Mandiant

USE CASES: APPLYING THREAT INTELLIGENCE

Beyond Mandiant Intelligence Subscriptions

Purchasing a Mandiant Advantage Intelligence subscription gives you world-leading intelligence at your fingertips. Maximizing this intelligence requires clear processes and effective application. Our **Applying Threat Intelligence** series of articles focus on straightforward, pragmatic, process-driven use cases to help organizations to put their intelligence subscription to work.

These **Applying Threat Intelligence** articles consist of use cases aligned to critical cyber defense functions. Each use case will provide an overview of one typical output or application from within each critical function with examples of their use within everyday threat intelligence operations. Each use case will demonstrate how world-leading intelligence practitioners use intelligence effectively to bolster their cyber defense.

Applying intelligence effectively requires understanding why you need intelligence in the first place. Knowing your critical assets and who (or what) threatens them. Knowing why your organization may be targeted and how the threats may strike. Knowing which business units within your organization need different types of intelligence, and when.

This series of articles is designed to demonstrate how to apply intelligence within your organization to achieve decision advantage – the ability to make the best-informed decisions at all levels and security functions with the right information available.

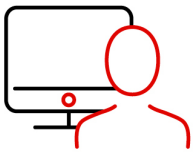
Cyber Defense Functions and Intelligence Use Cases

Each article within our Applying Threat Intelligence series focuses on one of the six (6) critical functions of cyber defense (below): Intelligence, Hunt, Respond, Command and Control, Detect, and Validate. Intelligence-led organizations align their personnel, technology, and processes against each of these critical functions to ensure a holistic and collaborative approach to cyber defense.

INTELLIGENCE
Guiding Light

HUNT
Threat Hunting and Compromise Assessment

RESPOND
Incident Response and Recovery



COMMAND AND CONTROL
Maintain the Mission

DETECT
Alert Monitoring and Investigation

VALIDATE
Targeted Testing and Controls Validations

Examples of Intelligence Use Cases within Each Critical Function

Intelligence informs and empowers each security function. Our Applying Threat Intelligence articles will focus on the following specific use cases:

1. Consumption and application of **Intelligence** across the organization enables faster, more accurate risk assessments of threats most likely to have significant impact on your organization.
2. **Hunt** activities use intelligence to methodically find active threats and adversaries within your organization that may have gone undetected.
3. Intelligence is used to provide context around investigations, incidents, and breaches-enabling an improved ability to **Respond**, minimizing factors such as threat exposure, adversary dwell time, and impact.
4. The **Command and Control** function keeps the other capabilities aligned, and harnesses intelligence to communicate threats clearly, take decisive action, and strategically improve your defense posture over time.
5. Intelligence informs and enables security monitoring teams to quickly **Detect** threat activity and prioritize events – reducing noise and alert fatigue.
6. Intelligence provides insight into the latest tactics, techniques, and procedures (TTPs) to continually assess and **Validate** the effectiveness of security controls.

Use Case Approach

To be actionable and contribute to the effective consumption of intelligence, each use case will answer the following questions:

- What is the intent of the intelligence? (i.e. what is to be accomplished?)
- Who will consume the intelligence?
- How will the intelligence be communicated?
- How will feedback on the intelligence be gathered?
- What additional intelligence sources are needed to fill existing information gaps?

Use Case Structure

For each use case and cyber defense function the following are defined:

- Common objectives and goals for threat intelligence application
- A series of actions to achieve the goals of the use case
- Specific outcomes an organization might expect when the use case is implemented
- Cyber defense roles and capabilities typically required for the use case to be successfully implemented

Following the Applying Threat Intelligence Articles

The **Applying Threat Intelligence** articles have wide applicability to a variety of different cyber roles and functions, from those leading cyber defense teams to those seeking to deepen their cyber security knowledge.

For each of the main cyber defense functions, Mandiant will publish one or more intelligence use cases, with more articles being added over time. Our Intelligence subject matter experts (SMEs) are also committed to revising and evolving these use cases. As we gather your feedback and help individual customers overcome challenges with threat intelligence, we'll make those lessons learned available to you through the Advantage platform.