Plex AI Security FAQs

Last updated 05/10/2024

Q: How is my data being protected?

A: All interactions among system components, including AI, are secured through encrypted channels utilizing TLS 1.2. Within your PlexTrac instance, all AI components utilize PlexTrac's RBA system to guarantee appropriate access controls. This ensures that client, reports, and classification requests adhere to configured access controls, thereby maintaining security and integrity when utilizing generative components.

Q: What kind of security testing was completed?

A: PlexTrac's security team performed testing of the embedded solution for AI-related vulnerabilities including but not limited to:

- *Prompt injection (direct and indirect)*
- *Model poisoning*
- *Model theft*
- *Insecure response encoding*
- *Sensitive data leaks*
- *Cross client/tenant authorization bypasses*

Q: What data sources are utilized to train the AI model?

A: PlexTrac's AI model is trained using open source cybersecurity and vulnerability data. This includes but is not limited to:

- *CVE Data*
- *Cyber Threat Intelligence Feeds*
- *GitHub Top 100*
- *Open source penetration testing datasets*

Q: When I submit something, what happens to the data?

A: The solution's current model operates in a pre-trained capacity. The system and underlying components do not currently learn over time or retain user submissions beyond the requirement to process the submission and provide a generative response.

Q: Is my data being used to train your AI?

A: No. The solution does not currently learn over time based on user submissions. Any model updates or additional training is performed by PlexTrac's team in a controlled environment separate from production systems. Once complete, these sort of updates are applied tocustomer-facing AI systems to ensure all relevant training data remains as up-to-date as possible.

Q: Will my data be mixed with other companies' data?

A: No. The AI system is configured to keep your data private just like your PlexTrac instance. The solution does not utilize a shared or "customer trained" model in order to prevent mixture or cross-contamination of data within the AI component.

Q: Can I opt out of having AI turned on in my PlexTrac instance?

A: If AI is included in your PlexTrac plan, you may choose to keep the AI feature turned off by not enabling the license in your tenancy.

Q: Does the AI component interact with or depend on third-party systems such as Open AI?

A: No. Plex AI utilizes its own proprietary implementation, independent of OpenAI or other third-party systems. We use TLS encryption to ensure all data communication is protected and confined within PlexTrac's cloud environment, providing a dependable and secure experience without reliance on external platforms.

Q: What if I have additional security concerns that are not answered here?

A: If you are an existing PlexTrac customer, you can reach out to PlexTrac's security team to have any questions answered. Inquiries can be directed to *security@plextrac.com.*