CYWARE™

Cyware for Computer Emergency Response Teams (CERTs)

Protect your constituents through automated threat intelligence sharing and response.

Current Status of Threat Landscape for CERTs

Government institutions and agencies are at constant risk of getting attacked by cybercriminals. The increasing digitization of public services, legacy IT infrastructure, an ever-evolving geopolitical landscape, and custody of sensitive public data in government organizations are some of the primary reasons for the spike in attacks against government entities in the last few years. One of the major challenges faced by the security teams at national CERTs is the rise of well-funded nation-state actors who have the ability and resources to carry out sophisticated and damaging attacks.

To counter these challenges, leading CERTs are now relying on Cyware's solutions for their critical threat intelligence automation and response operations. Cyware's solutions enable CERTs to leverage advanced automation to ingest, analyze, and share strategic and technical threat intelligence on advanced threats. Furthermore, Cyware's threat response automation platform allows CERTs to draw contextual intelligence by connecting the dots between disparate threat elements and directly initiate and execute response workflow.

Cyware's Solution for CERTs

Cyware's solutions facilitate scalable and integrated management of security operations for CERTs and their constituent ecosystems. The modular platform works in an integrated manner to link threat investigation, triaging, and response operations with threat intelligence sharing through an efficient, automated process

Cyware's modular approach comprises of the following integrate platforms:

Collaborate

An automated threat alert aggregation and information sharing platform that equips key security personnel with information to improve situational awareness and resilience.

Intel Exchange

A smart, client-server threat intelligence platform (TIP) for ingestion, enrichment, analysis, and bi-directional sharing of threat data within your client network.

Respond

A threat response automation platform that combines cyber fusion and automation to stay ahead of increasingly sophisticated cyber threats in real-time.

The solutions fit perfectly into the security frameworks of CERTs allowing them to collect and normalize threat intelligence from multiple internal and external sources.
The advanced automation features enable real-time analysis, sharing, and direct actioning in deployed security tools. The cyber fusion capabilities allow security teams at CERTs to perform real-time intel enrichment from trusted sources to identify malicious attributes of the threat and accordingly triage and prioritize response actions. The solution comes with a multi-delivery alerting mechanism for the role, location, and sector-based alerting and remote actioning on security threats.

Cyware's solutions cover the two critical and widely-practiced security operations scenarios of CERTs.

