Introducing

The Cyber Fusion Center

Boost threat response with better collaboration between security teams

CYWARE™

Executive Summary

Rising security spending isn't enough to combat increasingly frequent and sophisticated cyber threats. The number of security incidents and breaches grows each year and will continue rising until security teams find a solution to their primary challenges:

- Too many alerts with too little context
- Siloed security functions
- Inefficiencies and duplication of tools and effort
- Poorly managed and standardized security data
- Lack of time to focus on proactive security functions
- Continued shortage of skilled cybersecurity professionals
- Lack of automation and orchestration for incident response and threat intelligence teams

Cyber fusion center platforms (CFC) were initially designed to address these challenges but haven't always delivered on their promise. The reason is that most platforms provide just one or two of the three core SOAR capabilities (security orchestration, automation, and response) and not well enough to substantially improve security processes or outcomes.

This white paper examines a solution to security challenges that builds upon SOAR technology and the cyber fusion center platform—and how it can improve collaboration and threat response.

Contents

Key Learning Points

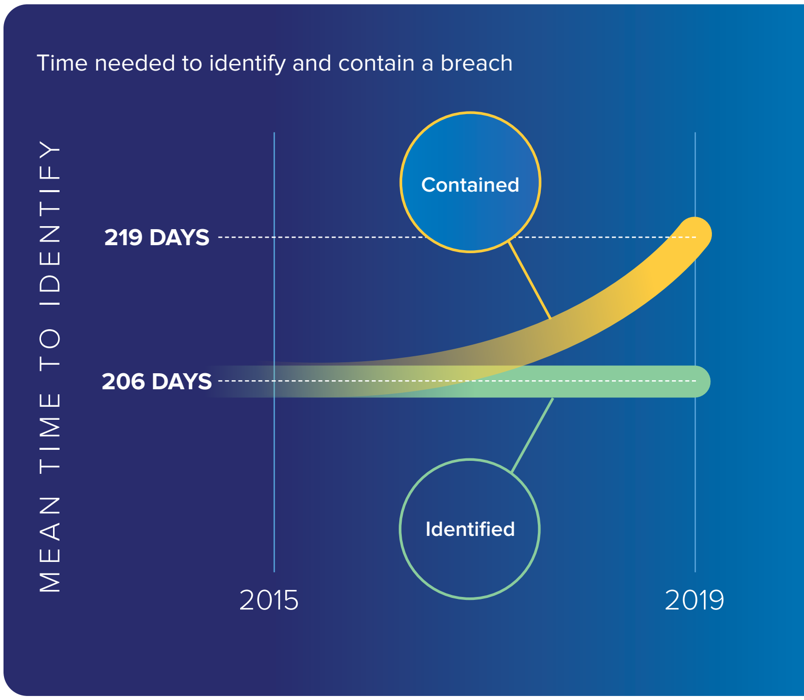
- As the threat landscape worsens, enterprise security teams are losing ground against their attackers. They now take an average of 219 days to identify and contain a security breach.
- Security teams are hamstrung by inefficiencies and collaboration challenges caused by a lack of integration between disparate security tools and processes.
- SOAR technology has failed to deliver on its promise and doesn't make a meaningful difference to the challenges faced by today's security teams.
- CFC platforms break down silos with a combination of SOAR functionality, enhanced threat intelligence, and situational awareness, enabling faster and more effective threat response.
- Enterprises should look beyond their borders by engaging with intelligence-sharing communities like ISACs that help all members build collective defense within and beyond their borders.

The Price of Inefficiency

The cybersecurity market has grown in value from $60 billion in 2011 to $150.4 billion in 2021 at a Compound Annual Growth Rate (CAGR) of 9.63%. Between now and 2027/28, industry analysts expect market growth to continue at a CAGR of between 9.4%–12.5%.

Despite this, the number of annual security incidents and data breaches has risen every year for the past decade, and the number of breached records hit a new high in Q1 2021.

