Mandiant

Datasheet

Cyber Defense Operations

Benefits

- **Extend your team's capabilities.** Fill critical roles in your detection and response team
- **Conduct knowledge transfer.** Train employees throughout the day
- **Identify areas for maturation.** Fully develop response group capabilities in line with their mission objectives
- **Practical transformation.** Focus on transformational objectives

Extend and transform your security operations program

Why Mandiant

Mandiant has been at the forefront of cyber security 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 Mandiant Cyber Defense Operations service helps organizations transform their detection and response programs through hands-on operational support from experienced consultants who specialize in event triage and analysis, incident response, threat intelligence, cyber security program development and organizational security transformation. These consultants fill critical roles in your SOC and lead transformation efforts to help you develop and sustain a more mature security program.

Our approach

First, Mandiant consultants evaluate your existing cyber defense program. This includes conducting team discussions, internal document review and tabletop exercises, as well as a technical validation of your program's detection capabilities. Using their evaluation and your own maturation goals, they work with you to define transformation goals and objectives.

Mandiant will then provide dedicated personnel to drive the agreed-on transformation initiatives. These personnel offer hands-on technical event triage, analysis, and investigation support using your technology stack. They support intelligence gathering, hunting, forensic investigation, transformation and case management. By operating within your

environment, they help ensure operationalized outcomes that effect long-lasting change in your environment.

Potential transformation goals (examples)

- Knowledge transfer
- Threat hunting program development
- Use case/playbook development
- Use case/playbook operationalizing
- Tool visibility assessment
- Technology assessment/rationalization
- IRP development
- Communications plan development
- IR process refinement
- IR capabilities assessment
- Tabletop exercises
- Metrics development

A Cyber Defense Operations engagement typically ranges from 2-6 months, but timing can vary based on the scope and nature of the engagement.