



Mandiant Consulting Services

Responding to critical breaches and empowering organizations to protect their assets

Mandiant Consulting Overview

Mandiant, a FireEye company, has over 14 years of experience at the forefront of cyber security and cyber threat intelligence. Our incident responders have been on the frontlines of the world's most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures.

We help organizations of all sizes remediate security breaches, identify vulnerabilities that attackers target to exploit, and provide guidance on closing security gaps to reduce the risk of a future cyber incident.

“Mandiant is at the forefront of helping organizations rethink how to prepare for security breaches.”

Michael Chertoff
Former Secretary of Homeland Security

Framework for Security Needs



The Mandiant Difference

Mandiant combines a deep understanding of attacker behavior with intelligence based on exceptional visibility into the evolving threat landscape and an extensive technology platform to do so with speed, scale and efficiency.

Expertise: Over 14 years of frontline experience responding to the most critical breaches. We see what the attackers did, how they did it, the tools and techniques they used and what they were after. This enables us to see the big picture, understanding evolving attacker behavior and motivations in a way others cannot.

Intelligence: Mandiant's intelligence-led approach to services incorporates industry-leading cyber threat intelligence from over 250 FireEye iSight intelligence experts, thousands of Mandiant investigations, FireEye products and our Managed Defense service for worldwide visibility into the rapidly evolving threat landscape.

Technology: Mandiant leverages FireEye endpoint technology, network sensors and analytics platforms that can operate from the cloud or on-premise depending on client needs, whether running Windows, Linux or macOS. Our technology enables a rapid response at greater scale, minimizing expense.



Summary of Selected Mandiant Services.

Security Function	Security Need	Service	Overview	Benefit
Incident Response	I am breached.	Incident Response Services	Investigate, contain, and remediate critical security incidents with speed, scale, and efficiency.	Resolve critical security incidents and establish long-term solutions to address systemic causes.
Assessment	Am I compromised?	Compromise Assessment	Identify past or present compromises of your environment, assess future risk of compromise based on your security hygiene and improve your ability to respond.	Know whether or not your organization is currently or was previously compromised.
	Am I exposed?	Red Teaming and Penetration Testing	Test your security posture using the same tools, tactics and procedures (TTPs) as the advanced attackers we see every day during our Incident Response engagements.	Identify previously undetected weaknesses before an attacker does.
		Industrial Control Systems Healthcheck	Minimally invasive assessment of an industrial facility's overall cyber security posture, bridging between IT and OT security.	Understand your ICS's exposed vulnerabilities and establish a plan to reduce your system's cyber security risk.
	Am I prepared?	Response Readiness Assessment	An independent maturity assessment of your security monitoring and response capabilities, informed by our experience on the front lines of incident response.	Learn how to improve your organization's defense posture to find and stop attackers faster.
		Security Program Assessment	An in-depth evaluation of your organization's information security programs across ten key security domains, each of which is mapped to compliance, security and industry frameworks.	Evaluate the effectiveness of your information security program to improve your security posture and reduce business risk.
		Incident Response Retainer	Established terms and conditions for incident response services before a cyber security incident is suspected.	Significantly reduce incident response time, thereby reducing the overall impact of a breach.
Enhancement	How do I improve my capabilities?	Product, Intelligence and Expertise Training	Educate your security team on up-to-date threat knowledge and improve the operational skills they need to effectively combat the evolving cyber threat landscape.	Expose your team to learnings and training exercises based on real-world investigations, not theoretical scenarios.
	How I prioritize my response?	Cyber Threat Intelligence Services	Build cyber threat intelligence (CTI) processes and solutions within your organization's security operations that optimize your ability to consume, analyze and apply threat intelligence to protect the business.	Support your security operations team and influence executive decision making across the organization by designing intelligence-led security processes.
Transformation	How do I get there?	Cyber Defense Center Development	Transition your organization from a "reactive" compliance-based incident response to a "proactive" and mission-focused program that is fully aligned to your business priorities.	Develop and improve your security operations and incident response team capabilities.

To learn more about FireEye, visit: www.FireEye.com

