CYWARE™

Use Case

Web Defacement Response Automation

Cyber Vandalism

Web defacement attacks are a nuisance. In such attacks, cybercriminals take control of websites by exploiting vulnerabilities and change the visual appearance, often smearing the websites with political slogans. Organizations mostly respond to such attacks by first taking the website offline followed by the removal of the malicious code and patching of vulnerabilities. The manual response to the attack leads to high downtime impacting the organization and any services offered. The political propaganda unleashed by the cybercriminals on the website adds to the injury of the victim organization impacting its brand and status.

Undoing the Malicious Art with Automation

Security teams can leverage automated playbooks to detect and respond to such web defacement attacks. The automated playbooks standardize the response process from detection to response and remediation actions at machine speed.

The web defacement response automation playbook performs the following tasks:

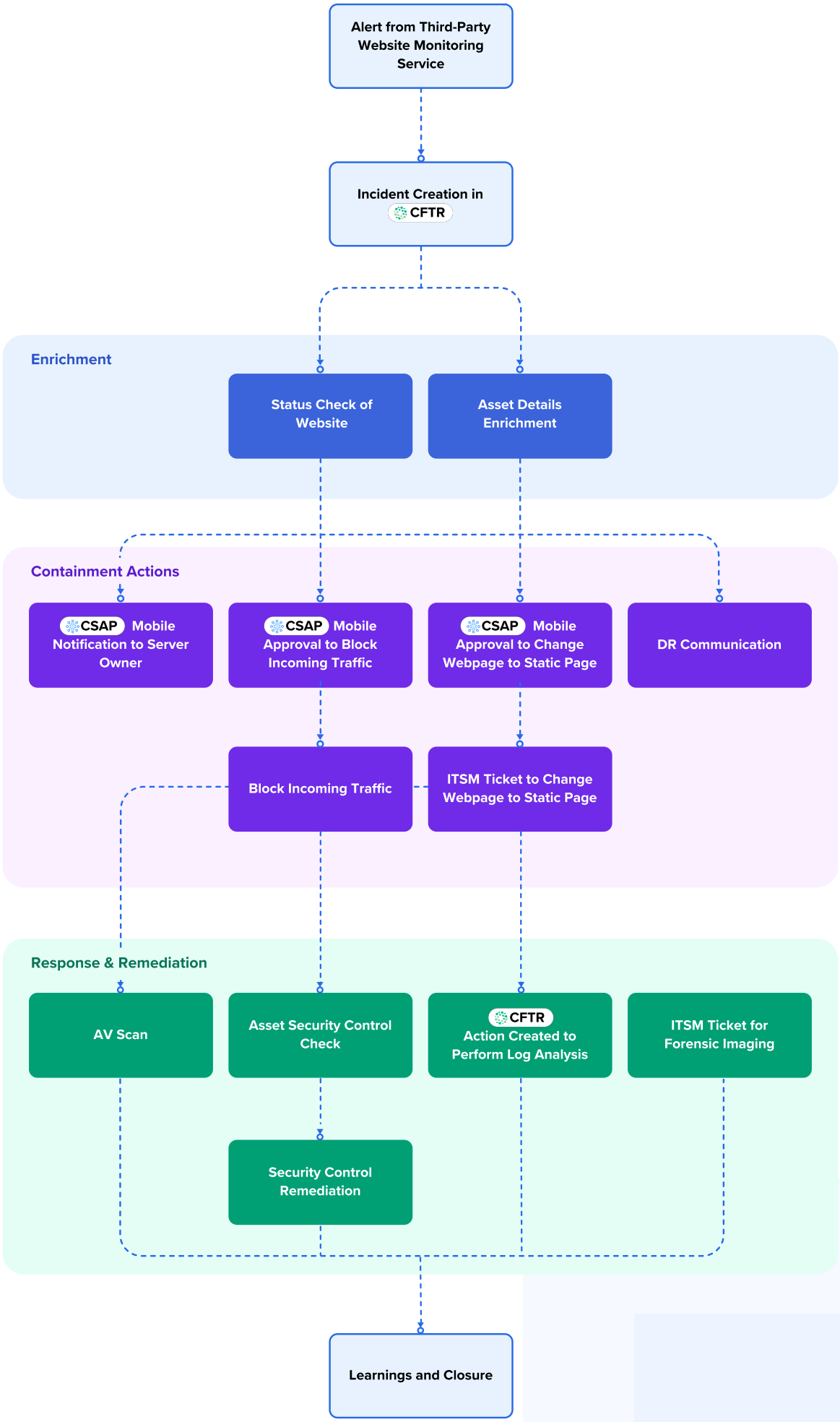
Incident Reporting

Upon receiving an alert from a third party website monitoring service about website defacement, an incident is created automatically in the Cyware Fusion and Threat Response (CFTR) platform.

Enrichment and Triaging

The following actions are triggered to enrich and triage the reported defacement alert before initiating any response actions.

- **Enrichment:** The playbook performs the automated enrichment of the targeted web application to fetch the server and server owner details.
- **Status Check:** The playbook automatically checks the current status of the web application page and updates the data in the incident.


Alert from Third-Party Website Monitoring Service
Incident Creation in CFTR
Enrichment
Status Check of Website
Asset Details Enrichment
Containment Actions
CSAP Mobile Notification to Server Owner
CSAP Mobile Approval to Block Incoming Traffic
CSAP Mobile Approval to Change Webpage to Static Page
DR Communication
Block Incoming Traffic
ITSM Ticket to Change Webpage to Static Page
Response & Remediation
AV Scan
Asset Security Control Check
CFTR Action Created to Perform Log Analysis
ITSM Ticket for Forensic Imaging
Security Control Remediation
Learnings and Closure

Containment

The playbook leverages CFTR to perform the following actions following the incident enrichment process:

• **Realtime Containment:**

