PROJECT REPORT

ON

“AGENTIC AI MODULE FOR SECURITY”

FOR

JIO PLATFORMS LIMITED

BY

Mrunmayee Mahesh Pande

UNIVERSITY OF PUNE

MASTER IN COMPUTER APLLICATION

Maharashtra Education Society’s

INSTITUTE OF MANGEMENT AND CAREER COURSES (IMCC), PUNE-411038

College Certificate



MAHARASHTRA EDUCATION SOCIETY'S
(SINCE 1860)

INSTITUTE OF MANAGEMENT & CAREER COURSES (IMCC)
(AUTONOMOUS)

Approved by AICTE and Recognized by Savitribai Phule Pune University, Pune
IMCC Campus, 131, Mayur Colony, Kothrud, Pune 411038, Maharashtra, India | Ph.: 020-2546 6271 / 73 | e-mail: info.imcc@mespune.in | https://imcc.mespune.in

NAAC Accredited with Grade A+

Ref. No. MES IMCC /442/2025-26 **Date:06/05/2026**

CERTIFICATE

This is to certify that the Project Report entitled

"Agentic AI Module for Security"

is prepared by

Mrunmayee M Pande

M.C.A. Semester IV Course for the Academic Year 2025-26 at M.E. Society's Institute of Management & Career Courses (IMCC), Pune - 411038. M.C.A Course is autonomous and affiliated to Savitribai Phule Pune University.

To the best of our knowledge, this is an original study done by the said student and important sources used by him/her have been duly acknowledged in this report.

The report is submitted in partial fulfillment of M.C.A Course for the Academic Year 2025-26 as per the rules and prescribed guidelines of Savitribai Phule Pune University.

Dr Shilpa Parlikar
Project Coordinator

Ms. Manasi Shirurkar
Programme Coordinator

Dr. Ravikant Zirmite
Head, Dept of MCA MES IMCC

Dr. Santosh Deshpande
Director, MES IMCC

External Examiner

Head Office: 'MES Bhavan', 1214-1215, Sadashiv Peth, Pune - 411030, Maharashtra, India. | Ph.: +91-020-41038100 | www.mespune.in

Internship / Company Certificate



Letter of Internship

01.Dec.2025

Mrunmayee Pande

MES IMCC

Dear Mrunmayee Pande ,

Subject : Internship Letter

We are pleased to offer you the Internship in **Develop an Agentic AI Module for securit** from 01.Dec.2025 to 30.May.2026. Mentioned below are the terms of internship as accepted by you.

1. **Non Remunerative Learning Opportunity:** The internship is a non-remunerative temporary assignment and you will not receive any monetary compensation or stipend for the same. This does not give any right for claiming employment in the organization at present or in future.
2. **Voluntary Participation:** The participation in the internship is totally voluntary and you are at the liberty to leave the internship anytime during its duration by informing your project guide. The company also reserves right to alter or modify this duration at any point of time.
3. **Eligibility Criteria:** This internship is offered based on the eligibility criteria and information submitted by you. As per the eligibility criteria, you must be enrolled in a full time degree/diploma program with a govt. recognized institute, your institute must allow you to do internship with us and you must be minimum 18 years of age while accepting this internship.
4. **Confidentiality:** You will maintain confidentiality and secrecy of the information shared with you. You will not make presentation of the company data without prior permission of the company.
5. **Adherence to processes and protocols:** During the internship, you will adhere to all processes, operational standards / protocols as may be communicated by the company.
6. **Accident Liability**: During and in the course of the term of internship, the company shall not be viable for any injury/accident , if caused for any reason whatsoever.
7. **Handover of Company Assets / Documents:** At the end of the internship or as may be advised, you will handover company assets and any documents related to the assignment to the company.
8. **Certificate of Completion:** On successful completion of your internship, you will submit your project report to receive a certificate of internship.

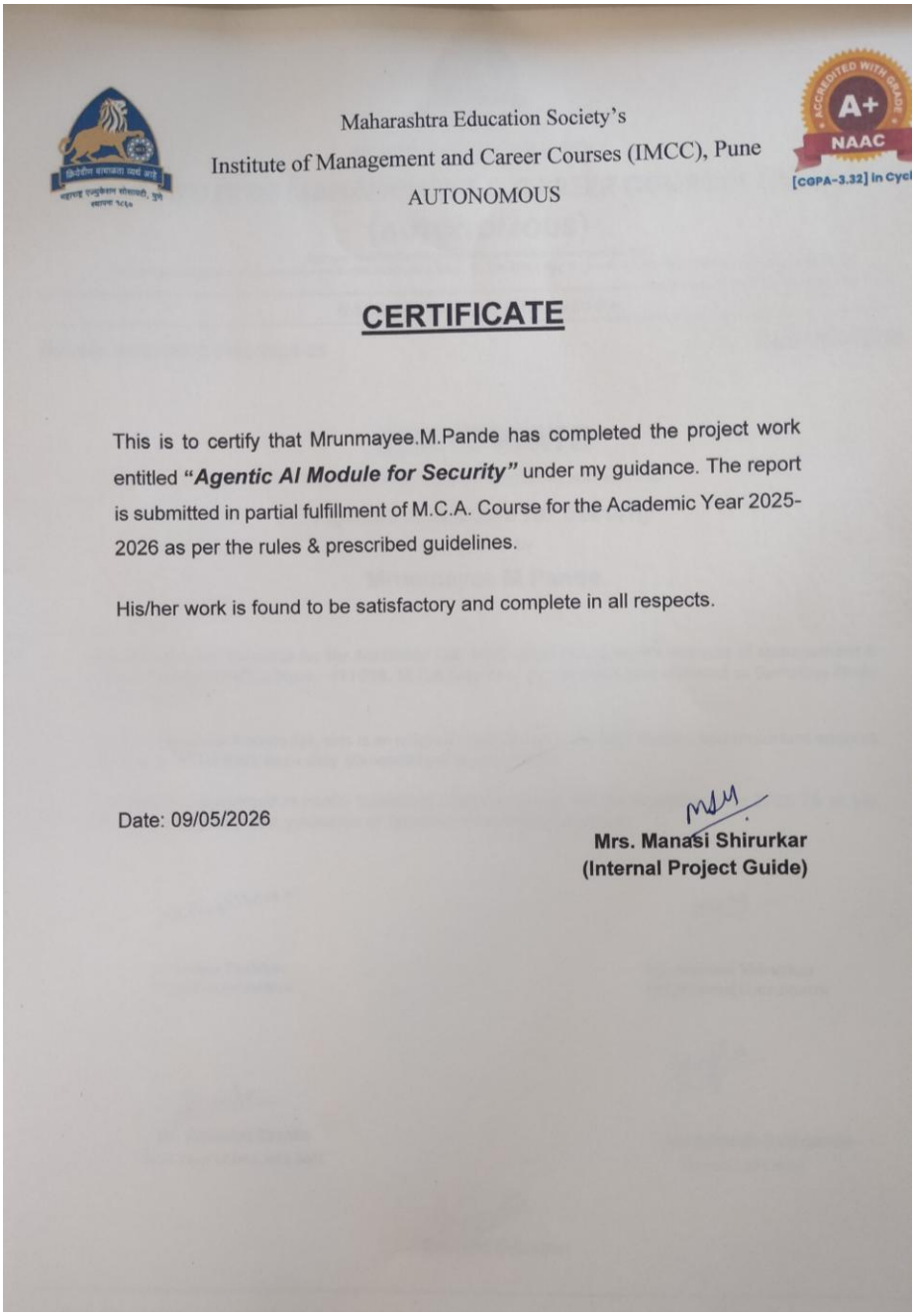
In case you do not meet eligibility criteria or if any discrepancy is found in the information submitted by you then the internship offer stands null and void.

We wish you all the best.

Yours sincerely,
for Jio Platforms Limited

Authorized Signatory

Guide Certificate



Maharashtra Education Society's
Institute of Management and Career Courses (IMCC), Pune
AUTONOMOUS

A+ NAAC

[CGPA-3.32] in Cyc

CERTIFICATE

This is to certify that Mrunmayee.M.Pande has completed the project work entitled ***"Agentic AI Module for Security"*** under my guidance. The report is submitted in partial fulfillment of M.C.A. Course for the Academic Year 2025-2026 as per the rules & prescribed guidelines.

His/her work is found to be satisfactory and complete in all respects.

