Mandiant

Google Cloud Security

# Mandiant Cybersecurity Consulting Services

***The expertise you need, when you need it***

Today's threat landscape poses many business challenges from ransomware to insider threats to vulnerable supply chains. Organizations must go beyond technology solutions to evaluate their specific business threats and understand how to best strengthen their cyber defenses.

Mandiant leverages its hand-on experience with unparalleled threat intelligence and incident response to help organizations tackle their top security challenges. We help organizations defend against the latest threats and prepare to respond to compromise—ultimately building confidence and advancing their cyber defenses.

## The Mandiant Difference

Mandiant has been at the forefront of cyber security and threat intelligence since 2004. Our incident responders are on the frontlines of the world's most complex breaches. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques, and procedures.

Mandiant helps organizations quickly get back to business after a security breach and applies frontline expertise to guide effective threat detection, preparation, and to reduce business risk and build overall resiliency—before, during, and after an incident.

For more information visit **cloud.google.com/security/mandiant**

## Summary of Select Mandiant Services

| Security Function | Security Need | Services | Overview | Benefit |
|---|---|---|---|---|
| **Incident Response**<br>*Tackle breaches confidently* | Stop a breach | Incident Response Services | Activate the best-in-business experts to complete in-depth attack analysis, perform crisis management over the response timeline, and recover business operations after a breach. | Resolve critical security incidents and establish long-term solutions. |
| | Flexible proactive services | Mandiant Retainer | Pre-negotiated 2-hour response time and pre-paid funds available for investigation, education, intelligence, and consulting services. | Easily adapt to changing security priorities without reworking contracts. |
| | Put Mandiant on speed dial | Incident Response Retainer | Retain Mandiant experts with 2-hour response times to enable faster and more effective response to cyber incidents. | Reduce the impact of a cyber incident. |
| | Check for past and ongoing attacker presence | Compromise Assessment / Custom Threat Hunt | Hunt for past or present compromises of your environment, assess future risk of compromise based on your security hygiene, and improve your ability to respond. | Identify evidence of compromise to mitigate the impact of cyber threats and improve the overall security posture. |
| | Prepare to respond | Crisis Communications Planning and Response | Build an incident communications approach to protect stakeholders, minimize risk, and preserve brand reputation. | Align crisis communications with technical response activities and develop playbooks for incidents including disclosure requirements. |
| **Strategic Readiness** | Assess security controls and security posture | 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. |
| | Simulate real-world incident scenarios | Tabletop Exercise | Test your organization’s cyber incident response plan with scenario gameplay. | Quickly and efficiently identify gaps between documented process and actual response. |
| | Prepare for a ransomware attack | Ransomware Defense Assessment | Evaluate your ability to prevent, detect, contain, and remediate a ransomware attack. | Uncover strengths and weaknesses of your security controls and operations against ransomware. |
| | Assess inherited cyber risk | Cyber Security Due Diligence | Execute security due diligence on acquisitions, supply chain, and third-party integrations to uncover risks beyond your reach. | Identify business risk to improve security program capabilities and ensure combined security health and overall maturity alignment with remediation recommendations. |
| | Mature cyber defense capabilities | Cyber Defense Center Development | Design and grow a security operations program to defend against advanced threat actors. | Improve defense posture to reduce impact of security incidents, and build consensus on security improvements and resource prioritization. |
| | Evaluate risk | Cyber Risk Management Services | Evaluate your risk exposure for effective decision-making and risk mitigation by identifying risks most relevant to your organization and understanding the potential harm they pose to your business. | Advance your business approach to cyber risk management. |

| Security Function | Security Need | Services | Overview | Benefit |
|---|---|---|---|---|
| **Strategic Readiness** *(cont.)* | Integrated intelligence expertise | Advanced Intelligence Access | A dedicated intelligence expert embedded within your security team delivering bespoke research and analysis and guided intelligence implementation. | Accelerate decision-making and improve business agility to address threats and focus defenses, strengthening your cyber strategy and security posture. |
| | Targeted intelligence expertise | Essential Intelligence Access | Part-time intelligence experts collaborating remotely with your team to deliver personalized research and analysis. | Inform decision-making to address threats and focus defenses, strengthening your cyber strategy and security posture. |
| | Up-lift intelligence capabilities | Intelligence Program Development | Design and develop your organization's cyber threat intelligence capabilities and implement best-practices together with expert consultation. | Equip your organization with the essential skills and capabilities to achieve your CTI vision. |
| | Threat-informed defense | Threat Diagnostic | Telemetry-based analysis reveals the cyber threats targeting your organization, allowing effective threat prioritization and insights into how those threats are likely to impact you. | Reduce organizational risk by validating the effectiveness of your security controls and increase team efficiency by decreasing false positives. |
| | Upskill security staff | Mandiant Academy | Training to evolve your organization's security skills including instructor-led training, on demand training and certification programs. | Stay ahead of cyber criminals with skills training on the latest security techniques and threats. |
| **Secure AI** | Secure AI | Secure the Use of AI | Assess the architecture, training data defenses and applications built on AI models. | Identify and address security gaps to secure your AI systems. |
| | Assess and Verify AI controls | Red Teaming for AI | Identify and measure risks to AI systems deployed in production with attacks unique to AI services. | Test and assess the defenses you have in place to secure your AI systems. |
| | Use AI for Cyberdefense | Maximizing AI for Defenders | Operationalize the use of AI in the critical functions of cyber defense. | Utilize AI to enhance your cyber defenses. |
| **Technical Assurance** *Battle-test your security* | Verify controls and operations | Red Team, Purple Team Assessments | Test your security posture against the latest attacker tactics, techniques and procedures (TTPs) we see on the front lines of Incident Response. | Identify previously undetected weaknesses before an attacker does. |
| | Measure security control effectiveness | Penetration Testing | Assess how vulnerable your most critical assets are to cyber attacks. | Pinpoint and reduce vulnerabilities and misconfigurations in your security systems. |
| | Improve cloud security posture | Cloud Infrastructure Assessments | Improve cyber defenses through better cloud architecture and configurations. | Mitigate risk by reducing your cloud attack surface from common exploitation techniques. |
| | Verify configurations and posture | Active Directory Security Assessment | Mitigate the risk of Active Directory misconfigurations, process weaknesses and exploitation methods. | Reduce risk and impact of a security incident by hardening a common attack surface. |
| **Defend** | Supplement security operations | Managed Defense | An expert-driven 24x7 service that combines frontline experience with industry-leading technology and intelligence. | Comprehensive protection from advanced and emerging threats. |
| | Managed threat hunting | Mandiant Hunt | Continual managed threat hunting using the latest adversary techniques. | Uncover hidden threats and reduce the potential impact of an incident. |