# Cyware Situational Awareness Platform (CSAP)

## A real-time threat information sharing and communication platform for faster and better informed cyber threat response

More and more, organizations are putting their businesses at ever-greater risk by failing to keep up with the increasing volume of alerts and to truly comprehend these risks given the constantly changing threat environment. Compounding the problem is the singular nature of most security tool interfaces (too many screens) and the lack of cross-communication within security organization.

To get ahead of the situation, security teams need a solution that enables them to efficiently deal with security alerts and do so more effectively through better communication, greater collaboration, and expanded knowledge of the threat landscape. They need a tool that will allow them to more quickly collect, analyze, and respond to alerts in real-time, thus reducing the organization's overall cyber risk exposure

Cyware Situational Awareness Platform (CSAP) is a real-time threat information sharing and communication platform that enables you to systematically share accurate and actionable strategic threat intelligence. CSAP automatically ingests structured and unstructured threat intelligence, including TI feeds from external sources and alerts from internally deployed security tools, to quickly identify, prioritize, and respond to threats. CSAP's unique mobile capability is the underpinning for a powerful "On-the-Go" availability of information and platform access that empowers security teams to take action in real-time or warn employees of an immediate crisis.

CSAP is true a cybersecurity force multiplier. It's strategic threat intel-driven approach ensures faster and better-informed responses.  It drives improved collaboration between security teams, breaking down communication silos and improving overall security team efficiency and effectiveness.

## CSAP Capabilities

### Strategic Threat Intelligence Sharing

- Automated Intel Ingestion & Dissemination
- On-the-Go Sharing via Mobile
- Analyst Enrichment and Anonymization
- Mitre ATT&CK™ Heat Mapping
- Directed Sharing Based on Role, Location and/or Business Group

### Complete Threat Communication

- Custom Alerts and Notifications
- Automated RSS Conversion and Alerting
- Out-of-Band Crisis Notification
- Mobile-enabled Communication via SMS, CSAP Mobile App, Voice Call or Email

### Advanced Alert Orchestration

- Multi-source Ingestion, Aggregation, and Noise Removal
- AI-driven Analyst Interaction
- Remote Alert Actioning via Mobile
- Automated Email Ingestion and Conversion

### Enhanced Security Collaboration

- Trusted Sharing Communities
- Encryption-based Secure Messenger
- Mobile-enabled Incident Reporting
- One-click Security Support
- Customizable Metrics-based Reporting

## Gain a Better Understanding of Threat Landscape

- Deploy a strategic threat intel-driven approach to exchange and manage alerts on incidents, breaches, and security trends to ensure end-users are aware of the cyber threats facing your organization.

- Automate alerts from various sources into human-readable security updates and receive real-time information on new threats, techniques, and malware without having to manually look to multiple sources.

- Gain greater visibility of existing and emerging threats tthrough actionable, information sharing.

## Improve Cyber Awareness & Resilience

- Create, receive, and share real-time role, location and business purpose-based alerts via the web, email or mobile to power constant, reliable situational awareness.

- Aggregate unique OSINT threat intelligence feeds and vulnerability & malware early notifications to provide actionable alerts with employees, vendors, customers, peers and more.

- Enhance collaboration between various internal teams and key stakeholders, such as CISO, SOC Manager, Analysts, etc. through threat specific discussions in a closed and trusted environment.

