Mandiant

Datasheet

Mandiant Retainer

Highlights

- Accelerate incident response times by contacting on-call expert incident investigators
- Transact flexibly with designated funds for services throughout the year
- Address changing priorities and plans without reworking contracts
- Easily add-on services when goals expand
- Access a team with varied skills and capabilities, not just an individual
- Upskill team members with relevant training
- Do all the above at a predictable cost

The incident response and cybersecurity experts you need, when you need them

Rethink your approach to acquiring cybersecurity expertise. Instead of using budget to hire a single expert for one role, you could have access to a team of cybersecurity experts with diverse skillsets.

The Mandiant Retainer is an annual subscription that helps extend your cyber defense capabilities and capacity by providing flexible access to a wide range of industry-leading security experts. The retainer provides you with flexible access to incident responders, consulting services, threat intelligence analysts, and training led by elite security practitioners.

Breaches happen. Respond confidently.

With the Mandiant Retainer, you will receive an incident response retainer with 2-hour response times, pre-negotiated incident response rates, and pre-established terms and conditions. This means that if a breach occurs, you can call Mandiant and we can begin the investigation immediately.

Plans change. We can change with you.

The retainer also includes pre-paid funds that can be used throughout the year to help you strengthen your cyber defense capabilities. They can be used for Mandiant consulting engagements, Mandiant Academy training, and for ad-hoc requests from alert investigations to malware analysis.

The best part is that as your priorities change throughout the year, you can access the services you need without having to rework contracts.

What you get

Incident Response Retainer

Call on Mandiant incident response experts to respond to active breaches and minimize the impact of an attack.

- Experts are on-call 24x7 in the event of a suspected breach
- Remote incident response support provided with 2-hour response times
- Breach investigation and response is delivered by Mandiant incident responders and malware analysis teams
- Terms and conditions are pre-defined before an incident occurs

Proactive services

Enhance your preparedness and security capabilities to provide resilience against compromise and see how your security program performs under pressure with simulated attacks against your environment.

- Redeem pre-paid funds to request investigations, education, intelligence and consulting services to extend and develop expertise, increase resilience, and validate defenses.
- Services are delivered by industry-leading Mandiant consultants and intelligence experts
- Services can be customized to meet your goals

Sample proactive services:

Cybersecurity readiness

- Penetration testing
- Cloud security assessments
- Tabletop exercises
- Red Team assessment
- CISO services

Education

- Inside the mind of an APT
- Malware analysis
- All access Mandiant Academy passes
- Mandiant Academy certifications

Threat intelligence

- Applied intelligence mentorship
- Dark web analysis
- Cyber threat profile

Ad-hoc requests

Engage Mandiant analysts to gain attacker insights, investigate alerts, and answer your toughest security questions, providing additional support in your day-to-day security operations.

Example ad-hoc requests:

- Actor/group attribution
- Interpretation of media events
- Domain and IP address intelligence
- Malware analysis
- Customer network traffic analysis
- Binary or domain hostility check
- Alert investigation
- Finished intelligence reports

Experienced specialists by your side

Mandiant responds to some of the world's largest breaches. We combine our frontline expertise and deep understanding of global attacker behavior to respond to incidents and help organizations prepare their cyber defenses against compromise.

Google Cloud

For more information visit
cloud.google.com