Cybersecurity Program Assessment

Benefits

- Identify and reduce cybersecurity risks in your environment
- Prioritize cybersecurity investment and resources to meet your business objectives
- Understand the effectiveness of your existing security controls
- Raise executive-level awareness of cybersecurity challenges, program gaps, and related breach impact

Why Mandiant

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. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques, and procedures.

Evaluate your cybersecurity program to prioritize investments, increase resiliency, and reduce risk

Overview

The Mandiant Security Program Assessment provides an independent maturity assessment of your organization's cybersecurity program across four core critical areas: security governance, security architecture, cyber defense, and security risk management.

After an in-depth, collaborative analysis of your existing program, we provide best practice recommendations to improve your security posture based on your specific risk profile and level of security maturity.

Our methodology

Mandiant experts provide an in-depth evaluation of your organization's four core security program domains (Fig 1). They use a purpose-built approach, rooted in our collective frontline expertise and aligned with key industry standards and frameworks.

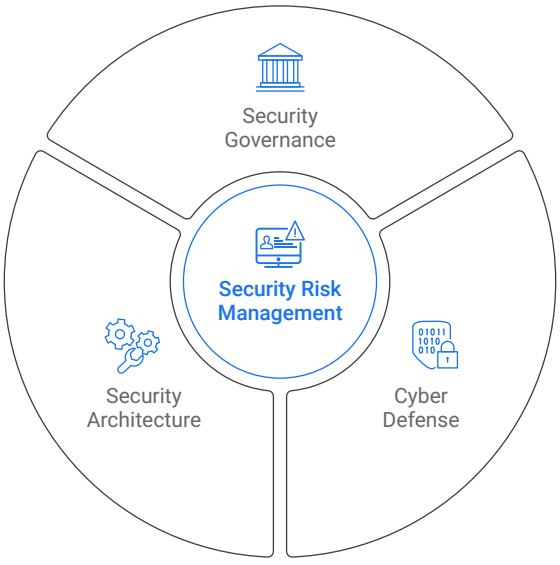

FIGURE 1. Four core security domains assessed.

Our experts begin by reviewing documentation of your existing security program capabilities and practices. They concurrently collect relevant industry sector threat intelligence and critical data on business components affecting your specific environment. Following this initial analysis phase, Mandiant experts facilitate a series of interactive workshops to understand your organization's current cybersecurity maturity and design an effective future program model to meet your business needs.

Our workshops cover emerging topic areas from each of the four core security domains, such as cloud security architecture, application security, supply chain risk management, and threat intelligence.

Next, our experts deliver a detailed report of their findings with strategic and tactical recommendations for improvement. Our experts also provide a multi-year implementation roadmap to help meet your organization's short- and long-term cybersecurity goals.

To ensure long-term success and sustainability, our experts can also:

- Use the Mandiant Security Validation platform to perform security effectiveness evaluations against roadmap action implementation
- Conduct Mandiant Red Team Assessments and Mandiant Penetration Testing to ensure best practice detection and response capabilities are practiced
- Perform additional security architecture and configuration reviews to improve or enhance defenses.

Mandiant is committed to delivering the highest degree of fidelity as an outcome to this service, enabling your organization to move from the design phase to operational efficacy.

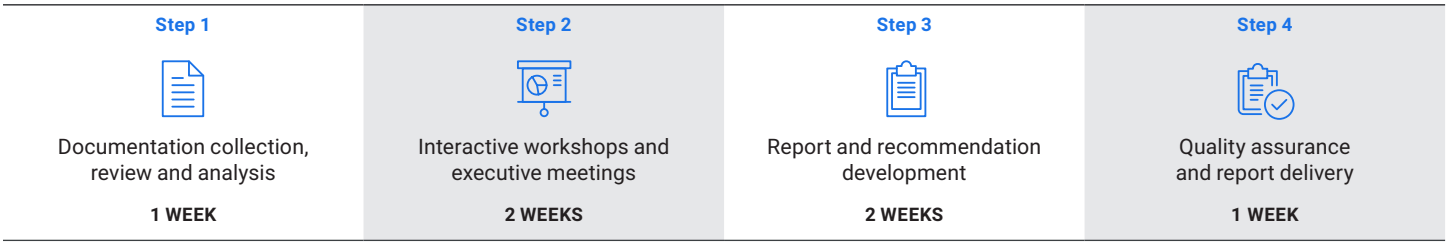

FIGURE 2. Service workflow and engagement timeline.

Engagement outcomes

- **Executive summary.** A high-level overview of your organization's program maturity, areas of strength, opportunities for improvement, and implementation roadmap.
- **Assessment results and future state target.** Identification of critical security function domains that require further development coupled with a targeted future-state maturity model.
- **Actionable roadmap.** A strategic and tactical plan with prioritization recommendations to help enhance your organization's security maturity across all four core security domains.
- **Industry sector threat intelligence.** A deep understanding of global attacker behavior affecting your industry through extensive incident response experience into actionable threat intelligence.
- **Executive and technical briefings.** Presentations of assessment results to both executive and technical stakeholders.