CYWARE

Use Case

Remote to Local Exploit Response Automation

A Threat from Afar

Remote to local exploits can have dangerous consequences for organizations as it allows cybercriminals to run malicious codes by exploiting security vulnerabilities. Such an exploit is used for data theft, business disruptions, and also for spying purposes. The dwell detection time for manual response processes in detecting such attacks is very high. Furthermore, the mean-time-to-respond (MTTR) also ends up being high because incident response analysts have to perform several time-consuming checks and scans in containing the threat.

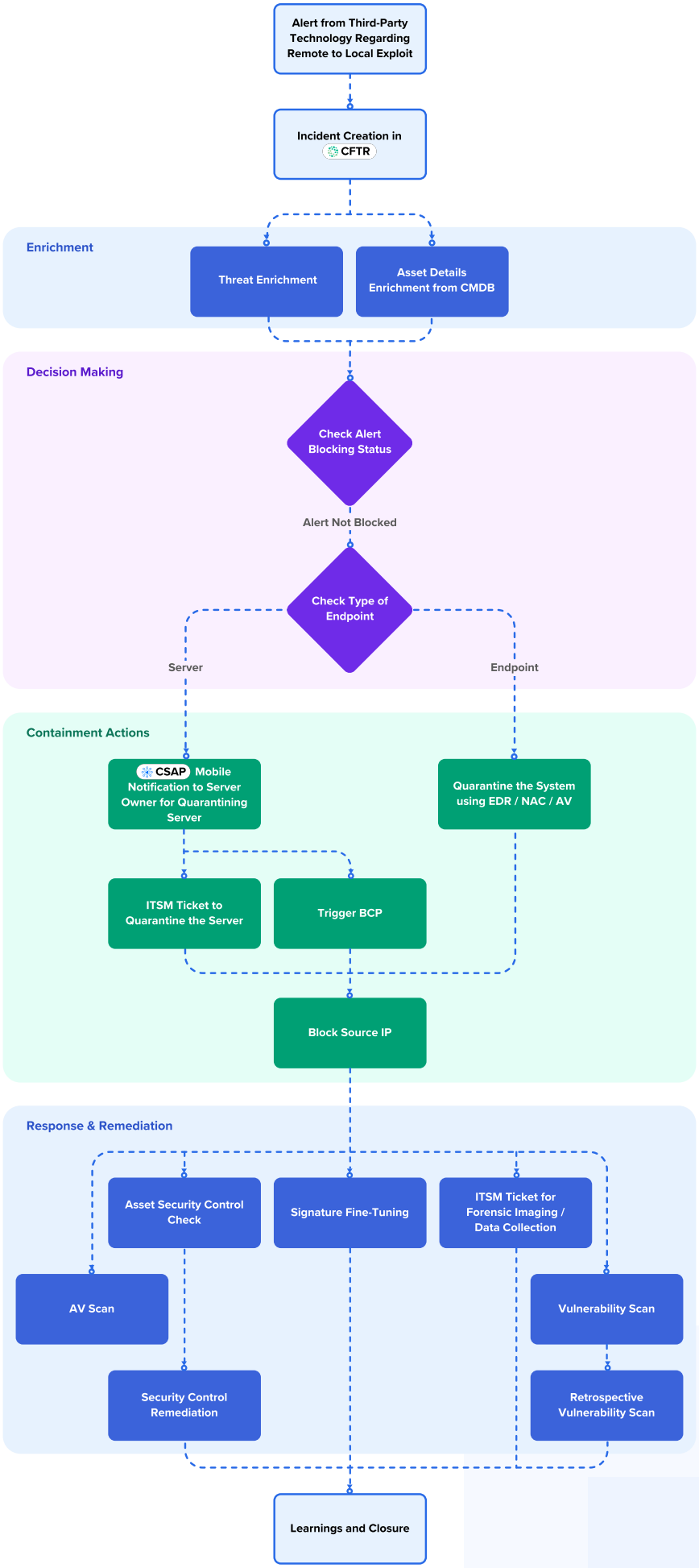
Nipping the Exploit in the Bud with Automation

Automated playbooks can reduce the overall dwell detection time and the mean-time-to-respond to mere seconds by coordinating the incident investigation, enrichment, analysis, and containment processes.