It's not just the number of breaches that are concerning. The time needed for security teams to identify and contain breaches has also risen over time. From 2015– 2019, Mean Time To Identify (MTTI) security breaches remained at 206 days, while MTTC rose from 69 to 73 days. In total, that means security teams need 219 days to identify and contain a security breach.



More Spending = More Problems?

It's no surprise that security teams need more time to contain breaches. Enterprise IT environments constantly grow in scope and complexity, forcing security teams to continually grow and adopt new technology and processes. The recent surge in remote working has only exacerbated this problem.

Many enterprises have multiple security functions to cope with growing needs, often distributed across a wide area. From SOCs and IR teams to threat intelligence, red teams, vulnerability management, and more, today's security teams are more diverse and spread out than ever before. While each of these functions is vital, this added complexity presents a new challenge: more silos.

Each security function has its own objectives, systems, and battles. By running each security discipline in isolation, several issues arise:

- Duplication of processes, tools, and effort
- Wasted attention and energy on unproductive activities
- Minimal human and technical integration
- Limited and inefficient communication
- Poor data management, structure, and awareness

These issues lead to a more significant problem:
Poor efficiency and degraded security outcomes.

Many security teams have understandably tried to spend their way out of this problem with a best-of-breed approach. However, as tools grow in number and complexity, security teams only become more overwhelmed. It's no longer enough for teams to build an optimized model that relies on adding more tools—the more you add, the more security teams have to manage.

Technology Challenges

An Exabeam study found security operations teams ranked their top three pain points as:

1. Keeping up with security alerts
2. Coordinating information between security and IT
3. Poor security tool integration

While tools like SIEMs, firewalls, AVs, and EDRs play an essential role, they don't support security teams to coordinate information, resources, and capabilities to tackle cyber threats proactively.

Instead, security teams are left drowning in a sea of alerts that's devoid of context or prioritization.

What Security Teams Need

To contain incidents more quickly, security teams need to become more proactive. However, this isn't going to happen if each security function is left to solve its own problems, develop its own processes, and procure its own tools. Security teams need to take a more collaborative and intelligence-driven approach.

There's nothing inherently wrong with having lots of security tools. Often, they are necessary to ensure each key discipline is adequately covered. However, forcing teams to contend with dozens of disparate, disconnected tools wastes resources and limits effectiveness.

Security teams need a unified solution that enables the functionality of the entire technology stack while allowing security disciplines to collaborate, communicate, and share resources.

> “**The problem is getting worse faster than we're getting better.** We're not catching up, we're losing ground. So we have to think, how can we approach this problem more cleverly, and how can we help each other get through it?”

Tony Sager

CHIEF EVANGELIST, THE CENTER FOR INTERNET SECURITY

Source: https://youtu.be/OZLO-xekp3o

Critically, intelligence sharing shouldn't be limited to within the enterprise.

Information Sharing and Analysis Centers (ISACs) in industries like healthcare and financial services have grown in scope and now play a crucial role in improving threat response. Outside of the United States, similar entities such as CERTS or private and non-profit sharing groups exist with the same goals. A complete solution to the challenges above must include a threat intelligence sharing capability that supports inter-enterprise collaboration to make security more proactive.

Any unified solution should support four key functions:

1. Threat management and response
2. Collection and analysis of threat intelligence and data
3. Process automation and orchestration
4. Situational awareness and information sharing

Doesn’t SOAR Solve These Problems?

SOAR burst onto the security scene in 2014 under several different names, including Integrated Cybersecurity Orchestration Platforms (ICOP). At first, these solutions focused purely on automation and orchestration to manage security data and initiate remediation processes.

