CYWARE™

Respond
CFTR

Respond (CFTR)

An End-to-End Incident Management and Threat Response Automation Platform

With a constantly evolving threat landscape, organizations are struggling to keep pace. With the challenges of talent shortage and analyst fatigue, they need security tools that will allow them to be more efficient and effective with their limited resources. Many organizations are turning to threat response automation solutions to better leverage cyber threat data and proactively respond to security threats.

Respond (CFTR) platform is a complete threat response automation solution that provides case/incident management, malware management, threat actor and vulnerability management, and security orchestration and automation capabilities while seamlessly integrating with deployed security technologies.

Respond leverages real-time strategic, tactical and operational threat intelligence, and cyber data fusion capabilities to produce a 360-degree view of adversary behavior.

It empowers security teams to effectively combat threats by collecting, visualizing, and correlating reliable threat data from multiple security tools and sources for delivering an automated threat response.

Respond promotes faster investigation, remediation, and control, while also making it easier for SOC managers and senior executives to measure ROI across the entire incident response lifecycle using a single platform.

CAPABILITIES AND BENEFITS

Early Threat Prevention

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

Advanced Detection and Proactive Analysis

- Real-time Threat Intelligence and Cyber Data Fusion
- Contextualized Threat Landscape Mapping
- Fully Customizable Form Management for Incidents
- End-to-End Threat and Incident Analysis
- MITRE ATT&CK Navigator Framework

