CYWARE™

Use Case

Malware Alert Investigation

A Malicious Enemy

Attacks involving malware are one of the most common tactics used by cybercriminals. The number of daily detected malware is increasing on average and the types and variations continue to evolve. Organizations need to improve and speed up their threat response procedure and strategies to detect and contain malicious software as quickly as possible. The solution is to automate malware detection and containment.

Through the Detective Lens of Automation

Using automated playbooks, a malware attack can be automatically detected, investigated, and contained even before it spreads and damages your network.

The malware alert investigation playbook performs the following tasks

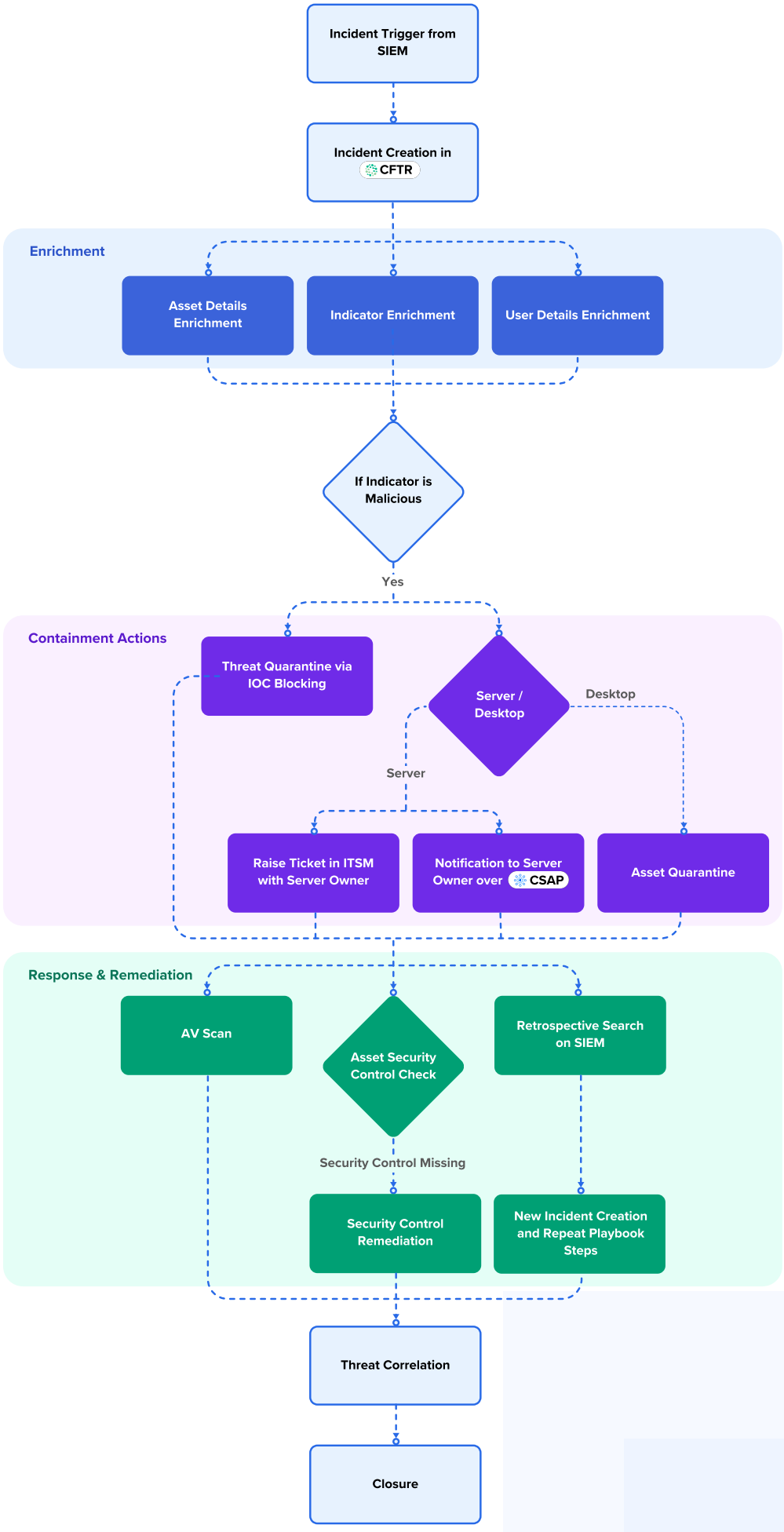
Incident Trigger

Upon getting an alert from the SIEM, the playbook automatically creates an incident in the Cyware Fusion and Threat Response (CFTR) platform.

Incident Enrichment

The incident enrichment process comprises of several steps:

- **Threat Intelligence Lookup**: After the Incident has been created, a threat intelligence lookup is initiated to fetch more information about the malware detected from Cyware Threat Intelligence eXchange (CTIX) or VirusTotal.
- **User Enrichment**: The playbook then queries Active Directory to fetch the user details.
- **Asset Enrichment**: As a last step in the incident enrichment process, a query to the CMDB is made to fetch the asset details associated with the affected user.


Incident Trigger from SIEM
Incident Creation in CFTR
Enrichment
Asset Details Enrichment
Indicator Enrichment
User Details Enrichment
If Indicator is Malicious
Yes
Containment Actions
Threat Quarantine via IOC Blocking
Server / Desktop
Desktop
Server
Raise Ticket in ITSM with Server Owner
Notification to Server Owner over CSAP
Asset Quarantine
Response & Remediation
AV Scan
Asset Security Control Check
Retrospective Search on SIEM
Security Control Missing
Security Control Remediation
New Incident Creation and Repeat Playbook Steps
Threat Correlation
Closure

Response and Remediation

The response and remediation process comprises of several steps:

- **Containment**:
  - If the hash is found to be malicious, an action is initiated to block it in the Endpoint Detection and Response (EDR) tool.
  - **For Desktop / Laptop**: The asset is quarantined using NAC / EDR, to prevent the malware spread on other assets in the network.
  - **For Server**:
    - The asset quarantine ticket is created in the ticketing system and assigned to the respective asset owner.
    - A mobile notification is sent via the Cyware Situational Awareness Platform (CSAP) to the asset owner for immediate attention.
- **Security Control Remediation**:
  - The affected user's system is checked for the existing security controls installed.
  - If the security controls are missing, a ticket is raised in the ITSM tool for remediation.

Threat Correlation

The playbook automatically queries CTIX or malware sandbox results to identify the associated TTPs of the malware for further investigation and threat correlation.

Learning and Closure

As a final step, an action is created in CFTR to provide remediation and document all lessons learned. Once all the investigation actions are completed, the incident is closed.

Cyware Advantage

End-to-End Visibility

Security automation allows you to gain complete visibility into malware campaigns by performing investigations at machine speed using past threat data and enrichment from multiple intel sources.

Reduce Malware Risk

By leveraging security automation, you can lower the risk of malware infection by monitoring all malware-related activities and analyze critical detection parameters for IOCs, tactics, and techniques.

Draw Contextual Intelligence

To effectively respond to a malware incident, the automated playbook helps you draw contextual intelligence on related threat campaigns, predict attackers' next actions, and observe the threat patterns, by correlating seemingly isolated threats and incidents.

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310

cyware.com | sales@cyware.com

855-MY-CYWARE