Insider Threat Security Services

Benefits

- Reduce operational risk and minimize impact of insider threat incidents and data theft
- Improve insider threat security program based on actual findings and leadership consensus
- Prioritize insider threat program budget and resources
- Identify gaps in your technology stack's ability to properly detect and prevent insider threats
- Increase organizational return on security program investment
- Get advanced, continuous security expertise and insider threat protection with Mandiant Advantage™

Uncover and manage insider threats by implementing risk-based security program capabilities

Overview

To properly mitigate the frequency and impact of insider threats, security-conscious organizations must not only implement data loss prevention processes, but also deploy and establish dedicated staff, behavioral analytics and security information event management capabilities.

Mandiant provides complete attack lifecycle protection against insider threats by assessing your existing insider threat program and building out capabilities to effectively monitor, detect and respond to them.

We do this in two ways. The **Mandiant Insider Threat Program Assessment** is a point-in-time evaluation of existing insider threats in your specific environment, while the **Mandiant Insider Threat Security as a Service** provides an operational security program to ensure effective and continuous insider threat prevention, detection and response. These services are offered separately but can be combined based on customer needs and project scope.

Insider Threat Program Assessment

This assessment is designed for security-conscious organizations that need to enhance or develop their insider threat program. Mandiant uses a “follow the data” security model to deliver actionable, organization-specific recommendations to identify weaknesses and vulnerabilities across existing safeguards, improve program capabilities, mitigate impact of incidents, and reduce the overall risk of insider threats.

What We Do

First, Mandiant experts use a combination of documentation review, analysis and deep-dive workshops to rigorously evaluate your organization's insider threat program effectiveness against three core domains: people, processes, and tools.

Processes
Review operational processes and documentation to track types of data and people accessing that data.

People
Monitor personnel from hire to exit, as well as third parties such as subcontractors, consultants, interns, and affiliates with access to sensitive data.

Tools
Examine the tools in place that address human resources, physical security, supply chain management, information technology, and customer relations platforms.

Next, based on gaps, weaknesses and vulnerabilities found in your environment, we provide tailored recommendations and an actionable roadmap to support the development and improvement of your organization's immediate and future insider threat program needs. This will minimize the impact and cost of a security incident caused by accidental or intentional insiders.

Tiered Model

To meet your specific business needs, Mandiant offers a three-tiered model to support various organizational objectives.

TABLE 1. Insider Threat Program Assessment tiers.

	Tier 1 New program build	Tier 2 Existing program assessment	Tier 3 Advanced program assessment and implementation
Engagement Timeline	4 weeks	6 weeks	12 weeks
Service Components	Buildout of baseline insider threat program capabilities and roadmap to sustainability	Strategic assessment of existing insider threat capabilities with actionable improvement roadmap	Comprehensive assessment of existing capabilities, hands-on skills training and threat hunting implementation, coupled with a Technical Security Posture Assessment*

*Our Technical Security Program Assessment is the result of a partnership among **Mandiant, innerActiv and Trust Farm** that uses proprietary technologies and tradecraft to determine whether insider threats of any kind are present in your environment.

Why Mandiant Solutions

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

Insider Threat Security as a Service

This subscription-based service provides your organization with continuous, full-spectrum insider threat visibility and prevention with incident response expertise and real-time threat intelligence delivered through the Mandiant Advantage™ platform (Fig. 1). This service is ideal for organizations with a growing remote workforce and high-value data with potential to be stolen and used against your organization.

How It Works

First, our experts use your existing SIEM technology to monitor for possible insider threats and the dark web based on keywords that help support insider threat investigations, possible data leaks, and online discussions related to potential future business efforts such as mergers and acquisitions.

Next, we provide executive briefings and insider threat profiles based on our findings of your program strengths and weaknesses coupled with insider threat intelligence relevant to your specific environment.

Insider Threat Security as a Service supports an ongoing operational security program to ensure effective and continuous insider threat prevention, detection, and response.

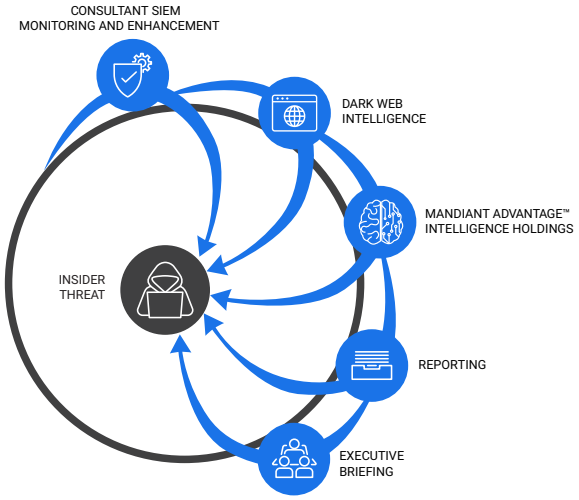

Figure 1. Service methodology.