Deloitte.

Intelligence-led threat hunting

Introduction

The primary role of an Intelligence Team within a cybersecurity operation is multifaceted, encompassing the gathering, storage, analysis, and dissemination of actionable intelligence. This intelligence is crucial for enhancing the effectiveness of various security functions within an organization. By providing timely and relevant information, the Intelligence Team enables other security units to make informed decisions, respond to threats more efficiently, and mitigate potential risks.

For the HUNT Team, which is tasked with proactively searching for threats within an organization's network, the support of the Intelligence Team is indispensable. The Intelligence Team provides the HUNT Team with critical insights and data, enabling a more informed and targeted approach to threat hunting activities. This creates an intelligence-led threat hunting operation (Intel-led HUNT). This collaboration enables the HUNT Team to identify and neutralize threats before they can cause significant harm to the organization.

This report provides a strategic overview of how an Intelligence Team can best support a HUNT Team. It begins by highlighting the common challenges faced by both teams, such as the sheer volume of data, the complexity of modern threats, and the need for real-time analysis. Understanding these challenges is essential for developing effective strategies and solutions.

Next, the report defines how intelligence should be fed into HUNT activities. It outlines the types of intelligence that are most valuable for threat hunting, such as tactics, techniques, and procedures (TTPs) of threat actors; behavior-based and anomalous activity insights; and contextual information about potential threats. By integrating this intelligence into their workflows, the HUNT Team can prioritize their efforts, focus on the most significant threats, and improve their overall efficiency.

Furthermore, the report explains how Deloitte's Security Operations Center Operate Services (SOC Operate Services) integrate this process. Our services leverage advanced technologies and methodologies to provide an efficient integration between the intelligence and HUNT Teams. It facilitates intelligence gathered is not only accurate and relevant but also actionable and timely, enabling the HUNT Team to respond swiftly and effectively to emerging threats.

Challenges in supporting Intel-led HUNT operations

In theory, the collaboration between the Intelligence Team and the HUNT Team should be seamless, creating a synergistic relationship where intelligence-driven insights directly inform and enhance threat-hunting activities. This ideal scenario envisions a fluid exchange of information, where the Intelligence Team provides imely, relevant, and actionable data that allows the HUNT Team to proactively identify and mitigate potential threats. However, several common pitfalls can hinder this support, which disrupts the flow of information and reduces the overall effectiveness of both teams. These challenges may include issues such as communication breakdowns, data silos, differing priorities, and a lack of standardized processes. Additionally, the sheer volume and complexity of data can make it difficult to extract meaningful insights and act on them promptly. Addressing these pitfalls is crucial for fostering a productive collaboration that enhances the organization's cybersecurity posture.

Common pitfalls:

1 Outdated intelligence feeds

Relying on stale threat intelligence that no longer reflects the current threat landscape leads to ineffective hunting. The dynamic nature of threat actors means that tactics and tools change rapidly, requiring up-to-date intelligence to be relevant. Sometimes old data is all you have, but ensuring that the HUNT Team is aware of the age of intelligence can enable them to have better situational awareness going into their investigation.

2 Communications breakdowns and data silos

As an organization grows, so does the complexity of how teams communicate. It can become very easy for small groups to set up their own communication channels. This by itself is not bad; however, when the broader team is left out of small conversations, it can cause critical information to be missed. This leads to siloed information, and often the duplication of efforts. Ensuring that actionable information from these small groups is known on a broader level of the organization is essential for successful Intel-led HUNT operations.

3 Differing priorities

Depending on organizational structure, the HUNT Team and the Intelligence Team may have conflicting priorities. This may be due to client demands or maybe just poorly set up communication channels. If the Intelligence Team is focused on a different threat than what HUNT is gearing up to investigate, neither team is going to benefit the other. Ensuring both teams are on the same page can help make the process smoother and more effective.

4 Information overload

Information is key, but too much of a good thing can ruin its ability to be useful. Providing the HUNT Team with an excessive amount of intelligence data can be detrimental and dilute the effectiveness of intelligence. Filtering the noise to provide actionable insights is crucial for effective support.

