Automation Use Cases Menu

CYFLARE
The threat stops here.

Use Case 1

Firewall Policy Update

Integration to make routine changes such as adding an IP address to a blacklist or query the whitelist.

Common CyFlare Response Actions (CRA)

- Write blacklist
- Read blacklist (to see if already added)
- Update geoblocking from CKB (potential)

Supported Integrations

paloalto NETWORKS
CHECK POINT
CISCO
FORTINET

Available Integrations

JUNIPER NETWORKS
SONICWALL

Use Case 2

Network Isolation

Integrates with networking tools and platforms to isolate or remove a device from the network.

Common CyFlare Response Actions (CRA)

- Get/terminate sessions
- Quarantine/unquarantine address
- Add/remove IP to address set

Supported Integrations

Cisco ISE

Available Integrations

CLOUDFLARE
JUNIPER NETWORKS
Cisco ISE

Use Case 3

Isolate/Unisolate Endpoint

EDR integration to take response action on the endpoint in the event of a confirmed or likely threat.

Common CyFlare Response Actions (CRA)

- Shut down machine
- Isolate from network
- Connect to network

Supported Integrations

SOPHOS
SentinelOne
CROWDSTRIKE

Available Integrations

See EDR Integrations List

Use Case 4

Scan/Remediate/Rollback Endpoint

Step two after isolation. Scan action will be part of next steps after isolating endpoint. Remediate and rollback will be done after contacting customer and confirming threat.

Common CyFlare Response Actions (CRA)

- Initiate AV Scan
- Remediate (clean) threats
- Rollback machine

Supported Integrations

SOPHOS
SentinelOne
CROWDSTRIKE

Available Integrations

See EDR Integrations List

Use Case 5

Disable/Enable User Account

This response action is invoked when there is a high probability the account or device has been compromised. To safeguard against account takeover and additional compromise a user account can be disabled until properly investigated.

Common CyFlare Response Actions (CRA)

- Enable User Account
- Lock User Account (permanently or for X amount of time)

Supported Integrations

Active Directory
G Suite

Available Integrations

Identity and Access Management (IAM)
okta

Use Case 6

Email Integration

Integrate to recall confirmed or potential phishing emails from mailboxes to minimize the risk of interacting with malicious URLs.

Common CyFlare Response Actions (CRA)

- Quarantine email from mailbox(es)

Supported Integrations

G Suite
Office 365
proofpoint
TARGETED ATTACK PROTECTION (TAP)

Available Integrations

IRONPORT
mimecast