Mandiant

Datasheet

Mandiant SecOps Transformation Services

Benefits

- **Expertise:** Augment your team with access to world-class Mandiant cybersecurity experts
- **Threat visibility:** Improve and validate visibility and detection with guidance tailored to your needs
- **Validation:** Test your Google SecOps deployment and defenses
- **Prioritization:** Focus security efforts and track progress via custom target operating model development

Why Mandiant?

- **For over two decades**, Mandiant has served as a trusted advisor to thousands of organizations. We combine our frontline expertise and deep understanding of global attacker behavior to help organizations prepare and defend their cyber defenses against compromise.
- **Organizations worldwide** use our services to improve their security posture, gain a deeper understanding of threat activity, and assess their defenses against real threats

Integrate and optimize Google SecOps with Mandiant cyber defense experts

To enhance and modernize your security program, a robust technology platform is essential. You also need reliable visibility, advanced analytics, comprehensive training, and continuous feedback and validation of your cyber defenses.

Google SecOps is a highly scalable, cloud-native security operations platform and Mandiant experts can empower you to effectively realize its transformative potential and operationalize it in your organization.

Mandiant experts deliver personalized strategic guidance and program management using best practices to help you transform your cyber defense program with Google SecOps.

Mandiant SecOps transformation services offer:

- **Strategic guidance** on integrating Google SecOps into your organization, including target operating model (TOM) development assistance
- **Threat-driven strategies**, including visibility, detection, and automation roadmaps and guidance to shift to a more proactive posture
- **Evaluation** of your best-practice Google SecOps deployment via visibility and detection health checks and testing
- **Fast access to experts** in the event of a cyber incident via a Mandiant Retainer that includes 2-hour incident response times

Mandiant experts will work with your team, share best practices to guide and accelerate your security transformation. We'll help you plan, optimize, and validate your Google SecOps deployment ensuring you achieve its full potential.

Mandiant SecOps Validate

Define your threat visibility detection roadmap and validate your defenses

Gain confidence in your existing or planned Google SecOps deployments through guided validation and optimization of specific Google SecOps elements such as logging and detection best practices.

Mandiant develops a visibility and detection roadmap along with health checks to identify gaps and opportunities to help you achieve your security objectives. You receive a Mandiant Retainer with 2-hour incident response times for fast access to experts in the event of a cyber incident.

Mandiant SecOps Optimize

Optimize Google SecOps in the critical functions of your cyber defense

Improve your security posture by optimizing your visibility and detection strategy, developing a customized target operating model, and validating the effectiveness of your Google SecOps detections.

Mandiant delivers a target operating model that defines your organization's ideal future state, detailing how your people, processes, and technology will work together to achieve business objectives and maximize your Google SecOps investment. Guidance on detection and engineering methodology to reduce false positives and drive higher fidelity alerts is provided along with a threat profiling methodology to reduce risk. A Mandiant Retainer is included with 2-hour incident response times for fast access to experts in the event of a cyber incident

Mandiant SecOps Transform

Implement and optimize Google SecOps to truly transform your cyber defenses

Drive security operations maturity, transitioning your security posture from reactive to proactive with guidance and best practices for effective SOC transformation. Mandiant designs, develops and helps you implement a customized target operating model that optimizes your Google SecOps investment.

Mandiant builds an end-to-end transformation strategy and provides program management and operational support to guide and accelerate your transformation to a highly mature and proactive security posture. An embedded Mandiant cyber defense engineer helps optimize your continuous detection/continuous response (CD/CR) framework. Throughout, transformation program metrics and cyber defense metrics tracking is provided to measure outcomes and monitor progress against key milestones. A Mandiant Retainer is included with 2-hour incident response times for fast access to experts in the event of a cyber incident.

Mandiant SecOps transformation services and deliverables

Deliverables Included	Service Type		
	Validate	Optimize	Transform
Visibility and detection roadmap development	✓		
Visibility and detection healthcheck	✓		
Target operating model		✓	✓
Visibility, detection, and automation prioritization strategy and roadmap		✓	✓
Detection and engineering methodology guidance		✓	✓
Threat profiling methodology		✓	✓
Visibility and detection validation		✓	✓
End-to-end transformation strategy and support			✓
Program management and operational support			✓
Embedded Mandiant cyber defense engineer to help you optimize your continuous detection/continuous response (CD/CR) framework			✓
Ongoing transformation program metrics and cyber defense metrics tracking			✓
Continuous purple teaming to validate Google SecOps detections			✓
Incident Response Retainer with 2-hour incident response times	✓	✓	✓

At Mandiant, we're ready to support you, wherever you are in your security journey. Schedule a free consultation to discuss your specific security needs and how Mandiant can help you achieve your program goals.