Cyber Defense Center Development

Benefits

- **Improve your defense posture.** Identify and close gaps in your security monitoring and response capabilities to protect against advanced threats.
- **Build consensus on security improvements.** Enhance internal collaboration and communication by sharing knowledge and prioritizing improvements.
- **Reduce impact of security incidents.** Improve your detection and response capabilities to minimize cyber risk.
- **Prioritize budget and resources.** Allocate security spending and resources to strengthen your defensive posture and improve overall response.

Build up your own resilient security operations program

Why Mandiant

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques, and procedures.

Overview

The Cyber Defense Center Development service helps organizations build an effective security operations program that minimizes organizational risk and reduces the impact of security breaches. Based on a security model that maps directly to your strategic goals, we offer recommendations grounded in first-hand experience. Our consultants work closely with your organization to align your security program to support an Adaptive Defense strategy.

Our approach

Mandiant experts have in-depth knowledge of the tactics, techniques, and procedures used by advanced threat actors. We work with your organization to build and implement core capabilities and processes into your program.

To effectively detect and respond to attacks, an incident response program needs effective processes and procedures, with the appropriate people and technology, and metrics evaluating the effectiveness of the program. Based on our experience responding to critical security incidents, Mandiant experts have developed a framework with six core capabilities that underpin a resilient security program. The framework addresses:

- **Governance.** Does your organizational structure align with the overall business goals and mission statement?
- **Communications**. Do you have processes in place to promote effective information sharing between internal and external entities?
- **Visibility.** Are technologies and processes in place to generate awareness of activities that are occurring on your systems and networks?
- **Intelligence.** Does your threat intelligence inform and enhance security planning, vulnerability management, and incident response activities?

- **Metrics.** Do your incident response metrics align with the overall business goals and objectives while driving continuous improvement within the security organization?
- **Response.** Are established technologies and processes in place that the security team can use to identify, categorize, investigate, and remediate adverse security events?

During the engagement, we work with your organization to build and implement a program with core foundational processes and technologies. We can also assist with short-term security monitoring until your staff is established and equipped to assume ownership.

TABLE 1. Cyber Defense Center Development phases.

Stage	Objective	Tasks
Foundation	Establish a base to effectively respond to incidents and apply resources in an efficient manner.	• Outline an escalation matrix and incident response workflow • Create strategic and program management plans • Design performance metrics and reporting plans
Integration	Incorporate new processes, procedures, and technology into your operational environment.	• Develop and conduct training • Establish operational service level agreements • Deploy and configure technology
Operation	Execute on the operational and analytical processes and provide monitoring capabilities.	• Provide initial monitoring capability • Continually mature operational and analytical process • Transition roles to security team or provide staff augmentation

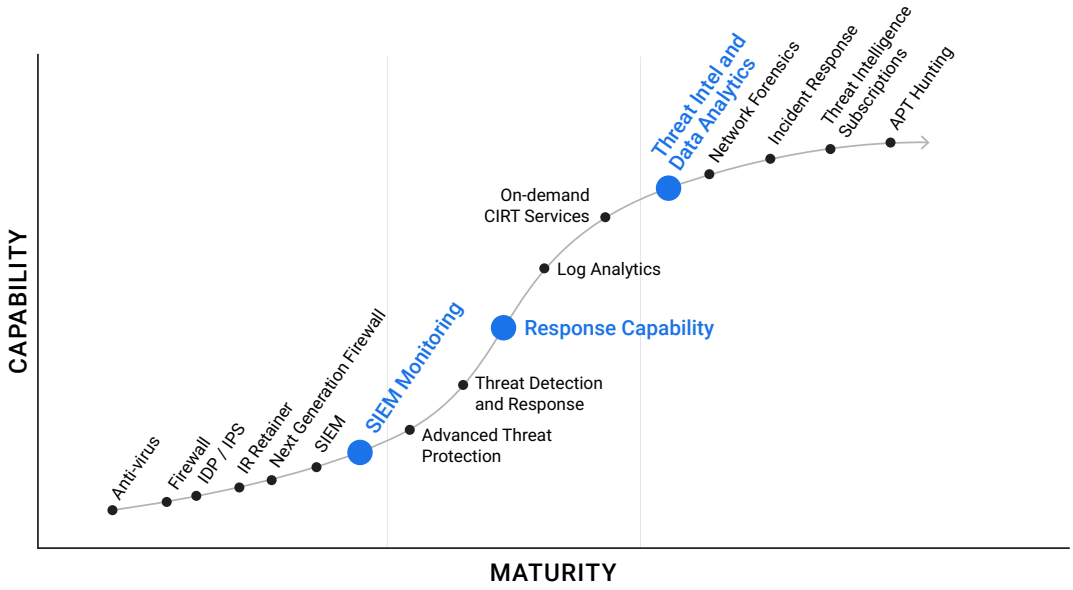

FIGURE 1. Cyber defense program development model.

Based on our six core capabilities framework, the Cyber Defense Center Development service enables an organization to transition from a reactive incident response methodology to a predictive and mission-focused program that is fully aligned with the business.