Date: 09/05/2026

Mrs. Manasi Shirurkar
(Internal Project Guide)

Acknowledgement

I take this opportunity to express my sincere gratitude to **Maharashtra Education Society's Institute of Management and Career Courses (IMCC), Pune** for providing me with the platform to undertake my internship project titled *"**Agentic AI Module for Security**"* as a part of the Master of Computer Applications (MCA) curriculum.

I would like to extend my respect to my project guide for their invaluable guidance, continuous support, and constructive feedback throughout the duration of this project. Their mentorship played a crucial role in shaping the direction and successful completion of this work.

I am especially grateful to **Jio Platforms Limited** for providing me with the opportunity to work on a real-world cybersecurity project. The exposure to practical challenges, industry tools, and advanced technologies has significantly enhanced my technical knowledge and understanding of modern security systems.

I also express my sincere appreciation to all the faculty members of the MCA department for their encouragement and academic support during the course of this project.

Mrunmayee M Pande

Student MES IMCC

Roll No: 2401149

Index with page numbers

Chapter	Content	Page Number
Chapter 1	Introduction	
1.1	Company Profile	1
1.2	Abstract	1
1.2.1	Scope	2
1.2.2	Diagrams	3
1.3	Cybersecurity Fundamentals	5
1.3.1	Cybersecurity Fundamentals	5
1.3.2	Cybersecurity Landscape	6
1.3.3	Cybersecurity Challenges in Different Sectors	8
1.4	Cybersecurity Landscape	10
1.5	Cybersecurity Challenges in Different Sectors	13
Chapter 2	Literature Review	
2.1	Overview of Existing Research	16
2.2	Identification of Research Gaps	17

2.3	Relevance to Research Focus	18
Chapter 3	Threat Landscape Analysis	
3.1	Common Cyber Threats	19
3.2	Advanced Persistent Threats (APTs)	20
3.3	Threat Actor Profiling	20
3.4	Vulnerability Assessment	20
Chapter 4	Security Control and Technologies	
4.1	Network Security	21
4.2	Endpoint Security	22
4.3	Identity and Access Management (IAM)	23
4.4	Data Protection	23
4.5	Security Information and Event Management (SIEM)	24
Chapter 5	Snapshots of Project	26s

Chapter 1: Introduction

1.1Company Profile

Reliance Industries Limited (RIL) and Jio Platforms Limited are one of India's largest and most diversified multinational organizations, headquartered in Mumbai, operating across sectors such as energy, petrochemicals, telecommunications, retail, and digital services. Within the organization, the Information Risk Management (IRM) division is responsible for managing cybersecurity risks, ensuring data protection, and maintaining the security posture of enterprise systems.

As part of the team within IRM, the focus is on leveraging Artificial Intelligence and Machine Learning to enhance security operations through intelligent threat detection, automated incident response, and advanced analytics.

The project "Agentic AI Module for Security" is developed in alignment with these objectives, aiming to modernize security operations by integrating automation, orchestration, and AI-driven decision-making, thereby addressing real-world cybersecurity challenges at an enterprise scale.

1.2 Abstract

This project presents an advanced **LLM-driven AI SOAR platform** designed to automate cybersecurity operations using real-time log processing, intelligent threat detection, and automated response mechanisms.

The system accepts structured JSON security logs through a user interface or API, processes and normalizes them, and performs asynchronous threat analysis using a Large Language Model (LLM). Unlike traditional rule-

based systems, this platform relies on **context-aware reasoning**, incorporating historical memory of attack patterns and IP behaviour to identify threats.

The platform integrates a **streaming pipeline and continuous background worker** to enable real-time analysis of incoming logs. Threats are enriched using external intelligence sources and presented in a structured **SOC-style format**, including detailed explanations of the threat, its impact, and recommended actions.

Additionally, the system supports **automated response execution** through MCP tools such as IP blocking and reputation checks. A WebSocket-enabled dashboard provides live updates, threat visualization, and system metrics, enabling efficient monitoring and decision-making.

This implementation demonstrates how AI-driven automation can significantly improve detection accuracy, reduce response time, and enhance overall security posture.

1.2.1 Scope

User Requirements

- Upload and process security logs (JSON format)
- Real-time threat detection and analysis
- Intelligent threat explanation and summarization
- Threat intelligence enrichment (IP reputation)
- Automated response execution (e.g., block IP)
- Live monitoring dashboard
- Incident reporting and tracking

Module Specifications

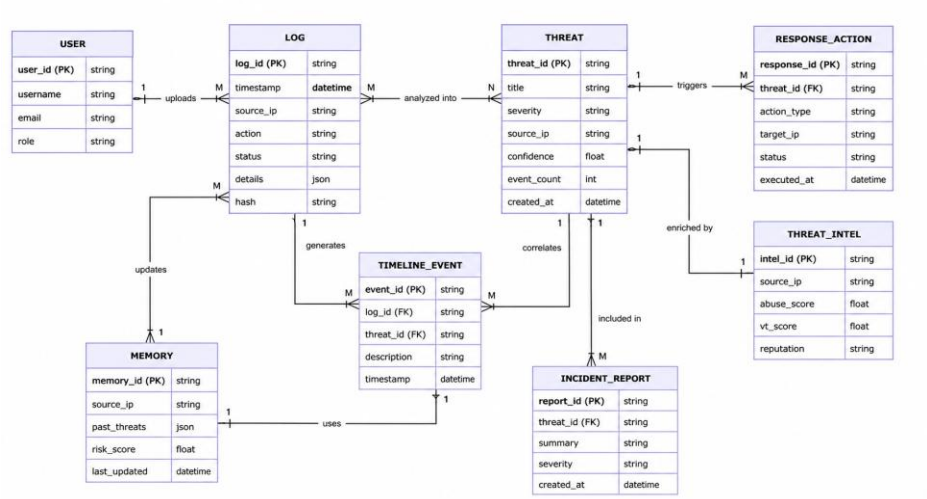
- Log Ingestion Module (API + UI)
- Log Processing & Normalization Module
- Streaming Pipeline (In-Memory / Redis / Kafka)
- Continuous Analysis Worker
- LLM-Based Threat Analysis Engine
- Threat Intelligence Module (AbuseIPDB / VirusTotal)
- Memory & Correlation Engine
- MCP Tool Execution Module
- Incident Reporting Module
- Real-Time Dashboard (Streamlit with WebSocket)

Tech Stack

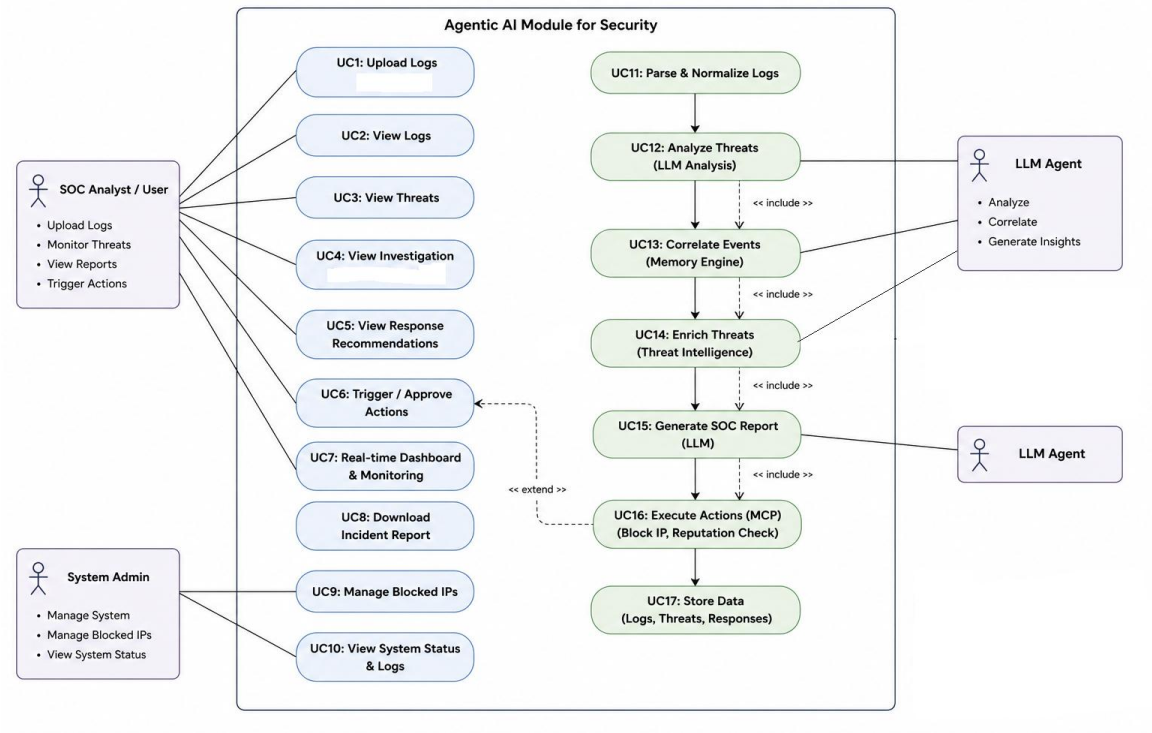
Layer	Technology
Backend	FastAPI (Python)
AI Framework	LangChain + Ollama
Frontend	Streamlit
Database	SQLite
Data Processing	Pandas
Streaming	In-Memory
Communication	WebSocket

