DATENBLATT

MANDIANT®
A FireEye® Company

Mandiant Consulting Services

Lösungen für schwerwiegende Sicherheitsvorfälle und Unterstützung von Unternehmen beim Schutz ihrer Ressourcen

Mandiant Consulting: Überblick
Mandiant, ein Unternehmen von FireEye, ist seit über vierzehn Jahren ein Vorreiter in den Bereichen Cybersicherheit und Cyber Threat Intelligence (CTI). Unsere IT-Notfallteams sind bei den gravierendsten Sicherheitsvorfällen weltweit im Einsatz. Sie verstehen sowohl aktuell aktive und neue Hacker als auch die Tools, Taktiken und Prozesse, die diese Hacker nutzen und ständig weiterentwickeln.

Wir unterstützen Unternehmen jeder Größe dabei, Sicherheitsvorfälle zu beheben, Schwachstellen zu identifizieren und ihre Systeme durch die Schließung von Sicherheitslücken vor zukünftigen Angriffen zu schützen.

„Mandiant ist die erste Adresse für Unternehmen, die erstklassigen Schutz vor Sicherheitsverletzungen benötigen."

– **Michael Chertoff,**
ehemaliger US-Minister für innere Sicherheit (Homeland Security)

Rahmen zur Stärkung der Cybersicherheit

Vorteile von Mandiant

Mandiant verbindet detaillierte Kenntnisse über Angreiferaktivitäten mit Bedrohungsdaten, die einen außerordentlich guten Überblick über die aktuelle Bedrohungslage geben einerseits, und eine umfassende und leistungsstarke Technologie-Plattform andererseits, die eine schnelle, skalierbare und effiziente Bereitstellung von Services ermöglicht.

Know-how: Wir unterstützen Unternehmen seit über 14 Jahren bei der Reaktion auf kritische Vorfälle. Wir analysieren die Vorgehensweise, Tools, Techniken und Ziele der Angreifer, um uns einen umfassenden Überblick zu verschaffen. Dadurch können wir die Motivationen und Methoden der Angreifer nachvollziehen.

Bedrohungsdaten: Dank Bedrohungsdaten von über 250 FireEye iSIGHT Intelligence Experten, Tausenden Mandiant-Berichten, FireEye-Produkten und unserem Managed Defense Service, gewähren die Services von Mandiant Kunden Einblicke in die sich schnell wandelnde Bedrohungslage.

Technologie: Mandiant nutzt Lösungen zum Endpunktschutz, Netzwerksensoren und Analyseplattformen von FireEye, die je nach Kundenanforderungen sowohl in der Cloud als auch On-Premises einsetzbar sind und mit Windows, Linux und macOS kompatibel sind. Unsere Technologie ermöglicht es Unternehmen, schneller und umfassender auf Bedrohungen zu reagieren und somit die Kosten zu reduzieren.

FireEye

Ausgewählte Mandiant Services

Funktion	Anforderung	Service	Überblick	Vorteil
Incident Response	**Hacker sind eingedrungen!**	**Incident-Response-Services**	Schnelle, umfassende und effiziente Untersuchung, Eindämmung und Behebung von kritischen Sicherheitsvorfällen.	Reaktion auf kritische Sicherheitsverstöße und Einrichtung langfristiger Lösungen für strukturelle Sicherheitslücken.
Bewertung	**Sind wir infiltriert worden?**	**Vorfallseinschätzung**	Wir identifizieren vergangene oder aktuelle Angriffe auf Ihre IT-Umgebung und schätzen unter Berücksichtigung Ihrer Sicherheitspraktiken ein, wie groß das Risiko zukünftiger Angriffe ist. Sie können die Ergebnisse nutzen, um Ihre Notfallpläne und Abwehrbereitschaft zu verbessern.	Informationen über aktuelle oder frühere Sicherheitsverletzungen im Unternehmen.
	Sind wir anfällig für Angriffe?	**Red-Team-Operationen und Penetrationstests**	Unsere Experten testen Ihre Sicherheitsinfrastruktur mit den Tools, Taktiken und Prozessen (TTPs) moderner Angreifer, die wir aus unserer täglichen Incident-Response-Praxis kennen.	Identifizierung bislang unbekannter Schwachstellen, bevor Angreifer sie ausnutzen.
		Prüfung industrieller Steuersysteme (Industrial Control Systems, ICS)	Wir unternehmen eine minimalinvasive Analyse des Sicherheitsniveaus der Industrieanlage, die IT- und OT-Sicherheit (Operational Technology, Betriebstechnik) einschließt.	Identifizieren Sie die Schwachstellen in Ihren ICS und entwickeln Sie einen Plan, um das Risiko für Ihr System zu minimieren.
	Sind wir vorbereitet?	**Beurteilung der Fähigkeit zur Angriffsabwehr**	Wir nehmen eine unabhängige Einschätzung der Effizienz Ihrer Überwachungs- und Reaktionsfähigkeiten auf Grundlage unserer Praxiserfahrung im Bereich Incident Response vor.	Verbesserung Ihres Sicherheitsstatus, damit Sie Angreifer schneller aufspüren und stoppen können.
		Bewertung von Sicherheitsprogrammen	Die Sicherheitsprogramme Ihres Unternehmens werden in zehn Bereichen bewertet, jeweils im Hinblick auf Compliance, Sicherheit und branchenspezifische Frameworks.	Sie können die Effektivität Ihrer IT-Sicherheitsmaßnahmen und -prozesse evaluieren, um Ihren Sicherheitsstatus zu verbessern und das Risiko eines Angriffs zu reduzieren.
		Incident-Response-Bereitschaftsdienst	Wir ermöglichen es Ihnen, grundlegende Bedingungen für Incident-Response-Services festzulegen, bevor ein Sicherheitsvorfall aufgedeckt wird.	Dadurch werden die Reaktionszeiten erheblich verkürzt und somit auch die Auswirkungen einer Sicherheitsverletzung minimiert.
Verbesserungen	**Wie können wir die Cyberabwehr stärken?**	**Training zu Produkten, Bedrohungsdaten und Know-how**	Informieren Sie Ihr Sicherheitsteam über die aktuelle Bedrohungslage, damit es besser darauf vorbereitet ist, effektiv auf dynamische Bedrohungen zu reagieren.	Unterstützen Sie Ihr Team mit Kursen und Übungen, die auf realen IR-Einsätzen – statt auf theoretischen Szenarien – basieren.
	Wie sollten wir Gegenmaßnahmen priorisieren?	**Bedrohungsdaten-Services**	Binden Sie Prozesse und Lösungen für die Nutzung von Bedrohungsdaten in Ihr Sicherheitsprogramm ein. Ziel ist es, Ihre Fähigkeit zur Einspeisung, Analyse und praktischen Anwendung von Bedrohungsdaten zum Schutz Ihres Unternehmens zu verbessern.	Durch die Entwicklung von auf Bedrohungsdaten gestützter Sicherheitsmaßnahmen können Sie Ihr Sicherheitsteam unterstützen und bei der unternehmensweiten Entscheidungsfindung mitwirken.
Modernisierung	**Wie erreichen wir diese Ziele?**	**Aufbau eines Cyber Defense Centers**	Gehen Sie von einer „reaktiven", primär an Compliance-Vorgaben ausgerichteten Incident-Response-Strategie zu einem „proaktiven", zielgerichteten Sicherheitsprogramm über, das den Anforderungen Ihres Unternehmens gerecht wird.	Entwicklung und Verbesserung Ihrer Sicherheitsstrategie sowie der Fähigkeiten Ihres Computer Incident Response Teams (CIRT).

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)/
info@FireEye.com