Members:
Hameed Ullah – 211086
Furqan Rafique – 211106
Hassan Imam – 212074
Supervisor: Mr. Hilmand Khan

Balancing Security and Privacy in SIEM Logs

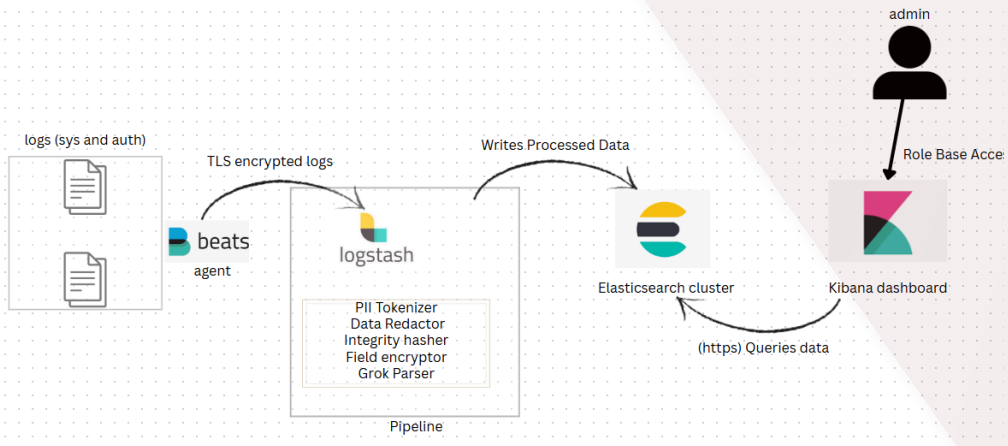
Problem Statement

SIEM systems handle sensitive logs that often contain PII. Traditional systems lack built-in privacy controls, making them vulnerable to data breaches and non-compliance with data protection laws like GDPR and CCPA.

Proposed Solution

We designed a secure, privacy-aware SIEM pipeline using the ELK Stack. It applies encryption, tokenization, and role-based access to protect log integrity and confidentiality while supporting real-time threat monitoring.

System Architecture



Key Features / Results

- Tokenization of IPs and usernames (SHA-256)
- TLS-encrypted pipelines (end-to-end)
- Role-based access in Kibana
- Privacy-focused dashboards
- Real-time performance maintained

Tools & Technologies Used

- Filebeat
- Logstash
- Elasticsearch
- Kibana
- Ubuntu
- TLS, SHA-256

Future Scope and Commercial Potential

Can be adapted for healthcare, finance, or government sectors. Future integration with SOAR tools and AI-based anomaly detection is planned.

QR Code

Contact

Email: hamafr77@gmail.com
LinkedIn: https://pk.linkedin.com/in/hameed-ullah-9423a91b5