# OmniSecure

## AI-Powered Endpoint Security Monitoring Agent

## 1. Introduction

OmniSecure is an **AI-powered endpoint security monitoring agent** designed to detect suspicious activities, abnormal system behavior, and potential cyber threats in real time.

Unlike traditional antivirus software that relies on signature-based detection, OmniSecure uses:

- **Behavioral monitoring**
- **Machine learning (anomaly detection)**
- **AI-based threat reasoning (Scaledown API)**

This enables detection of **unknown, zero-day, and behavior-based attacks**.

## 2. Objectives

The primary objectives of OmniSecure are:

- To monitor system behavior continuously
- To detect suspicious activities at the endpoint level
- To analyze anomalies using machine learning
- To correlate multiple security events
- To generate explainable, AI-driven threat verdicts
- To provide actionable security intelligence

## 3. System Overview

OmniSecure operates as a **host-based security agent** that collects telemetry from the operating system and analyzes it locally before involving AI for high-level decision-making.

### High-Level Workflow

1. Monitor system activity
2. Detect abnormal or suspicious events
3. Aggregate and correlate events
4. Trigger AI analysis when risk is high
5. Log threat verdicts and recommendations

# 4. Architecture

## Architectural Layers

AI Analyzer

(Scaledown AI API)

↓

Threat Intelligence Layer

- Event Correlation

- Threat Scoring

- Anomaly Detection (ML)

↓

Monitoring Layer

- System Monitor

- Process Monitor

- File Integrity Monitor

- Network Monitor

## 5. Module Description

### 5.1 System Monitoring Module

**Purpose:**
Monitors overall system health.

**Metrics Collected:**

- CPU usage
- Memory usage

**Security Value:**
Detects abnormal resource spikes often caused by malware, cryptominers, or exploits.

### 5.2 Process Monitoring Module

**Purpose:**
Monitors all running processes.

**Detection Logic:**

- Suspicious process names
- High CPU-consuming processes

**Security Value:**
Identifies malicious or unauthorized executables.

### 5.3 File Integrity Monitoring (FIM)

**Purpose:**
Monitors changes in sensitive directories.

**Events Detected:**

- File creation
- File modification
- File deletion

**Security Value:**
Critical for detecting ransomware and unauthorized file tampering.

### 5.4 Network Monitoring Module

**Purpose:**
Tracks active network connections.

**Detection Logic:**

- Outbound connections
- Unusual destination ports

**Security Value:**
Detects command-and-control (C2) communication and data exfiltration attempts.

### 5.5 Anomaly Detection Module (Machine Learning)

**Algorithm Used:**
Isolation Forest (Unsupervised Learning)

**Features Used:**

- CPU usage
- Memory usage
- Process count
- Network connection count
- Time context (hour of day)

**Security Value:**
Detects zero-day and unknown threats without prior signatures.

### 5.6 Event Bus

**Purpose:**
Acts as a shared event buffer.

**Functionality:**

- Stores recent security-relevant events
- Enables correlation between modules

**Security Value:**
Allows multi-stage attack detection.

### 5.7 AI Analyzer (Scaledown API)

**Purpose:**
Provides high-level threat reasoning and explanations.

**Responsibilities:**

- Analyze correlated security events
- Determine threat severity

- Generate human-readable explanations
- Recommend mitigation actions

**Why AI Is Used Here:**
AI excels at reasoning, pattern interpretation, and explanation—tasks unsuitable for rule-based logic alone.

## 6. AI Integration Strategy

OmniSecure uses a **hybrid AI approach**:

| Layer | Technique |
|---|---|
| Detection | Rule-based + ML |
| Reasoning | Large Language Model (Scaledown) |
| Output | Explainable intelligence |

Only **summarized events** are sent to the AI, ensuring:

- Privacy preservation
- Low API cost
- Fast response time

## 7. Threat Scoring & Correlation

Each suspicious event contributes to a **threat score**.

**Example Scoring:**

| Event | Score |
|---|---|
| AI anomaly detected | +40 |
| Suspicious process | +30 |
| File deletion | +20 |
| Unusual network port | +10 |

When the threat score exceeds a threshold:

- Events are correlated
- AI analysis is triggered

## 8. Logging System

All events are logged with:

- Timestamp
- Severity level (INFO / WARNING / CRITICAL)

- Description

Logs are stored locally in:

logs/events.log

## 9. Installation & Setup

### Prerequisites

- Python 3.10+
- Windows OS
- Scaledown AI API key

### Dependency Installation

```
pip install -r requirements.txt
```

### Environment Variable Setup

```
setx OMNISECURE_AI_KEY "your_scaledown_api_key"
```

## 10. Running the System

```
python agent/main.py
```

The agent runs continuously and writes logs automatically.

## 11. Security & Ethical Considerations

- OmniSecure must only be used on authorized systems
- No credential harvesting or spying features are included
- AI is used strictly for security analysis

## 12. Limitations

- User-mode monitoring only (no kernel hooks)
- No real-time UI (CLI/log-based)
- Requires baseline data for anomaly detection

## 13. Future Enhancements

- Real-time SIEM dashboard
- MITRE ATT&CK mapping
- Ransomware behavior classification
- Go-based high-performance agent
- Cloud-based centralized threat intelligence

## 14. Conclusion

OmniSecure demonstrates how **AI, machine learning, and system-level monitoring** can be combined to build a modern endpoint security solution.

It serves as:

- A practical cybersecurity research project
- A real-world EDR/UEBA prototype
- A strong AI + security portfolio system