paloalto NETWORKS

XSOAR MATURITY FRAMEWORK

CURRENT STATE

Common Pain Points

Without Security Automation

- No Deduplication of Alerts
- Manual Workflows and heavy reliance on external ticketing systems
- Limited SOC automation
- Tier 1 is performing majority of information gathering
- Limited or Missing Metrics (MTTR, MTTD, etc)
- Manual end user interaction (sending emails requesting information)

DESIRED STATE

Automation Goals

Automation Goals

- Centralization location of security events
- Deduplicate alerts and reduction of false positives
- Automated and Semi-Automated workflows for SOC incidents
- Leveraging Threat Intelligence to provide more context to IOCs
- Empower Tier 1 to make decisions quicker which more accuracy with automated enrichment.
- Create meaningful metrics to build out confidence in SOC processes
- Automate as much manual communication as possible

Implementation Strategy

1. Ingesting alerts from various sources
2. Utilize Pre-processing rules to deduplicate alerts
3. Establish a baseline for how long it takes to work a incident manually**.** (This will be used post-use case completion to determine how much time has been saved using Automation).
4. Determine which use case you want to prioritize for automation (Example: if phishing takes the longest and requires the most time from an analyst, that would be good starting point)
5. Define a use case. This step is where Customer Success can provide assistance. We will look to simplify and streamline the incident response processes.
6. Utilize SLAs, Timers and Dashboards to create Metrics

Case Studies

https://www.paloaltonetworks.com/cortex/customer-stories

Common Initial Use Cases

1. Case Management
2. Phishing
3. Data Enrichment and Threat Intelligence
4. Malware
5. Network Security

Case Management

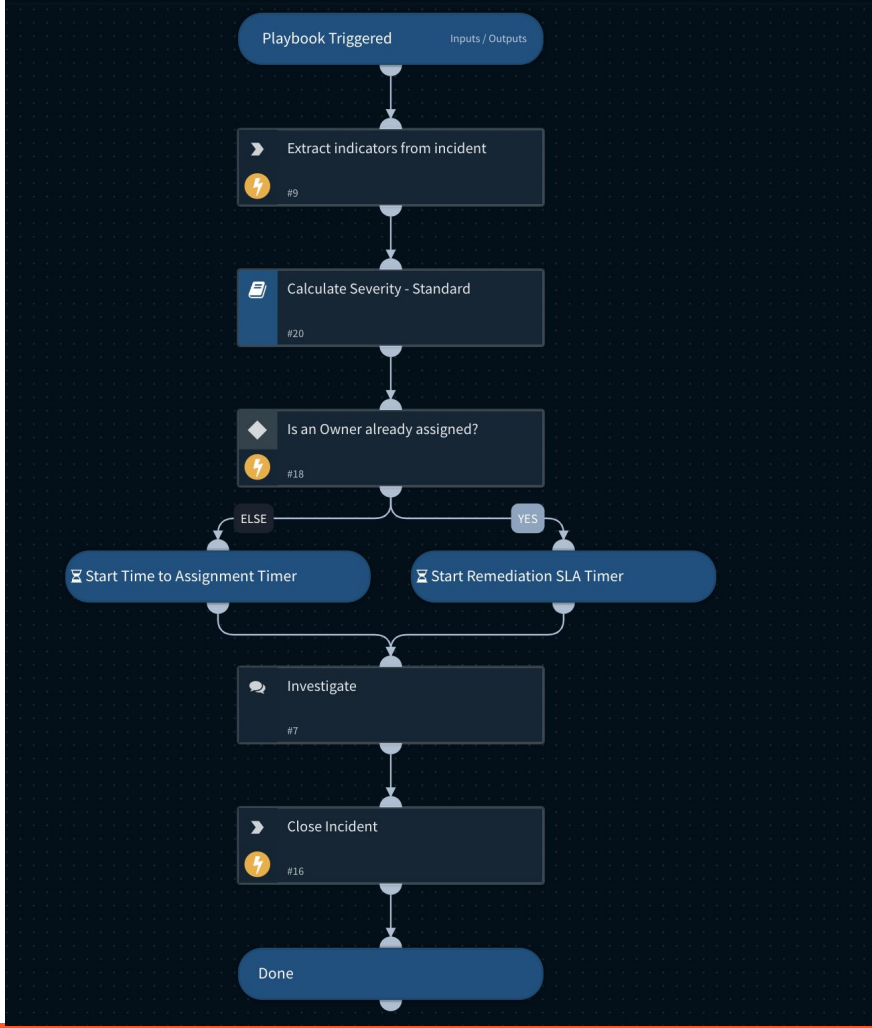
Pull ticket information from Service Now

- Set Priority (P1, P2, P3)