1.2.2 Diagrams

ERD


USER
user_id (PK) string
username string
email string
role string
LOG
log_id (PK) string
timestamp datetime
source_ip string
action string
status string
details json
hash string
THREAT
threat_id (PK) string
title string
severity string
source_ip string
confidence float
event_count int
created_at datetime
RESPONSE_ACTION
response_id (PK) string
threat_id (FK) string
action_type string
target_ip string
status string
executed_at datetime
THREAT_INTEL
intel_id (PK) string
source_ip string
abuse_score float
vt_score float
reputation string
TIMELINE_EVENT
event_id (PK) string
log_id (FK) string
threat_id (FK) string
description string
timestamp datetime
MEMORY
memory_id (PK) string
source_ip string
past_threats json
risk_score float
last_updated datetime
INCIDENT_REPORT
report_id (PK) string
threat_id (FK) string
summary string
severity string
created_at datetime
uploads
analyzed into
triggers
enriched by
generates
correlates
updates
included in
uses

Use Case


Agentic AI Module for Security
SOC Analyst / User
• Upload Logs
• Monitor Threats
• View Reports
• Trigger Actions
System Admin
• Manage System
• Manage Blocked IPs
• View System Status
UC1: Upload Logs
UC2: View Logs
UC3: View Threats
UC4: View Investigation
UC5: View Response Recommendations
UC6: Trigger / Approve Actions
UC7: Real-time Dashboard & Monitoring
UC8: Download Incident Report
UC9: Manage Blocked IPs
UC10: View System Status & Logs
UC11: Parse & Normalize Logs
UC12: Analyze Threats (LLM Analysis)
UC13: Correlate Events (Memory Engine)
UC14: Enrich Threats (Threat Intelligence)
UC15: Generate SOC Report (LLM)
UC16: Execute Actions (MCP) (Block IP, Reputation Check)
UC17: Store Data (Logs, Threats, Responses)
<< include >>
<< include >>
<< include >>
<< include >>
<< extend >>
LLM Agent
• Analyze
• Correlate
• Generate Insights
LLM Agent

1.3 Cybersecurity Fundamentals

Cybersecurity refers to the practice of protecting systems, networks, applications, and data from unauthorized access, attacks, and damage. With the rapid growth of digital infrastructure, organizations generate massive volumes of security data, making manual monitoring ineffective.

Traditional security systems rely heavily on predefined rules and signature-based detection, which are insufficient against modern, evolving threats. As a result, there is a growing need for intelligent, automated, and adaptive security systems.

The proposed AI SOAR platform addresses these requirements by combining:

- automated log processing
- real-time threat detection
- AI-driven reasoning
- automated response mechanisms

This approach transforms cybersecurity from a reactive model to a proactive and intelligent system.

1.3.1 Fundamentals

The foundation of cybersecurity is based on the **CIA Triad**:

1. Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized users.

In this system:

- Access to logs and threat data is controlled via backend APIs

- Sensitive information is handled securely during processing

2. Integrity

Integrity ensures that data is accurate, consistent, and protected from unauthorized modification.

In this system:

- Logs are validated and normalized before analysis
- Hash-based deduplication ensures data consistency
- Structured JSON outputs prevent ambiguity

3. Availability

Availability ensures that systems and data are accessible when needed.

In this system:

- Continuous background worker ensures uninterrupted analysis
- Real-time WebSocket updates ensure constant visibility
- Streaming pipeline supports scalable data processing

Beyond the CIA triad, modern cybersecurity also includes:

- Authentication & Authorization
- Monitoring & Detection
- Incident Response

The proposed system integrates all these aspects into a unified AI-driven platform.

1.3.2 Cybersecurity Landscape

The modern cybersecurity landscape has evolved significantly due to technological advancements and increasing digital adoption.

1. Explosion of Security Data

Organizations generate logs from:

- network devices
- servers
- applications
- cloud platforms

Manual analysis is no longer feasible.

This system uses **automated log processing and LLM analysis**.

2. Increasing Sophistication of Attacks

Modern attacks are:

- multi-stage
- stealthy
- adaptive

Examples:

- brute force → credential compromise
- lateral movement → privilege escalation
- data exfiltration

This system detects such patterns using:

- event correlation
- memory-based reasoning

3. Shift from SIEM to SOAR

- **SIEM** → detection only
- **SOAR** → detection + response

This project implements a **SOAR system with AI intelligence**.

4. Adoption of Artificial Intelligence

AI is increasingly used for:

- anomaly detection
- classification
- decision-making

This system uses:

- LLM for reasoning
- structured SOC-style output

5. Real-Time Security Requirements

Organizations require:

- instant detection
- immediate response

This system uses:

- streaming pipeline
- background worker
- WebSocket updates

1.3.3 Challenges in Different Sectors

1. Enterprise Sector

Challenges:

- alert fatigue
- large-scale infrastructure
- multiple tools

Solution:

- LLM-based summarization reduces noise

- unified dashboard simplifies monitoring

2. Cloud Environments

Challenges:

- dynamic resources
- misconfigurations

Solution:

- real-time log ingestion
- automated analysis

3. Financial Sector

Challenges:

- fraud detection
- strict compliance

Solution:

- structured threat reports
- high-confidence detection

4. Healthcare Sector

Challenges:

- sensitive data
- high impact of breaches

Solution:

- secure processing
- anomaly detection

5. Government & Critical Infrastructure

Challenges:

- APT attacks
- national security risks

Solution:

- event correlation
- timeline-based analysis
- memory-based threat tracking

1.4 Cybersecurity Landscape

The cybersecurity landscape has undergone a significant transformation due to rapid digitalization, cloud adoption, and the increasing complexity of IT infrastructures. Organizations today operate in highly interconnected environments where data flows continuously across networks, applications, and devices. This has led to an exponential increase in the volume, velocity, and variety of security data.

Traditional cybersecurity approaches relied heavily on manual monitoring and rule-based systems. While these methods were effective for known threats, they are no longer sufficient to handle modern attack techniques, which are dynamic, multi-stage, and often designed to evade detection.

One of the major developments in this landscape is the evolution from **Security Information and Event Management (SIEM)** systems to **Security Orchestration, Automation, and Response (SOAR)** platforms. SIEM systems focus primarily on log aggregation, correlation, and

alerting. However, they require significant manual intervention for investigation and response, leading to delays and inefficiencies.

SOAR platforms address these limitations by integrating multiple security tools and automating workflows, enabling faster and more efficient incident response. Despite this advancement, many existing SOAR solutions still depend on predefined rules and lack the ability to perform intelligent reasoning or adapt to new attack patterns.

In recent years, Artificial Intelligence has emerged as a key enabler in cybersecurity. AI techniques, particularly Large Language Models (LLMs), allow systems to:

- analyze complex and unstructured data
- identify hidden patterns
- provide contextual understanding of threats
- generate human-readable explanations

The proposed system builds upon this evolution by introducing an **LLM-driven AI SOAR platform** that combines real-time data processing with intelligent decision-making.

A key feature of modern cybersecurity systems is the ability to operate in **real-time**. Organizations require immediate detection and response to minimize damage. This is achieved through:

- **streaming data pipelines**, which continuously process incoming logs
- **background workers**, which perform automated analysis without manual triggers
- **WebSocket-based communication**, which enables live updates to the user interface

The system implemented in this project incorporates all these elements. Logs are ingested through APIs or a user interface, processed and normalized, and then published to a streaming broker. A continuous analysis worker consumes these logs, performs LLM-based threat analysis, and generates structured outputs. These outputs are enriched with external threat intelligence and stored in a database for further investigation.