In 2017, Gartner coined the term SOAR and expanded the definition to:

> ***Solutions that combine incident response, orchestration and automation, and threat intelligence management capabilities in a single platform.***

To achieve this, a SOAR tool must provide:

INCIDENT RESPONSE & MANAGEMENT

VULNERABILITY MANAGEMENT
CASE AND INCIDENT MANAGEMENT
WORKFLOWS
INCIDENT DATA MANAGEMENT
AUDITING, LOGGING, AND REPORTING

THREAT INTELLIGENCE COLLECTION, ANALYSIS & SHARING

THREAT INTELLIGENCE AGGREGATION
CURATION
DISTRIBUTION
ALERT ENRICHMENT
VISUALIZATION

ORCHESTRATION & AUTOMATION

INTEGRATION WITH OTHER TOOLS
PROCESS AND WORKFLOW AUTOMATION
PLAYBOOK MANAGEMENT

In Security Orchestration, Automation and Response: Rise of the Independents, Aite Group lays out eight further capabilities that a SOAR solution should provide in addition to these core functions:

1. **Integration** with all security tools, with a low- or no-code solution for custom integrations
2. **Alert triage** capabilities, including enrichment of alerts with contextual data
3. **Case management** tools built into the SOAR solution
4. **Built-in playbooks** (e.g., for SOC optimization) and no-code playbook creation
5. **Vulnerability management** augmentation using playbooks, automation, and integrations
6. **Risk scoring** for security incidents based on threat intelligence and industry frameworks
7. **Multi-tenancy** (several SOAR instances deployed on one host) with role-based access control
8. **Standards** for security processes based on accepted frameworks like MITRE ATT&CK

If SOAR tools provided all this in a single, unified platform, they would help address some of the efficiency and collaboration issues faced by security teams.

However...

Typically, most SOAR tools provide only **two-thirds** of what they promise.

Not All SOAR Tools Deliver SOAR

In practice, most SOAR tools only provide two-thirds of the value proposition at most. They focus too heavily on orchestration and automation, while incident response (IR) functions are lackluster, and threat intelligence (TI) capabilities are practically absent. Case management workflows, which are crucial to support inter-team collaboration, are usually lacking and treated as a secondary function.

While integration is a core component of SOAR, it usually lacks it—particularly between tools developed by different vendors. Most SOAR tools also fail to provide orchestration and automation across cloud and on-premise solutions or outside of the security stack. To deliver on the promise of SOAR, organizations need orchestration between security, engineering, DevOps, and IT operations workflows no matter where they are hosting… but this simply hasn't been available.

According to the Aite report mentioned above, alert triage capabilities alone can reduce analysts' effort to triage alerts by 95%. Yet, these capabilities are rudimentary in most SOAR solutions. Similarly, effective integration, automation, and orchestration tools can boost incident response rates by up to 90%—but again, since most SOAR tools lack critical capabilities, the majority of SOAR customers aren't able to realize these benefits.

These issues are so prevalent that some organizations use several SOAR tools to obtain all of the functionality—including SOAR layers built into other security tools. This may provide extra capabilities, but it further complicates the technology stack and creates more alignment issues.

SOAR Doesn't Address the Real Problem

Even if SOAR tools delivered the full value proposition, they still wouldn't address the real problem faced by security teams: the need for collaboration and collective defense.

To minimize the frequency and severity of incidents and breaches, security teams need to improve cross-functional collaboration and information sharing—both inside the enterprise and across intelligence-sharing communities. They also need to cut down on duplication of tools and effort, focusing financial and human resources on the highest value tasks.

However, one huge issue stands in the way of achieving this: with so many conflicting tools and processes, vital security and threat data are often poorly managed.

Common issues include:

- Inability to share data between tools and functions
- Lack of data normalization and standardization
- Not collecting vital security data
- Lack of clarity on what data tools collect and where it is stored
- Difficulty enriching and operationalizing threat intelligence
- Inability to determine the true severity of threats based on geography, industry, etc.

The lack of data management makes effective information sharing and collaboration between security functions impossible. Worse, since individuals often don't know what data is available, they may be missing out on resources that could improve their effectiveness.