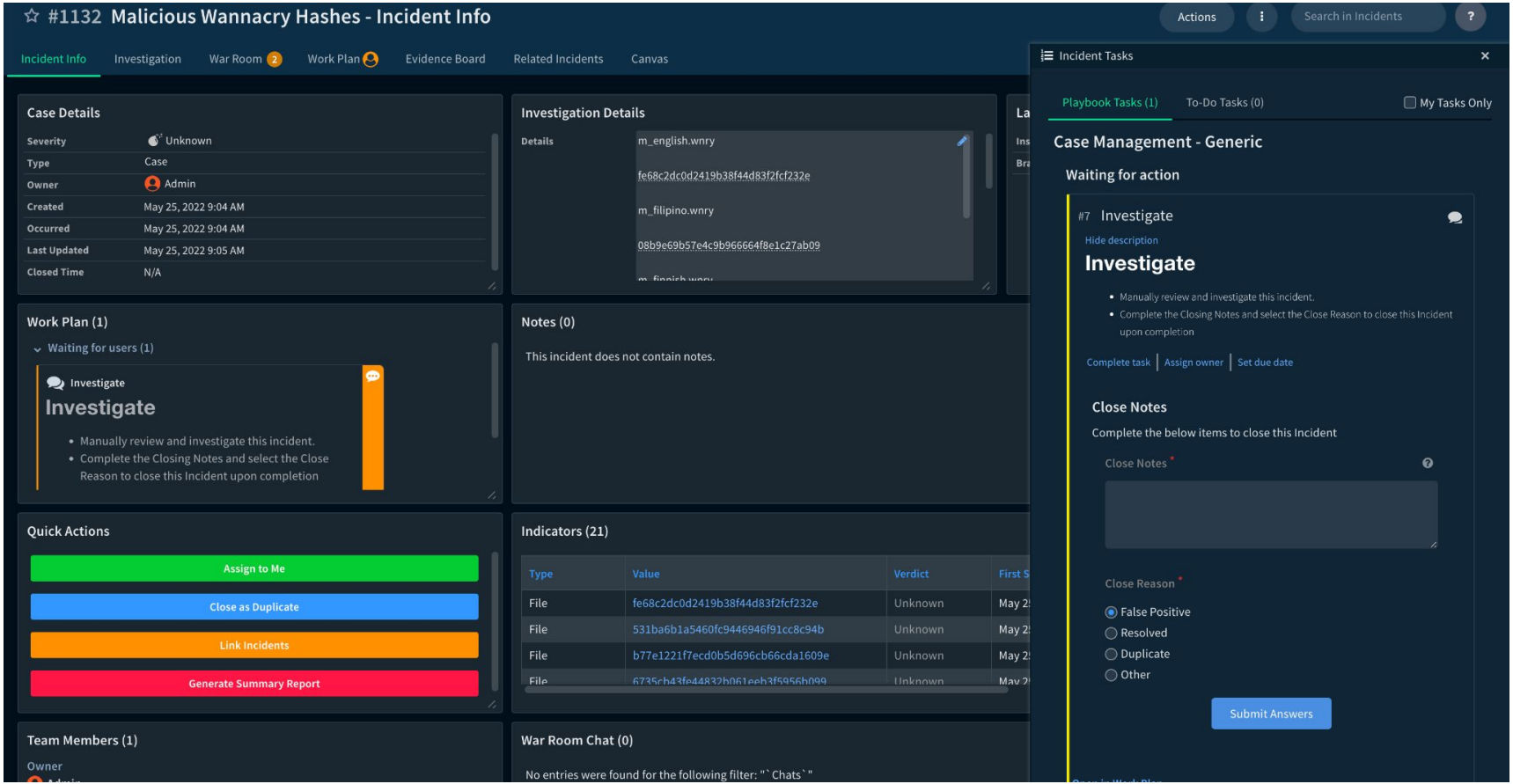
Playbook Logic

- Extract Indicators from the incident
- Determine severity
- Assign to Analyst
- Perform Investigation
- Close

https://xsoar.pan.dev/docs/concepts/use-cases#case-management



Case Management Incident Layout



Potential Process Flow

Incident Playbook (Ingestion)

1. Cortex XDR Incident
2. Prisma Saas Alert
3. Prisma Cloud Alert
4. Okta Alert
5. WinEvent Alert
6. Linux Alert
7. Proofpoint Alert
8. G-Suite Alert
9. GCP Alert
10. Support Requests
11. NGFW Alert
12. Abuse Reports
13. Onboarding/Offboarding
14. Expanse Alert
15. Monitoring Alert
16. Password Spray Alert

Analysis Subplaybooks (Enrichment)

Upon Trigger

1. Calculate Severity
2. Start SLA Timers
3. Notification

Gather Details

1. User Enrichment
2. Host Enrichment
3. URL Enrichment
4. Domain Enrichment
5. Email Address Enrichment
6. File Enrichment
7. IP Enrichment
8. Related email search
9. Related log search
10. Forensic capture
11. Ask user a question

Containment Sub-playbooks (Analyst/User Actions)

1. Lock AD user account
2. Lock AD service account
3. EDL Block (IP/Domain/URL)
4. PAN-DB re-categorization
5. Block email sender
6. Quarantine email
7. Quarantine files
8. Quarantine device
9. Disable project

