Cyware Fusion and Threat Response (CFTR)

A Complete Security Orchestration, Automation, and Response (SOAR) Solution

In today's world of constantly evolving and an ever-expanding threat landscape, security organizations are struggling to keep pace. Coupled with the challenges of talent shortages and analyst fatigue, they need security tools that will allow them to be more efficient and effective with their limited resources. More and more, security organizations are turning to Security Orchestration, Automation, and Response solutions to better leverage cyber data and proactively respond to security threats.

Cyware's Fusion and Threat Response platform is a complete SOAR solution that provides threat and vulnerability management, security operations orchestration, and automated incident response, seamlessly integrating with your current security environment. CFTR leverages real-time strategic, tactical, and operational threat intelligence and cyber data fusion capabilities to produce a 360-degree view of an adversary. It empowers organizations to effectively combat threats by collecting, visualizing and correlating reliable threat data from multiple security tools and sources for delivering automated threat response.

CFTR promotes faster investigation, remediation, and control and makes it easier for SOC managers and senior management to measure ROI across the entire IR lifecycle using a single window of analysis.

Capabilities and Benefits

Early Prevention

- Strategic & Tactical Threat Intelligence Ingestion and Aggregation
- Comprehensive Asset Management- Digital and Human
- Vulnerability, Malware & Threat Actor Databases