Another important aspect of the modern cybersecurity landscape is the need for **contextual awareness and correlation**. Isolated analysis of individual events is insufficient to detect complex attacks. The system addresses this by maintaining **memory of past events and IP behavior**, allowing it to correlate new activities with historical patterns.

Furthermore, modern systems emphasize **automation of response actions**. Instead of merely detecting threats, systems must take immediate action to mitigate risks. This project achieves this through an MCP-based tool execution layer, which enables actions such as IP blocking and reputation checks.

Overall, the cybersecurity landscape is shifting toward:

- intelligent automation
- real-time processing
- integrated security workflows
- AI-driven decision-making

The proposed AI SOAR platform represents this next generation of cybersecurity systems, moving beyond reactive approaches to a **proactive, autonomous, and intelligent security model**.

1.5 Cybersecurity Challenges

Despite significant advancements in cybersecurity technologies, organizations continue to face numerous challenges in effectively detecting, analyzing, and responding to threats. These challenges arise due to the increasing complexity of systems, the volume of data, and the sophistication of modern cyberattacks.

1. Alert Fatigue

One of the most critical challenges is **alert fatigue**, where security teams are overwhelmed by a large number of alerts generated by monitoring systems. Many of these alerts are false positives or low-priority events, making it difficult to identify genuine threats.

Solution in this system:

- The LLM analyzes logs and produces **structured, summarized threat reports**
- Only meaningful threats are highlighted
- SOC-style output reduces noise and improves clarity

2. Slow Incident Response

Traditional systems require manual investigation and decision-making, leading to delays in responding to security incidents. This increases the risk of damage and data breaches.

Solution in this system:

- Automated threat analysis using LLM
- Immediate generation of recommended actions
- MCP-based execution of responses (e.g., IP blocking)

3. Tool Fragmentation

Organizations often use multiple security tools that operate independently, leading to inefficiencies and lack of coordination.

Solution in this system:

- Unified architecture integrating multiple components
- MCP server acts as a centralized interface for tools
- Seamless interaction between detection and response modules

4. Increasing Complexity of Attacks

Modern cyberattacks are multi-stage and involve techniques such as lateral movement, privilege escalation, and data exfiltration. Detecting such attacks requires correlating multiple events over time.

Solution in this system:

- Memory-based correlation engine
- Tracking of IP behavior across multiple events
- Timeline-based analysis for reconstructing attacks

5. Data Overload

Security systems generate massive amounts of log data, making manual analysis impractical.

Solution in this system:

- Log compaction and normalization
- Chunked and batched processing
- Asynchronous and parallel analysis

6. Lack of Skilled Professionals

There is a global shortage of skilled cybersecurity professionals, making it difficult for organizations to manage complex security operations.

Solution in this system:

- AI-driven automation reduces dependency on manual expertise

- LLM provides human-readable explanations
- Simplifies decision-making for analysts

7. Lack of Real-Time Processing

Many traditional systems operate in batch mode, resulting in delayed detection and response.

Solution in this system:

- Streaming pipeline for continuous data ingestion
- Background worker for autonomous analysis
- WebSocket-based real-time updates

8. Limited Threat Context and Intelligence

Systems often lack contextual information about threats, making it difficult to assess severity and impact.

Solution in this system:

- Integration with external threat intelligence (AbuseIPDB, VirusTotal)
- Enrichment of threats with reputation data
- Context-aware LLM analysis

9. Compliance and Reporting Requirements

Organizations must generate detailed reports for audits and compliance purposes.

Solution in this system:

- Structured SOC-style threat reports
- Automated incident summaries
- Persistent storage for audit trails

10. Scalability Issues

As organizations grow, security systems must handle increasing data volumes and complexity.

Solution in this system:

- Scalable streaming architecture (Redis/Kafka support)
- Distributed processing capability
- Efficient database storage

Chapter 2: Literature Review

2.1 Overview of Existing Research

Cybersecurity research has evolved from traditional monitoring systems to intelligent and automated platforms.

SIEM Systems

Examples:

- Splunk
- IBM QRadar

Capabilities:

- log collection
- centralized monitoring
- alert generation

Limitations:

- no automated response
- rule-based detection

SOAR Platforms

Examples:

- Cortex XSOAR
- Splunk SOAR

Capabilities:

- workflow automation
- incident response

Limitations:

- limited intelligence
- manual configuration

AI-Based Systems

Recent research focuses on:

- machine learning for anomaly detection
- predictive analytics

Limitations:

- lack of reasoning
- no explainability

2.2 Identification of Research Gaps

Despite advancements, several limitations exist:

1. **Rule-Based Detection**
    - fails for unknown threats
2. **Lack of Contextual Reasoning**
    - systems cannot explain threats
3. **No Memory-Based Correlation**
    - events analyzed independently

4. **Limited Automation**
    - human intervention required
5. **No Real-Time Intelligence**
    - delayed detection
6. **Fragmented Tools**
    - poor integration

2.3 Relevance to Research Focus

This project addresses these gaps by introducing:

- **LLM-Based Reasoning**
    - context-aware threat detection
- **Memory-Based Correlation**
    - tracking IP behavior over time
- **Real-Time Streaming Analysis**
    - continuous processing
- **Autonomous Background Worker**
    - no manual trigger required
- **Structured SOC Output**
    - explainable threat reports
- **MCP Tool Integration**
    - automated response execution

This approach represents a shift toward **intelligent, autonomous cybersecurity systems**.

Chapter 3: Threat Landscape Analysis

3.1 Common Cyber Threats

The system is designed to detect a variety of threats:

1. Brute Force Attacks

- multiple failed login attempts
- detected via repeated patterns

2. Port Scanning

- scanning multiple ports
- indicates reconnaissance

3. Privilege Escalation

- unauthorized access attempts
- abnormal behavior patterns

4. Data Exfiltration

- unusual data transfer
- large outbound activity

5. Suspicious IP Activity

- repeated malicious behavior
- flagged via threat intelligence

The system uses:

- pattern recognition
- LLM reasoning
- event correlation

3.2 Advanced Persistent Threats (APTs)

APTs are long-term, stealthy attacks.

Characteristics:

- multiple stages
- long duration
- targeted attacks

Detection in this system:

- correlating multiple log events
- building attack timelines
- analyzing historical patterns using memory

3.3 Threat Actor Profiling

Threat actors are classified as:

- script kiddies
- cybercriminals
- state-sponsored attackers

System Approach:

- IP reputation analysis
- behavioral tracking
- repeated attack detection

External sources:

- AbuseIPDB
- VirusTotal

3.4 Vulnerability Assessment

Vulnerabilities are identified through:

- repeated failed actions
- abnormal patterns
- system misconfigurations

System Capabilities:

- anomaly detection via LLM
- pattern recognition
- proactive risk identification

Chapter 4: Security Controls and Technologies

4.1 Network Security

Network security in the proposed system is implemented through continuous monitoring of incoming and outgoing traffic logs, identification of malicious sources, and automated enforcement of security controls.

The system analyzes network-related log fields such as source IP, destination, ports, and activity patterns. Suspicious behaviors such as repeated failed login attempts, port scanning, or abnormal traffic spikes are detected using LLM-based reasoning combined with pattern recognition.

A key feature of this system is the integration of **automated response mechanisms** through the MCP (Model Context Protocol) tool layer. When a malicious IP address is identified, the system can trigger actions such as:

- blocking the IP address
- performing reputation checks
- retrieving historical activity logs

Threat intelligence enrichment is performed using external services such as AbuseIPDB and VirusTotal, providing additional context about IP reputation and prior malicious activity.

This approach ensures that network threats are not only detected but also mitigated in near real-time, significantly reducing the risk of unauthorized access.

4.2 Endpoint Security

Endpoint security focuses on monitoring and protecting individual systems such as servers, user devices, and application hosts.

The system processes logs generated from endpoints, including:

- login attempts
- user activity
- process execution
- service interactions

These logs are normalized and analyzed to detect anomalies such as:

- unusual login patterns
- repeated access failures
- abnormal system behavior

Unlike traditional systems that rely on predefined signatures, this platform uses an LLM to interpret behavioral patterns and identify suspicious activity. This enables detection of previously unknown or evolving threats.

The system also correlates endpoint events with network-level data, providing a holistic view of potential security incidents. This integrated approach improves detection accuracy and reduces false positives.

4.3 Identity and Access Management (IAM)

Identity and Access Management (IAM) is implemented through continuous monitoring and analysis of authentication-related events.

