Unicis SOC Plan

Comprehensive breakdown of features and integrations for UNICIS SOC stack that includes Wazuh, TheHive, Zabbix, MISP, Cortex, and Shuffle SOAR.

Integrated Features

1. Centralised Incident Management

- Wazuh + TheHive:
  - Automate alert ingestion from Wazuh into TheHive to create structured cases.
  - Analysts triage Wazuh alerts in TheHive and enrich them with observables from threat intelligence (via Cortex and MISP).
- Zabbix + TheHive:
  - Send Zabbix performance or anomaly alerts to TheHive for further analysis.
  - Automatically create cases in TheHive when Zabbix detects critical infrastructure issues that may indicate security concerns.
- TheHive + Shuffle SOAR:
  - Use Shuffle to automate TheHive workflows, such as escalating alerts to incidents, assigning tasks, or notifying teams.

2. Automated Threat Intelligence Integration

- Wazuh + MISP:
  - Export Wazuh-detected IoCs (e.g., IPs, domains, hashes) to MISP for community sharing.
  - Use MISP threat feeds in Wazuh for correlation with logs and real-time alerts.
- MISP + TheHive:
  - Automatically correlate IoCs from MISP with incidents in TheHive.
  - Enrich TheHive cases with detailed threat actor profiles, tactics, and related indicators from MISP.
- MISP + Cortex:
  - Leverage Cortex analyzers to validate and enrich MISP IoCs (e.g., domain reputation, IP geolocation).
  - Cortex results can be fed back into MISP to keep threat intelligence updated.
- Shuffle + MISP:
  - Automate the ingestion of new threat feeds into MISP and push updates to Wazuh.
  - Trigger Shuffle workflows for MISP when new IoCs are detected, such as adding alerts to Wazuh or sharing them with other organisations.

3. Proactive Alert Management

- Wazuh + Zabbix:
  - Correlate Wazuh alerts with Zabbix metrics to identify suspicious activities with infrastructure context.
- Zabbix + Shuffle SOAR:
  - Automate responses to Zabbix alerts, such as restarting failing services or notifying teams about resource exhaustion.
- TheHive + Cortex:
  - When alerts in TheHive contain observables (IPs, domains, hashes), Cortex analyzers automatically enrich them with actionable intelligence.

- TheHive + Shuffle SOAR:
    - Use Shuffle to assign tasks in TheHive, send notifications to teams, and escalate alerts based on severity or case type.

4. Enhanced Visualisations

- Zabbix Dashboards:
    - Combine security alerts from Wazuh with performance metrics from Zabbix into unified dashboards.
- TheHive Analytics:
    - Analyse incident trends and response times, enhanced by enriched threat data from MISP and Cortex.
- Shuffle Dashboards:
    - Use Shuffle to create centralised dashboards displaying SOC-wide metrics: alert counts, case statuses, response SLAs, and resolved incidents.

5. Automated Playbooks

- Shuffle SOAR:
    - Automate multi-step responses, such as:
        - Triggering Cortex enrichment for new TheHive observables.
        - Updating MISP with new IoCs detected by Wazuh or validated by Cortex.
        - Quarantining affected endpoints using Wazuh triggers.
    - TheHive Playbooks:
        - Guide analysts through consistent incident response workflows:
        - Example: Phishing case playbook → Analyze email headers in Cortex → Cross-check domains in MISP → Update case findings in TheHive.

6. Improved Threat Detection

- Wazuh + Cortex:
    - Automatically enrich Wazuh alerts using Cortex analyzers (e.g., VirusTotal for file hashes, AbuseIPDB for IPs).
    - Highlight false positives or flag high-risk threats based on enrichment data.
- MISP + Shuffle SOAR:
    - Detect changes in MISP IoCs and trigger Shuffle workflows to alert Wazuh or update TheHive cases.
- Zabbix + MISP:
    - Correlate Zabbix anomaly alerts with known threat patterns in MISP, enabling proactive detection of infrastructure-based attacks.

Standalone Features

Wazuh

- Intrusion detection through log monitoring, anomaly detection, and file integrity checks.
- Host-based monitoring with custom rule sets for advanced threat detection.
- Compliance audits for standards like PCI-DSS, HIPAA, and GDPR.

TheHive

- Incident management with case tracking, observables, and collaboration tools.
- Playbook automation for standardised incident handling.
- Trend analysis for understanding recurring threats and response efficiency.

Zabbix

- Resource monitoring across servers, applications, networks, and databases.
- Trend analysis for resource utilisation and performance anomalies.
- Custom alerting for proactive response to potential issues.

MISP

- Centralised threat intelligence management and sharing platform.
- Import/export of IoCs in formats like STIX, JSON, and CSV.
- Advanced IOC correlation and search for identifying related campaigns.

Cortex

- Observable enrichment using powerful analyzers like VirusTotal, PassiveTotal, and WHOIS lookup.
- Automation of threat intelligence workflows with integration to other tools like MISP and TheHive.
- Supports hundreds of analyzers for advanced threat data insights.

Shuffle SOAR

- Orchestrates and automates workflows across all integrated tools.
- Provides a centralised automation hub to connect Wazuh, Zabbix, MISP, TheHive, and Cortex.
- Simplifies repetitive tasks like alert forwarding, case creation, and threat enrichment.

From:
https://handbook.unicis.tech/ - **Unicis Handbook**

Permanent link:
https://handbook.unicis.tech/pub/soc?rev=1732636807

Last update: **26.11.2024 16:00**