A Holistic Problem Requires a Holistic Solution

Vendors have tried to address security challenges by building small, individual solutions for each need. Many security vendors have purchased smaller companies to diversify, aiming to incorporate their capabilities into a larger product. However, this piecemeal approach typically creates products that integrate poorly and can't address the need for cross-functional collaboration and sharing.

Security leaders in the military and telecommunications identified the need for a holistic solution years ago. Their approach was to build physical cyber fusion centers where all security intelligence functions were housed in the same room. Combined with rigorous, well-documented operational processes, this enabled those organizations to promote collaboration and intelligence sharing.

Even this presents a problem for modern enterprises. With operations distributed across broad areas, building physical cyber fusion centers is not only cost-prohibitive—it's logistically impossible. Instead, enterprises need a solution that addresses security challenges while supporting distributed operations.

What about other security tools?

A combination of solutions like IR, TIP, OA, and case management tools would seem to address the full SOAR definition. In practice, thorough integration of these tools proves challenging, causing further issues with collaboration, data/intelligence sharing, and collective defense.

Introducing the First Virtual Cyber Fusion Center

A Virtual Cyber Fusion Center (vCFC) platform breaks down security silos. Like the physical approach, vCFC brings disparate security functions together to help them proactively defend the organization from cyber threats. A vCFC platform enables geographically dispersed or remote teams to collaborate and share systems, data, and intelligence, unlike a physical center.

vCFC delivers on the full promise of SOAR while expanding three capabilities: threat intelligence and integration and orchestration. While the SOAR definition requires a limited version of these capabilities, it's not enough to support effective collaboration between security functions.

vCFC adds a fourth capability, situational awareness. This gives security personnel everything they need to understand and respond to threats—not just incidents—at their source.

By combining these four capabilities and enabling seamless automation and orchestration across the entire technology stack, vCFC delivers what organizations really need: improved security outcomes through heightened collaboration between security functions and seamless orchestration across security, engineering, and IT operations workflows.

What's in a vCFC Platform?

SOAR

- Comprehensive threat response
- Case management workflows
- Vulnerability management
- Data management, audit, logging & reports
- Centralization of all security data
- Operational TI, integration & orchestration

THREAT INTELLIGENCE EXCHANGE

- Tactical and technical TI sharing
- Threat enrichment, correlation & analysis
- Customized TI panes for each function
- Any-to-any threat feed orchestration
- Threat mapping, e.g., to MITRE ATT&CK
- TI sharing with partners, clients, ISACs, etc.
- Automated threat blocking & rule updates

INTEGRATION & ORCHESTRATION

- Seamless integration of all security tools
- Normalized data for all security functions
- Cross-environment orchestration
- On-demand & event-driven orchestration
- Pre-built playbooks for common workflows
- Full audit trail of all playbook activity
- Cross-functional orchestration between security, engineering, DevOps, and IT operations

SITUATIONAL AWARENESS

- Real-time sharing of strategic threat information
- Automated threat alert aggregation
- Data sharing between security functions
- Role- and industry-based threat alerts
- Real-time communication & collaboration
- Private and group-level discussion
- Actioning threat alerts to TIPs

By combining these four capabilities, vCFC platforms allow all security functions—no matter their location—to collaborate and share information freely while eliminating the need for duplication of tools, data collection, and effort. This enables security teams to engage in more proactive threat response and contain incidents more quickly when they arise.

How vCFC Platforms Compare to Dedicated Solutions

vCFC is a fusion of technologies that is operated remotely through a single platform. It brings together the functionality of several cornerstone security tools:

- Threat Intelligence Platforms (TIPs)—both strategic (CSAP) and technical (CTIX)
- Incident Response Platforms (IRPs)
- Security Orchestration, Automation, and Response (SOAR)
- Case management

vCFC goes a step further than each of these tools. It adds a layer of integration and collaborative functionality that empowers security teams to respond faster and more effectively to cyber threats.