The system tracks:

- successful and failed login attempts
- user identities
- access patterns across systems

Brute-force attacks are detected by identifying repeated failed login attempts within a short time window. The LLM analyzes these patterns and classifies them as potential threats, providing explanations and recommended actions.

In cases of suspicious behavior, the system can:

- recommend account lockouts
- trigger IP blocking
- flag accounts for further investigation

This ensures that unauthorized access attempts are quickly identified and mitigated, strengthening overall system security.

4.4 Data Protection

Data protection in the system is achieved through secure handling, storage, and processing of security logs and analysis results.

All logs and generated threat reports are stored in a SQLite database, ensuring persistence and structured organization of data. The database maintains multiple entities, including:

- raw logs
- detected threats

- response actions
- investigation timeline
- incident reports

To maintain data integrity:

- logs are validated and normalized before storage
- duplicate entries are removed using hash-based deduplication
- structured JSON formats ensure consistency

Access to data is controlled through backend APIs, preventing unauthorized modifications.

Additionally, sensitive information is handled carefully during processing, ensuring that confidentiality and integrity are preserved throughout the system.

4.5 Security Information and Event Management (SIEM)

The proposed system functions as an advanced **SIEM + SOAR hybrid platform**, combining traditional log management capabilities with intelligent automation and response.

SIEM Capabilities

The system performs core SIEM functions such as:

- centralized log collection
- log normalization and validation
- storage and retrieval of security events
- real-time monitoring of system activity

SOAR Capabilities

Beyond SIEM, the system incorporates SOAR functionalities, including:

- automated threat detection using LLM

- workflow orchestration via background worker
- automated response execution using MCP tools
- integration with external threat intelligence sources

LLM-Based Threat Analysis

Unlike rule-based SIEM systems, this platform uses a **Large Language Model (LLM)** to perform:

- contextual threat detection
- pattern recognition
- reasoning-based classification
- generation of human-readable explanations

The LLM produces structured outputs containing:

- threat title
- severity level
- explanation of the attack
- impact assessment
- recommended actions

This significantly improves the interpretability and usefulness of alerts.

Memory and Correlation Engine

The system includes a memory component that stores:

- previously detected threats
- IP behavior patterns
- historical attack data

This enables:

- correlation of events across time
- detection of multi-stage attacks

- improved accuracy in threat identification

WebSocket-Based Live Monitoring

To support real-time visibility, the system uses WebSocket communication to push updates to the frontend dashboard.

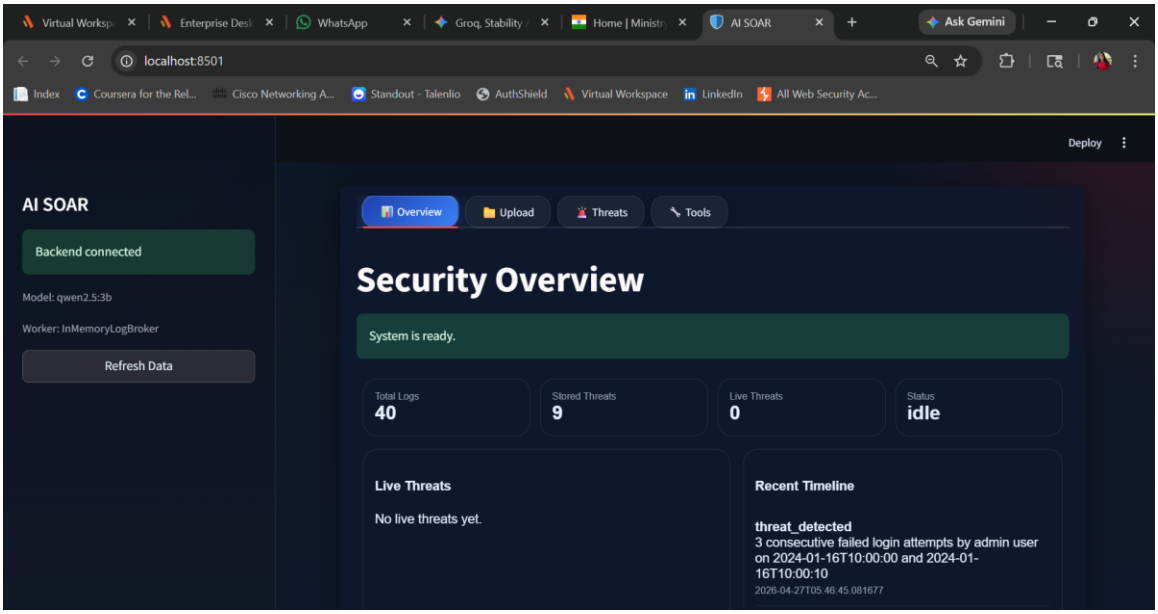
Features include:

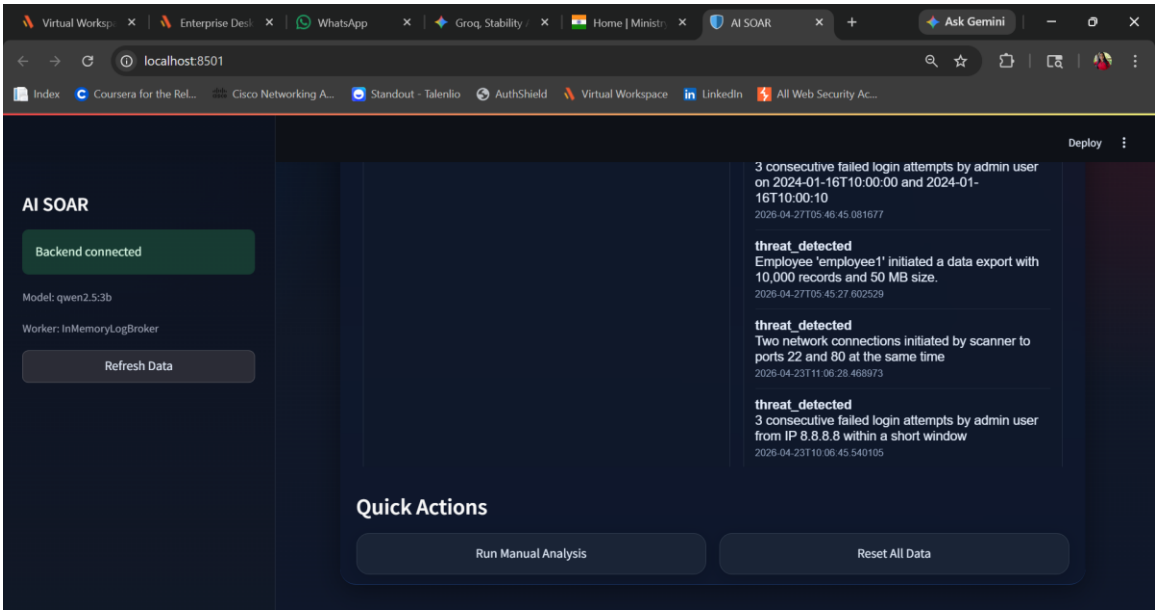
- live threat updates
- real-time metrics
- dynamic visualization of events

This eliminates the need for manual refresh and ensures continuous monitoring.

