THE

DEFENDER'S [ADVANTAGE]

EXECUTIVE SUMMARY

MANDIANT

The Defender's Advantage is the concept that organizations are defending against attacks in their own environment. This provides a fundamental advantage arising from the fact that they have control over the landscape where they will meet their adversaries. Organizations struggle to capitalize on this advantage.

7.5

Organizations subscribe to an average of Threat Intelligence feeds*

66.5%

66.5% still disseminate CTI through Email, PPT, Spreadsheets, Documents**

43%

Only 43% has documented CTI requirements**

Every day, organizations around the world are waking up to a fresh wave of increasingly sophisticated cyber-attacks. With prominent attacks such as ransomware and multifaceted extortion dominating the headlines, security leaders are scrambling for solutions while facing new cyber security requirements imposed by legislators and business leaders demanding answers. The reality facing security teams can at times feel like an uphill battle, with many losing ground against their adversaries due to lack of resources, expertise and misconfigured tools.

Unorganized, uncoordinated or siloed security activities cannot provide answers to the many questions posed by business leaders and stakeholders, nor can they give them confidence in their readiness. By focusing on how people utilize the tools at their disposal and developing capabilities to protect the business, organizations broaden their horizon beyond the SOC to the broader scope of Cyber Defense.

*Forrester Wave ETIS Q1, 2021
**SANS CTI Survey 2021

The Functions of Cyber Defense

Intelligence
Guiding Light

Hunt
Threat Hunting and Compromise Assessment

Detect
Alert Monitoring and Investigation

Respond
Incident Response and Recovery

Validate
Targeted Testing and Controls Validation

Command and Control
Maintain the Mission

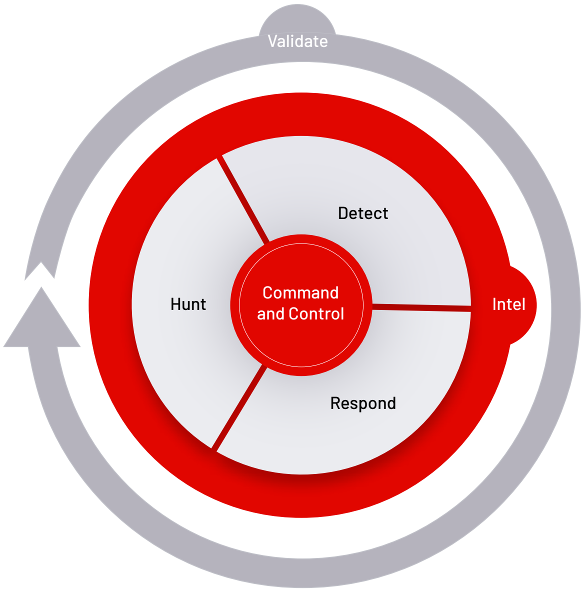
Cyber Defense is one of four closely integrated Information Security domains, with the other domains being Security Governance, Security Architecture and Security Risk Management. Comprised of six functions, Cyber Defense enables organizations to continue to operate in the face of threats.

Each Cyber Defense function represents different activities, actions or responsibilities that are focused on different goals, while collectively working together to identify and respond to threats facing the business. A paradigm shift is needed to move from standing up technologies to activate these functions; bring them together to significantly reduce the risk and impact of cyber-attacks to an organization.

When fully optimized and activated, Cyber Defense enables organizations to answer questions such as:

- Who is targeting us and what are they after?
- Have we been compromised?
- Would we know if we were compromised?
- Are we prepared to respond to a breach?
- Are our security investments effective?

Figure 1: The Functions of Cyber Defense in Action



> The Cyber Threat Profile is arguably the most important document for a cyber intelligence program. And most programs either don't have one or aren't using it to drive their operations.

Andrew Close, Principal Consultant, Intelligence Capability Development, Mandiant

The Intelligence Function

The lifeblood of Cyber Defense is cyber threat intelligence (CTI) which feeds into every cyber defense function. When implemented effectively, CTI delivers insight into attacker tactics, techniques and procedures (TTPs), their targets and motivations and helps uncover vulnerabilities that may exist in an organization's environment. It can explore the likelihood of an attack and also determine the organizational impact should an attack occur.