5 Irrelevant or non-actionable data

Often, an intelligence feed contains information that is too general or lacks context. An example is when Indicators of Compromise (IOCs) are shared with HUNT without accompanying TTPs or behavioral context to explain *how* that IOC is relevant. This can result in wild goose chases or wasted efforts on threats not pertinent to the environment. Intelligence should be customized to fit the specific industry, brand, and technology stack of the organization receiving it.

6 Over-reliance on IOCs

While IOCs (e.g., IP addresses, file hashes) are helpful for detecting known threats, they are often ephemeral and easily modified by attackers. This results in intelligence that becomes quickly outdated or limited in scope. This does not mean that IOCs do not have a place in a modern defensive strategy. They should augment the defensive strategy but not be the main component.

7 Lack of feedback mechanisms

Without a feedback loop between the HUNT Team and the Intelligence Team, it becomes impossible to confirm whether the intelligence being shared is *actually* relevant and actionable. This lack of validation means that hunting strategies and intelligence support cannot be refined or adjusted in response to real-world observations and outcomes. As a result, both teams miss valuable opportunities to improve their effectiveness and stay ahead of emerging threats.

8 Fixation on threat actors

It is common to become fixated on a specific threat actor when conducting intelligence for HUNT activities. While focusing on one group can be useful, it often limits the scope of analysis. For instance, although threat actor X may use a VPN exploit for initial access before deploying ransomware, many other threat actors employ the same technique. By concentrating solely on threat actor X, the Intelligence Team risks overlooking critical information that could provide the HUNT Team with a more comprehensive understanding of how the VPN exploit is leveraged across multiple adversaries. Adopting a broader perspective enables the team to develop more effective detection and response strategies.

How intelligence should feed into HUNT operations

To effectively support the HUNT Team, the Intelligence Team should shift its focus from merely providing IOCs to delivering intelligence that is centered around TTPs. This strategic pivot is essential because TTPs offer a more comprehensive understanding of threat actor behavior, enabling the HUNT Team to anticipate and identify threats with greater accuracy and efficiency. While IOCs are valuable for identifying known threats and can augment a threat HUNT, they often fall short in detecting new or evolving threats that do not yet have established indicators. IOCs by their very nature are post-incident artifacts. This means that they are point-in-time indicators that can be easily changed and modified by the threat group. By concentrating on TTPs, the Intelligence Team can provide deeper insights into the methods and strategies used by attackers, allowing the HUNT Team to develop more proactive and adaptive threat-hunting strategies. This approach not only enhances the ability to detect and respond to sophisticated threats but also fosters a more resilient and informed cybersecurity posture.

Organizations that are successful are *people-based*, designing processes around human needs rather than systems alone. They have robust easy to understand processes from beginning to end. An organization needs to have processes that detail out how to collect, store, triage, analyze, and disseminate intelligence so that it is repeatable and easily integrated into the target audience's processes. The most effective processes are those that are fully supported by the people who use them. It is crucial that users thoroughly understand each step of the process to ensure it enhances their experience, rather than hindering it or causing frustration.

Here's how intelligence can best be leveraged for HUNT activities:

1. Prioritize TTPs over IOCs

As discussed; by focusing on TTPs the Intelligence Team provides the HUNT Team with insights into *how* threat actors operate. Understanding the behaviors and methodologies of attackers, such as their lateral movement techniques or persistence mechanisms, enables HUNT analysts to identify threats that do not match specific IOCs but exhibit suspicious behavior patterns. Essentially, showing *how* a threat actor accomplishes an attack is more useful than just sharing the artifacts of a previous attack.

2. Build threat profiles and actor context

Develop comprehensive threat actor profiles that include information such as target sectors, motivations, known tools, and historical patterns of attack. This helps the HUNT Team develop hypotheses for their searches based on the most relevant and active threats in an industry as well as identify patterns of attack based on historical context. Again, this is NOT a list of IOCs associated with a threat actor, but rather a full profile that gives a comprehensive overview of the threat actor. Ideally it will also show other threat actors with similar attack patterns or cross over TTPs.

