CYBORG SECURITY

THE 5 TRAITS OF EFFECTIVE THREAT INTELLIGENCE

Establishing Actionable Intelligence for Cyber Risk Reduction

www.cyborgsecurity.com

Threat intelligence, often referred to as cyber threat intelligence (CTI) or more simply, intelligence, can be a controversial subject. This is, at least in part, caused by the wide variety of formats threat intelligence can take in the marketplace. Generally, security vendors trend towards quantity over quality, while specialized intelligence vendors favor contextualized intelligence. Despite the decision and implementation being highly technical, organizations often review offerings based on quantitative measures since non-technical employees often lead the purchasing process. Which leaves many organizations struggling to understand what is needed, how it can be evaluated, and what makes it effective.

According to the SANS 2020 Threat Hunting Survey , the challenge in making CTI effective in threat hunting depends on two factors. First, organizations need accurate, well-curated intelligence and an understanding of how it should be deployed in the environment. Second, organizations must place greater focus on finding quality, rather than quantity. While the formats of threat intelligence do vary, effective threat intelligence solutions take several attributes into consideration, including contextualization, evaluation, prioritization, customization, and decomposition.

1. CONTEXTUALIZATION

While context and "meta data" is often cited as bullet-point features of many solutions, it is inconsistently defined and difficult to evaluate. In the milieu of threat intelligence, the process of contextualization is providing the circumstances surrounding specific data and information, ultimately answering the six key questions: "who, what, when, where, why and, how?"

For instance, while threat feeds often provide millions, or even hundreds of millions of data points, the circumstances around indicators are often obscured or lost altogether, as is the nature of the threat. This lack of contextualization results in analysts having to pause sensitive investigations, wasting valuable time and exposing organizations to additional risk in order to "fill in the blanks."

Therefore, one of the most critical traits for the assessment of threat intelligence is the context it provides, which in turn allows for the effective evaluation of the data and information for organizations.

2. EVALUATION

Another trait common to successful threat intelligence solutions is a detailed evaluation of both the source and information itself. Data and information can originate from sources with varying levels of reliability and can provide information with differing levels of credibility. It is the adoption of such an evaluation system that can capture these related, but ultimately different facets.

An example of such data and information evaluation can be seen in what is often variously referred to as the Admiralty Code, the Admiralty System, or simply the NATO System. The Admiralty Code allows for the systematic and repeatable categorization of significant amounts of data. Through reliability and credibility ratings it allows analysts to evaluate the underlying data and information.

The result of this evaluation is that organizations are able to choose the types of data and information that they operationalize in their environments, evaluate that same data, and ultimately, assign it a meaningful prioritization.

3. PRIORITIZATION

A feature that has been found across many products and offerings in the security space is the adoption of some form of scoring system for threat detection and response. The concept behind such systems are well-founded: security analysts are continuously inundated with disparate alerts from various security controls, and such scoring systems can allow for the initial triage and investigation.

However, often, these scoring systems can be inflated or inconsistent, the result of which is a situation where every alert is critical. Such haphazard prioritization leads to the outcome described by the author Patrick Lencioni where "... if everything is important, then nothing is."

Therefore, prioritization must allow organizations to take into account the aforementioned contextualization and evaluation of the threat and allow for meaningful division of alerting in order to effectively manage analysts' time and effort, and to address the threats to the organization in a meaningful, risk-based, manner. Such prioritization, when combined with the contextualization and evaluation, allow for solutions to provide customization of that intelligence which is adaptable to various organizations' requirements and realities.

4. CUSTOMIZATION

Every organization is different, as such threat intelligence needs to incorporate the ability for customization in how organizations are able to consume it. Effective threat intelligence must be able to adapt to those requirements, rather than forcing organizations to adapt to it. This customization often comes in the form of APIs which allows organizations to "consume" the Intelligence as they see fit.

While such customization is important, often these APIs do not allow organizations to customize, or selectively retrieve data, information, and intelligence as it applies to established swim lanes, workflows, or standard operating procedures. For instance, the information a security analyst requires will differ significantly from the information that an intelligence analyst requires. Without that customization, a great deal of time and effort are wasted as teams are forced manually distill that data.

