Mandiant

SOLUTION BRIEF

AI Security Consulting Portfolio

Mandiant experts can help organizations utilize AI to enhance cyber defenses while helping safeguard the use of 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 your defenders.

As organizations deploy AI, it's critical to ensure that it is being secured and company policies are being applied to its use. Additionally, security teams are looking to use AI to improve their cyber defenses, but don't always know how to use AI to protect their organizations against cyber attacks.

Securing the use of AI: Assess the architecture, data defenses, and applications built on AI models.

Mandiant Consulting helps organizations identify opportunities to harden configurations of their AI systems. These consulting services include an AI Security Assessment, Threat Modeling drawn from Google Threat Intelligence, hardening recommendations based on Google's extensive experience protecting our own AI systems as well as other third-party technologies, and threat hunt missions.The Mandiant experts can also perform crown jewels assessment, guidance on data protection governance, and AI application reviews.

- Evaluate the end-to-end security of an AI implementation guided by the Google Secure AI Framework (SAIF).
- Assess the safeguards around training data and data protection governance.
- Review the security of custom applications built on AI models to identify weaknesses before attackers do.

Red Teaming for AI: Validate the defenses protecting AI systems

Mandiant Consulting helps organizations identify and measure risks to generative AI models deployed in production by performing attacks unique to AI services and against applications that rely on AI.

- Leverage the experience of Google red teamers and Mandiant experts applying the latest attacks seen on the frontlines.
- Determine if the controls protecting AI systems are effective against threats surfaced in Google Threat Intelligence.
- Assess a security team's ability to detect and respond to an active attack involving AI systems in a controlled environment.

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 by integrating AI into processes and procedures to allow investigations to run more efficiently.
- Create AI-based detections and analytics to identify and contain initial infections.
- Develop cyber defense talent by practicing incident response efforts using AI to respond to an attack via Mandiant's virtual environment, the ThreatSpace cyber range.

Mandiant's specialized consulting services have become an indispensable partner in safeguarding your digital assets. The Mandiant AI Security Consulting Portfolio provides guidance to both protect AI investments and leverage AI to strengthen their defenses. By addressing the unique risks AI systems present, Mandiant helps organizations implement robust security measures for AI systems and data. Furthermore, their expertise guides organizations on safely employing AI to streamline security operations, enhance investigative capabilities, and cultivate skilled cyber defense teams.