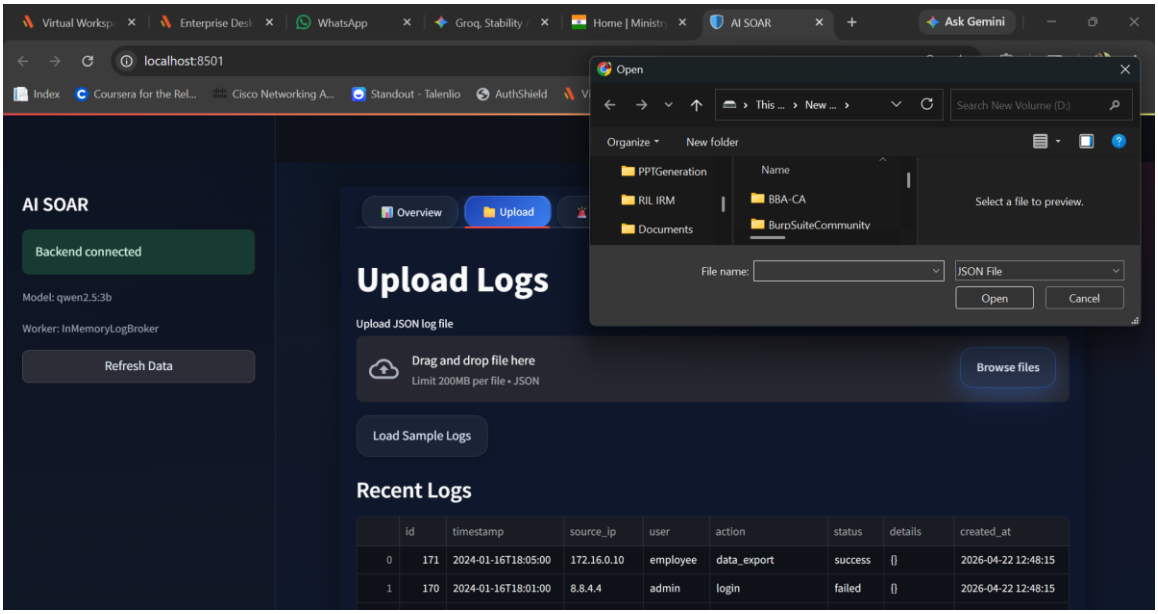
Chapter 5: Snapshots of Project

Overview

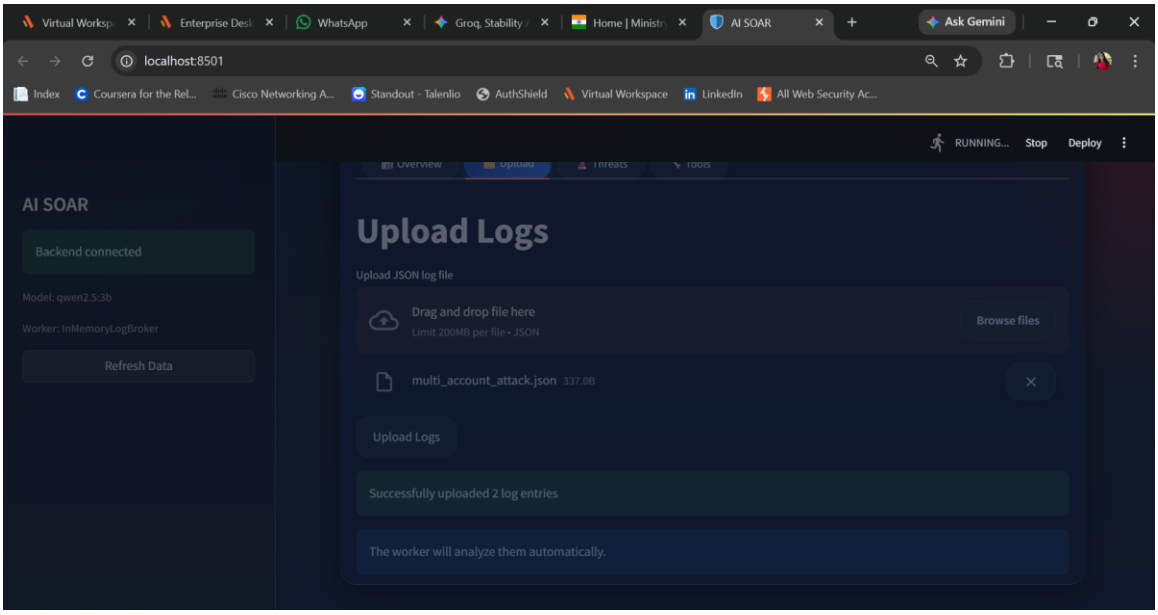




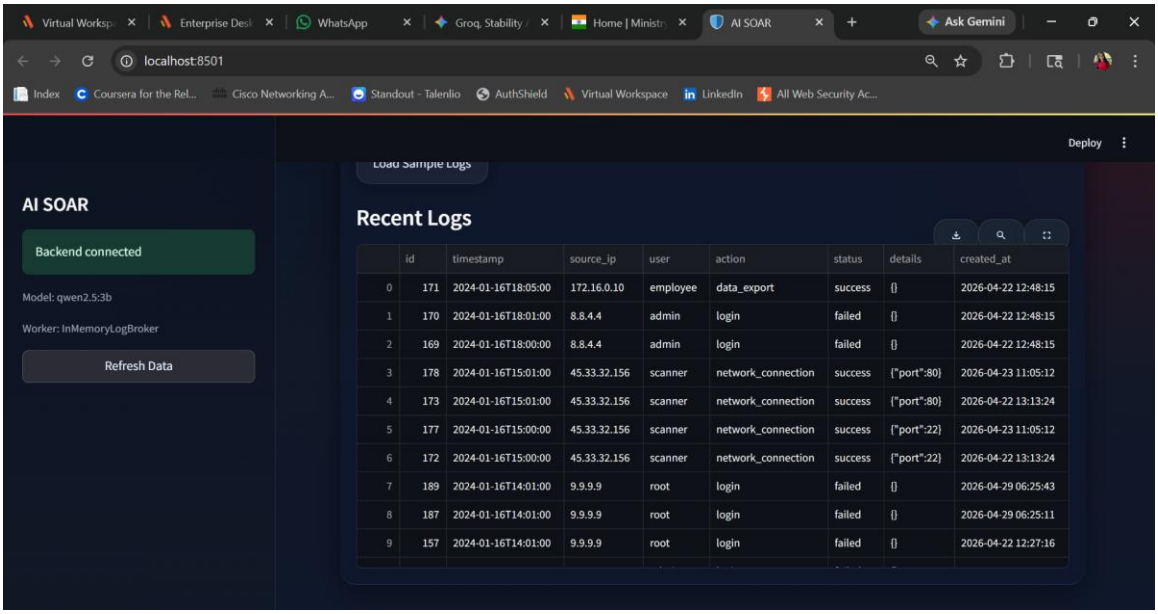
Upload Logs from Device



Successfully Logs Uploaded

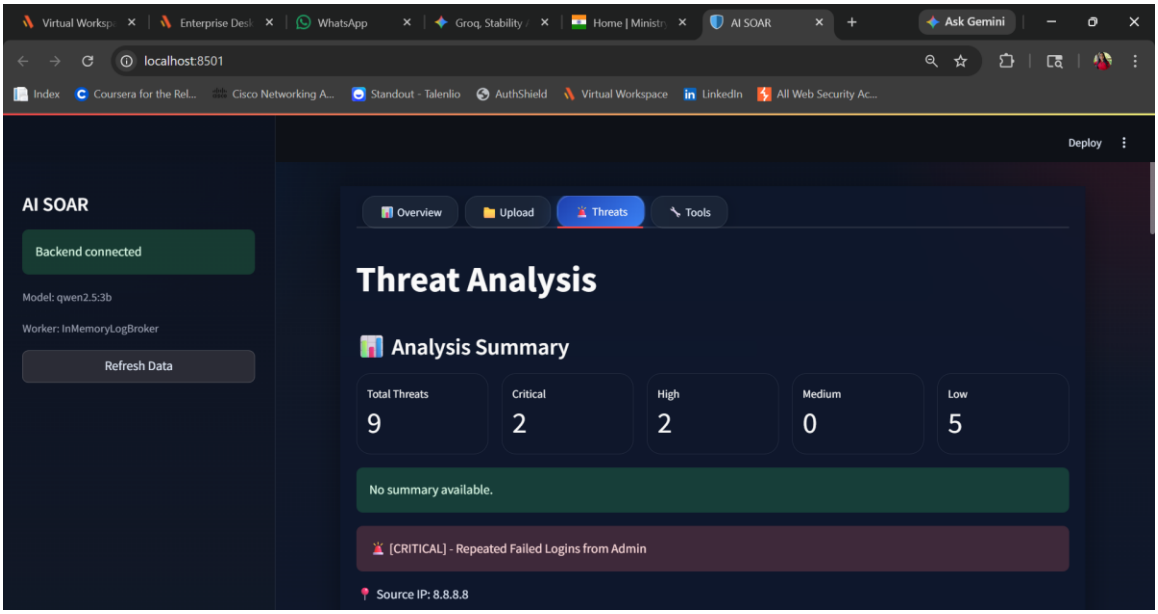


Recent Logs



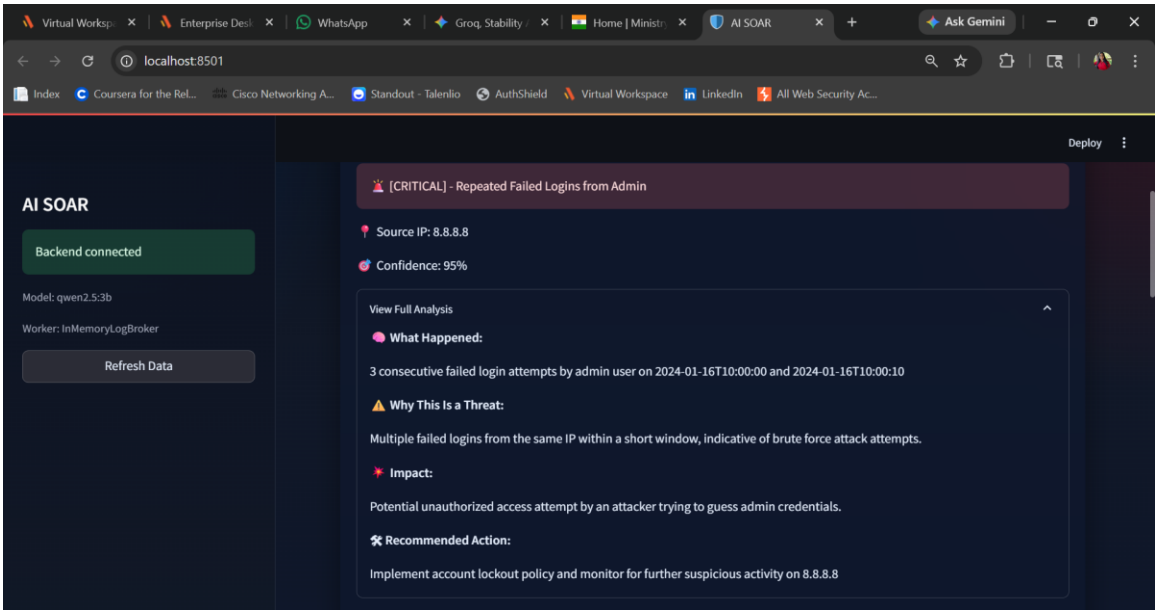
	id	timestamp	source_ip	user	action	status	details	created_at
0	171	2024-01-16T18:05:00	172.16.0.10	employee	data_export	success	{}	2026-04-22 12:48:15
1	170	2024-01-16T18:01:00	8.8.4.4	admin	login	failed	{}	2026-04-22 12:48:15
2	169	2024-01-16T18:00:00	8.8.4.4	admin	login	failed	{}	2026-04-22 12:48:15
3	178	2024-01-16T15:01:00	45.33.32.156	scanner	network_connection	success	{"port":80}	2026-04-23 11:05:12
4	173	2024-01-16T15:01:00	45.33.32.156	scanner	network_connection	success	{"port":80}	2026-04-22 13:13:24
5	177	2024-01-16T15:00:00	45.33.32.156	scanner	network_connection	success	{"port":22}	2026-04-23 11:05:12
6	172	2024-01-16T15:00:00	45.33.32.156	scanner	network_connection	success	{"port":22}	2026-04-22 13:13:24
7	189	2024-01-16T14:01:00	9.9.9.9	root	login	failed	{}	2026-04-29 06:25:43
8	187	2024-01-16T14:01:00	9.9.9.9	root	login	failed	{}	2026-04-29 06:25:11
9	157	2024-01-16T14:01:00	9.9.9.9	root	login	failed	{}	2026-04-22 12:27:16

