COMPONENT	**Specification**
CPU	8 CPU
Memory	32 GB RAM
Storage	500 GB SSD

Note: More storage needs to be added if records exceed 30 million.

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://repo.securaa.io/

Application configuration that fetches data from cloud and on-premises environments:

- Onprem :
  - IBM QRadar Security Intelligence
  - Nessus
  - Symantec Endpoint Protection
- Clouds:
  - AWS EC2 Instance.
  - Azure Compute.
  - Google Cloud platform.

Hardware Specification for Sia Service

To ensure optimal performance and scalability for SIA: Securaa's AI service, the following hardware requirements must be met. These specifications are designed to support the intensive computing tasks associated with AI workloads, including data processing, model training, and inference. By adhering to these recommendations, users can experience enhanced speed, efficiency, and reliability of AI operations.

This document outlines the minimum and recommended hardware specifications for deploying and maintaining SIA. Proper alignment with these requirements ensures smooth operation, reduced latency, and the ability to handle large datasets and complex algorithms efficiently.

1. Processor (CPU)

- **Model:** Intel or AMD
- **Cores:** 16 physical cores minimum (32 Cores recommended)

2. Memory (RAM)

- **Minimum Installed:** 64GB DDR4
- **Expandable Up To:** 128GB DDR4
- **Configuration:** 4 x 16GB DDR4-3200MHz DIMMs (for minimum requirement)
- **Slots Available:** At least 4 DIMM slots

3. Storage

- **Primary Drive:** 1TB SSD (Solid State Drive)
  - **Type:** NVMe M.2 SSD
  - **Purpose:** Operating System and Application installation
- **Additional Storage Options:**
  - Consider adding another SSD or HDD for data redundancy and backups, depending on the expected data usage and growth.

4. Operating System

- **OS:** Ubuntu (Latest Version)

5. Network

- **Ethernet Ports:** Dual 1GbE ports (2 x 1 Gigabit Ethernet)
  - **Optional:** 10GbE port if high network throughput is required
- **Network Interface:** Integrated on motherboard or dedicated NIC (Network Interface Card)