Real Time Monitoring and Compliance

## Implementation of Continuous Real-Time Monitoring & Compliance in Our Platform

Our platform integrates Continuous Real-Time Monitoring & Compliance as a core capability to ensure uninterrupted visibility across OT systems and full alignment with regulatory standards. Within our cybersecurity platform, this component provides live insights into system behaviour, environmental readings, and user activity while maintaining compliance with standards like NERC CIP, IEC 62443, and GDPR. It supports threat detection and forensic auditing through constant data collection and system oversight, functioning as the nervous system of the platform.

## How It Links to Other Modules

Each component in the system benefits from continuous insights and compliance assurance:

1. Ransomware Detection Engine → Provides behavioural input from monitored sensors and devices.

2. SOAR Engine → Enables audit-triggered response actions based on real-time conditions.

3. Backup & Recovery → Validates system state and backup integrity with timestamped logs.

4. Secure Communication & Logging → Encrypts monitored data and preserves audit records.

5. Advanced Threat Intelligence → Informs AI models with live data patterns from monitored networks and OT devices.

## Key Functions of This Feature

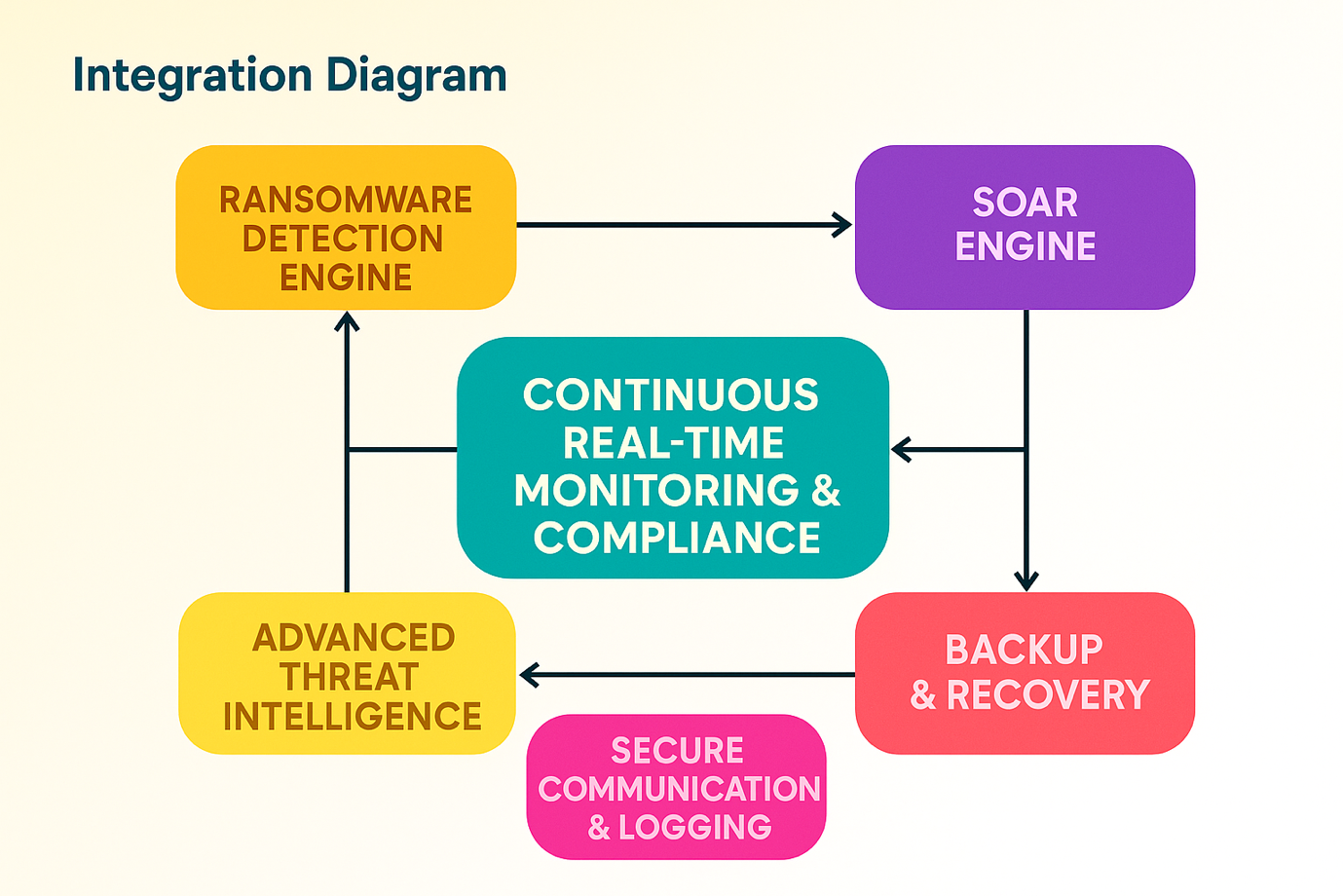
• Collects real-time telemetry from OT assets (Modbus, OPC UA, SCADA, etc.).  
• Tracks system behaviour, e.g., voltage, current, temperature, process cycles, file access, network flow.  
• Auto-generates audit trails for every monitored event for compliance validation.  
• Detects anomalous patterns like temperature spikes, protocol misuse, or sudden traffic bursts.  
• Offers compliance mapping to frameworks like IEC 62443, NERC CIP, and GDPR via reporting modules.