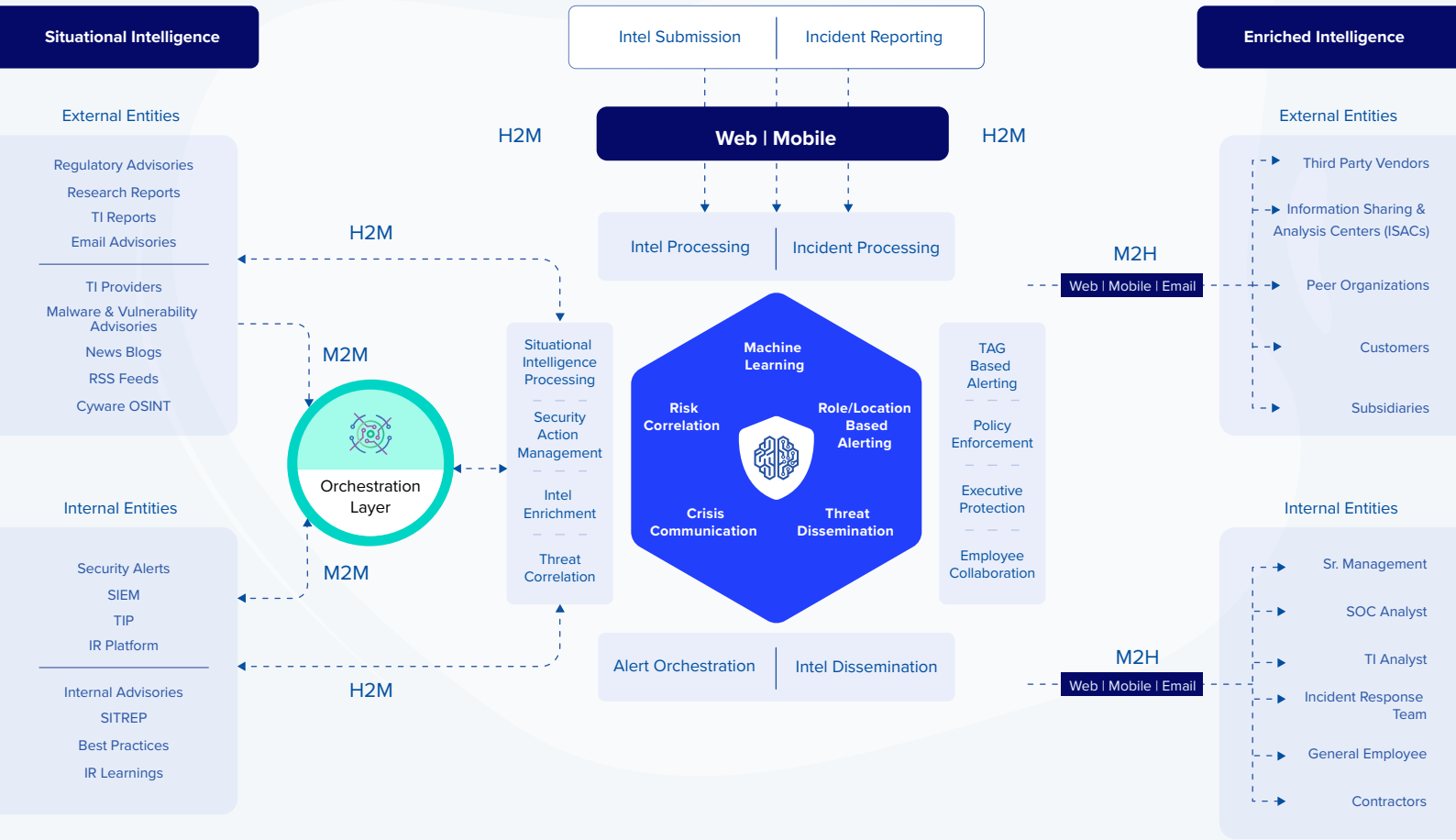## Faster and More Informed Responses = Better Decisions

- Deliver alerts automatically from SIEM tools, threat intelligence platforms, Intel feeds and vulnerability scanning tools, etc. to those who need to take action.

- Equip SecOps teams with automated threat intelligence ingestion and dissemination capabilities to quickly identify, prioritize and respond to threats.

- Orchestrate all security alerts into both human and machine-readable formats for AI-enhanced and prioritized alerts ready for human decision-making.

## Mobile-enabled Anytime, Anywhere Communication & Actioning

- Strengthen your first line of defense through actionable, real-time cyber situational awareness and incident response within a single, streamlined platform.

- Share accurate and actionable strategic threat intelligence over mobile and web apps, with or without analyst intervention, for faster threat detection, analysis, and response.

- Rapidly alert all or a select group of employees in case of emergency situations, like a large malware outbreak or major vulnerability disclosure, using the Crisis Notification feature.

# CSAP Architecture Diagram

## Situational Intelligence

### External Entities

Regulatory Advisories
Research Reports
TI Reports
Email Advisories

TI Providers
Malware & Vulnerability Advisories
News Blogs
RSS Feeds
Cyware OSINT

### Internal Entities

Security Alerts
SIEM
TIP
IR Platform

Internal Advisories
SITREP
Best Practices
IR Learnings

## Intel Submission | Incident Reporting

### Web | Mobile

Intel Processing | Incident Processing

H2M        H2M

H2M

M2M

Orchestration Layer

M2M

H2M

Situational Intelligence Processing

Security Action Management

Intel Enrichment

Threat Correlation

### Machine Learning

Risk Correlation

Role/Location Based Alerting

Crisis Communication

Threat Dissemination

TAG Based Alerting

Policy Enforcement

Executive Protection

Employee Collaboration

Alert Orchestration | Intel Dissemination

M2H
Web | Mobile | Email

M2H
Web | Mobile | Email

## Enriched Intelligence

### External Entities

Third Party Vendors
Information Sharing & Analysis Centers (ISACs)
Peer Organizations
Customers
Subsidiaries

