Mandiant

Solution Brief

AI Security Consulting Portfolio

As organizations increasingly deploy AI, they must ensure its security and compliance with company policies. Simultaneously, security teams seek to leverage AI to improve cyber defenses, but often don't know where to start. Mandiant experts can help your organization utilize AI to enhance cyber defenses while helping safeguard AI systems.

Assess the security of the entire AI pipeline.

Test the controls protecting your AI systems.

Increase the effectiveness of your defenders with AI.

Secure your AI systems and harness the power of AI for defense

Securing AI Services:

Assess the architecture, roles and controls, data defenses, and applications built on AI models to identify configuration hardening opportunities.

Our consulting services include an AI security assessment, threat modeling (informed by Google Threat Intelligence), hardening recommendations based on Google's extensive experience protecting both our own AI systems and third-party technologies, and threat hunt missions. Mandiant experts can also perform a crown jewels assessment, deliver data protection governance guidance, and AI application reviews.

- **AI governance framework:** Guidance on risk-based AI governance, aligned with the NIST AI Risk Management Framework **(AI RMF)**, Google Secure AI Framework **(SAIF)**, and **ISO/IEC 42001**. Includes development of a specialized risk assessment matrix for concise insights on the risks associated with new AI initiatives.
- **AI preparedness:** Ensures your AI applications launch into a secure environment with a pre-deployment environment security review. We help you identify and address any vulnerabilities in the hosting infrastructure before deployment with a focus on protecting your crown jewels.
- **AI security assessment:** Assess the security of AI applications being developed or in production. We rapidly pinpoint security deficiencies in the hosting infrastructure, understanding that these directly affect the overall security posture of your AI applications.

A gap analysis is performed over the following domains:

- Governance for AI and roles and responsibilities relative to AI development
- Architecture of AI applications (including IaaC)
- Controls
- Data security—examples include:
  - Training data
  - Metadata
  - Weights
  - Configuration data

- **AI threat model:** Comprehensively identify threats related to applications either in development or in production. We develop AI threat modeling, leveraging MITRE ATLAS, OWASP Top 10, and Mandiant GAIA.
- **Security and detection for AI:** Guidance on preparing your SOC to monitor and respond to AI applications. Includes incident response playbooks for AI applications (platform agnostic).

Red Teaming for AI:
Validate the defenses protecting AI systems

Mandiant Consulting helps organizations identify and measure risks to applications built with generative AI models by performing attacks unique to AI services. These AI red team assessments enable you to understand and test how effective your controls are in protecting you from security risks posed by agentic services and information retrieval applications.

- **Emulated real-world attacks:** Leverage the experience of Mandiant red team experts who apply the latest attacks unique to AI services seen on the frontlines and informed by Google's internal AI red team research.
- **Categorize attack surface:** Understand what a determined attacker could achieve by examining capabilities exposed through your application's AI interface.
- **Test controls:** Determine if the controls protecting your AI systems, sensitive data and crown jewels are effective against threats surfaced in Google Threat Intelligence and internal Google threat research.
- **Assess detection and response readiness:** Analyze your security team's ability to detect and respond to an active attack involving AI systems in a controlled environment.
- **Mitigation and defense recommendations:** Based on the assessment, receive practical recommendations for securing applications and data.

Maximizing AI for defenders:
Operationalize the use of AI in the critical functions of cyber defense.

Mandiant Consulting helps organizations understand how to augment their cyber defense capabilities through the use of AI. This can include leveraging AI that is built into security products such as Google Threat Intelligence, along with using standalone gen AI.

- **Reduce the toil on defenders performing repetitive tasks:** Integrate AI into processes and procedures to allow investigations to run more efficiently.
- **Improve threat detection:** Create AI-based detections and analytics to swiftly identify and contain initial infections.
- **Strengthen your team's skills:** Build cyber defense capabilities through hands-on incident response practice using AI in Mandiant's *ThreatSpace*, virtual range environment.
- **Accelerate security validation:** Generate scripts in seconds to rapidly test your cyber defenses.
- **Enhance threat hunting:** Utilize AI to develop industry-tailored threat hunt hypotheses.
- **Support new defenders:** Provide configuration changes for newer defenders or for those unfamiliar with specific security tools.

The Mandiant AI Security Consulting Portfolio provides expertise and guidance to both safeguard your AI investments and to leverage AI to strengthen defenses.

Our consultants guide you on how to safely employ AI to streamline security operations, enhance investigative capabilities, cultivate skilled cyber defense teams, and more.

Learn more: https://cloud.google.com/security/solutions/mandiant-ai-consulting