The automated playbook performs the following tasks

Incident Reporting

Once a remote to local exploit attempt is detected by security technology and an alert is being reported by the SIEM, the playbook automatically creates an incident in the Cyware Fusion and Response (CFTR) platform with all alert details captured.


Alert from Third-Party Technology Regarding Remote to Local Exploit
Incident Creation in CFTR
Enrichment
Threat Enrichment
Asset Details Enrichment from CMDB
Decision Making
Check Alert Blocking Status
Alert Not Blocked
Check Type of Endpoint
Server
Endpoint
Containment Actions
CSAP Mobile Notification to Server Owner for Quarantining Server
Quarantine the System using EDR / NAC / AV
ITSM Ticket to Quarantine the Server
Trigger BCP
Block Source IP
Response & Remediation
Asset Security Control Check
Signature Fine-Tuning
ITSM Ticket for Forensic Imaging / Data Collection
AV Scan
Vulnerability Scan
Security Control Remediation
Retrospective Vulnerability Scan
Learnings and Closure

Incident Enrichment

CFTR then performs several enrichment actions:

- **Asset Enrichment:** Asset enrichment from the CMDB is performed to identify the asset owner and the types of assets. This step includes two processes:
  - **Server:** An automated enrichment is done to fetch the server and server owner details of the affected server.
  - **Endpoint:** An automated enrichment is done to fetch the endpoint owner details of the affected endpoint.
- **Threat Enrichment:**
  - A lookup in Cyware Threat Intelligence eXchange (CTIX) or external threat intelligence sources is performed to identify the exploit and find out the associated vulnerability, malware, and threat actor related details.
  - An external IP lookup is performed on CTIX or the external threat intelligence source.

Containment

In this step, the Incident is checked to find out whether the triggered alert was blocked by security technologies like IPS and WAF.

- If the alert was blocked
  - The incident is updated with the threat intelligence enrichment details from the previous steps.
- If the alert was not blocked, the following actions are performed:
  - **Server:** A Cyware Situational Awareness Platform (CSAP) mobile notification is triggered to the application owner to approve the quarantine of the asset and trigger the Business Continuity Process (BCP) if required.
    - On approval from the application owner, an action to quarantine the system over an IT ticket is initiated.
    - On approval from the application owner, the BCP plan is triggered for the application in case of a larger impact.
  - **Endpoint:** The affected endpoint system is quarantined using security controls like EDR/AV/NAC
  - **IP Blocking:** The playbook automatically blocks the source IP on the firewall or perimeter security device.

Response and Remediation

- **Antivirus Scan:** The playbook runs an antivirus scan on the host to check for malware and backdoor presence on the server.
- **Forensic Data Collection:** A real-time query is performed on the EDR to fetch the details of the processes running in the memory of the impacted system and the incident is updated accordingly.
- **Vulnerability Scan:** The vulnerability scanner is initiated on the impacted server.
  - If a vulnerability is detected, a ticket is raised in the ITSM tool to loop in the patch management team to patch the vulnerability.
  - A retrospective scan is initiated to identify similar vulnerabilities on other servers and patching is initiated.
- **Signature Fine-Tuning:** If the attack was not blocked, a ticket is raised to fine-tune the signature in the security device and configured into the block mode.
- **Security Controls Check:** If the security software is missing on the impacted system, a ticket is raised in the ITSM tool for remediation.

Learnings and Closure

As the last step, the playbook creates an action in the CFTR to provide the incident response analyst with remediation and details on the lessons learned.

Cyware Advantage

Reduce Mean-time-to-Respond (MTTR)

The automated playbook reduces overall MTTR from days to seconds by coordinating multiple processes including detection, incident investigation, enrichment, and containment.

End-to-End Visibility

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

Track Targeted Exploit Campaigns

Through automated incident enrichment with data from multiple sources, incident response analysts can understand and counter the sophisticated tactics, techniques, and procedures (TTPs) used by specific threat actors.

1460 Broadway, New York, NY 10036

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