What vCFC Adds to Dedicated Tools

TIP

- Normalization of unstructured data into STIX/TAXII format
- Machine-powered enrichment, correlation & analysis
- Machine-to-Machine (M2M) internal dissemination and actioning
- Any-to-any external threat intelligence sharing to partners & ISACs

SOAR

- Provides the full SOAR value proposition, including incident management, TI & OA
- Enables cross-environment orchestration, including between internal & cloud tools
- Data management, including normalization, audit, logging & reporting
- Enables cross-functional orchestration between security, engineering, DevOps, and IT operations

IRP

- Comprehensive threat response, including for incidents, vulnerabilities & threat actors
- Easy collaboration & threat information sharing between security functions
- Bi-directional integration with SOAR, TI & case management functions
- Threat mapping to industry frameworks (e.g. MITRE ATT&CK)

Case Management

- Designed specifically for a security environment
- Integrates seamlessly with SOAR, IRP & TI capabilities
- Enables collaboration and collective defense between security functions

Threat vs. Incident Response:

Historically, incidents were a prerequisite for response. This incident management model is reactionary and no longer effective in a landscape where response time is critical—responding to a threat before it evolves into an incident changes this model from reactive to proactive. Focusing on threats such as malware, vulnerabilities, and threat actors before they become incidents, enabling security teams to move past the outdated incident response process.

Unlike dedicated tools, a vCFC platform is designed from the ground up with integration and collaboration in mind. vCFC integrates the capabilities of each security tool into a single platform that enables:

1. Real-time, standardized information sharing between security functions
2. Seamless collaboration between security functions to tackle threats

This level of integration is not limited to security tools developed by the vCFC vendor. A vCFC platform enables seamless vendor-agnostic integration and interoperability across the entire technology stack—no matter where it is hosted or which function it belongs to.

vCFC Platforms Improve Security Outcomes

By bringing security tools, capabilities, and data into a centralized platform, vCFC enables security teams to realize a host of benefits:

- Provides total security visibility, ensuring all functions have a clear view of current threats
- Ensures all personnel has real-time access to a full spectrum of normalized data and logs
- Enables all security functions to manage threats more proactively
- Combats alert fatigue by only alerting on threats that pose a genuine risk
- Improves situational awareness through internal and external TI sharing
- Breaks down security silos and fosters transparency and collaboration between functions
- Avoids human and financial resource wastage caused by duplication of tools and effort
- Enhances the speed and consistency of incident and threat response

Why is external intelligence sharing so important?

Threat groups and individuals share and sell the latest tools, malware, and offensive intelligence widely in the criminal community. This has led to cyber threats evolving faster than security controls, partially explaining why security outcomes are getting worse.

Intelligence sharing communities enable enterprises to share threat research and analysis with clients, vendors, peers, and subsidiaries. ISACs, in particular, promote intelligence sharing within a community of enterprises from the same industry to improve security outcomes for all members.

Intelligence sharing tips the scales back in favor of defenders and enables global collective defense.

Nothing Replaces the Fundamentals

Perhaps the most harmful idea in security is that a singular tool or platform alone can solve fundamental problems. No matter how much a vendor promises their tool or service will make up for lacking internal systems or processes… it can't.

People, Process, Technology

Achieving cyber fusion is a journey. A vCFC platform provides the vital technology aspect of security operations and threat response, but it sits on the foundation of well-trained personnel and established policies and processes. If security functions are understaffed, have inadequate training, or don't have solid processes in place, a vCFC platform can't solve that problem—no technology can.

Assuming an enterprise security team already has solid personnel, it can follow a simple (but not necessarily easy) process to lay the foundation for cyber fusion:

> “The need for efficiency in security can be met through the **augmentation of internal security processes** with offerings from security service providers.”
>
> (Emphasis ours)

Gartner

HYPE CYCLE FOR SECURITY OPERATIONS 2020

Laying the Foundation for Cyber Fusion

PHASE 1

Establish solid, repeatable processes that cover the fundamentals of each security function

Orchestrating bad processes is dangerous and can lead to costly errors that may not be noticed until it's too late. The simplest way to develop solid, standardized processes is to observe top performers from each security function and model processes on their actions.