## When It Becomes Useful

This feature becomes especially critical during:  
• Pre-attack phases, where subtle deviations may signal malicious activity.  
• Live attacks, where rapid anomalies in industrial processes can trigger automated containment.  
• Post-incident investigation, providing an unbroken timeline of environmental and system events.  
• Audits & reporting when detailed logs must prove due diligence and regulatory compliance.

## Integration Diagram

The diagram below illustrates how Continuous Real-Time Monitoring & Compliance is positioned at the heart of the platform’s data collection loop, feeding live insights to every other module:



This diagram visually represents the multi-stage malware infection process and how different tools and systems were used during your analysis.

### 1. Initial Stage – Infection Vector

• Phishing Email: The entry point is often a malicious phishing email.  
• Attachment: Contains a macro-enabled document (e.g., Word or Excel file) that, when opened, executes malicious code.  
Transition: User interaction triggers the macro to initiate the next stage.

### 2. Stage 1 – Macro Dropper (VBA Script)

• Executes when the user enables macros.  
• The VBA macro drops or downloads a loader.  
• Tool used: Static Analysis (e.g., oletools, OLEVBA) to inspect the macro script.  
Transition: Downloads the next payload from a remote server.

### 3. Stage 2 – Loader/Dropper

• Responsible for downloading and executing the main backdoor component.  
• Common techniques: obfuscation, anti-analysis methods.  
• Tools used: x64dbg, PEStudio, or ProcMon for behaviour observation.  
Transition: Injects the final payload (Conti ransomware) into memory.

### 4. Stage 3 – Conti Ransomware (Main Payload)

• Performs encryption of files.  
• Connects to Command & Control (C2) server.  
• Implements persistence mechanisms.  
• May use Living off the Land Binaries (LOLBins) for stealth.

Observed Behaviour:  
• Registry changes  
• Service creation  
• Encryption process monitoring.

### 5. Logging, Monitoring, and Detection

• Wireshark: To capture network communication (e.g., C2 traffic).  
• Snort/Suricata: For detecting suspicious activity and rules triggering.  
• Process Monitor: To log system activity during infection.

### 6. Security Framework Mapping

• MITRE ATT&CK: Techniques like Initial Access (T1566), Execution (T1059), Persistence (T1053).  
• ACSC Essential Eight: Highlighting gaps in controls such as macro control, patching, and application whitelisting.

### 7. Outcome & Defensive Recommendations

• Improved email filtering.  
• Endpoint Detection and Response (EDR).  
• Enhanced user awareness training.  
• Disabling macros by default.

## Summary

Continuous Real-Time Monitoring & Compliance serves as the central awareness hub in our Unified OT Ransomware Protection Platform. It empowers proactive defence, fuels intelligent automation, and guarantees regulatory conformity. With this feature, organizations can detect, respond to, and document every action — in real time — ensuring uptime, transparency, and resilience.