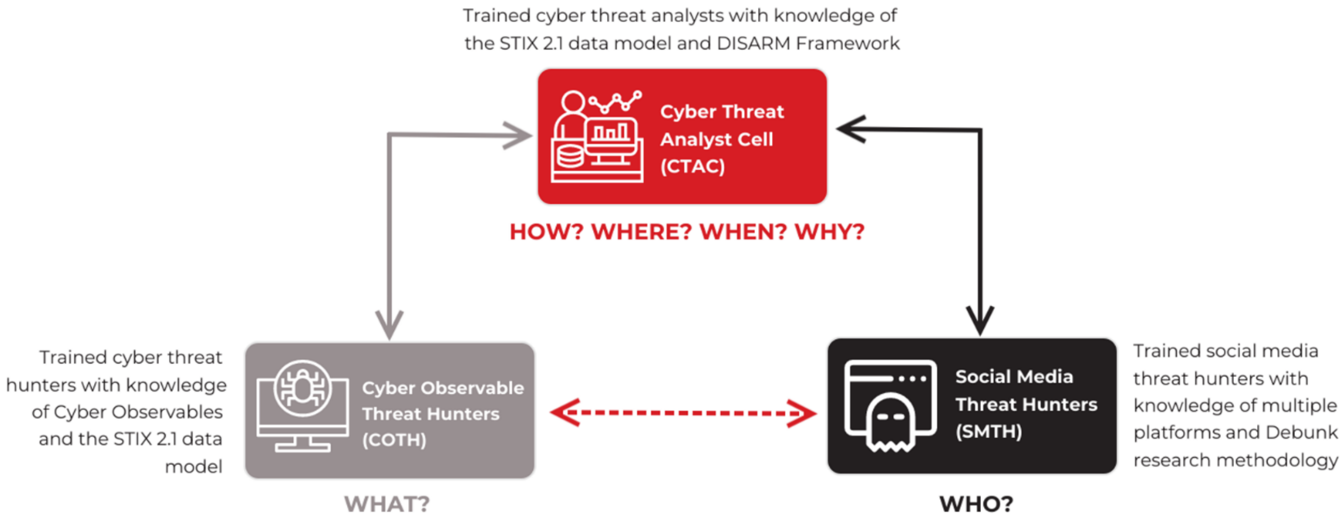
Introduction to Cyber Threat Hunting: One Methodology

By: Jane Ginn, MSIA, MRP

Prior to any cyber threat hunting operation, a team should conduct a systematic Priority Intelligence Requirements (PIR) analysis. The formal PIR planning process was formulated by the U.S. Army.[1] Our methodology is an adaption reconfigured for application to the cyber threat landscape. Importantly, we identify the key stakeholders including, but not limited to, teams, coaches, athletes, sponsors, broadcasters, transportation and hospitality providers and host country assets. We then systematically characterize the potential threat surface of each of these groups. A small snippet of our analysis of high-level likely attack surfaces are shown on Figure 8.

We then prioritize potential threats within the context of major geopolitical and news cycle concerns that may drive social media narratives and memes and/or threat actor lure design tailored to sports themes.

Once the event begins alerts and tips enter our SOC from either a social media or a technical telemetry source.


Trained cyber threat analysts with knowledge of the STIX 2.1 data model and DISARM Framework
Cyber Threat Analyst Cell (CTAC)
HOW? WHERE? WHEN? WHY?
Trained cyber threat hunters with knowledge of Cyber Observables and the STIX 2.1 data model
Cyber Observable Threat Hunters (COTH)
WHAT?
Social Media Threat Hunters (SMTH)
Trained social media threat hunters with knowledge of multiple platforms and Debunk research methodology
WHO?

The COTH and SMTH hunters share the information through our various secure communications channels and proceed using multiple platforms and open-source intelligence (OSINT) sources. The hunts proceed in parallel.

Analysts use a wide range of tools to characterize what we are observing and who might be behind the attack. To the extent possible we model our observations using version 2.1 of the Structured Threat Information Expression (STIX) modeling and sharing language.

As the evidence is collected, we test the validity of our assumptions against a formal process called the Analysis of Competing Hypotheses (ACH). This method was originally developed by an analyst at the U.S. Central Intelligence Agency (CIA). It is a methodology for evaluating multiple competing hypotheses for observed data. It was developed by Richards Heuer, Jr. in the 1970s.[2] We have adapted the method for our own use within the threat landscape and context of global sporting events. It is an eight-step process that helps the analyst systematically consider the underlying assumptions of an intelligence collection regime while continually testing the evidence presented by the digital artifacts that are discovered during the hunt.

As we work through the ACH process, we seek to answer questions like how, where, when and why about the threat actor(s), shaping our DSC methodology as shown by the above figure.

[1] https://smallwarsjournal.com/jrnl/art/importance-priority-intelligence-requirements-army-service-component-command-ascc-and

[2] Heuer, Richards J., Jr, "Chapter 8: Analysis of Competing Hypotheses", Psychology of Intelligence Analysis, Center for the Study of Intelligence, Central Intelligence Agency, archived from the original on June 13, 2007