Threat Analysis

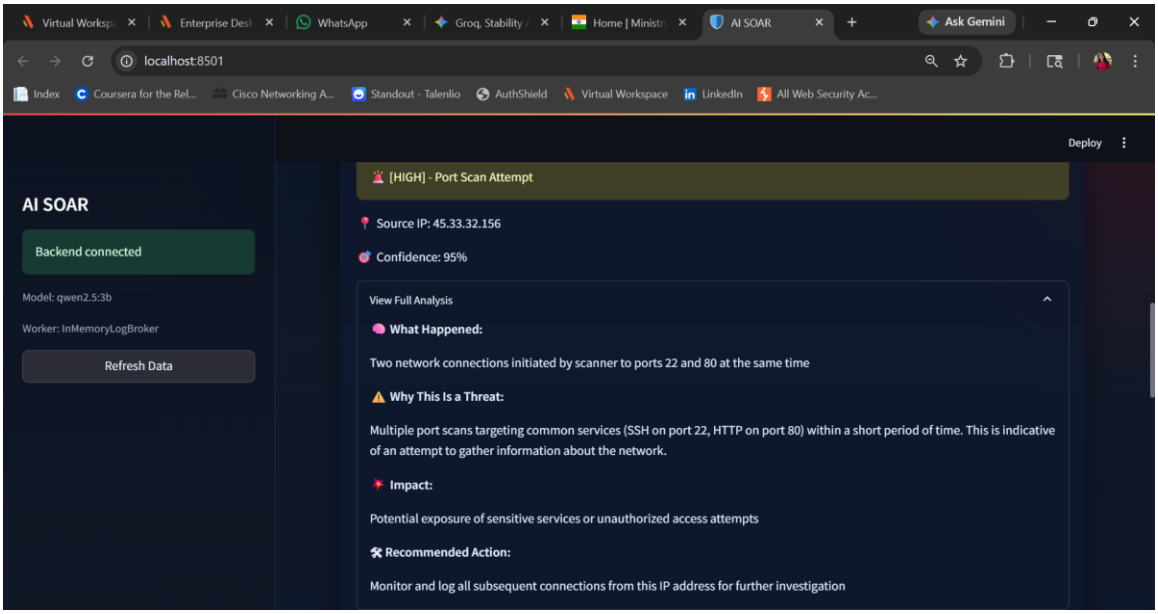


Level of Threat Analyzed

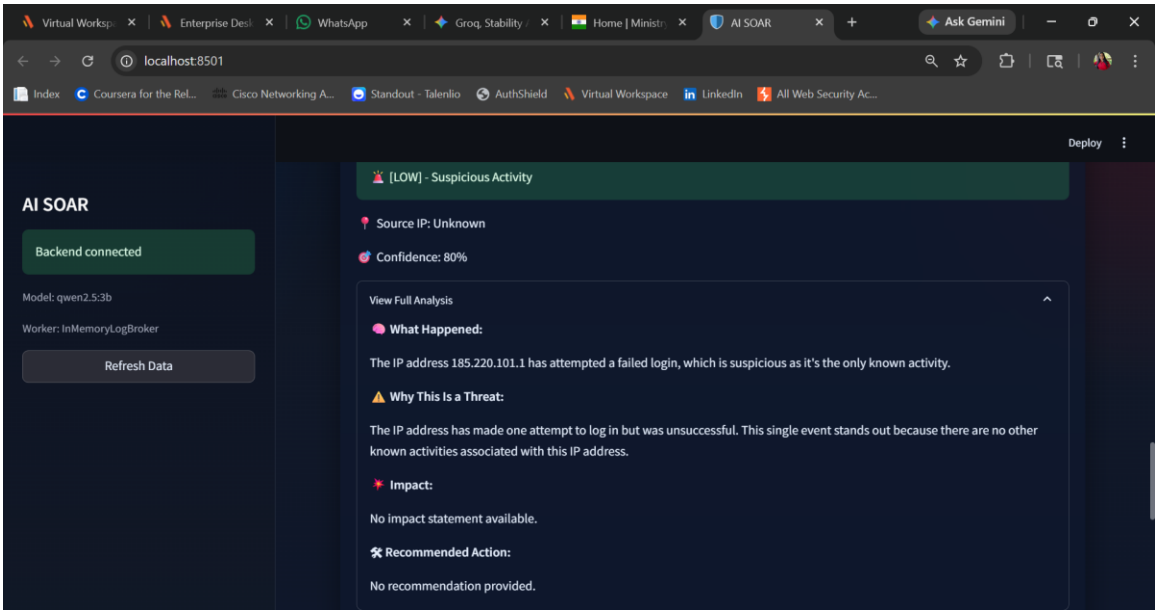
Critical



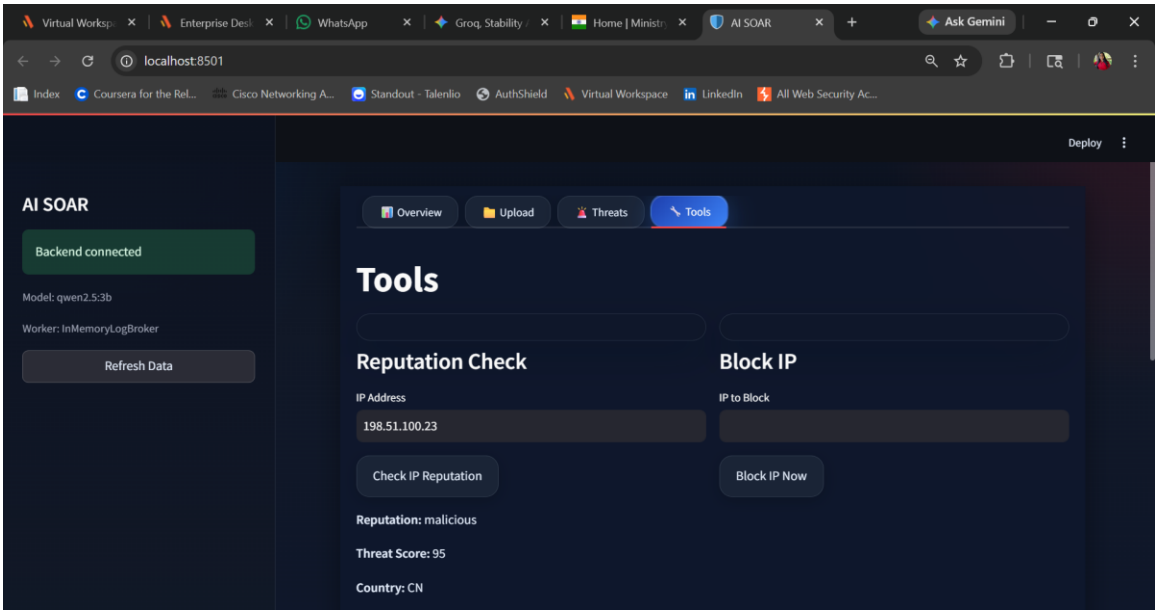
High


localhost:8501
Deploy
AI SOAR
Backend connected
Model: qwen2.5:3b
Worker: InMemoryLogBroker
Refresh Data
[HIGH] - Port Scan Attempt
Source IP: 45.33.32.156
Confidence: 95%
View Full Analysis
What Happened:
Two network connections initiated by scanner to ports 22 and 80 at the same time
Why This Is a Threat:
Multiple port scans targeting common services (SSH on port 22, HTTP on port 80) within a short period of time. This is indicative of an attempt to gather information about the network.
Impact:
Potential exposure of sensitive services or unauthorized access attempts
Recommended Action:
Monitor and log all subsequent connections from this IP address for further investigation

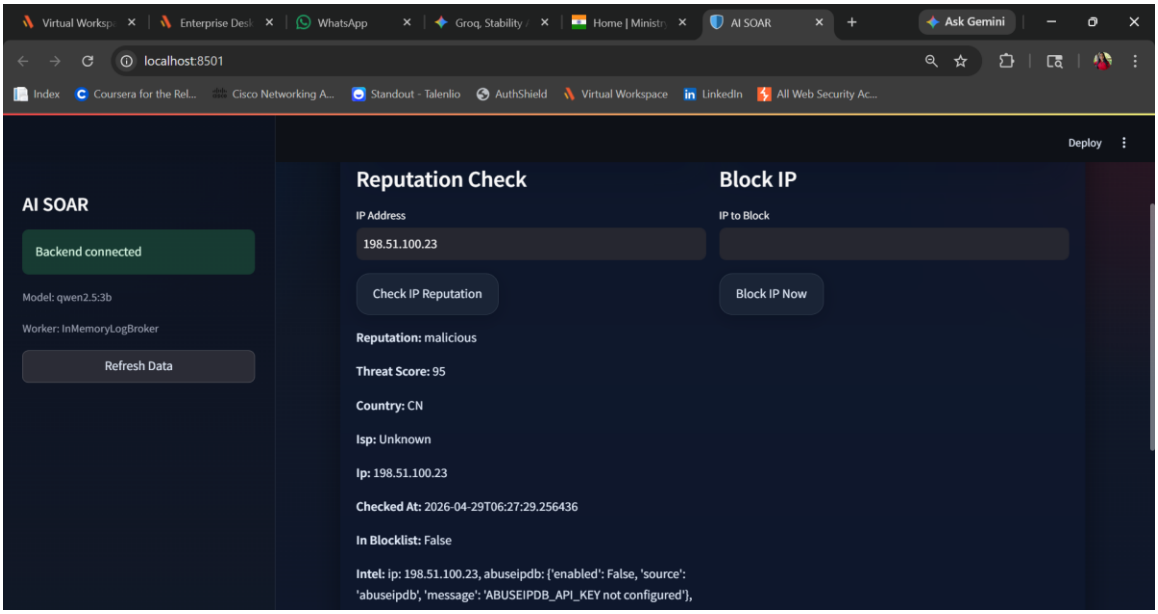
Low


localhost:8501
Deploy
AI SOAR
Backend connected
Model: qwen2.5:3b
Worker: InMemoryLogBroker
Refresh Data
[LOW] - Suspicious Activity
Source IP: Unknown
Confidence: 80%
View Full Analysis