Security teams can invest in dozens of the "best" intelligence subscriptions; however, even the best intelligence is wasted if it is not utilized properly. It is therefore important to understand who will consume the intelligence, what they will do with it and how it will be communicated before purchasing decisions are made.

The Hunt Function

The Hunt function uses intelligence to identify potential evidence of an active or previous compromise within an organization's environment. Using insight on a specific adversary, Hunt teams adopt the mindset of a threat actor to develop hypotheses regarding how the threat actor may have compromised the organization's security defenses, search the environment, gather further data, analyze the results and communicate the outcome. When threat hunting is activated as a function within Cyber Defense, organizations benefit from enhanced response capabilities, security improvements, enriched internal threat intelligence and new methods of threat detection.

The Detect Function

The Detect function identifies malicious behavior based on alert activity or observation. Threat intelligence lies at the core of effective detection, contextualizing and categorizing incidents, reports and data feeds to generate insights that define an attacker's objective and methodology. These insights are used to prioritize analysis and resolution of the threats that pose the most significant risk.

Many traditional SOC teams are facing overwhelming alert volumes for analysis as a result of too many data feeds, however modern SOC teams merge and unify multiple related alerts using automation, flagging high-fidelity cases for further investigation.

> Having an in-depth understanding of TTPs based on reliable threat intelligence is critical for SOC analysts. An understand of past breaches aids analysts in predicting future attacker activity to a single system and an enterprise-wide incident.

David Lindquist, Managed Defense Operations Manager, Mandiant

The Respond Function

The Respond function of the Cyber Defense domain is responsible for the response and remediation of compromise within an organization's environment. Following the identification of suspicious activity by the Detect and Hunt functions, the Respond team confirms if this activity is malicious and takes subsequent actions to take include: understand the full extent of the compromise, minimize the impact to the business, enable the business to resume normal operations and remove the threat from the environment.

To prevent repeat incidents, the Respond function must also identify any lessons learned and communicate any enhancements to the Command and Control team.

The Validate Function

The Validate function provides assurance that the security control ecosystem is operating as expected and is protecting critical assets. Security validation may be targeted, mission based, objective based or part of a continuous controls assessment, providing quantitative data to guide decision making regarding potential investment and cost savings. Through the use of simulated activity, an organization's people, processes and technology are safely tested with authentic, active attacks to evaluate their effectiveness and identify areas for improvement.

The Command and Control Function

Command and Control is responsible for maintaining the mission and orchestrating all other functions to prioritize Cyber Defense resources. An important role of Command and Control is to facilitate the flow of information between each function. In many cases, organizations build strong detection capabilities and tools, but demonstrate a poor response to incidents due to a lack of established and documented processes. During a major incident, Command and Control is primarily responsible for communicating and coordinating activities for investigation and remediation.

> It is very common for organizations performing their own incident response to panic and attempt a premature remediation. They often jump to remediation efforts and introduce changes that complicate the investigation. This whack-a-mole approach will lengthen the investigation, cause incomplete remediation efforts and can lead to repeat attacks.

Eric Scales, Vice President, Mandiant

Activating Cyber Defense to Capitalize on The Defender's Advantage

Cyber Defense functions not only need to be established; they also need to be activated and operationalized against attackers. The functions of Cyber Defense do not have to be activated all at once. Capabilities can be built up and matured over time. To accelerate the activation of Cyber Defense capabilities, organizations leverage strategically selected SaaS and managed services to provide full Cyber Defense coverage, microservices for targeted needs and expert resources for in-house deployment and operations development. Organizations need to focus on the areas that matter most to them and employ accelerators to galvanize their defender's advantage.

In the Defender's Advantage, Mandiant delivers comprehensive, step by step advice on how to advance an organization's security capabilities to build a robust, comprehensive security program, enabling them to take command of their own environment and turn the tide on their attackers.

Get your free copy of **The Defender's Advantage** today
www.mandiant.com/defenders-advantage

If you want to galvanize your cyber defenses, Mandiant's experts are on hand to provide guidance, help and support. **Click here to start the conversation today.**
www.mandiant.com/contact-us

About Mandiant

Effective security is based on the right combination of expertise, intelligence and technology. Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for organizations of all sizes. Offerings span the range of consulting, automated defense,managed detection and response, threat intelligence and security validation for provable and transformative Cyber Defense.

Learn more at **www.mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

MANDIANT