Cyware Fusion and Threat Response (CFTR)

An End-to-End Threat Response Automation Platform

With a constantly evolving and ever-expanding 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. More and more, organizations are turning to threat response automation solutions to better leverage cyber threat data and proactively respond to security threats.

Cyware’s Fusion and Threat Response (CFTR) platform is a complete threat response automation 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 adversary behavior. It empowers organizations to effectively combat threats by collecting, visualizing, and correlating reliable threat data from multiple security tools and sources for delivering an automated threat response.

CFTR 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 Prevention
- Strategic and Tactical Threat Intelligence Ingestion and Aggregation
- Comprehensive Digital and Human Asset Management
- Vulnerability, Malware, and 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 intelligence from multiple trusted sources to produce a comprehensive, accurate, and actionable view of adversary behavior.

- Extend beyond incident management to manage and respond to all kinds of security threats such as attack campaigns, malware, vulnerabilities, and threat actors.

- Connect the dots between intelligence 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 extensive KPIs to evaluate the performance of 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 an auditable archive of all the changes made by different users.

Gartner:
By 2022, 50% of all SOCs will transform into modern SOCs with integrated incident response, threat intelligence, and threat hunting capabilities.
### Problems faced by SOC / IR / Intel Teams

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on Incidents and Not Threats</td>
<td>Specialized threat management modules for incidents, malware, vulnerabilities, and threat actors</td>
</tr>
<tr>
<td>Analyst Fatigue</td>
<td>Alert orchestration, automated playbooks, and single window IR lifecycle management to increase efficiency</td>
</tr>
<tr>
<td>Lack of Alert Prioritization for Incident Response</td>
<td>Prioritize with contextual intelligence and machine learning</td>
</tr>
<tr>
<td>Lack of Intel for Incident Investigation</td>
<td>Gain visibility through integrations with external sources and internal IT/Security tools</td>
</tr>
<tr>
<td>Manual Response</td>
<td>React faster and smarter with automated playbooks</td>
</tr>
<tr>
<td>Disjointed Response Procedures</td>
<td>Leverage a single window for IR lifecycle management</td>
</tr>
</tbody>
</table>

### 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
Automated 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, and others
- Automate SOC workflows with playbooks for optimum analyst participation and 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

Deployment Environments

We provide multiple deployment options for our products, giving our customers the flexibility to utilize all our product features by choosing the model that best 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

About Cyware

Cyware provides threat intelligence sharing and cyber fusion products to security teams across the world. Cyware’s innovative solutions include capabilities for strategic and tactical threat intelligence sharing, cyber fusion, security orchestration, and incident response.

Cyware’s solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for customers.

Cyware
1460 Broadway New York NY 10036

cyware.com | sales@cyware.com

855-MY-CYWARE