Frequently Asked Questions (FAQs) for SecureGen AI

June 19, 2025

What is SecureGen AI?

SecureGen AI is a network intrusion detection system that combines signature-based detection using Suricata with anomaly-based detection powered by machine learning. It leverages federated learning for collaborative, privacy-preserving model training.

How does SecureGen AI work?

The Service captures network packets and uses Suricata for signature-based detection of known threats. Benign packets are analyzed using machine learning models trained via federated learning to detect anomalies. Detected anomalies generate new rules for future detection, enhancing adaptability.

What are the benefits of using SecureGen AI?

- **Enhanced Accuracy:** Combines signature and anomaly-based detection for improved threat detection.
- **Privacy Preservation:** Uses federated learning and encryption to keep data local.
- **Adaptability:** Continuously updates rules to address new threats.

How is my data protected?

Your raw network data remains local. Only encrypted model parameters are shared for federated learning, secured with CKKS homomorphic encryption and verified using Halo2 zero-knowledge proofs.

Can I use SecureGen AI for my organization?

Yes, SecureGen AI is designed for organizations seeking advanced network security with privacy compliance. Contact our sales team at huzaifamateen426@gmail.com for deployment options.

What datasets are used for training the model?

The model is trained on standardized datasets, including UNSW-NB15, Bot-IoT, ToN-IoT, and CSE-CIC-IDS2018, converted to NetFlow-based feature sets.

How often is the model updated?

The model is updated periodically through federated learning rounds, incorporating new data from participating organizations to enhance detection capabilities.

Is SecureGen AI compliant with data protection regulations?

Yes, the Service is designed to comply with regulations like GDPR by ensuring raw data stays local and using privacy-preserving techniques.

How do I get started with SecureGen AI?

Contact our sales team at huzaifamateen426@gmail.com to discuss deployment options, including cloud-based or on-premise solutions, and subscription plans.

Who can I contact for support?

For technical support, reach out to our support team at huzaifamateen426@gmail.com.