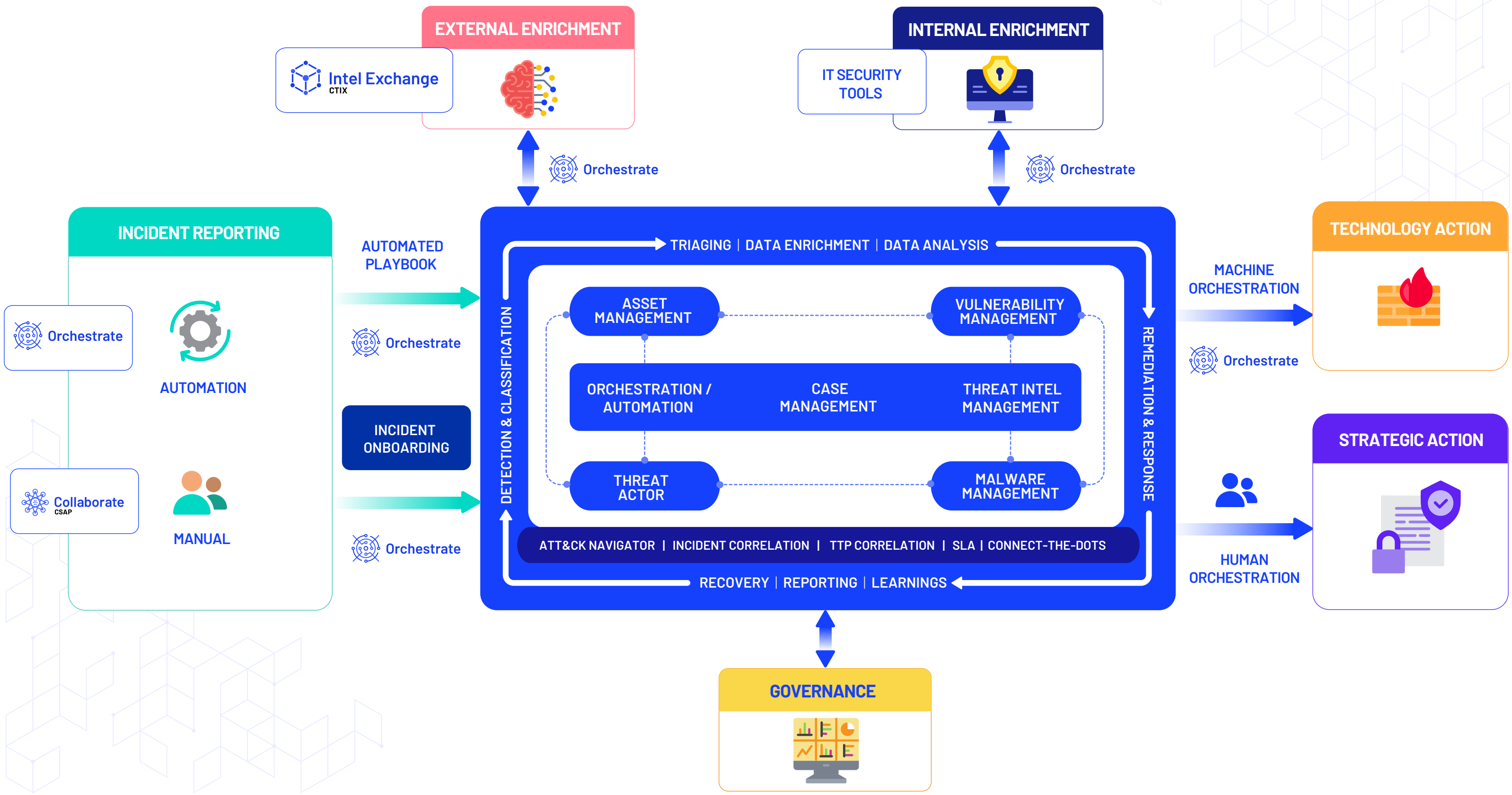
Automated Threat Response Management

- Multi-Tenant MSSP Dashboard
- Seamless Integration with Deployed Security Tools
- Advanced Automation Playbooks
- Machine-to-Human Orchestration
- Auditable Tracking and ROI Measurement

Advanced Machine Learning Capabilities

- Recommendation Engine for Analyst Allocation
- Historic Incident Analysis and Automated Incident Correlation
- Attack Prediction and Threat Response Suggestion

CYBER DATA FUSION ENHANCED RESPONSE PLATFORM



360-DEGREE THREAT MANAGEMENT

- Fuse disparate intelligence from multiple trusted sources to produce a comprehensive, accurate, and actionable view of the adversary.
- Go beyond incident management to manage and respond to all security threats including malware, vulnerabilities, and threat actors.
- Connect the dots between intelligence and incidents with the incident visualizer to unearth latent threat patterns.
- Unmask the attackers' 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 ATT&CK Navigator heatmap to produce a continuous threat footprint by mapping down TTPs used by threat actors against reported incidents.
- Identify high-risk devices and users in the organization's network and take appropriate actions against them.

MULTI-TENANT MSSP DASHBOARD

- View all data for multi-tenants from a single source and enable data grouping and tenant-wise data sharing based on tenant's consent.
- Foster multi-tenancy for incident management, resource management, and SLA management.

BUILD YOUR OWN MODULE

- Build customizable modules with no restrictions based on the organization's business needs.
- Create custom dashboards and fields for enhanced threat visibility and analysis.

COMMUNICATION CHANNELS INTEGRATION

- Share case/incident-based updates with extended teams for better visibility and collaboration.
- Enable seamless threat information sharing with Slack integration.

RULES ENGINE

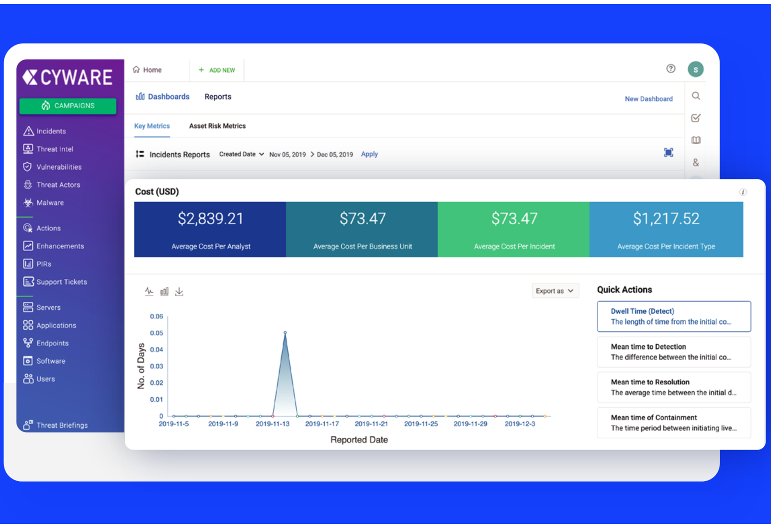
- Automate triggers/actioning based on incident status change to reduce manual errors and save analyst time.

FULLY CUSTOMIZABLE FORM MANAGEMENT

- Create multiple case/incident workflows.
- Create custom phases as per the organization's business requirements.
- Leverage an extensive list of fields used across all case/Incident Workflows through the field library.
- Display fields according to conditional logic based on specific use cases.
- Reuse already created phases making sure users don't have to build the form from scratch.
- Map set of parameters to a case/incident workflow, enabling it to be automatically used for the incident.

