CYWARE™

CASE STUDY

Major Professional Sports Leagues Win the Collective Defense Game with Cyware

OVERVIEW

Several major professional sports leagues faced challenges in effectively collaborating and sharing threat intelligence with their franchisees. The associations governing the leagues sought a solution for building Hub and Spoke-based **Information Sharing and Analysis Organizations (ISAO)** that would enable them to collectively defend their communities through fully automated bidirectional threat intelligence sharing and collaboration with their respective franchisees.

CHALLENGES

1 Inadequate Collaboration

Failure to effectively collaborate, share insights, and address common security challenges with franchisees in a unified manner.

2 Lack of Bidirectional Sharing

Absence of bidirectional threat intelligence flow impeded full threat visibility and a collective defense approach.

3 Reactive Approach to Threats

The franchise teams lacked early warning threat alerts, advisories, and crisis notifications resulting in the lack of proactive actioning.

4 Scalability Issues

Inhibited growth and scale in threat intelligence operations due to lack of integration of diverse security tools and process automation at the Hubs.

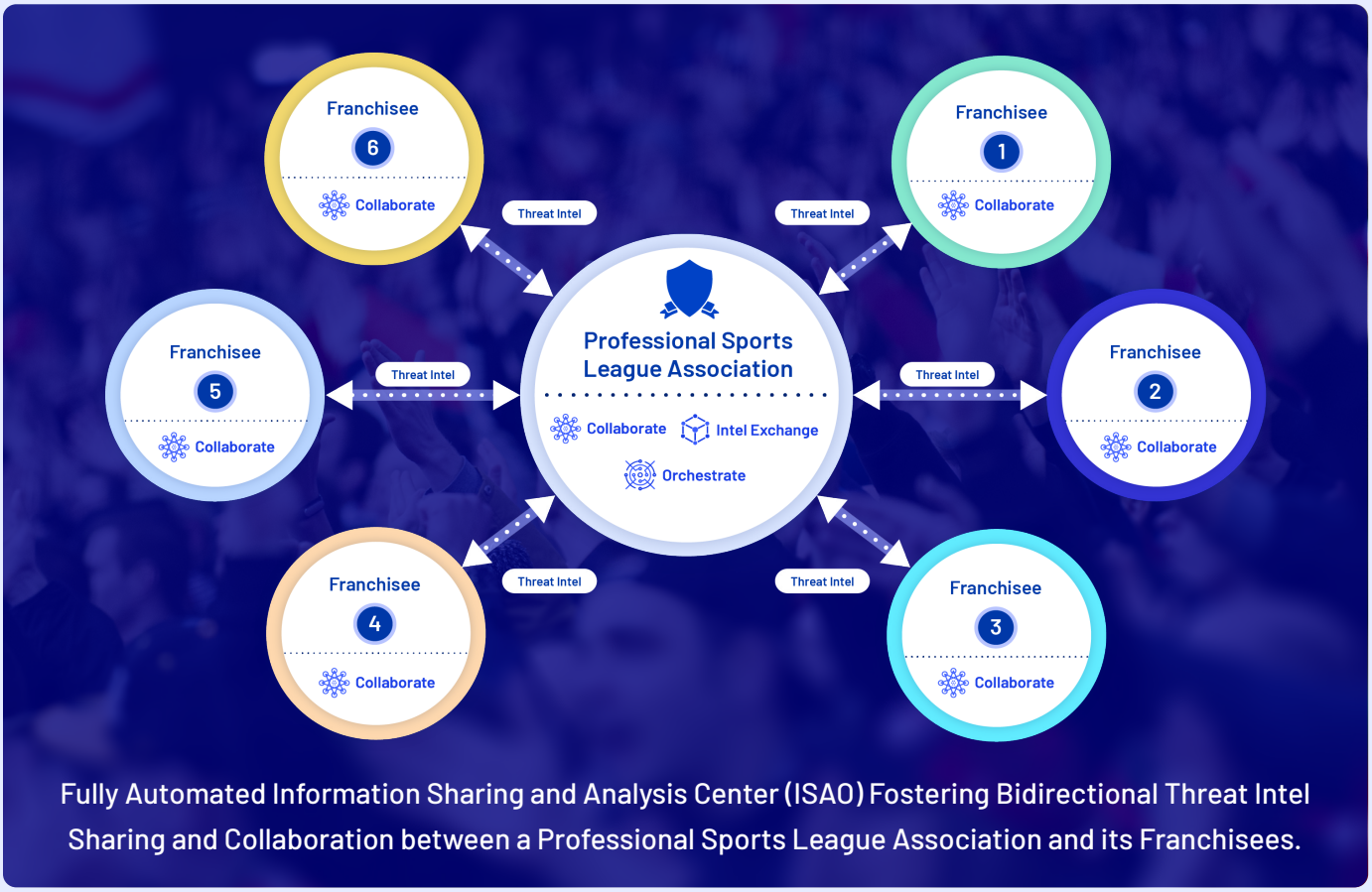
SOLUTION: BUILDING THREAT INTELLIGENCE SHARING COMMUNITIES FOR COLLECTIVE DEFENSE