PHASE 2

Start orchestrating processes

Most enterprise security teams waste a tremendous amount of time on unproductive, repetitive tasks. Orchestrating and automating solid security processes can save a tremendous amount of time and free personnel to focus on higher-value tasks.

Note: Audit trails are essential for orchestrated processes to ensure errors are picked up quickly.

PHASE 3

Progress to virtual cyber fusion

Once an enterprise has basic orchestration built on solid, repeatable processes, it can begin to consider the broader benefits of vCFC. By collecting, analyzing, and sharing threat intelligence, and providing the right tools, enterprise security teams can streamline battle rhythms, increase visibility and cooperation between functions—and ultimately, improve security outcomes.

Human-free orchestration is a pipe dream

Many security automation vendors sell the idea that human analysts can be "orchestrated out" of processes altogether. Not only is this not true, but it also creates a false sense of security that genuine threats are mitigated automatically, when in fact, they could be missed altogether, and nobody would know. In practice, a human almost always needs to be involved in the loop at some stage to make informed decisions about the severity and appropriate response to each threat.

Managing Risk with a vCFC Platform

Most security teams focus on threats and incidents. At a higher level, teams should use risk calculations to decide how and when to allocate resources and develop new capabilities.

However, calculating cyber risk is a challenge. Historically, enterprise security teams have either shunned cyber risk measurement or relied on non-ideal approaches, including:

- External risk assessments. These typically rely on generic processes, aren't well-tailored to the enterprise, and only provide point-in-time risk awareness.
- Complex mathematical models. Some of these are very accurate, but the process is arduous and consumes a lot of time and resources. (Source)

vCFC platforms provide enterprises with an opportunity to measure and track cyber risk in a more realistic and tailored manner. This approach relies on two core vCFC capabilities:

1. **Situational awareness.** Comprehensive and focused threat intelligence helps security teams build a vivid picture of their threat landscape, including the actors and threats they are most likely to encounter. This allows them to identify the most appropriate actions to take and controls to implement.
2. **Post-incident analysis.** After an incident, security teams should always complete threat and response analysis. vCFC platforms provide total visibility and audit trails, making it easy to identify the technology, processes, and individuals contributing to an incident. This makes it easy for security teams to identify areas for improvement.

Combined, these capabilities enable security teams to allocate resources to the areas that pose the greatest risk to their organization.

A Cyber Fusion Center in Action

Financial Institution Slashes Time-to-Respond with Cyware's vCFC Platform

The Challenge

The bank's security team often receives intelligence from government agencies on serious threats. Reports often arrive on weekends or at the end of the day, making it hard to take action promptly.

Incident response processes were often slow and disconnected. The team worked with solutions that didn't integrate, forcing them to spend valuable time manually switching between systems transferring data, and updating security devices with IoCs for automated detection and blocking.

"The pain point was repetitive tasks," explains the bank's CISO. *"Our slow processes made it hard to respond to new threats. It sometimes took us 2-3 days to respond, which put us at too much risk."*

The Solution

The team explored several solutions but was concerned about working through third parties for implementation and ongoing support. In Cyware, they found a partner they could have a two-way relationship with and would work with them to develop new features, playbooks, and use cases.

Cyware's vCFC platform enables the security team to integrate its technology stack and orchestrate response processes across security tools and functions. This allows the team to reduce its time to respond to and contain threats significantly. In many cases, the team has automated large portions of each process, removing unnecessary human involvement and further improving response time.

Since implementing vCFC, the security team has seen huge improvements, including:

- Faster Median Time to Respond (MTTR)
- Reduced manual effort on mundane tasks
- Reduced cyber risk
- Reduced risk of human error

"It's been a dramatic change to our performance and operations," explains the CISO. *"Even during the pandemic with more attacks, we needed fewer people to respond to incidents. We're responding to new incidents and intelligence much faster, and more of the team can focus on proactive tasks."*

Next Steps

After experiencing significant improvements from implementing a vCFC, the bank plans to expand the solution to cover its subsidiaries.

