NXLog

CUSTOMER CASE STUDY

NXLog enables autonomous security log collection for QNB Finansbank

NXLog enables autonomous security log collection for QNB Finansbank

QNB Finansbank — founded on October 26, 1987, as Finansbank A.Ş and became the first private bank that went public in Turkey. In June 2016, Finansbank A.Ş was acquired by Qatar National Bank S.A.Q (QNB Group), the largest bank in Qatar, the leading financial institution in the Middle East and Africa region. QNB Group provides services in more than 1,100 locations with its network of over 4,300 ATMs.

In 2023 net profit reached TRY 33 billion 172 million. As of December 31, 2023 total number of branches are 436 with 11,756 employees.

RELATED INDUSTRIES

- Consumer Banking
- SME/SMB Banking
- Corporate Banking
- Private Banking
- e-Finance

BUSINESS DEMAND

Enable cybersecurity and operations monitoring for better security posture and robustness.

CHALLENGE

Establish unified log collection pipeline to get events from various sources including thousands of ATMs from branch offices. Process events on agents and filter out excessive data to decrease load on SIEM. Route logs both to security systems and general purpose data lake.

SOLUTION

- NXLog Enterprise Edition

BUSINESS RESULTS

- Unified and autonomous log collection pipeline has been built.
- Security posture improved with broader log collection coverage.
- Operations team is able to leverage logs data in the data lake.

BACKGROUND

According to IBM, the average cost of a data breach reached an all-time high of USD $4.45 million in 2023 worldwide. This represents a 2.3% increase from the 2022 cost of USD $4.35 million and, taking a long-term view, the average cost has increased 15.3% from USD $3.86 million in the 2020.

Along with healthcare, the financial industry sits at the top of the list with an average cost of USD $5.90 million per data breach, while the mean time to identify and contain breaches reached 277 days. It's worth mentioning that breaches identified by an organization's own security teams and tools are significantly less expensive, costing nearly USD $1 million less than incidents disclosed by the attacking parties.

To decrease the mean time to detecting a breach, implementing security log management is a must. According to research, the impact of 27 factors on the mean cost of a data breach had been identified, and half of cost mitigators rely heavily on log collection, including SIEM/SOAR, DevSecOps, incident response, threat hunting, and AI/machine learning–driven insights.

Establishing a robust log collection pipeline is crucial for any financial organization — especially one with a continuously growing infrastructure, where a large attack surface both for internal and external threat actors is exposed.

IBTech, founded by QNB Finansbank, is in charge of the full cycle of R&D, infrastructure management and maintenance for QNB Finansbank and its subsidiaries, including cybersecurity.

CHALLENGES & SOLUTION

In order to maintain a comprehensive and consistent defense-in-depth, IBTech's security team has to collect logs across hundreds of QNB Finansbank branches and across many different endpoints like office computers, servers, and network equipment. In the case of QNB, each endpoint produces a diverse set of log types including Windows, macOS and Linux operating system logs, application logs, anti-virus events, EDR logs, PowerShell logs, Sysmon logs, and others required for real-time and on-demand analysis.

QNB Finansbank operates a large ATM network consisting of thousands of cash dispensers from various vendors, all with different software generating important security log data. As a vital part of business operations, their ATM network must be entirely covered by log collection.

According to their security policy, all valuable log data has to be continuously collected, properly filtered (to avoid over-flooding at network and storage levels), normalized according to specific schemas, and sent out to multiple destinations both for security (SIEM, UEBA, etc.) and operation analysis (general purpose data lake). Typically, many different tools are required to achieve proper log collection from disparate sources. In large infrastructure environments, it makes the process very complicated and introduces many points of failure. In order to simplify, streamline, and make log acquisition a robust process, building a unified and autonomous log collection pipeline is required.

NXLog Enterprise Edition has been chosen among other tools due to its versatility, powerful data transformation features, and wide range of integration options. NXLog Enterprise Edition was successfully deployed across the whole infrastructure to more than 15,000 endpoints in just a matter of weeks, and then integrated with SIEM solution smoothly.

IBTech's security team employed a hybrid log collection strategy with both NXLog Enterprise Edition agents installed on endpoints locally and deployed on the network to serve as a remote log collectors. In both cases, a heavy data filtration policy has been applied that helps ensure only required data is ingested into security systems, like SIEM and UEBA, and improve the overall performance of their security operations.

RESULTS

A unified, autonomous log collection pipeline was successfully implemented with NXLog Enterprise Edition. Data is collected from disparate log sources with proper data filtrations and transformations. NXLog Enterprise Edition agents feed both security tools and the operations team's data lake by routing the event stream accordingly. The log collection pipeline powered by NXLog Enterprise Edition requires minimal efforts on maintenance, cutting costs significantly and increasing the overall robustness.

"The whole log collection pipeline becomes powerful and easy to maintain with NXLog. We appreciate NXLog's configurability and its advanced log processing engine. It allows us to filter out up to 80% of the events right on the endpoints and feed security systems with only those data that make sense for security operations," says **Ahmet Uygut, Expert Architect, Ibtech-Security Incident Management And Monitoring**

"One of the main challenges for us was to enable log collection from branch offices and ATM network. NXLog provides us with numerous options to integrate with heterogeneous data sources and helped to create both flexible and robust log collection architecture to support security and operations team."

SOLUTIONS

NXLog

Enterprise Edition
Manager
Add-Ons

REQUEST A FREE TRIAL

For more information on NXLog visit our **website**, checkout our **integrations' page** or **schedule a meeting** with one of our representatives

Contact us: nxlog.co

Youtube LinkedIn Twitter