CSAP Mobile Notification: An alert notification along with the screenshot of the current web page is sent to the application owner via the Cyware Situational Awareness Platform (CSAP) mobile app. The alert notification also contains several other requests:

•Approval for blocking of inbound traffic until the static page is uploaded

•An action is assigned to replace the website with a static page.

•Disaster Recovery (DR) communication is initiated.

Block Inbound Traffic: On approval from the application owner, the WAF or firewall rule is initiated to block all the inbound traffic for the web application.

Static Website Replacement: On approval from the application owner, CSAP triggers the action to change the website with a static page.

Trigger DR: On approval from the app owner, communication with the DR team is initiated to keep the DR server and services in place.

Response and Remediation

• **Antivirus Scan:** The remediation process begins with an antivirus scan on the host to check for malware.

• **Security Compliance Check:** Thereafter, CFTR checks for the details of security software installed on the server through UEM. If the security software is missing, a ticket is raised in the ITSM for the same.

• **Log Analysis and Investigation:** An action is created in CFTR to perform log analysis of the server to find the root cause of the incident.

• **Forensic Imaging:** An ITSM ticket is raised to perform forensic imaging and investigation on the server to perform the Root Cause Analysis.

Learning and Closure

As the last step, a CFTR action is created to provide the analyst with remediation and lessons learned.

Cyware Advantage

Reduce Detection Times

Since a web defacement attack can impact the website uptime and brand image of the organization, the automated playbook plays an important role in detecting the threat at machine speed instead of relying on manual processes.

Respond Faster to Minimize Downtime

The playbook automates all response processes including blocking of inbound traffic and ensures speedy decision-making by looping in human intelligence for restoring the website to regular traffic more quickly and effectively.

Going Beyond Incident Investigation

In addition to the response, the playbook also helps capture the long term learnings from the incident to put in place the long term strategic controls to thwart any such future attempts by using the unique capabilities of the fusion center.

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

cyware.com | sales@cyware.com

855-MY-CYWARE