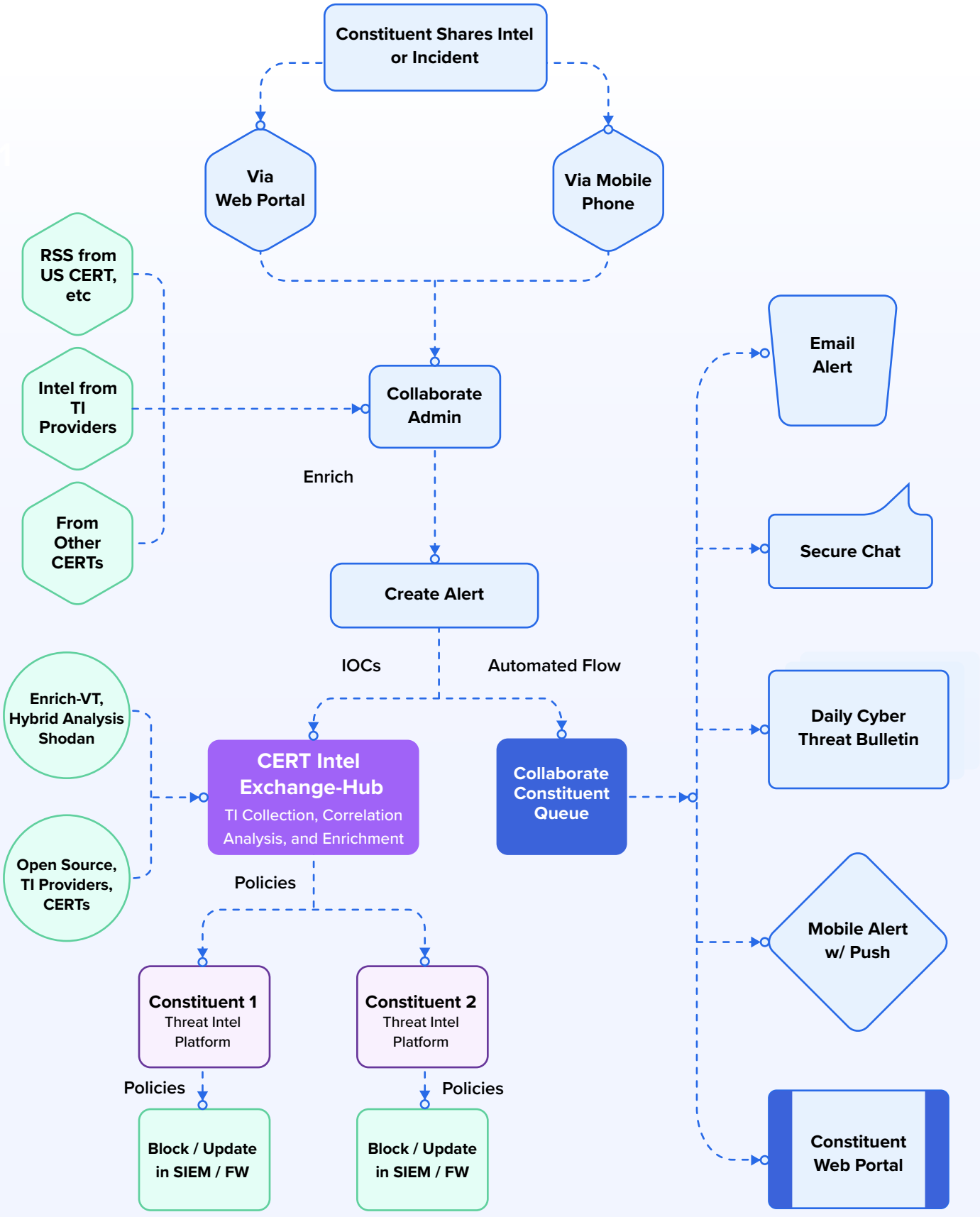
Scenario 1

This scenario is when information sharing in the CERT is fully automated and includes strategic and technical intelligence from internal and external sources. This includes multi-source intel collection, enrichment, analysis, and bi-directional sharing of human-readable and machine-readable STIX-collections of threat indicators of compromise (IOCs), tactics and techniques (TTPs), kill chain mappings, exploitability mappings, artifacts, and logs with constituents.

Scenario 2

This scenario is when the CERT is involved in taking direct threat response actions in the environment of its constituents in addition to facilitating automated threat intelligence sharing. The scenario includes threat investigation, triaging, and response using advanced automation. The scenario also includes the cyber fusion-driven collaboration between the disparate security teams at the CERT to deliver a coordinated and 360-degree response.

