ataccama

Statement on AI, Vulnerability Management, and Emerging Threats

C1 - Public document

Ataccama recognizes that AI is accelerating both the discovery of software vulnerabilities and the speed at which they are exploited, and that adversaries increasingly rely on automated, AI-driven techniques. We have adapted our security program to this reality - hardening how we build our products, using AI to strengthen our own defenses, and governing our use of AI responsibly.

Governing our use of AI

Our use of AI, including in software development, is governed by an AI governance program aligned with recognized frameworks such as the NIST AI Risk Management Framework. AI-generated code is subject to mandatory human review, and a cross-functional governance body oversees the responsible adoption of AI across the company. We have assessed our obligations under the EU AI Act, our vendor due diligence considers the AI capabilities and risks of the services we rely on, and all staff complete mandatory training on responsible AI use.

Using AI to strengthen security

We apply AI-enabled capabilities across our secure software development lifecycle and security operations - including in threat modeling, code and application security testing, vulnerability analysis, and incident investigation. These capabilities complement, and do not replace, our established practices and human oversight: people review and approve security-relevant decisions and changes. As the threat landscape accelerates, we have correspondingly accelerated detection, triage, and patching for critical, actively exploited issues.

Our vulnerability management program includes:

- Secure software development practices
- Automated and AI-assisted security testing
- Software composition and dependency analysis
- Infrastructure vulnerability scanning
- Penetration testing
- Controlled release management

We assess whether vulnerabilities are applicable to Ataccama products or services and prioritize remediation based on severity, exploitability, exposure, and business impact. For Ataccama-managed services, security updates are handled through standard operational, change, and release processes. Where customer-managed, private-cloud, hybrid, or local components are affected, we provide relevant guidance, mitigations, or patch information based on severity and applicability. Critical, actively exploitable, or high-impact issues are addressed through expedited mitigation, patching, or emergency change processes; other findings are remediated through planned release and maintenance cycles.

We remain committed to transparent, risk-based communication with customers regarding material security issues, required customer actions, and remediation timelines. Customers requiring detail on our AI security and governance controls can request our full controls statement under NDA. For more information, please reach out to your Customer Success Manager.