"The improvements we've seen in response times and reducing manual work have been huge, and we're ready to roll out the platform across our entire portfolio," explains the CISO. "We've already partially deployed Cyware at our subsidiary banks, and we'll now continue to a full implementation."

Checklist for Choosing a CFC Platform

Module Requirements

- SOAR (in line with the full Gartner definition)
- TI sharing and exchange
- Cross-environment orchestration and automation
- Situational awareness

Platform Capabilities

- Full integration across CFC functions and all other security tools
- Normalization and standardization across all security data sets
- Full threat response capabilities, including case management, data management, and audit
- Powerful threat intelligence collection, correlation, and analysis capabilities
- On-demand and event-driven process orchestration and automation
- Real-time threat information sharing, role-based alerts, and inter-function communication
- Threat mapping to common security frameworks (e.g. MITRE ATT&CK)
- Automated threat context and removal of false-positive threat alerts
- Threat visualization and automated enrichment of threat data
- Recommended analyst actions to improve standard outcomes and reduce analyst fatigue
- External threat intelligence sharing with customers, partners, ISACs, etc
- Automated operationalization of threat intelligence to TIPs
- Ability to customize and assign threat severity scoring

Questions to Ask

- Does the platform provide the full SOAR value proposition, or is it just one or two functions?
- Can it support orchestration across any security process or tool?
- Does it include a dedicated, fully integrated, security-focused case management system?
- Does it support H2H, H2M, and M2M intelligence-sharing inside the enterprise and externally within intelligence-sharing communities?
- Will it enable security teams to normalize and standardize security data and intelligence?
- Can it support seamless, vendor-agnostic integration across the entire technology stack?
- How does the platform compare to dedicated TIP, IRP, SOAR, and case management tools?

Boost Threat Response with Cyware

Cyware is the first company to offer a holistic, integrated solution to the problems faced by today's enterprise security teams. Our modular vCFC platform combines the entire SOAR value proposition with the industry's leading threat intelligence exchange and situational awareness capabilities.

