Mandiant

THE ROLE OF THREAT INTELLIGENCE IN INCIDENT RESPONSE

This article explores **the role of intelligence** in providing tactical and operational assistance to incident response efforts. Through the collection, analysis, and sharing of internal and external threat intelligence, incident responders can reduce threat actor dwell time and the potential impact on the organization.

Read Time: 5-7 Min

Intelligence and related TTPs illustrate how adversaries conduct their operations, providing insight into how the incident at hand may unfold. More tactical intelligence may also help the responder to develop pivot points within their analysis and indicate where they should be focusing next to ensure thorough eradication of the adversary's presence.

How and when intelligence and threat data traverse cyber defense technology can also play a critical role during response. The ability to extract and correlate threat intelligence within technical solutions can improve the efficacy of response. By interconnecting intelligence and response systems, incident-specific artifacts and evidence can be cross-referenced and exchanged with intelligence, providing important context and clarity to the investigation.

From a process perspective, incident response procedures and playbooks should reference the threat intelligence role during specific phases or activities. During containment and mitigation efforts, intelligence can be used to determine incident scope, along with the capability and intent of the threat actor.

Intelligently prepare for, investigate, and respond to incidents

The Respond function of the Cyber Defense domain is responsible for the response and remediation of suspicious activity in an enterprise environment.

There are several benefits that threat intelligence can offer to improve the efficiency and effectiveness of an organization's ability to prepare for and respond to breaches.

Objectives and Key Actions

Within this use case, the intelligence analyst or provider will often function as part of a matrix team investigating an incident. In addition to the above process and technology considerations, intelligence skills and expertise are likely to be called upon both before and after an incident. This can be key to ensuring your organization is ready to respond to the current incident, as well as the next one. Additionally, the intelligence function will often be engaged during the recovery phase, providing recommendations of corrective actions to prevent similar attacks in the future.

When your organization is ready to integrate threat intelligence within a Respond function, consider the following activities as a starting point.

Intelligence Integration with Playbooks

Integration points should be defined in incident response playbooks, and intelligence requirements of the incident response team should be well-established and communicated across the broader cyber defense function. Teams must be clear about the types of intelligence expected by incident responders; this typically includes precursors and indicators, attack vectors, some level of attribution, and recommended actions. In addition, responders should be conversant with

the assistance that the intelligence function is able to provide. Most importantly, intelligence integration process points, inputs, and outputs should be tested and practiced. Tabletop exercises for response playbooks are a common approach to test these intelligence integrations points.

Initial Triage

When a potential threat is detected, the intelligence function can assist in confirming the accuracy of the information provided by the alert, help in determining if it represents an actual threat, and help in deciding whether it is actionable. This normally includes data gathering and research using various internal and external sources and can result in any number of outputs. By assisting at this stage, intelligence can help in the process of graduating an alert to an incident (or not) and beyond that, help in determining the associate risk and priority of the incident against others in the investigation queue.

Investigative Support

Progressing past the initial stages, intelligence provided to deeper investigations can include a broad range of inputs: threat actor attribution (if possible), known TTPs, related indicators of compromise, recommended courses of action, and incident scoping guidance based on known adversary behavior and intent. The intelligence function should seek to provide all relevant information from its holdings in a form that is consumable by the incident response team and their associated tooling. Intelligence should first enrich and validate all the current information. Secondly, it should provide responders with a comprehensive view of the TTPs that may be in play across the entire kill chain of the attack. The MITRE ATT&CK Framework is a helpful standard to communicate this in a structured and repeatable way across different actors and incident types.

In the early stages of an investigation, it is often not possible to provide full attribution (for example, attribution to a specific actor or group). As such, the intelligence function will need to remain in close contact with the investigation so that the relevant TTPs may be refined as new information in discovered. One important element outside of TTPs that responders will require are assessments of the motives of the threat actor. This can be used to understand the potential objective of the attack, locate where else the attacker may be in the environment, and thus help to understand the impact and extent of the attack. This level of intelligence provides value as the effort moves into containment and eradication of the threat from the environment.

Throughout the incident, it is often expected that the intelligence function continually supports the investigation by providing pivots of data discovered by the responders. It is not uncommon for investigations to reach dead-ends.

Intelligence can help in the following ways:

- Providing additional information that enables the team to either move past the dead-end
- Verifying the end of the investigation has been reached
- Confirming there is not enough information to move forward at that time

Post-Incident Intelligence Reporting

Beyond the investigation itself, the intelligence function is often called upon to contribute to the production of the post incident reporting. This includes an attempt to validate threat sources, vectors of attack and vulnerabilities exploited, actor attribution (if possible), and gap analysis of the organization's ability to prevent similar attacks or incidents. All this information prepares the organization to return to the beginning of this use case and prepare to detect and respond to future threats.

Collation and Sharing

It may be that intelligence and incident response teams are sharing high volumes of information throughout the

investigation. The intelligence function is often called upon to ensure that all of the information is thoroughly collated and normalized. The goal is to make it accessible to support additional research, intelligence production, and incident response efforts. Exchanging indicators of compromise from investigations with a broader holding of intelligence will help validate aspects of the compromise and generate new threat data that can be fed into the larger intelligence lifecycle. It is recommended that due to the volume of data, this activity takes place within a Threat Intelligence Platform (TIP) that is appropriate to the needs of the organization. Integration of incident response tools and data with a TIP can also make sharing more efficient. This activity may also require specialist skills in data management or other technical skills required to gain the most from the platform through integrations and automation.

The unique needs of the organization, along with the specific design of your own cyber defense function, will often lead to variations on these approaches. While we recommend sticking to the general principles of this use case, ultimately, we encourage organizations to adapt these practices in ways that are best suited for their success.