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 extensive KPIs to evaluate the performance of your processes and individual analysts and identify bottlenecks in SIEM rules, playbooks, and staff performance.
- Leverage threat briefings to initiate discussions on incidents, vulnerabilities, actions, and other threats within rules and playbooks.
- Gain the ability to log each field-level user activity to have an auditable archive of all the changes made by different users.



Incidents Reports Created Date Nov 05, 2019 > Dec 05, 2019 Apply

Cost (USD)

$2,839.21	$73.47	$73.47	$1,217.52
Average Cost Per Analyst	Average Cost Per Business Unit	Average Cost Per Incident	Average Cost Per Incident Type

Quick Actions

Dwell Time (Detect)
The length of time from the initial co...

Mean time to Detection
The difference between the initial co...

Mean time to Resolution
The average time between the initial d...

Mean time of Containment
The time period between initiating live...

CUSTOMIZABLE THREAT RESPONSE ANALYTICS

SLA tracking and dedicated indicators for ROI measurement across the entire incident response lifecycle.

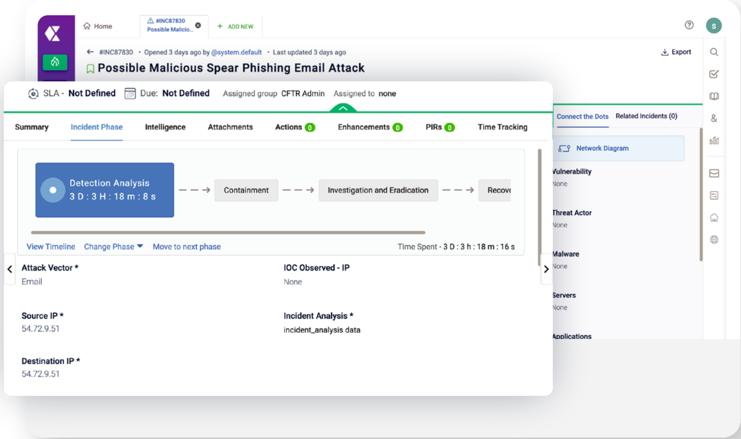
Technology efficacy measurements to ensure state-of-the-art management reporting.

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 INCIDENT RESPONSE LIFECYCLE MANAGEMENT

- End-to-end incident response 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, orchestration, and containment technologies.



#INC87830 • Opened 3 days ago by @system.default • Last updated 3 days ago

Possible Malicious Spear Phishing Email Attack

SLA - Not Defined Due: Not Defined Assigned group CFTR Admin Assigned to none

Detection Analysis 3 D : 3 H : 18 m : 8 s → Containment → Investigation and Eradication → Recove

Time Spent - 3 D : 3 h : 18 m : 16 s

Attack Vector *
Email

IOC Observed - IP
None

Source IP *
54.72.9.51

Incident Analysis *
incident_analysis data

Destination IP *
54.72.9.51

Vulnerability
None

Threat Actor
None

Malware
None

Servers
None

Applications

END-TO-END THREAT RESPONSE AND MANAGEMENT

- INCIDENT AND CASE MANAGEMENT
- MULTI-TENANT MSSP DASHBOARD
- CONNECT THE DOTS
- MALWARE AND VULNERABILITY MANAGEMENT
- THREAT ACTOR MANAGEMENT
- ASSET MANAGEMENT
- ATT&CK NAVIGATOR
- AUTOMATION RULES ENGINE
- INCIDENT COST METRICS AND ANALYSIS
- CENTRALIZED GOVERNANCE
- IOC-TTP MAPPING
- SLACK INTEGRATION
- ACTION LIBRARY
- BUILD YOUR OWN MODULE
- SLA TRACKING
- ANALYST MAPPING AND ROSTER MANAGEMENT

DOCKER-BASED DEPLOYMENTS

We provide Docker-based 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 & PRIVATE CLOUD
- ON-PREMISE
- HYBRID

ABOUT CYWARE

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation SOAR (security orchestration, automation, and response) solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout.

Cyware's Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.

111 Town Square Place Suite 1203, #4 Jersey City, NJ 07310
cyware.com | sales@cyware.com | 855-MY-CYWARE