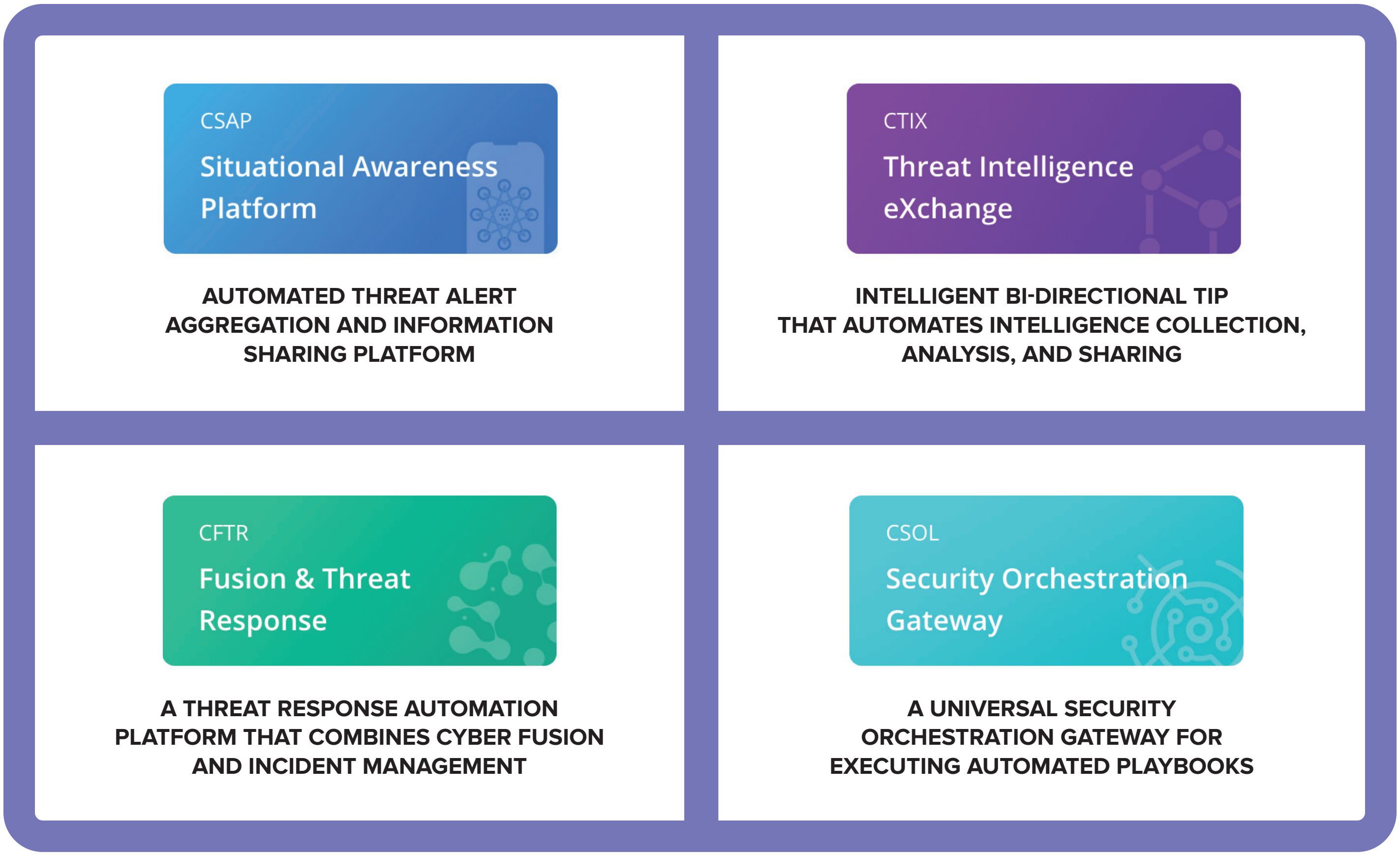
Combined, these four modules allow disparate security teams to collaborate, share common datasets, and proactively mitigate cyber threats. At the same time, teams can exchange intelligence with peers, customers, and more through public and private intelligence-sharing communities, allowing defenders to tip the scales back in their favor.

Cyware was built by practitioners, for practitioners.

As a security leader, CEO Anuj Goel built some of the industry's first physical cyber fusion centers. Seeing the challenge posed by dispersed security teams, he founded Cyware to enable the same level of collaboration and information sharing—regardless of location.

To see how Cyware can help your enterprise security team boost collaboration and improve threat response, arrange a DEMO today.

Cyware: the Modular vCFC Platform



CSAP

Situational Awareness Platform

AUTOMATED THREAT ALERT AGGREGATION AND INFORMATION SHARING PLATFORM

CTIX

Threat Intelligence eXchange

INTELLIGENT BI-DIRECTIONAL TIP THAT AUTOMATES INTELLIGENCE COLLECTION, ANALYSIS, AND SHARING

CFTR

Fusion & Threat Response

A THREAT RESPONSE AUTOMATION PLATFORM THAT COMBINES CYBER FUSION AND INCIDENT MANAGEMENT

CSOL

Security Orchestration Gateway

A UNIVERSAL SECURITY ORCHESTRATION GATEWAY FOR EXECUTING AUTOMATED PLAYBOOKS

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only ***virtual*** cyber fusion center platform with next-generation SOAR (security orchestration, automation, and response) technology. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies of all sizes and needs.

CYWARE™

228 Park Avenue S #77147
New York, NY 10003-1502
855-MY-CYWARE • sales@cyware.com

www.cyware.com