Tools for Implementing Automated Incident Response & Containment

# 🧰 1. SOAR (Security Orchestration, Automation, and Response)

• Tools:  
 - TheHive + Cortex: Open-source combo for incident response and automated actions.  
 - Shuffle: Lightweight Python-based SOAR engine with web-based playbook builder.  
 - Splunk SOAR: Enterprise-grade commercial solution for complex automation.  
  
• Purpose:  
 - Create and run automated playbooks.  
 - Integrate with detection and backup APIs.  
 - Handle conditional logic, retries, and multi-step containment workflows.

# 🖥️ 2. System Isolation & Control

• Tools:  
 - Custom Python scripts (e.g., using `paramiko`, `psutil`, `os`, `subprocess`).  
 - Network microsegmentation tools (e.g., Cisco ISE, AWS Network Firewall).  
  
• Purpose:  
 - Isolate compromised devices or services.  
 - Kill specific suspicious processes or halt ICS routines.

# 🔄 3. Playbook Trigger & Event Integration

• Tools:  
 - FastAPI, Flask (webhooks for threat signals)  
 - MQTT or REST APIs to connect with detection engine  
  
• Purpose:  
 - Link threat detection with immediate response triggers.  
 - Pass context (device ID, threat type, hash) to SOAR engine.

# 📣 4. Notification & Alerting

• Tools:  
 - Slack API, Microsoft Teams Webhooks  
 - SMTP libraries for email alerts  
 - ELK stack for centralized dashboards  
  
• Purpose:  
 - Notify SOC teams instantly when a response is triggered.  
 - Deliver enriched context for rapid decision-making.

# 🔐 5. Secure Logging

• Tools:  
 - Python `logging`, `hmac` for tamper-proof logs  
 - ELK Stack, Wazuh for visualization  
 - HashiCorp Vault for key and secret management  
  
• Purpose:  
 - Log every step of the incident response.  
 - Ensure logs cannot be erased or altered post-attack.

# 📋 6. Backup Coordination

• Tools:  
 - API integration with AWS S3 snapshot service  
 - Trigger local/edge backup agents  
  
• Purpose:  
 - Initiate just-in-time snapshots before encryption.  
 - Restore clean system states automatically.

# 📊 Recommended Tool Stack

|  |  |
| --- | --- |
| Feature | Tool(s) |
| Playbook orchestration | TheHive, Cortex, Shuffle, Splunk SOAR |
| Process/network isolation | Python scripts, Firewall APIs |
| Response triggers | FastAPI, REST hooks, MQTT |
| Notification | Slack, Email, ELK Stack |
| Logging | Python `logging`, HMAC, ELK, Vault |
| Backup interaction | AWS API, edge agents |

# ✅ Summary

These tools enable a resilient and responsive defense system that reacts in real time to ransomware activity. By leveraging SOAR platforms, secure APIs, and intelligent automation, the platform reduces incident response time from hours to seconds, minimizes manual work, and ensures operational continuity in critical OT environments.