3. Context-rich intelligence briefings

Regularly deliver briefings that provide a broad view of the current threat landscape, including new emerging threats, notable campaigns, and shifts in attacker strategies. Tailor these briefings to include implications for the specific environment, ensuring the HUNT Team can prioritize their activities. This briefing should be different from one that is aimed at executives or cyber awareness as it will involve technical knowledge that may be unnecessary in the other types of briefs.

4. Highlight anomalous behaviors

Intelligence should include examples of anomalous behaviors observed during previous incidents, such as unusual network traffic, unexpected file system changes, command-line history, or abnormal user behavior. These behavioral patterns give the HUNT Team a basis for developing detection logic that goes beyond matching simple signatures but rather looking for how a threat can manifest on the impacted system.

5. Use threat models

Mapping intelligence to a common framework provides the HUNT Team with a structured understanding of the attack lifecycle [1,2,3]. Effective communication requires speaking the same language, using a known framework can eliminate potential confusion. Furthermore, by using an agreed upon framework the HUNT Team can strategically focus their efforts to uncover ongoing or past intrusions. Mapping to something like MITRE ATT&CK® goes beyond just sharing behavioral context. It also enables detection opportunities that can help support HUNT operations as well as continuous monitoring efforts.

6. Operational insights for Hunt hypotheses

Use intelligence to feed specific hypotheses into the HUNT Team's operations. For example, if intelligence indicates a threat actor is known for using credential stuffing as an initial access method, this can inform a hunting activity focused on analyzing login patterns and failed access attempts across the network. Rather than sharing what threat actors are trending, Intelligence Teams should look for opportunities to highlight specific attack vectors and behaviors. This can support a more holistic defense mindset that looks to identify attacks regardless of their origin.

7. Continuous update of TTPs

The Intelligence Team should maintain an up-to-date repository of TTPs and share any observed shifts in attacker behavior with the HUNT Team. If direct updates to the HUNT Team would be too logistically difficult, the HUNT Team should have full access to the repository built by the Intelligence Team. Additionally, access to the repository can allow HUNT to request specific information to fill intelligence gaps without causing the Intelligence Team to make duplicative efforts. These overall enable HUNT analysts to adapt their searches to reflect the latest techniques employed by adversaries.

