SUCCESS STORY

flare

National Sports Organization Earns a Gold Medal with Insights into Targeted Threats

The Customer

Athletic committee with a mission to support National Sport Organizations (NSOs) at every stage of an athlete's journey

Organization with more than 3,500 members across three levels of governance

Getting Security in Shape Before an International Event

As preparation for a large international sporting event, the national sports organization realized that it needed additional insight into its external attack surface since threat actors increasingly target teams and events. In 2020, the UK's National Cyber Security Centre (NCSC) found that 70% of sporting organizations experienced at least one cyber attack every year. Often, attacks target connected stadiums as a way to gain attendee data.

For large international events like the ones our customer supports, threat actors become more sophisticated and varied. As many teams use data analytics to optimize their strategies, attackers increasingly target this either to provide the competition with insights or for financial gain. Additionally, international competitions are prime targets for nation-state actors with geopolitical agendas.

> "Flare's rapid deployment processes got our team up and running in only a few hours so that we could gain near-immediate insights in the face of imminent threats."
>
> **- IT Director, National Sports Organization**

For example, a 2016 attack by the ransomware group Fancy Bear targeted WADA, an international independent agency that works to remove substance abuse from sports. The attackers gained unauthorized access to data from an account created specifically for the Rio 2016 Olympic Games to obtain confidential data about athletes whose medications fall under the Therapeutic Use Exemptions (TUE).

As part of maturing its athlete and governance member data protection strategy, the national sports organization sought to correlate threat intelligence to derive insights that would further improve its proactive monitoring capabilities.

Challenges: Lacking Context for and Insight into Targeted Threats

As athletes prepared for the 2024 Summer Olympic Games, the national sports organization received briefings from security partners who stated that targeted threats were imminent. At the time, the organization gained information from:

- Insurance companies providing threat intelligence
- Quarterly attack surface reviews that only provided technical insights about networks and assets

While the athletic organization used this data to mitigate risk, the siloed information created challenges when trying to build targeted insights and detections.

At the time, the organization relied on manual processes for mitigating access-based attacks by enforcing strict password requirements, like regularly changing passwords and requiring multi-factor authentication (MFA). Our customer sought to aggregate all threat intelligence and gain additional context around threats targeting the upcoming event, specifically seeking insight into leaked credentials.

With the urgency around the large international sporting event, the organization began researching solutions that would enable them to create a cohesive, centralized location for monitoring activities outside of its traditional perimeter. After seeing a presentation from one of Flare's competitors, the security team saw that this solution could support them to drive improved security outcomes.

While our now-customer reviewed other tools, their modular pricing models placed them outside of the security team's budget. Flare's pricing model included everything the team needed.

Implementation: Immediate Visibility for Enhanced Threat Protection

Within just a few hours of setup, the sports organization's IT team began seeing immediate value, gaining more targeted risk insights from the depth of available context provided by Flare. The Flare team provided suggestions for setting up domains, containers, and identifiers. Based on these recommendations, the IT team was immediately self-sufficient and able to implement additional risk mitigations and fortify their defenses further. After implementing these initial risk mitigation improvements, the IT team identified additional use cases for other stakeholders.

With holistic and centralized visibility into the external attack surface, our customer knew that Flare's insights would enable it to respond to emerging threats that targeted the sporting event. For example, during the initial trial period, the IT team identified some leaked credentials. Since the organization had no prior centralized threat intelligence monitoring capabilities, implementing Flare added important context that enhanced the team's confidence in its security posture.

With Flare, the national sports organization could more rapidly mitigate threats related to brute force, credential stuffing, and password spray attacks. Today, our customer has expanded its use cases to include data leak monitoring, identifying leaked documents or assets. The IT team can now efficiently and effectively monitor for threats related to ongoing activity in the wild.

> “During the demo and proof of concept, the Flare team gave our team suggestions on best practices for setting up domains, containers, and identifiers. Once we were up and running, we were self-sufficient and able to act on things right away. Once we remediated the first layer of threats, we dug into deeper levels of what was useful for other stakeholders. The demo & POC were helpful in being able to access features and see where the platform fit into daily security updates.”
>
> - IT Director, National Sports Organization

Benefits: Improved Security Insights and Monitoring within a Week

With the IT team up and running within a week, the sports organization achieved near instant benefits. With a pretty straightforward domain lacking many identifiers or silos, the organization’s one hour onboarding session with Flare’s team enabled meaningful results within minutes. By reducing noise, the IT team was able to focus solely on relevant, time-sensitive threats.

Our customer experienced waves of activity in the three to four months before and one to two months after the international sporting event. Since then, it has evolved its Flare use to manage daily monitoring. For example, the organizations found that threat actors commonly try to spoof their domain, setting up lookalike domains to engage in fraudulent ticket sales. Using Flare enables the IT team to mitigate this reputation risk with public and internal communications.