Automated Incident Response & Containment

Our platform includes Automated Incident Response & Containment as a core cybersecurity capability to ensure the fastest possible reaction to ransomware threats and advanced persistent attacks.  
  
When an attack is detected, the platform immediately isolates infected OT systems to prevent lateral movement. This functionality is critical to protecting the broader network, especially in operational technology environments like SCADA, PLCs, and HMIs where the damage can quickly escalate.

# 🔗 How It Links to Other Modules

- Ransomware Detection Engine → Triggers the incident response sequence as soon as a threat is confirmed.  
- SOAR Engine → Executes automated playbooks such as device isolation, process shutdown, backup initiation, and system rollback.  
- Secure Backup & Restore → Called by SOAR to restore affected systems to their last known safe state.  
- Secure Logging → Logs every automated response action for compliance and forensic review.  
- Admin Dashboard → Provides visual insight and real-time control over response workflows.

# ⚙️ Key Capabilities of the Response Engine

- Immediate Isolation: Automatically detaches infected OT assets from the network to stop ransomware spread.  
- Automated Playbooks: Uses SOAR to initiate predefined responses like:  
 - Pausing dangerous processes (e.g., PLC commands)  
 - Initiating just-in-time backups of active configurations  
 - Rebooting or locking down exposed nodes  
- Notification System: Alerts the cybersecurity team instantly with actionable intelligence (device ID, threat vector, file path, hash, time).  
- Smart Restore Triggers: Works with the backup module to restore clean snapshots as part of the response loop.  
- Low-Latency Execution: All actions are performed in milliseconds to reduce time-to-containment.

# 🧠 When It Becomes Useful

- During active ransomware execution  
- When behavioral analysis flags high-risk processes  
- As part of recovery after partial encryption  
- During pre-defined policy enforcement (e.g., access anomaly)

# 📊 Integration Diagram (Described)

[Ransomware Detection Engine]  
 ↓  
[SOAR Engine] → [Automated Response Playbook]  
 ↓ ↓  
 [Secure Logging] [Backup & Restore Trigger]  
 ↓ ↓  
 [Alert Admins] [System Rollback]

# ✅ Summary

Automated Incident Response & Containment transforms the traditional reaction-based cybersecurity approach into a proactive defense loop. It ensures threats are mitigated before they cause widespread damage and supports recovery without requiring human intervention at every stage. The result is a self-contained security mechanism that matches the speed and stealth of modern ransomware with automated resilience.