Eradication/Remediation Subplaybooks

1. Re-image request
2. Password Reset
3. Search and destroy
4. External website takedown
5. Revoke physical badge access
6. Kill sessions

Post-Incident Metrics

1. Metrics incl. effort
2. Record alert fidelity
3. Timeline

Suggested Timeline

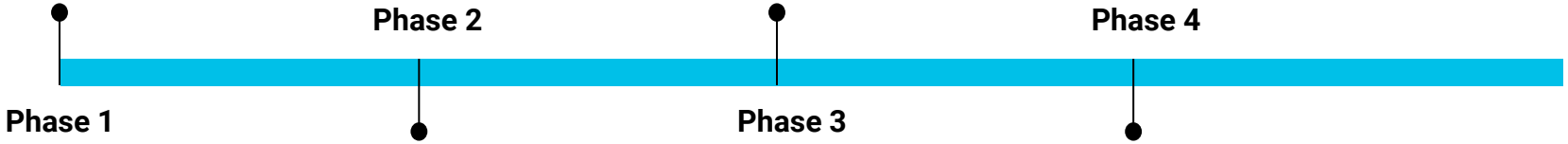
Use Case Development Stages

Case Management

Service Now Ticket Mirroring, and incident/event centralization. Deduplication of alerts, basic enrichment, process adoption and user training. First level SLA and metrics.

Optimizing and Automating Tier 1 tasks

Developing content around handling the Analysis and Detection phases. Determining what processes can be simplified and automated to fit into XSOAR playbook (Standardization).



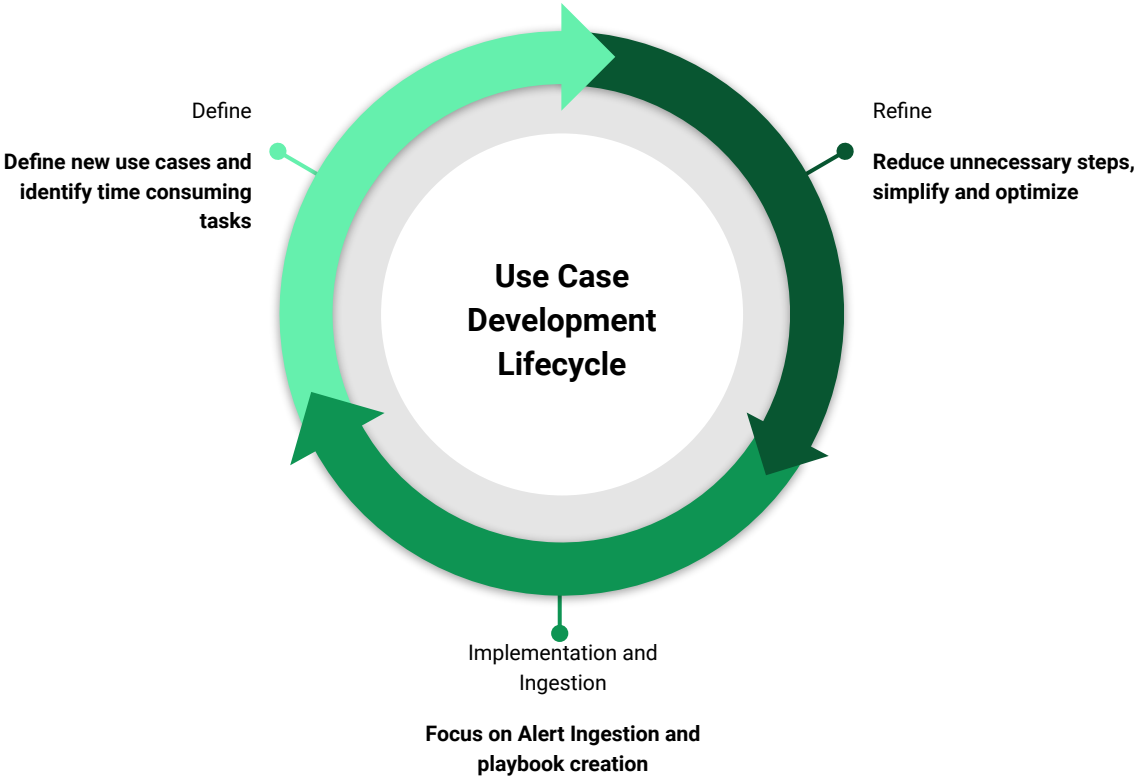
Data Enrichment and Threat Intelligence

Focus on user, endpoint, IOC, incident enrichment. Automate external communication workflows (emails, data collection tasks). Make use of allow/block lists and threat intelligence.

Containment, Layouts and Metrics

Focus on building out containment sub-playbooks (Quarantine Emails, Quarantine Files, Password Reset). Customization of incident layouts, deeper level metrics and reporting. Tier 2 process automation focus.

New Use Case Development Life Cycle



Case Studies

Customer Case Studies and Use Cases

1) Case Studies
2) Telecom Industry Use Cases
3) Energy and Utilities Use Cases