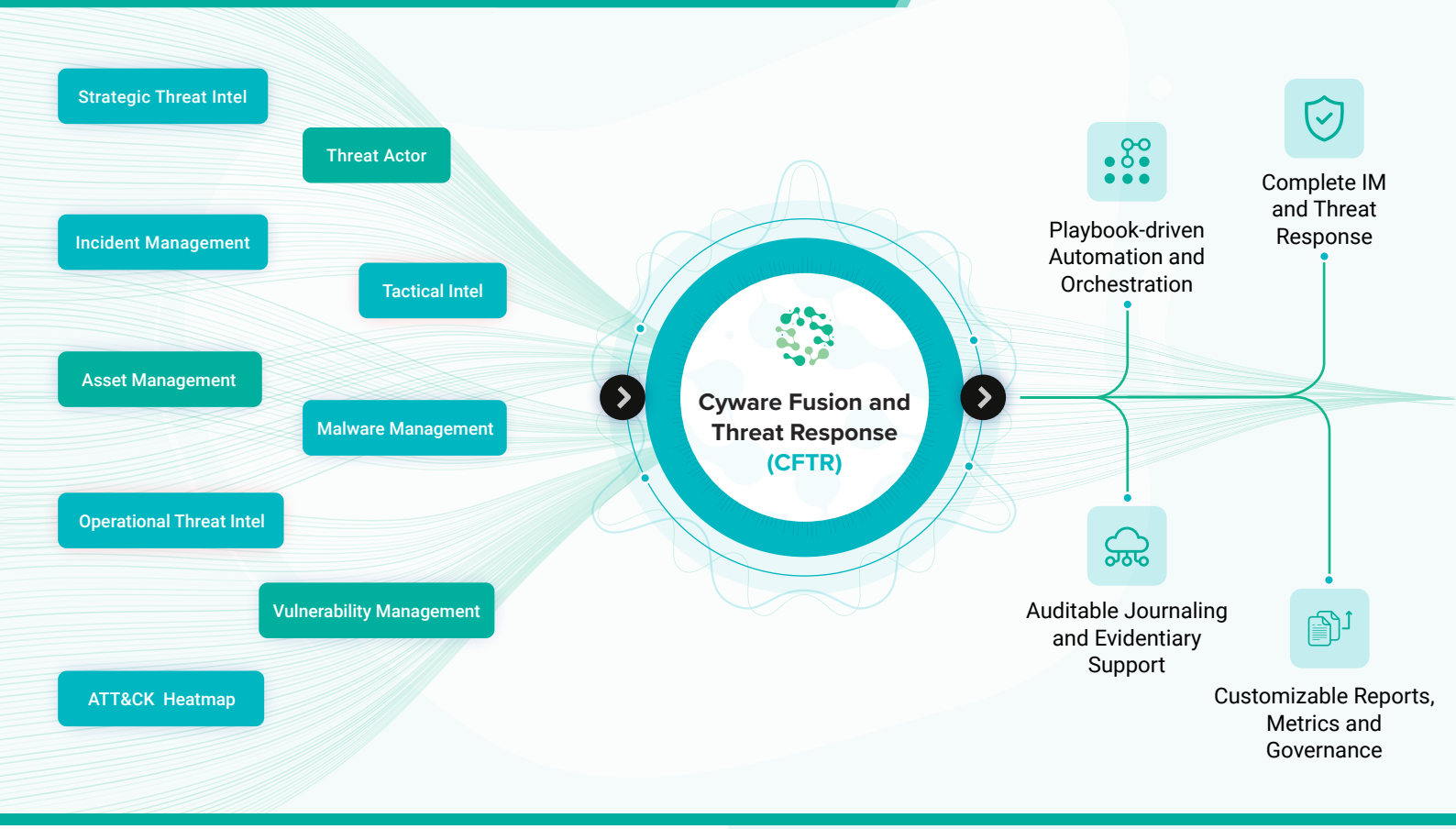
Advanced Detection & Proactive Analysis

- Real-time Threat Intelligence and Cyber Data Fusion
- Contextualized Threat Landscape Mapping
- End-to-End Campaign Management
- MITRE ATT&CK Navigator Framework

Automated Response & Management

- Seamless Integration with Deployed Security Tools
- Advanced Playbooks
- Machine-to-Human Orchestration
- Auditable Tracking and ROI Measurement

Cyber Data Fusion Enhanced Response Platform



360-degree Threat Management

- Fuse disparate Intel from multiple trusted sources to produce a comprehensive, accurate, and actionable view of the adversary
- Extend beyond incident management to manage and respond to all kinds of security threats such as campaigns, malware, vulnerabilities, and threat actors
- Connect the dots between Intel and Incidents to unearth latent threat patterns and accordingly strategize and prioritize response
- Unmask the attacker's tools and tricks by clearly mapping Indicators of Compromise (IOCs) such as IPs, Domain Names, URLs and Hashes with the Tactics, Techniques and Procedures (TTPs),
- Leverage customized ATT&CK Navigator Heatmap to produce a continuous threat footprint by mapping down TTPs used by Threat Actors against reported Incidents

SOC Metrics and Governance

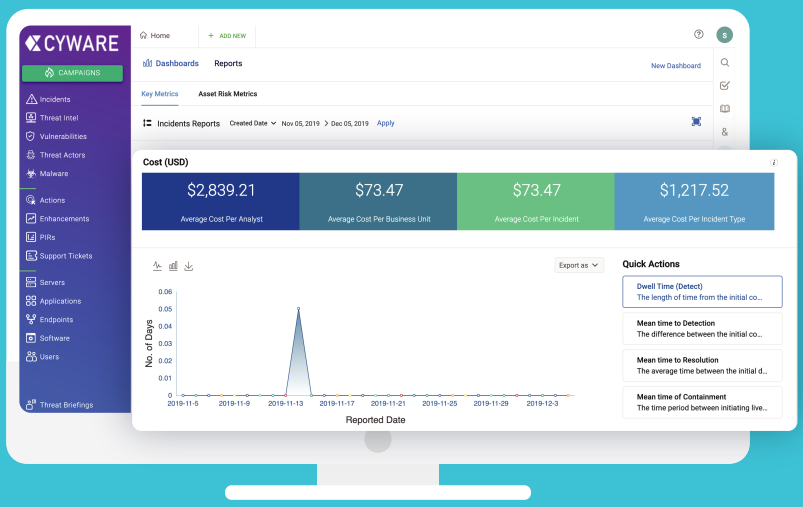
- Quantify incident costs through measurable indicators such as the average cost of an incident, cost per incident type, average cost per analyst, average cost per business unit, and many more with thousands of built-in cost metrics
- Define extensives KPIs to measure your processes and individual analysts as well as identify bottlenecks in SIEM rules, playbooks, and staff performance
- Leverage threat briefings to initiate discussions on incidents, vulnerabilities, actions, and other threats within rules, playbooks, and staff performance
- Gain the ability to log each field level user activity to have auditable records of who changed what and when

Gartner:

By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually

Move Beyond Antiquated IR Platforms to Become Truly Cyber Resilient

Problems faced by SOC / IR / Intel Teams	How CFTR Solves them
Focus on Incidents and Not Threats	Specialized Threat Management Modules for Incidents, Malware, Vulnerabilities, Threat Actors
Analyst Fatigue	Cyber Fusion, Alert Orchestration, Automated Playbooks Single Window IR Lifecycle Management
Alert Prioritization for Incident Response	Contextual Intelligence, Machine Learning
Lack of Intel for Incident Investigation	Integration with External Sources and Internal IT / Security Tools
Too many IT and Security Tools	Security Orchestration
Manual Response	Automation Playbooks
Disjointed Response Procedures	Single Window IR Lifecycle Management