> ***On the whole, effective threat intelligence is actionable, and consistently shares the traits of contextualization, evaluation, prioritization, customization and decomposition.***

Such customization through robust APIs is a critical trait for successful threat intelligence solutions. It allows for focused, relevant, information retrieval as well as the application of decomposition modeling for intelligence.

5. DECOMPOSITION

Another consideration that threat intelligence teams and solutions often struggle with, is what has been colloquially referred to as "digital hoarding." While this concept can be important to the intelligence process, its usefulness diminishes significantly when applied to threat detection and analysis. One of the core characteristics of operationalized threat intelligence, is its timeliness. Many indicators decrease in value--from a traditional security analysis standpoint--as they age and as actors transition to new infrastructure and tactics, techniques, and procedures (TTPs). This often results in organizations trying to cope with significant false positive alerts, all of which must be investigated thoroughly.

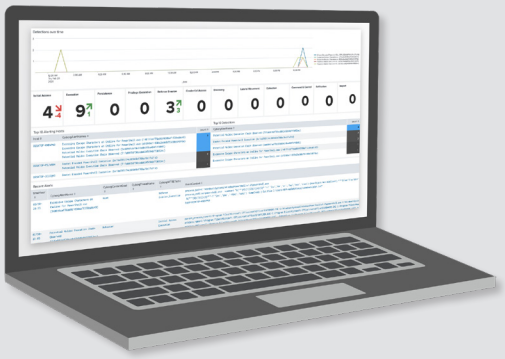
As such, one of the crucial traits of effective threat intelligence is the implementation of decompositional modeling (decay modeling). This type of modeling, which slowly reduces the value of an indicator based on age and observed activity, enables organizations to retain vast quantities of data, information, and intelligence for further analysis, while selectively reducing operationalized reporting and indicators which are less relevant for conventional security analysis. This results in analysts focusing on current and relevant threats while simultaneously enabling detailed querying and analysis when required.

EMPOWERING SECURITY ANALYSTS THROUGH THREAT INTELLIGENCE

Threat intelligence can often be "messy" and confusing for organizations with both nascent and well-established security practices alike. Despite this challenge, the evaluation and implementation of intelligence solutions does not need to be complicated. On the whole, effective threat intelligence is actionable, and consistently shares the traits of contextualization, evaluation, prioritization, customization and decomposition. Solutions that offer these traits will empower security analysts, streamline the triage and investigative processes, and ultimately, will reduce the overall risk to organizations, their members and customers alike through more rapid detection and response.

THE DIFFERENCE IS IN CONTEXTUALIZATION OF INTELLIGENCE

Cyborg Security's Contextualized Operations Readiness Engine (C.O.R.E.) threat hunting platform was created with the understanding of these five traits, with an emphasis on contextualization.



Offered via a subscription-based model, C.O.R.E provides SOC analysts with the added contextual information about threats that they simply can't get from automated threat feeds or open source detections. This includes missing threat details about current attacks, TTPs, and mapping against common frameworks like MITRE ATT&CK and Cyber Kill Chain. The groundwork is laid by world-class researchers and threat-hunters and provided in easy-to-ingest formats.

Cyborg C.O.R.E. was developed with the realities of the modern SOC in mind. This is a platform built to boost the human factor, not replace it.

To learn more, about Cyborg and the C.O.R.E. platform, please contact us.

CYBORG SECURITY

ABOUT CYBORG SECURITY

The best threat hunting minds. The best threat hunting ammo. The only real threat hunting platform.

Cyborg Security is a pioneer in cybernetic threat hunting, delivering advanced, actionable threat hunting content via a first-of-its kind single platform. Cyborg's unique platform leverages the best and largest pool of threat hunting human assets and resources, applies techniques and proprietary patent pending technology, and delivers continuously updated content, context, scripts, and playbooks to be leveraged by internal teams. Cyborg provides the platform to proactively threat hunt, without outsourcing or the need to hire direct, scarce skill sets.

CONTACT US

801 International Parkway, Suite 500
Lake Mary, FL 32746

info@cyborgsecurity.com
www.cyborgsecurity.com