White Paper

Managed Intelligence™

An Overview on Signature and Personality-Based Attributions to Mitigate Risk for the Business

Continuing with Nisos' series on providing context to enable actionable outcomes for Security Operations Centers (SOCs), we examine the differences between signature and personality-based attributions and how each plays a role for enterprises in prioritization efforts to define and defend threats. By focusing on the technical signatures and open source intelligence (OSINT) footprint of a group of actors, signature-based attribution efforts allow enterprises to contextualize their findings and better address the coverage gaps in security controls. Threat intelligence or actual incident events are often used by SOCs to test hypotheses or identify previous actions of an adversary. These signatures also form the basis for metrics that enable security resources to increase their own programs that illustrate how they reduced risk exposure to the business.

Signature Attribution

Targeting a user or group of users, based on signatures related to activity and/or artifact collection, connecting the individual(s) to a group or profile of interest.

Personality Attribution

Targeting a specific, defined user. This is not always defined by an individual; attributions can be performed on a specific piece of information, like an email or social media account handle.

Background

In government, signature and personality targeting is often performed to gather information, analyze the information in order to derive intelligence, and use that intelligence to inform action and/or strategic planning. While these intelligence paradigms are not identically replicable within the private sector, similar methodologies in signature and personality-based attribution can be used as mitigations for the risk to business.

Security professionals often must adjust their actions against a threat through the lense of the business. More times than not, this manifests in some administrative action rather than a law enforcement action (increasing security controls, termination, civil litigation, etc). To that end, security professionals focus more on signature-based attribution allowing them to discover more threats based on these signatures.

We create detailed profiles on attacks and attackers by gathering, correlating, and analyzing different types of information, all focused on building context. These data points paint a picture of the attacker's tactics, techniques, and procedures (TTPs).

We take these raw data points (traditional cyber threat information) and blend them with contextual open-source intelligence to further enrich the profile of the attack and create actionable intelligence. Our deep knowledge and experience in human and technical analysis domains allow for greater resolution into the means and motives of an attack.

When available technical data is enriched with cyber threat feeds and open-source intelligence, the TTPs of an event create definitions for context gathering. In most cases, these definitions can be categorized into one of two "modes of attribution" - signature-based attribution or personality-based attribution. These two modes will often shape the approach an investigator takes with a case.

Signature-Based Attribution

Signatured-based attributions focus on a user or group of users, based on signatures related to activity and/or artifact collection, connecting the individual(s) to a group or profile of interest. This is the most common mode of attribution a CISO or CSO will pursue primarily because the malicious activity creates a profile that, once enriched, identifies signatures of the attack.

When looking at signature-based attribution, we are looking for the TTPs of the threat actors. This can help a client better understand how to manage the attacks; whether it is a coordinated disinformation campaign; financially-motivated hacking; or intelligence collection against the brand, personnel, or crown jewels of the company. The TTPs of a group are tied to the platforms they use for their reconnaissance, collection and dissemination (social media, third-party paste websites, virtual private servers, file shares, etc). A malicious actor (or group) will have expertise in tools, attack methods, command and control configurations, media platforms, messaging methods, etc. All of this expertise is leveraged against a company's key terrain within cyberspace in order to achieve the desired effect of the actor(s).

To bring better context to a threat, the ability to signature an action usually allows for clear prioritization efforts because the modes, methods, and means they are undertaking generally give indications of levels of sophistication. Simply put, the greater the sophistication, the greater level the threat, and the higher the prioritization. When an incident occurs carrying indicators or evidence of a compromise from a previously known adversary, knowledge of these signatures allows security teams to quickly prioritize new coverage gaps and apply mitigations.

Personality-Based Attribution

Personality-based attributions focus on targeting a specific, defined user. This is not always defined by a name; attributions can be performed on a specific piece of information, like an email or social media account handle.

When we conduct personality-based attribution, it's often in response to a specific incident. Legal departments or outside counsel are generally involved with the intent of the investigation to enable an action against the threat actor or group. This type of attribution is often performed with leads of a name, company, or social media account, rather than an action or remediation event. The personality-based attribution looks for a single source of truth, typically, who or where is the person or group.

Personality-based attributions can be the starting point of an investigation. For example, a social media account is spreading disinformation about a company to cause harm to the brand. In this instance, a personality-based attribution will kick off with the objective of providing the single source of truth: who is the user of the social media account. Signature-based attributions can transition into personality-based attribution if a client deems the true identities of the threat actor or group behind a signature are of value to uncover.

Conclusions

Pursuing personality-based attributions requires security maturity, risk tolerance and resources - often the mitigation solution lies effectively in the tuning and implementation of security controls. When reviewing intelligence to evaluate technology control-based mitigations, signature-based attributions often provide sufficient concrete context and allow for the institution of relevant metrics to define and combat the threat.

This article is the second in a series providing context to threat information that should lead to actionable outcomes in support of the business.

For additional information, visit www.nisos.com or contact info@nisos.com.