Scenario 1: Threat Intelligence Automation and Sharing Model for CERTs

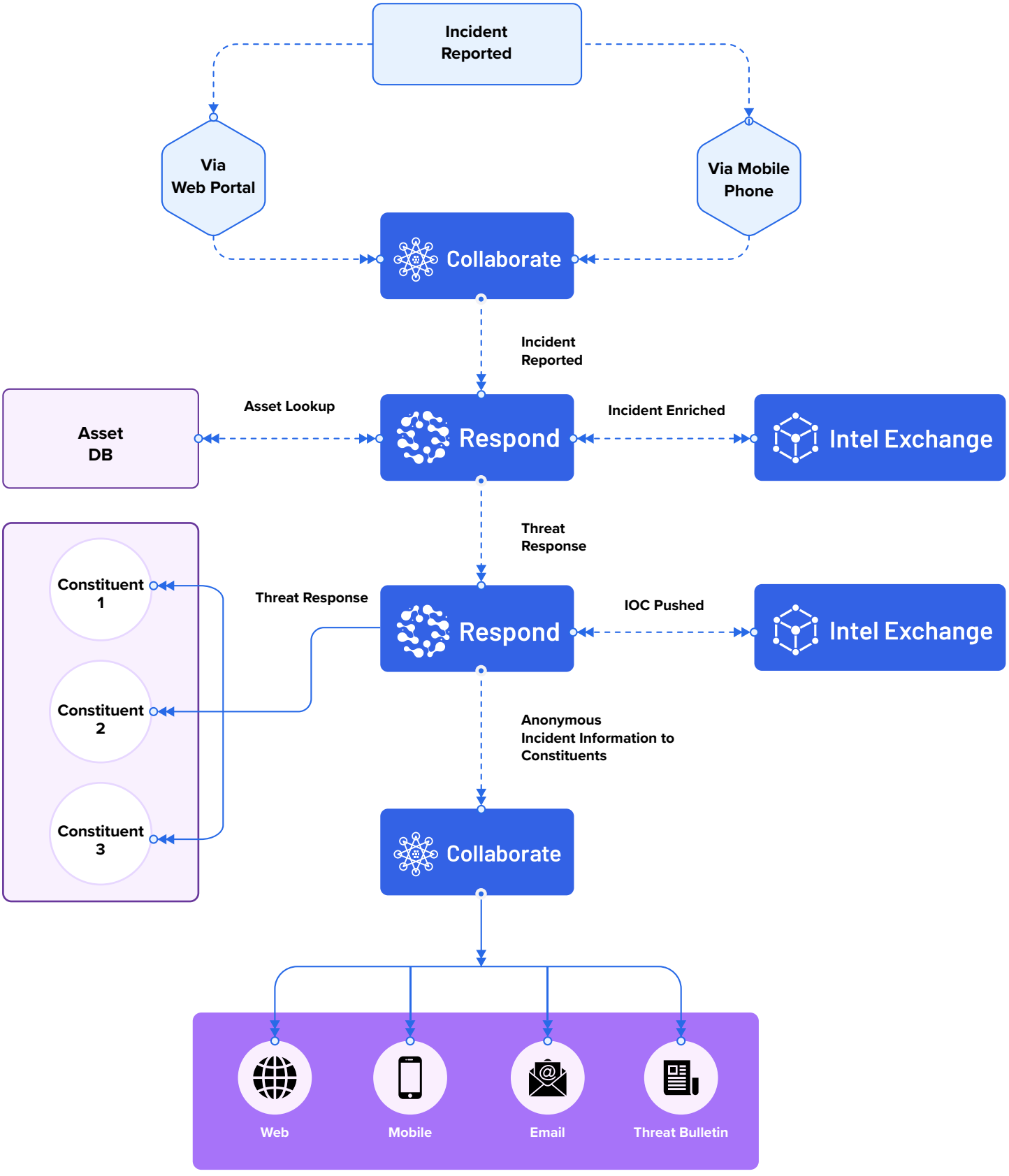


Note: This model assumes that some CERT Constituent organizations have a pre-deployed threat intelligence platform.

Scenario 1:
Use Cases and Benefits for CERTs

1. Enable Constituents to Share Advisories and Threat intelligence
2. Collect Strategic Threat Intelligence from Non-Constituent Sources
3. Ingest Threat Indicators of Compromise (IOCs)
4. Alert Federal, State, and Local Constituents in Real-Time (<30 seconds)
5. Share Anonymized and Enriched Indicators and Incident Data with Constituents
6. Indicate Early Warning Threat Level to Constituents
7. Normalize Structured and Unstructured Intel in Multiple Formats
8. Enrich Threat Intelligence From Trusted Sources
9. Automatically Analyze, and Share IOCs without Direct User Involvement
10. Validate Intel through Fully Configurable Automated Confidence Scoring
11. Foster Discussion-Driven Collaboration with Constituents

Scenario 2: Threat Response Automation Model for CERTs



Scenario 2:
Use Cases and Benefits for CERTs

1. Automate Incident Investigation, Triaging, & Response
2. Foster Collaboration through Cyber Fusion
3. Connect-the-dots between Security Threats
4. Take Actions Directly within the Constituent's Environment
5. Reduce Response Times with Unlimited Orchestration Playbooks

An Essential Overview

Capability	Scenario 1	Scenario 2
Enable constituents to share advisories and threat intelligence	✓	✓
Collect strategic threat intelligence from non-constituent sources	✓	✓
Ingest threat indicators of compromise (IOCs)	✓	✓
Alert federal, state, and local constituents in real-time (<30 seconds)	✓	✓
Share anonymized and enriched indicators and incident data with constituents	✓	✓
Indicate early warning threat level to constituents	✓	✓
Normalize structured and unstructured intel in multiple formats	✓	✓
Automatically, analyze, and share IOCs without direct user involvement	✓	✓
Validate intel through fully configurable automated confidence scoring	✓	✓
Foster discussion-driven collaboration with constituents	✓	✓
Multiple alerting and notification channels	✓	✓
Automate incident investigation, triaging, & response	—	✓
Foster collaboration through cyber fusion	—	✓
Connect-the-dots between security threats	—	✓
Take actions directly within the constituent's environment	—	✓
Reduce response times with unlimited orchestration playbooks	—	✓

CYWARE™

111 Town Square PlaceSuite 1203,
#4 Jersey City, NJ 07310

cyware.com | sales@cyware.com

855-MY-CYWARE