PostecH

Technical specifications

Tunich

SOC Assistant AI

Product:	Tunich
Document version:	1.0.0
Document Type:	Technical Specifications
Date of preparation:	August 28, 2025
Author:	Postech

TECHNICAL SPECIFICATIONS

On-premise software platform for automating the initial analysis of security tickets

Product:	Tunich SOC Assistant AI
Product version:	1
Document Type:	Technical Specifications
Date:	July 20, 2025
Classification:	Commercial
Contact:	sales@ postech.us

Table of Contents

1. GENERAL DESCRIPTION

Solution Name: Tunich SOC Assistant AI

Type: On-premise software platform for automating the initial analysis of security tickets

Version: 1.0 (MVP)

Architecture: Modular, based on containerized microservices

Licensing Model: Annual subscription license (includes support and updates)

2. TECHNICAL OBJECTIVE

Automate the triage and initial enrichment process of security incident tickets using a locally executed specialized language model (LLM), integrating knowledge from cybersecurity frameworks.

3. TECHNICAL ARCHITECTURE

3.1 Component Diagram

[Ticket Sources] → [API Gateway] → [Main Orchestrator] → [Local LLM] → [Knowledge Bases]
(Email, SIEM, API) (FastAPI) (Python/Node.js) (Llama/Mistral/ DeepSeek R1) (Vector DB + SQL)
↓
[Ticket Generator]
↓
Ticketing System] or [Web Frontend]

3.2 Main Components

Component	Technology	Description
API Gateway	FastAPI (Python)	Single point of entry for tickets, authentication management, and rate limiting
Processing Engine	Python 3.10+	Orchestration of the analysis flow and pipeline management
LLM Model	Flame 3/Mistral (Open Source)	tunable language model for security analysis
Knowledge Base	ChromaDB / Weaviate + PostgreSQL	Vector storage for semantic search in reference frames
Frontend (Optional)	React + TypeScript	Interface for reviewing and adjusting generated tickets

Component	Technology	Description
Orchestration	Docker + Docker Compose	Dockerization and service management

4. FUNCTIONAL SPECIFICATIONS

4.1 Processing Capabilities

- **Ticket Ingestion:** Support for email (IMAP/POP3), REST API, webhooks , and CSV/JSON files
- **Automated Analysis:** Entity Extraction (IPs , domains, hashes, CVEs), initial classification
- **RAG queries:** Semantic search in knowledge bases of:
    - MITRE ATT&CK® (Tactics, Techniques, Sub-techniques)
    - NIST Cybersecurity Framework (v1.1 and higher)
    - ISO/IEC 27001:2022 (Annex A - Controls)
    - (Optional) Internal SOC Playbooks
- **Output Generation:** JSON-structured tickets with:

json

```
{
"id": "INC-2024-001",
"Summary": "Enriched Analysis",
" classification ": "Malware/Phishing",
"risk": {"level": "High", "score": 85},
  " frames ": {
" mitre ": ["T1566.001", "T1204.002"],
" nist ": ["PR.AC-4", "DE.CM-1"],
   "iso27001": ["A.8.2", "A.12.6"]
},
"mitigations": ["List of recommended actions"],
"evidence": ["Relevant fragments of the analysis"]
}
```

4.2 Integrations

- **Ticketing Systems :** API for ServiceNow , Jira Service Management, Zendesk
- **SIEM:** Compatibility with Splunk ES, IBM QRadar , Microsoft Sentinel (via API)
- **SOAR:** Webhooks for Palo Alto XSOAR, Splunk SOAR, TheHive

5. SYSTEM REQUIREMENTS

5.1 Minimum Hardware

Resource	Minimum Specification	Recommended Specification
CPU	8 modern cores (Intel i7/AMD Ryzen 7 or higher)	16+ cores (Xeon/EPYC)
RAM	32 GB DDR4	64+ GB DDR4/DDR5
Storage	500 GB SSD NVMe	1 TB SSD NVMe (RAID 1 recommended)
GPU (Optional)	NVIDIA T4/ (24GB VRAM)	NVIDIA A100/A6000 or 2x RTX 4090 (VRAM 80GB)
Grid	1 Gbps Ethernet	10 Gbps for high-volume environments

5.2 Base Software

- **Operating System:** Ubuntu Server 22.04 LTS / RHEL 9 / Rocky Linux 9
- **Runtime:** Docker Engine 24.0+, Docker Compose 2.20+
- **Dependencies:** NVIDIA Container Toolkit (if using GPU), Python 3.10+

6. SAFETY SPECIFICATIONS

6.1 Security Features

- **Isolation:** All components run in isolated containers
- **Encryption:** TLS 1.3 for communications, encryption at rest for sensitive data
- **Authentication:** JWT + OAuth2 for APIs , support for LDAP/Active Directory
- **Audit:** Complete activity logs (ingestion, processing, access)
- **No internet access:** Fully local operation (air-gap compatible)

6.2 Compliance

- Designed to facilitate compliance with:
    - ISO 27001/27002
    - NIST SP 800-53
    - GDPR/LGPD (local data processing)
    - Sectoral (PCI DSS, HIPAA depending on configuration)

• 7. PERFORMANCE AND SCALABILITY

7.1 Performance Metrics

Metrics	MVP objective	Scaled Target
Tickets/hour	100-200	1000+
Latency per ticket	< 30 seconds	< 10 seconds
Availability	99.5% (Basic SLA)	99.95%
Recovery Time (RTO)	< 4 hours	< 1 hour

7.2 Scaling Strategies

- **Horizontal:** Addition of processing workers
- **Vertical:** GPU/CPU resource enhancement for the LLM model
- **Cache:** Implementing Redis for frequent queries
- **Load balancing:** For multiple instances of the analytics engine

8. IMPLEMENTATION AND MAINTENANCE

8.1 Implementation Process

1. **Assessment (1 week):** Audit of environment and specific requirements
2. **Preparation (1 week):** Hardware provisioning and base configuration
3. **Deployment (3 days):** Automated installation via Ansible scripts
4. **Configuration (1 week): Initial** fine- tuning , integrations, knowledge loading
5. **Testing (2 weeks): POC with historical data,** prompt adjustment

8.2 Maintenance

- **Updates:** Monthly security patches, quarterly feature updates
- **Backup:** Daily incremental strategy + weekly full backup
- **Monitoring:** Health dashboards , proactive alerts, accuracy metrics
- **Support:** Silver/Gold/Platinum levels (8x5, 16x5, 24x7)

9. TECHNICAL ROADMAP

Phase 1 (MVP - Current)

- Basic ticket analysis
- Integration with MITRE ATT&CK and NIST CSF
- Output in JSON/structured formats

Phase 2 (6 months)

- Fine- tuning of the model with customer data
- SOAR integration for automated responses
- Analytical Dashboard for SOC Metrics

Phase 3 (12 months)

- Specialized models by threat type
- Predictive trend analysis
- Open API for internal developers

10. SUPPORT AND WARRANTIES

- **Warranty:** 1 year on software components
- **Support SLA:** Response in < 4 hours for critical issues
- **Knowledge updates:** Quarterly for reference frameworks
- **Documentation:** Complete (administration, API, troubleshooting)
- **Community:** Access to customer portal with KB and best practices