CYWARE™

Use Case

Ransomware Alert Response

Protect Your Data, and Your Wallet

Ransomware attacks have grown in numbers and severity over the last few years. The average cost and downtime due to ransomware attacks have also been on the rise. Without implementing adequate detection and response measures, organizations can end up losing access to their valuable data and even incur damages to their reputation in cases of stolen data being leaked by threat actors.

Move Faster with Automation

Ransomware operators typically design their exploits to spread laterally across an organization's network in an attempt to infect and encrypt data on as many devices as possible from a single execution. An automated playbook-driven response process has proven to be an effective solution for containing such attacks in their early stages.

The ransomware response playbook performs the following tasks

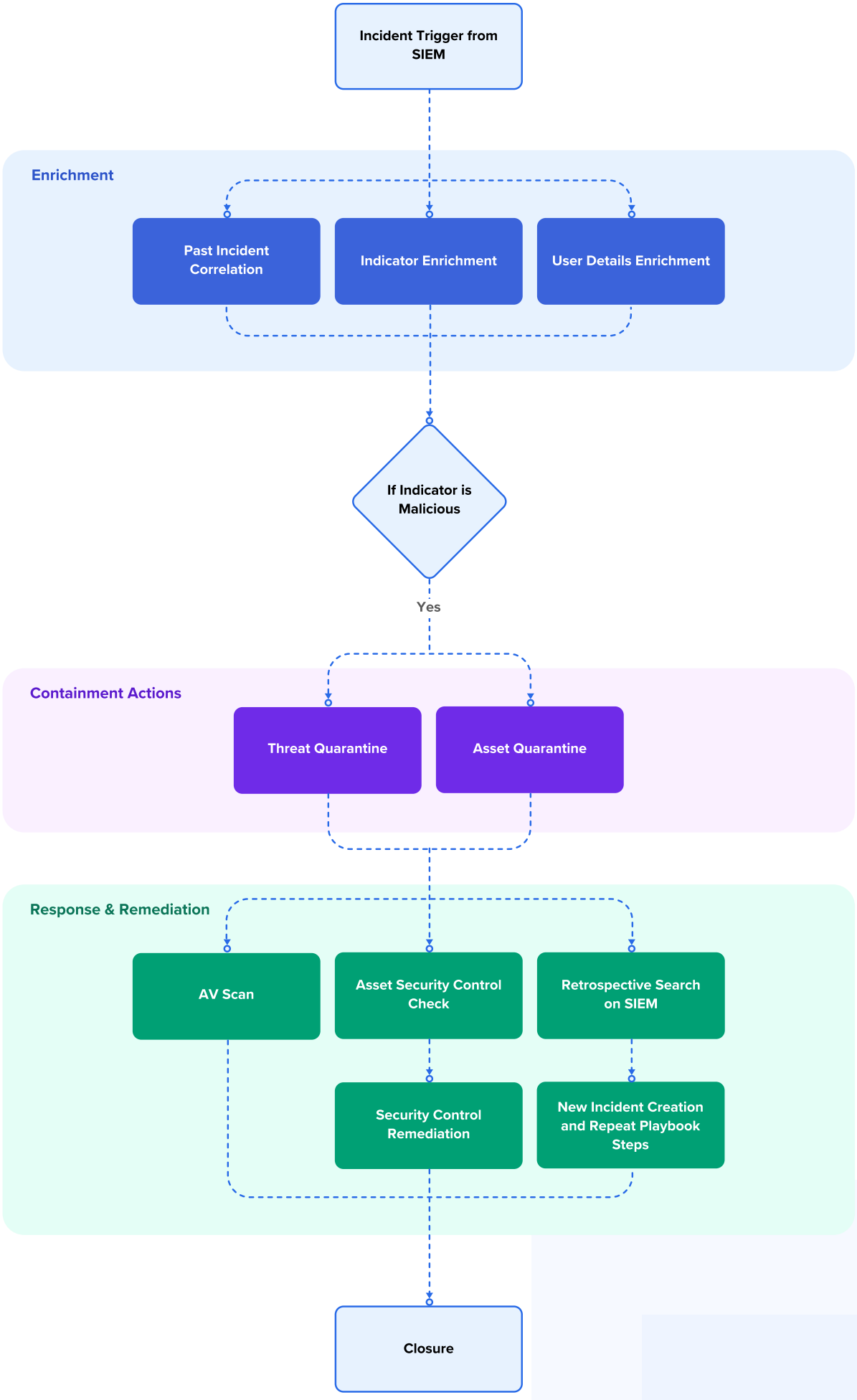
Incident Trigger

After receiving a ransomware alert from the SIEM tool, the incident is automatically created and investigated in the Cyware Fusion and Threat Response (CFTR) platform.

Incident Validation

The incident validation phase involves incident correlation and enrichment:

- **Incident Correlation**: CFTR fetches the host and user information and correlates it with past investigations to connect the dots between different threat elements.
- **Incident Enrichment**:
  - **Indicator Enrichment**: CFTR orchestrates with Cyware Threat Intelligence eXchange (CTIX) and other threat intelligence sources to fetch malware hash reputation.
  - **User Details Enrichment**: The Active Directory is queried for fetching more information on the impacted user.


Incident Trigger from SIEM
Enrichment
Past Incident Correlation
Indicator Enrichment
User Details Enrichment
If Indicator is Malicious
Yes
Containment Actions
Threat Quarantine
Asset Quarantine
Response & Remediation
AV Scan
Asset Security Control Check
Retrospective Search on SIEM
Security Control Remediation
New Incident Creation and Repeat Playbook Steps
Closure

Containment Action

If the alert is found to be genuine after initial triage has completed, the below actions need to be taken immediately to determine the impact and scope of the ransomware attack. Swiftly performing these critical actions will also assist in stopping the spread of ransomware across other devices on the network.

- **Threat Quarantine:** The malicious hash is blocked on the Endpoint Detection and Response (EDR) tool.
- **Asset Quarantine:** The impacted user asset is quarantined using the endpoint security control like EDR / NAC agent / NAC network policy / AV policy tool.

Response and Remediation

In order to ensure complete threat response, the playbook performs the following actions:

- **Antivirus Scan:** An antivirus scan is performed on the affected and associated assets to ensure the infection has been contained and hasn't spread. This is then communicated to the user.
- **Security Control checks:**
  - **Asset Security Control Status:** The CFTR platform is queried to check for the security software and patch history on the affected user's asset.the user.
  - **Security Control Patching:** If unpatched or no security software is found on the affected asset, a ticket is raised in the ITSM.
- **Retrospective Search on SIEM:** The SIEM is queried again for similar alerts to ensure that no other assets or machines are affected.

New Incident Creation

If new assets or machines are discovered then an incident is created in CFTR for the newly detected asset or machine.

Closure

If required, the CFTR platform is leveraged for any remediation action, and steps are repeated. If the asset is found clean, it is unquarantined and the incident is closed.

Cyware Advantage

Reduce Detection and Response Times

Since a ransomware infection can spread very quickly across a network of connected devices, the automated playbook plays an important role in countering the threat at machine speed instead of relying on slower, manual processes.

Standardized Response Process

A ransomware response automation playbook helps standardize the response actions for threats behaving similarly and it also helps incorporate learnings from previous incidents.

Simplify Security Governance

An automated playbook simplifies the governance of security teams to execute the ransomware response process with limited resources.

228 Park Ave S #77147 New York,
New York 10003-1502

cyware.com | sales@cyware.com

855-MY-CYWARE