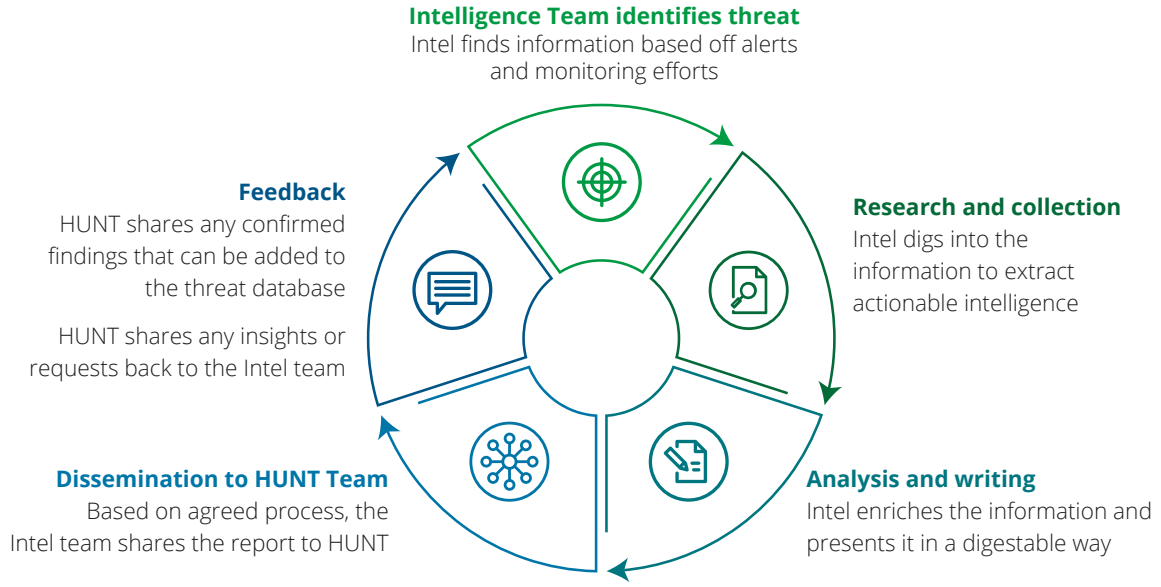

Figure 1. Deloitte's intelligence process for HUNT support

SOC Operate Service: Intel-led threat hunting

Our SOC Operate Services are built on an integrated, intelligence-driven approach to effectively support HUNT operations. By leveraging advanced threat intelligence and efficient collaboration, we enable proactive detection and response to emerging threats. This methodology benefits our clients through enhanced visibility, timely insights, and protection against sophisticated adversaries. Through continuous monitoring and analysis, our services assist organizations to stay ahead of evolving risks and maintain a resilient security posture.

Here's how our service facilitates effective collaboration:

1. **Efficient intelligence integration**: Deloitte's Cyber Security Intelligence (CSI) team collects and curates threat intelligence from a variety of sources, emphasizing TTPs over IOCs. This data is continuously fed into our detection mechanisms and made available to the HUNT Team through an easy-to-use dashboard so their HUNT activities are aligned with the latest intelligence.

2. **Constant feedback loop**: CSI and HUNT have established a close working relationship within the SOC Operate Services that allows the HUNT Team to report back on the relevance and effectiveness of the intelligence provided. The Intelligence Team can suggest investigations, and the HUNT Team can request information on specific TTPs or threat actors for their investigations. This loop facilitates real-time validation and refinement of the intelligence process, enabling our hunting strategies to evolve with the threat landscape.

3. **Contextualized alerts and threat briefings**: CSI provides contextualized threat reports directly to the HUNT Team, which include behavioral indicators, affected assets, observed command-line artifacts, possible attacker goals, and any other intelligence that is relevant to the investigation. HUNT support documents are tailored for the specific environment and client that the HUNT Team is investigating. This enables the HUNT Team to investigate these leads effectively and fine-tune their hunting efforts based on real-world evidence.

4. **Integrated threat actor profiles**: CSI maintains up-to-date profiles of multiple threat actors, including their TTPs, targeted sectors, and known campaigns. Additionally, specific tools are tracked as well, giving HUNT a better understanding of the threat landscape. This intelligence is directly accessible by the HUNT Team, helping them quickly generate hunting hypotheses relevant to the current threat environment.

5. **Collaborative investigations**: Our platform supports *cross-team collaboration*, where both the intelligence and HUNT Teams can document findings, share insights, and update detection logic based on observed adversary behaviors. This collaborative environment means the latest intelligence directly informs hunting activities and vice versa. Furthermore, it creates a much broader and more adaptive environment where the Intelligence and HUNT Teams can respond quickly to identified threats.

Case study

Deloitte's Cyber Intelligence Team (CSI) began tracking the emergence of an EvilAI campaign, where EvilAI was masquerading as legitimate signed productivity tools and artificial intelligence utilities. The following scenario underscores the critical importance of seamless collaboration between the Intelligence Team and the HUNT Team to provide actionable and timely services to clients [4].

Here's a detailed look at how collaboration between HUNT and Threat Intelligence can be optimized to effectively address such threats:

Initial detection and identification

1. **Intelligence team's contribution**:
   - The Deloitte CSI team began tracking the emergence of an EvilAI campaign.
   - CSI initiated working on a report that could be shared with HUNT and other various teams as needed.
   - CSI continued to look for additional information related to the threat to ensure all relevant information was added to the report.
2. **HUNT Team's role**:
   - The HUNT Team had already established what visibility they have into various client systems so that the CSI team can tailor reports to be relevant.
   - HUNT was notified of the event before the report was finished so that they were prepared and ready to act once the report was completed.