Cyware deployed its suite of automated threat intelligence sharing and collaboration solutions, a preferred choice of all major global information sharing communities (ISACs and ISAOs) for fostering collective defense. The suite of solutions enables **"Hub and Spoke"** based automated bidirectional threat intelligence sharing and collaboration between the sports associations (Hubs) and their respective franchise teams (Spokes). As part of the deployment, Collaborate, Intel Exchange, and Orchestrate were implemented.

Collaborate is a platform designed specifically for swift and effective security collaboration, offering bidirectional alert and advisory sharing capabilities. The sports associations (Hubs) operate their respective ISAOs through an Analyst Portal, disseminating crucial advisories, alerts, crisis notifications, and threat intelligence to franchise members via a Member Portal. This Member portal also empowers franchisees to engage in secured discussions, request additional information on threats, and share back threat intelligence with the ISAO Hubs.

Intel Exchange is an automated Threat Intelligence Platform (TIP) designed for ingestion, enrichment, analysis, prioritization, actioning, and bidirectional sharing of threat data. Deployed at the ISAO Hubs, this platform enables the associations to gather, enrich, and analyze threat intelligence from their own monitoring and detection tools, external threat intelligence subscriptions, enrichment databases, and intelligence shared by members.

Orchestrate is a vendor-neutral, low-code orchestration and automation platform. It connects the Collaborate and Intel Exchange platforms with all internal and external threat intelligence sources at the ISAO Hubs, enabling threat intelligence orchestration, analysis, and real-time delivery to franchise members.



Fully Automated Information Sharing and Analysis Center (ISAO) Fostering Bidirectional Threat Intel Sharing and Collaboration between a Professional Sports League Association and its Franchisees.

USE CASES SOLVED

By implementing Cyware's solutions, the sports associations witnessed significant enhancements in their cyber operations, bolstering their security posture and mitigating potential threats effectively. The key uses cases included:

1. **Bidirectional Threat Intelligence Sharing**
   Bidirectional, streamlined threat intelligence sharing between the associations and franchise members using the Hub and Spoke model.

2. **Early Warning Threat Advisories**
   Automated distribution of cyber threat advisories, reports, alerts, and internal threat intelligence notifications from the associations (Hubs) to franchisees (Spokes).

3. **Threat Intelligence Aggregation and Analysis**
   Automated enrichment, analysis, and IOC scoring of threat intelligence aggregated from franchisees and external feed providers.

4. **Real-Time Crisis Notifications**
   Real-time delivery of crisis notifications to franchise members through multiple delivery channels.

5. **Threat Hunting and Investigations**
   Automated collection, correlation, and analysis of indicators of compromise (IOCs) from various sources to proactively hunt the threats targeting the communities.

6. **Automated IOC Blocking**
   Automated blocking of high-confidence IOCs in Endpoint Detection and Response (EDR) tools at the ISAO Hubs.

7. **Automated Alert Triaging**
   Automated retrieval and triaging of false positive alerts generated by the detection and monitoring tools at the ISAO Hubs.

BENEFITS AND OUTCOMES

The sports associations and their franchise members have experienced several significant benefits, including improved incident response, threat detection, and overall resilience against cybersecurity threats. The key benefits realized include:

Collective Defense

The implementation of the Hub and Spoke sharing model creates a highly-collaborative ecosystem for the associations and all franchise members, resulting in a collective defense against common threats.

Enhanced Situational Awareness

Real-time threat advisories, alerts, and crisis notifications delivery to franchisees ensures continuous and updated situational awareness for their respective communities.

Preemptive Threat Management

The integration and analysis of multi-source threat intelligence facilitates proactive threat hunting and investigation, allowing the sports associations to detect and respond to emerging threats promptly.

Proactive Threat Actioning

Automation of threat intelligence analysis, triaging, and sharing processes at the Hubs ensures high-confidence threat intelligence is consumed, processed, and proactively actioned by franchise teams.

Increased Efficiencies

Automation of processes at the Hub and Spoke level ensures improved collaboration and flow of relevant and contextual threat data in the communities, thereby enhancing SecOps efficiency for the communities.

For more information you can reach us at :

Cyware

111 Town Square Place Suite 1203 #4,
Jersey City, NJ 07310
sales@cyware.com | www.cyware.com

CYWARE™