praetorian

DATA SHEET

LLM Attacks Chains

KEY BENEFITS

Focus on the risks that truly matter

Tailor the most appropriate technological or process-based mitigation

Assess the strength of these defenses against real-world attacks

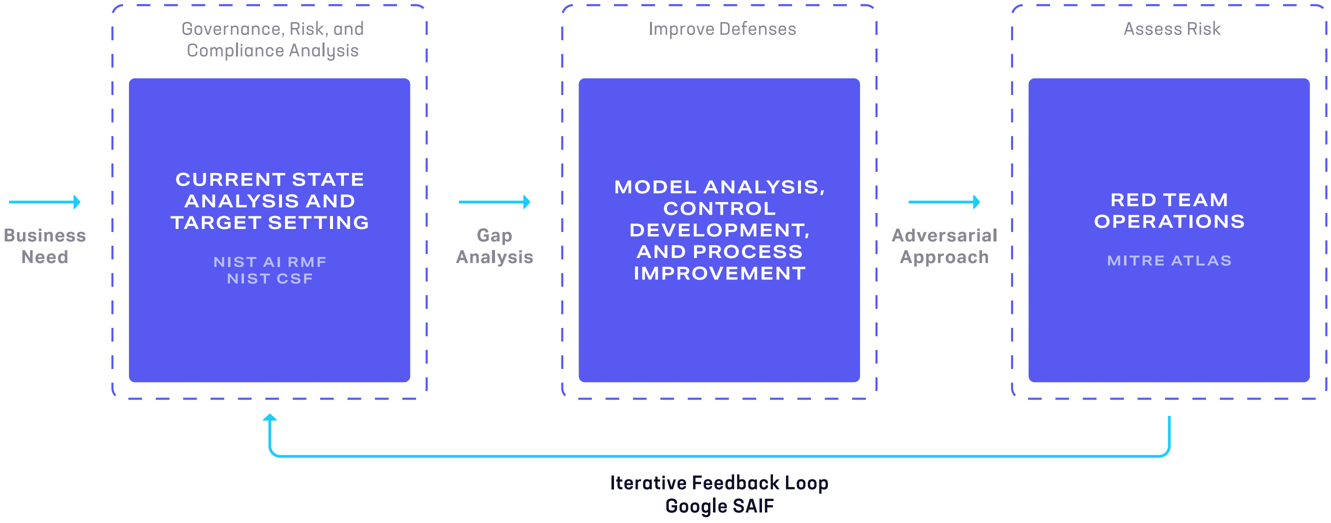
YOUR CHALLENGE

Your enterprise uses artificial intelligence and machine learning systems to transform your products and services. This can introduce supply chain risk from third party AI products, additional regulatory requirements around the use of PII in training data, and another level of complexity to your security program as a whole. You need a partner with a cross-functional team to help you solve crucial problems related to risk management, security, privacy, and compliance.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian's proprietary assessment methodology leverages industry-standard frameworks and in-house adversarial expertise to:

- Understand the most salient risks associated with an organization's use of AI and ML
- Develop technical and process-based controls to solve these problems
- Test the efficacy of these controls using our industry-leading offensive security team
- Establish feedback loops between red team/blue team operations that permit fast iteration on security controls



OUR SOLUTION: CAPABILITIES OVERVIEW (CONT'D)

Our methodology begins with a risk management approach to AI threats. Praetorian's Governance, Risk, and Compliance experts use the NIST AI Risk Management Framework and NIST Cybersecurity Framework to analyze the organization's current state and identify gaps that pose crucial threats. We then develop a bespoke threat model that accounts for the most salient risks and outlines the mitigations we recommend. Our team then helps develop the security controls and model enhancements that close the most critical gaps. Our final step is to engage in targeted red team testing wherein we use the MITRE ATLAS framework to assess the efficacy of these controls and recommend improvements.

The partnership permits repeated iterations of control development and testing over the entire secure software development lifecycle.

WHY PRAETORIAN

Praetorian has assembled a cross-functional team of enterprise architects, ML research scientists, DevOps engineers, and red team operators. Following the Google Secure AI Framework, we have based our approach on the principle that a team with diverse skillsets can better identify issues, improve defenses, and emulate real-world scenarios.

WHO NEEDS THIS SERVICE

- **Complex enterprises** developing novel uses of AI technology
- **Risk owners** anticipating regulatory scrutiny around the use of PII
- **Product owners** developing AI models with a robust security posture
- **Organizational leaders** who need a formal AI security program

SPECIFIC SERVICE OFFERINGS

- Enterprise-level NIST CSF assessment
- AI-specific NIST AI RMF assessment
- Development of bespoke model-based security controls
- Development of an AI-specific threat model
- Targeted red team testing

DELIVERABLES

Risk Management Exercise:

- Current state
- Target state
- Gap analysis

Defensive Improvement Exercise:

- Technical security controls
- Process design documentation

Adversarial Operations:

- Assessment report including findings, steps to reproduce, and recommendations for improvement

Praetorian
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive cyber security company whose mission is to prevent breaches before they occur. We help our customers minimize the likelihood of compromise by using an adversarial perspective to uncover material risks the same way attackers do.