Leveraging intelligence for investigation

1. **Access to detailed reports**:
   - The HUNT Team accesses the intelligence report on EvilAI, gaining insights into the malware's specific TTPs.
   - HUNT can then generate hypotheses and search queries to begin investigations for each client.
   - This information helps the HUNT Team to refine their search parameters and focus on identifying specific signs of EvilAI's presence within the network.
2. **Actionable insights**:
   - The intelligence report includes details on the kill chain associated with EvilAI, extracting specific indicators and behaviors that will support detection.
   - Armed with this knowledge, the HUNT Team can look for specific signatures, commands, device changes, and other behaviors associated with EvilAI. This improves their chances of detecting the malware or confidently ruling out potential involvement.
   - After the investigations are complete, HUNT can provide any feedback or relevant findings to the CSI team for additional processing.
3. **Tools/integration:**
   - To be successful the HUNT Team and Intelligence Team need to be fully aware of each other's tools. HUNT needs to have access to all the intelligence reports, and the Intelligence Team needs to have visibility into the search tools used by HUNT.
   - This cross-access collaboration reduces confusion and makes both teams more efficient. HUNT can directly pull the reports needed and share feedback as warranted. Likewise, the Intelligence Team can see what visibility HUNT has within a system and can tune reports to share intelligence that is relevant.

Future outlook

As organizations continue to expand their data intake, the sheer volume and complexity of information necessitate advanced solutions to manage and analyze this influx effectively. Intelligence Teams stand to benefit significantly from the integration of automation and AI augmentation, which can process vast amounts of data at unprecedented speeds. This enables identifying patterns, anomalies, and potential threats that might otherwise go unnoticed.

AI-driven tools can sift through and categorize data, providing preliminary analysis and highlighting areas of interest. However, the ultimate effectiveness of this approach hinges on a Human-in-the-Loop (HITL) model, where skilled analysts perform the critical task of fine-tuning and *validating* the AI-generated insights. This human oversight ensures that the nuanced understanding and contextual judgment that only experienced professionals can provide are applied before the intelligence is disseminated.

By combining the strengths of AI with human expertise, organizations can achieve a more robust and accurate analysis, enhancing their overall cybersecurity posture. Increasing defenders' ability to improve speed and visibility into threats will ensure they keep pace with threat actors that are implementing AI for malicious purposes.

Conclusion

Effective collaboration between intelligence and HUNT Teams is critical to strengthening an organization's cybersecurity posture. By gathering, analyzing, and delivering timely, actionable, and relevant intelligence, the Intelligence Team enables HUNT operations to proactively identify and neutralize threats before they can cause significant harm. This intelligence-led approach allows the HUNT Team to prioritize efforts, focus on the most pressing risks, and respond swiftly to emerging threats.

Deloitte's SOC Operate Services are designed to efficiently integrate intelligence into threat hunting workflows. Leveraging advanced technologies and methodologies, our services provide intelligence that is both actionable and relevant, enabling security teams to make better informed decisions. This integrated approach helps organizations overcome common challenges, such as data complexity and the need for real-time analysis, ultimately enhancing the effectiveness and efficiency of their security operations.

Authors

Will Burns
Deloitte US
Managing Director
Deloitte & Touche LLP
wburns@deloitte.com

Adelina Kaza
Deloitte US
VP, Solution Delivery
Senior Manager
Deloitte & Touche LLP
adkaza@deloitte.com

David An
Deloitte US
Cyber Threat Intelligence Manager
Manager
Deloitte & Touche LLP
davidan3@deloitte.com

Christopher Easton
Deloitte US
Managed Threat Services Team Lead
Senior Solution Delivery Manager
Deloitte & Touche LLP
cheaston@deloitte.com

Nakoa Cox
Deloitte US
Cyber Threat Intelligence Team Lead
Senior Solution Delivery Lead
Deloitte & Touche LLP
nakcox@deloitte.com

References

1. MITRE, “MITRE ATT&CK,” Mitre.org, 2025. https://attack.mitre.org/
2. Lockheed Martin, “Cyber Kill Chain,” *Lockheed Martin*, 2025. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. S. Caltagirone, A. Pendergast, and C. Betz, “The Diamond Model of Intrusion Analysis,” *apps.dtic.mil,* Jul. 05, 2013. https://apps.dtic.mil/sti/citations/ADA586960
4. J. F. Bonaobra et al., “Evilai operators use AI-generated code and fake apps for far-reaching attacks,” Trend Micro, https://www.trendmicro.com/en_us/research/25/i/evilai.html

Deloitte.