What Happened:
The IP address 185.220.101.1 has attempted a failed login, which is suspicious as it's the only known activity.
Why This Is a Threat:
The IP address has made one attempt to log in but was unsuccessful. This single event stands out because there are no other known activities associated with this IP address.
Impact:
No impact statement available.
Recommended Action:
No recommendation provided.

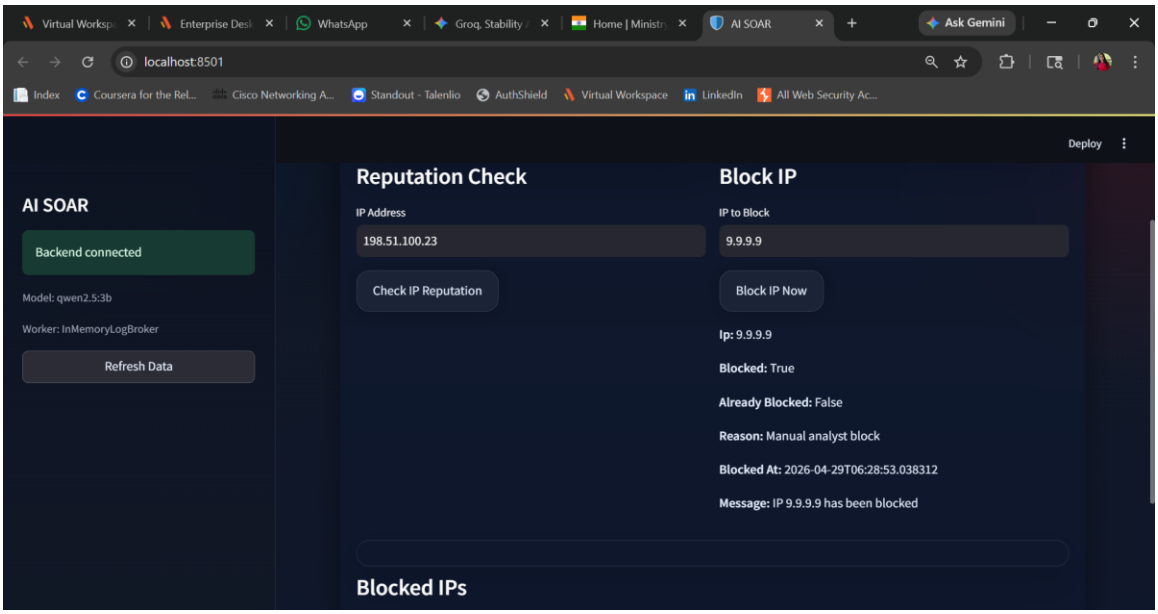
MCP Tools



Reputation Check



Block IP


Virtual Worksp
Enterprise Desk
WhatsApp
Groq, Stability /
Home | Ministr
AI SOAR
Ask Gemini
localhost:8501
Index
Coursera for the Rel...
Cisco Networking A...
Standout - Talenlio
AuthShield
Virtual Workspace
LinkedIn
All Web Security Ac...
Deploy
AI SOAR
Backend connected
Model: qwen2.5:3b
Worker: InMemoryLogBroker
Refresh Data
Reputation Check
IP Address
198.51.100.23
Check IP Reputation
Block IP
IP to Block
9.9.9.9
Block IP Now
Ip: 9.9.9.9
Blocked: True
Already Blocked: False
Reason: Manual analyst block
Blocked At: 2026-04-29T06:28:53.038312
Message: IP 9.9.9.9 has been blocked
Blocked IPs