Mandiant

DATASHEET

Cybersecurity Due Diligence Service

Benefits

- Ensure cyber security health is advantageous for purchase and selling opportunities
- Identify and prevent security-related risks before completing full business integration
- Reduce incident impact with corrective cyber risk management program capabilities
- Understand and verify existing network security controls of selected organization
- Preserve brand reputation as a security-conscious organization

Identify and mitigate inherited cyber risks connected to business transactions and systems out of direct control

Overview

Organizations that pursue mergers and acquisitions, hold a portfolio of companies or foster third-party relationships to strategically develop their business, unknowingly increase their cyber attack surface through these business changes. Traditionally, due diligence is conducted across various business functions such as legal and finance. However, when combining two or more separate entities, the analysis of cyber security risk management practices and security maturity is just as critical.

With Mandiant CyberSecurity Due Diligence Service, our experts analyze multiple cyber environments and business risk profiles to improve security program capabilities and provide actionable remediation recommendations to ensure combined security health and overall maturity alignment.

Our methodology

First, Mandiant experts conduct a collaborative workshop with your leadership team to scope the situation. This workshop helps define how our experts should proceed with the engagement to meet your organization's specific due diligence needs—ranging from mergers, acquisitions (including independent acquisitions), divestures and asset management pipelines.

Second, our experts determine the services plan most applicable to your business needs. Mandiant presents you with a relevant menu of offerings to achieve the highest quality of cyber due diligence for your specific objectives. We consider potential business impact, business relationships, forms of access and system integration.

Company A [buyer] agrees to the purchase terms of Company B [acquired entity]. Company A's leadership team is ready to begin the integration of both networks quickly, but there is concern regarding potential security gaps between the two organizations that would increase Company A's attack surface and risk vulnerability.

Mandiant experts perform the following engagement delivery to meet Company A's cybersecurity due diligence needs.

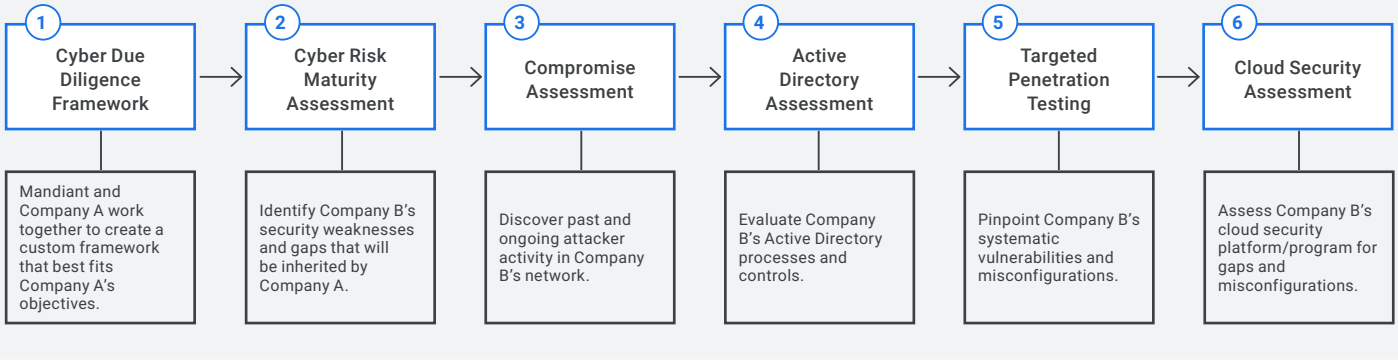

FIGURE 1. Sample engagement scenario. Each engagement performed (services, phases, sequence) is specific to individual client needs.

Last, these purpose-built services are delivered in a phased format—beginning with strategic assessments and leading to technical evaluations, in most cases. Mandiant continuously collaborates with the client to maintain a suitable phased delivery of services to meet the client organization's evolving business objectives.

Engagement outcomes

- **Executive briefing.** Visibility into target security maturity levels and recommended integration plan investments
- **Actionable roadmap.** Path to achieve security program improvements and logical integration steps for full business integration
- **Tactical recommendations.** Actions to enable remediation for short- and long-term success of the purchasing organization, selling organization or existing product and service portfolio

Why Mandiant

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders are on the frontlines of some 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.