### Internal Entities

Sr. Management
SOC Analyst
TI Analyst
Incident Response Team
General Employee
Contractors

**M2M - Machine to Machine | H2M - Human to Machine | M2H - Machine to Human**

---

# Machine-Powered, Mobile-Delivered Collaborative Cyber Threat Defense

- Send real-time security alerts and crisis notifications to your employees

- Empower employees to share threat intelligence on mobile

- Collaborate with your colleagues over built-in Secure Messenger

- Automate security alerts from all deployed tools
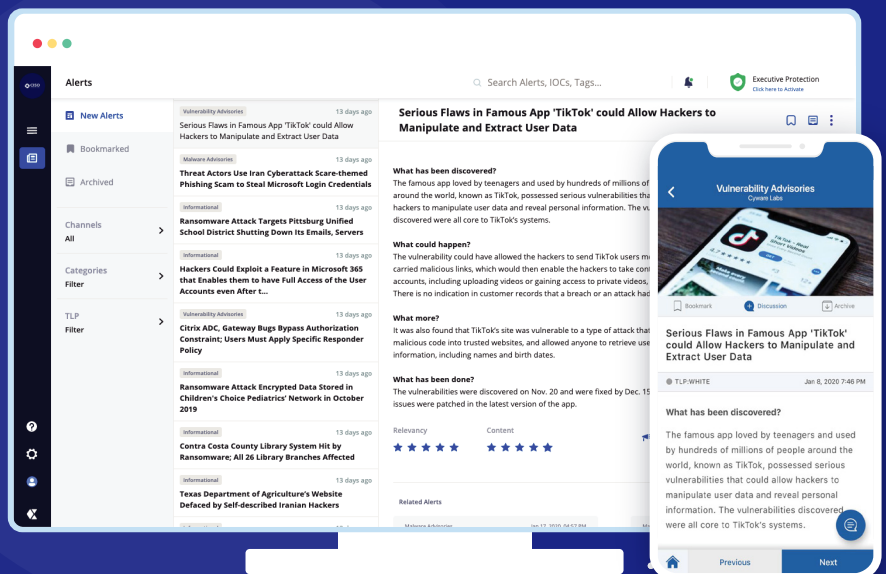
# The CSAP Advantage

**CENTRALIZED DASHBOARD**
Manage all security alerts using a single, centralized, easy-to-use dashboard with performance metrics, graphs providing insights into alerting, intel sharing and user activity.

**CYWARE ALERTS**
Gain access to unlimited real-time, expertly analyzed and enriched threat alerts to proactively neutralize risks from malware, vulnerabilities, and data breaches to stay ahead of the bad actors.

**EXECUTIVE PROTECTION**
Empower key stakeholders with the ability to rapidly notify cyber or physical security teams about threats with one-click personal concierge security support.

**DETAILED REPORTS AND METRICS**
Create and view reports based on various metrics and gain in-depth insight into the organization's security readiness, based on alert engagement status and CSAP mobile app launch status.

**INTEL EXTRACTION**
Extract Intel in a standardized format from a URL with just a click of a button on your mobile device and quickly share it with responsible security teams.

**IOC SHARING**
Develop a potent defensive mechanism against threats by proactively sharing and blocking IOCs through your mobile device.

**KNOWLEDGE BASE**
Create an extensive knowledge base of Threat Briefs, Standard Operating Procedures, Company Policies and share access with employees for easy and quick referencing via mobile and web app.

**SURVEY TOOL**
Garner the opinion of your employees on various issues, measure if your message is being heard, and create more impactful company policies through targeted surveys.

## Deployment Environments

We provide multiple deployment options for our products, giving our customers the flexibility to make use of all the product features by choosing the best model that suits their business needs.
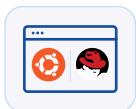
Public and Private Cloud

On-Premise

Hybrid

Air Gapped

## System Requirements

System requirements will change based on the considerations of high availability and backups.

**Operating System**

**16** CPU Cores

**32** GB Memory

**100** GB Storage

## About Cyware

Cyware Labs is a product-based cybersecurity provider headquartered in New York, USA. Cyware offers a full-stack of innovative cyber fusion solutions for strategic, tactical, technical and operational threat intelligence sharing, security automation and full threat response.

Cyware's solutions are designed to inculcate cyber resilience and promote secure collaboration between organizations. Cyware's products while enhancing threat visibility, also deliver the needed control for a proactive response by providing organizations with an automated context-rich analysis of threats without losing the element of human judgment.

**CYWARE™**

**Cyware®**
1460 Broadway New York NY 10036

cyware.com | sales@cyware.com        855-MY-CYWARE