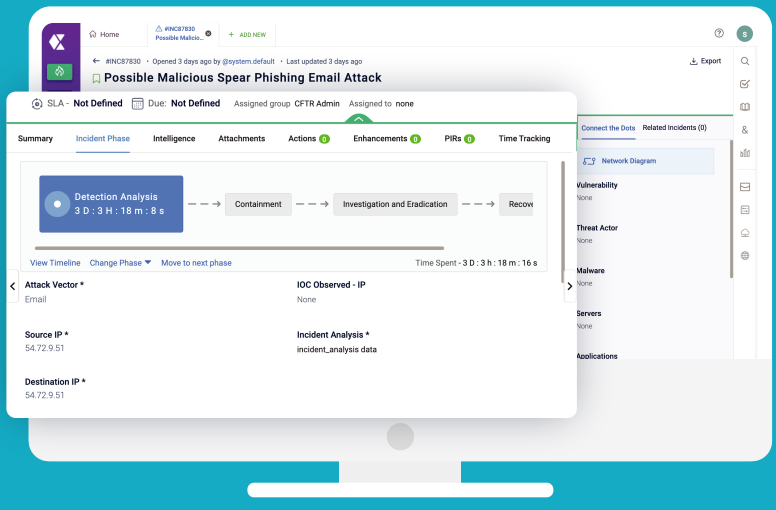


Metrics-driven Response Analytics

- SLA Tracking and dedicated indicators for ROI measurement across the IR lifecycle
- Technology efficacy measurements to ensure state-of-the-art management reporting
- Customizable reports to visualize and quantify the ROI
- Over 100 out-of-the-box widgets along with the ability to create custom widgets

Single Window IR Lifecycle Management

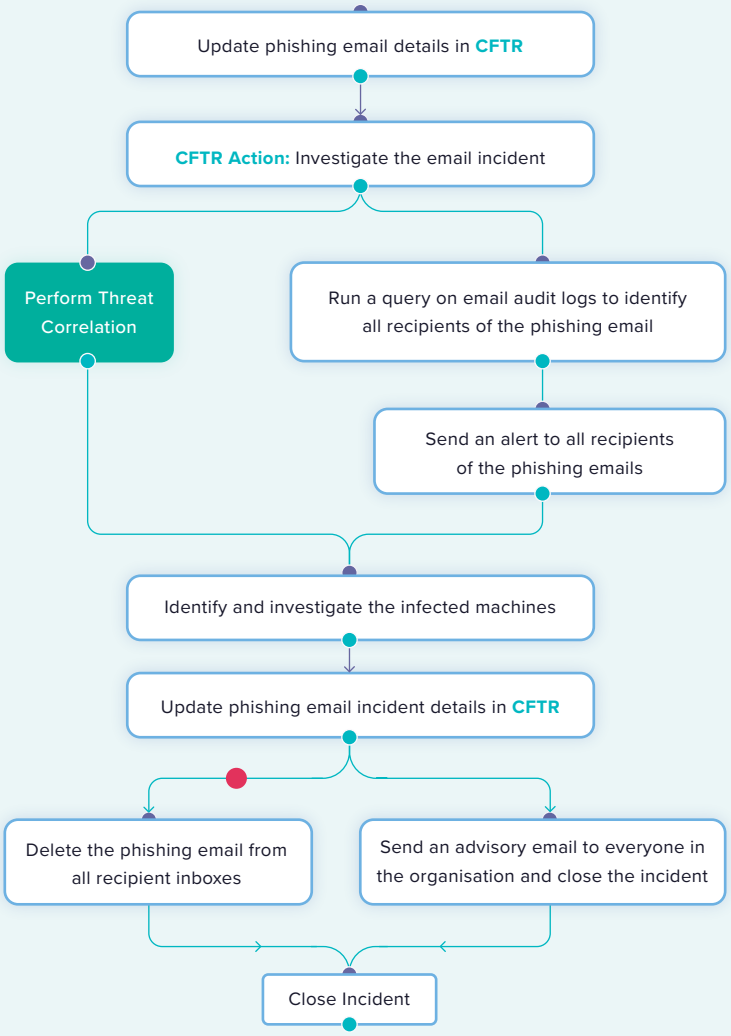
- End-to-end IR lifecycle management with proactive threat defense operations
- Integrated platform for detection, analysis, enrichment, investigation, containment, recovery, and governance
- Specialized management and response features for threat intelligence, threat actor, malware, digital assets and vulnerability tracking
- Centralized incident tracking and orchestration containment technologies



360-degree Threat Management

- Automate repetitive manual tasks such as data collection and enrichment, incident-response processes, all in a matter of seconds
- Deliver countermeasures at machine speed by orchestrating with other security solutions such as SIEM, IDS/IPS, F/W, UEBA, etc.
- Automate SOC workflows with Playbooks for optimum analyst participation, high availability
- Build custom Playbooks for any incident type with intuitive drag and drop workflow
- Gain access to our exclusive Playbook library with hundreds of prebuilt Playbooks

Automated Custom Playbooks



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	CPU Cores	Memory	Storage
	16	32 GB	100 GB

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