Advanced Threat Intelligence Integration

1. Overview

This implementation outlines how to incorporate **Advanced Threat Intelligence Integration** into the OT Ransomware Protection & Incident Response Platform. The goal is to enable the platform to make smarter, faster, and more informed security decisions using real-time external threat data.

2. Objective

The main objectives of this integration are to:

- Keep the system updated with the latest ransomware tactics, techniques, and indicators.
- Correlate internal events with global threat data for accurate detection.
- Enhance the decision-making process in response and recovery.
- Support compliance with logging and audit trails based on threat context.

3. Key Features of This Integration

- **Real-Time Threat Feed Ingestion**
  - Continuously pull data from trusted sources (e.g., MITRE ATT&CK, MISP, AlienVault OTX, etc.).
- **Threat Correlation and Enrichment**
  - Compare internal alerts with known IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques, and Procedures).
- **Threat Context Scoring**
  - Assign severity levels to threats to prioritize incident response actions.
- **Feed-Driven Automation**
  - Use threat data to guide response playbooks, deception updates, and recovery decisions.

4. Implementation Steps

Step 1: Connect to External Threat Intelligence Sources

- Deploy or subscribe to a threat intelligence platform (e.g., MISP).
- Set up STIX/TAXII connections to gather data like:
    - IP addresses
    - Domains
    - File hashes
    - Exploited vulnerabilities
    - Threat actor profiles

Step 2: Normalize and Store Threat Data

- Create scripts (e.g., in Python) or use connectors to format threat feed data into JSON or STIX 2.1 format.
- Store threat data in a centralized intelligence database accessible by other platform modules.

Step 3: Integrate with Detection Engine

- Feed threat indicators into the Ransomware Detection Engine.
- Use threat data to train or update ML models and correlate anomalies with known attack signatures.

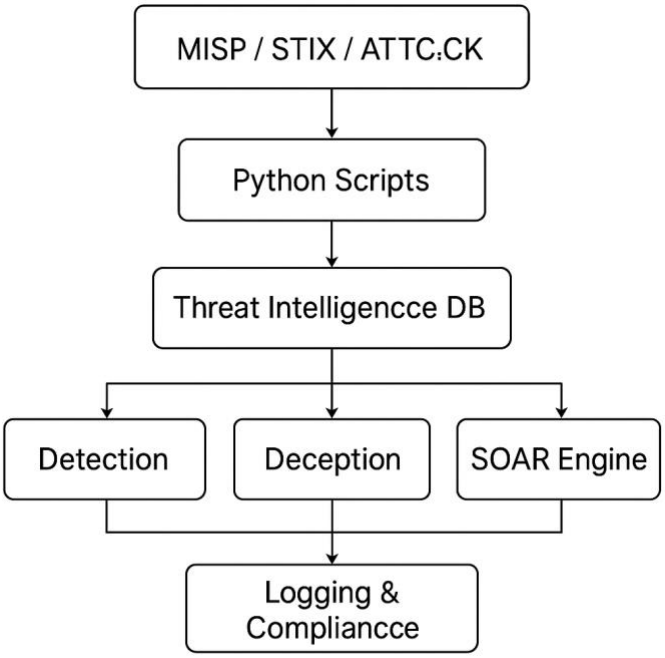
Step 4: Enhance Incident Response (SDAR)

- Define automated response rules based on threat severity (e.g., isolate if threat score > 80).
- Use intel metadata (e.g., attacker country, TTP) to guide recovery actions and escalation levels.

Step 5: Support Forensics & Compliance Logging

- Every time threat intel is used (matched or triggered), log the action with:
    - Timestamp
    - Source of threat intel
    - Impacted systems
- This supports GDPR, IEC 62443, and NERC CIP audit requirements.

5. Flow Diagram



6. Expected Outcomes

- System always has the latest intel on ransomware variants and campaigns.
- Faster, more informed responses to attacks based on real-world data.
- Smarter deception and detection based on current adversary behavior.
- Better compliance and auditability through enriched forensic logging.

7. Conclusion

By implementing Advanced Threat Intelligence Integration, the OT cybersecurity platform gains the ability to proactively defend against threats. It acts not only on internal signals but also on evolving global threat knowledge—making it adaptive, context-aware, and resilient.