CYWARE

Use Case

Denial-of-Service (DoS) Alert Mitigation

A Tsunami of Traffic

In a Denial-of-Service (DoS) attack, threat actors flood a targeted system's network by directing lots of traffic towards it, from multiple systems under their control. It is a common tactic used by attackers via a network of compromised systems to render an online service unusable. DoS attacks can end up hurting an organization's reputation by affecting its services uptime, customer activity, and business operations. The motives behind DoS attacks can also include extortion, hacktivism, cyber warfare, corporate rivalry, amongst others.

Automation to Change the Game

To effectively and rapidly break the chain of DoS attacks, security teams can utilize an automated DoS response playbook. The automated playbook standardizes the response process from detection to blocking of the malicious indicators from where attacks are sourced.

The DoS alert automation playbook performs the following tasks

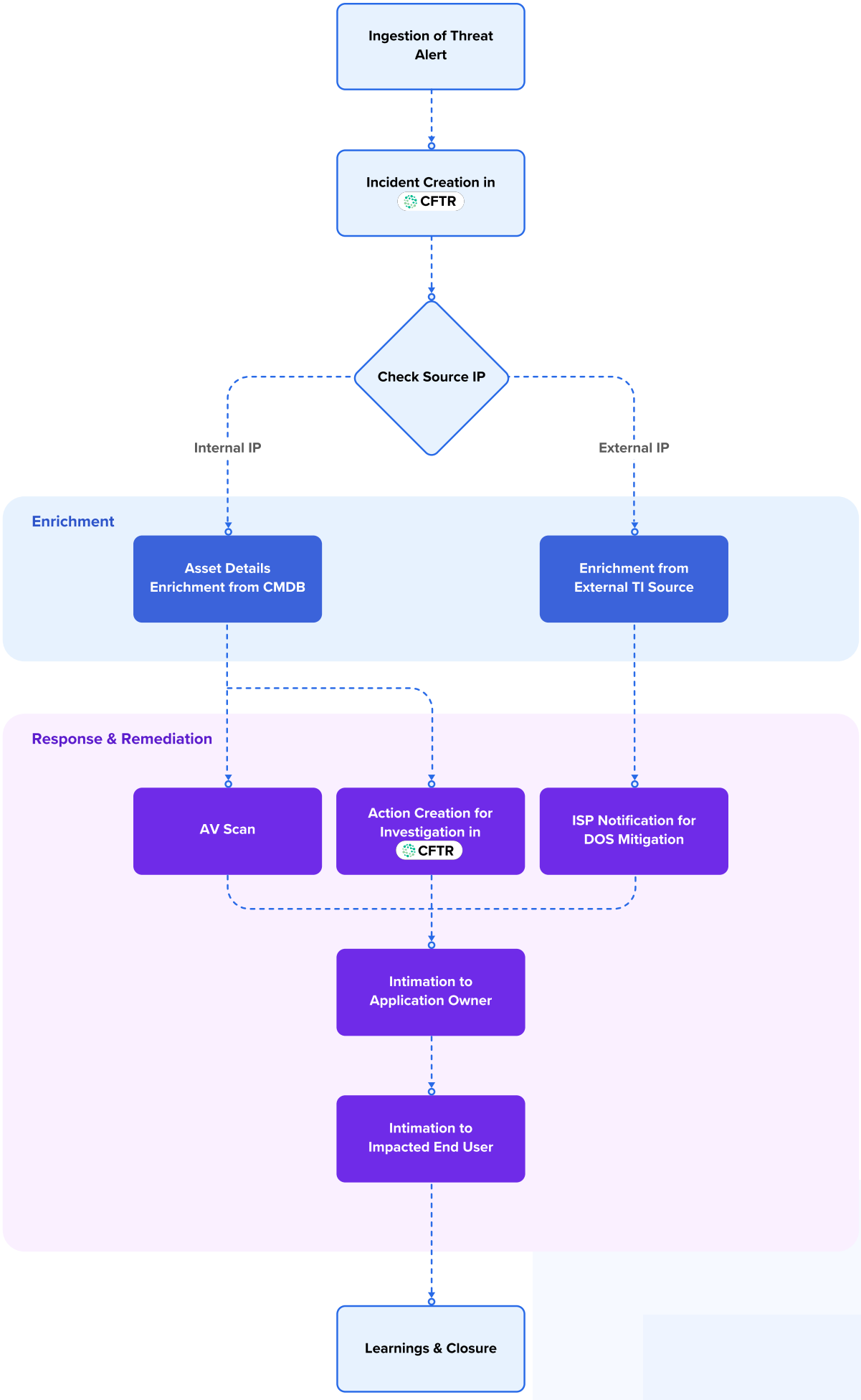
Ingestion of Threat Alert

The playbook triggers after receiving an alert on the sudden and unusually large number of requests.

Triaging and Analysis

After receiving an alert, an incident is automatically created in the Cyware Fusion and Threat Response (CFTR) platform and multiple processes are carried out in parallel to ensure swift action is taken:

- **If Internal Source IP:**
  - **Asset Management Query:** The asset management module of the CFTR platform is queried to check whether an internal IP address is making such requests. If no such data is found, then the Unified Endpoint Management (UEM) tool is queried for further information.
- **If External Source IP:**
  - **IOC Enrichment:** For external IP involved in initiating the high volume of traffic, the Cyware Threat Intelligence eXchange (CTIX) platform or similar threat intelligence sources are queried for the reputation and nature of the indicator (IOC).


Ingestion of Threat Alert
Incident Creation in CFTR
Check Source IP
Internal IP
External IP
Enrichment
Asset Details Enrichment from CMDB
Enrichment from External TI Source
Response & Remediation
AV Scan
Action Creation for Investigation in CFTR
ISP Notification for DOS Mitigation
Intimation to Application Owner
Intimation to Impacted End User
Learnings & Closure

Response Actions

If the IP is validated as being malicious, an incident is automatically created in the CFTR platform and the following processes are initiated:

- **If Internal IP Involved:**
  - **Antivirus Scan:** An antivirus scan is run on the involved source machine.
  - **Action:** An action is created in the CFTR platform to investigate, remediate, and resolve the incident.
- **If External IP Involved:**
  - **ISP Intimation:** The Internet Service Provider (ISP) is further communicated over email/ticket about the incident and requested to initiate the DoS mitigation.
- **Notifications:**
  - **App Owner Notification:**
    - The application owner of the impacted target application is notified to further investigate the alert.
    - The affected asset owner of the machine initiating the attack is informed about the incident in case of internal machine initiating the attack
  - **End-user Notification:** The end-user using the applications are notified for any impact on operations.

Learnings and Closure

- **True Positive:** If traffic found is malicious, respective steps to counter such an attempt in the future are documented within the learning module of CFTR.
- **False Positive:** For false alarm, the notification is sent to the respective team to further fine-tune the signatures configured on other network devices or SIEM rules.

Cyware Advantage

Reduce Detection Times

By automating the DoS alert function, security teams can receive an early warning about various types of DoS attacks such as application-layer attacks, protocol attacks, and volumetric attacks.

Coordinated Response Actions

The automated playbook performs the incident investigation, indicator enrichment, and response actions in parallel so as to manage the response to the high frequency of malicious activity.

Avoid Manual Intervention

By using automation, security teams can avoid relying on manual processes to detect and respond to break the DoS attack chain at machine speeds.

1460 Broadway, New York, NY 10036

https://cyware.com | contact@cyware.com | Call us at 855-MY-CYWARE