Deployment of AI Solutions

In-Class Case Study 1

Ahmad Iqbal, Muhammad Hasan Zaheer,

Basant Singh, Mohammed Anas

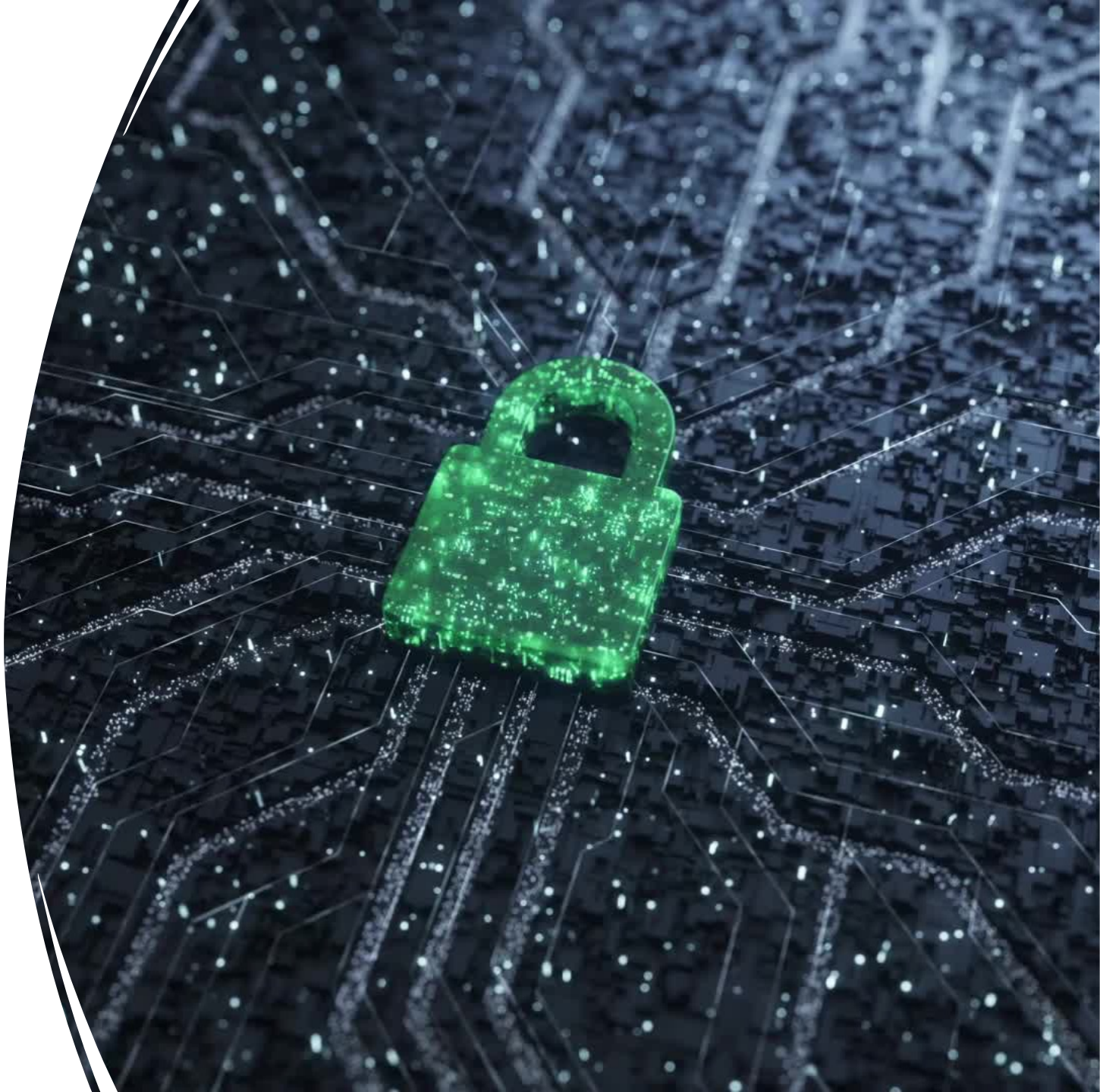
Secure Trust Bank

Secure Trust Bank is a British retail and commercial banking business founded in 1952 that is listed on the London Stock Exchange.

Secure Trust Bank's robust security measures were breached, potentially exposing client information despite their strong detection systems and encryption methods.

Problem Background

- Experienced hackers targeted Secure Bank, exploiting a previously unknown vulnerability in their web application, gaining unauthorized access to consumer accounts and attempting unauthorized transactions.



Action on attack

- Secure Bank's security staff faced challenges in identifying the sophisticated attack due to complex strategies employed by the hackers, making it difficult to detect subtle patterns and anomalies indicating a persistent compromise

Application of ML

Secure Bank partnered with a top data science company to develop a machine learning-driven anomaly detection solution, enhancing their security capabilities.

By leveraging historical customer transaction data, Secure Bank trained a machine-learning model to identify fraudulent behavior by establishing a baseline of common trends and actions associated with honest consumer interactions.

Solution

1

Secure Bank used real-time transaction data to continuously analyze suspicious activity through their machine learning system, incorporating various variables and external fraud indicators.

2

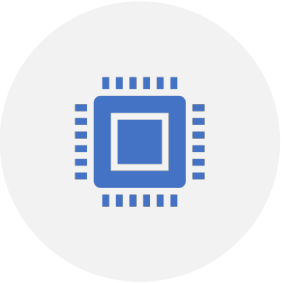
Following implementation, the machine learning system alerted Secure Bank's security team to a potentially fraudulent transaction with anomalous traits, triggering investigation.

3

In response to the alert, the security team promptly initiated incident response procedures, freezing the affected account and investigating further. The machine learning system detected similar patterns across multiple accounts, indicating a coordinated attack.

Fraudulent patterns found using ML

Anomaly Detection: ML algorithms learned normal behavior from historical network traffic data to detect anomalies and potential security threats in real-time.



Behavior-based Detection: ML algorithms identified patterns associated with various attacks, enabling the system to detect and block unknown threats like malware infections, DDoS attacks, and unauthorized access attempts.

Real-time Response: ML-based IDS systems provided real-time alerts, empowering security teams to respond swiftly and efficiently to mitigate potential threats and optimize resource allocation.

Adaptive Learning: ML models adapted and improved over time, learning from new data to stay effective against emerging attack techniques and evolving threats.

Machine Learning Contribution

The security team collaborated with the data science company to refine the machine learning model, leveraging investigation results for improved accuracy and reduced false positives

Secure Bank increased investment in advanced machine learning algorithms and continuous monitoring systems, recognizing the need to enhance security measures beyond traditional approaches.

Secure Bank's machine learning-based security solution became a robust defense against cyberattacks, consistently detecting and preventing fraudulent activity, setting a new industry standard for banking security.

Conclusion

ML implementation in the IDS improved security by detecting undetectable attacks, reducing MTTD and MTTR, and lowering false positive rates.

ML-based IDS enhanced threat detection and safeguarded critical systems and data from cyber threats.

References

- https://owasp.org/www-project-securebank/
- https://www.securetrustbank.com/