Business challenge

To better detect potential data threats and facilitate compliance with rigid industry mandates, Unibank Commercial Bank Open Joint-Stock Co. needed to enhance its existing security systems.

Transformation

Banks house a lot of valuable information, and cybercriminals know it. To protect against breaches, Unibank engaged IBM Business Partner ScienceSoft to implement IBM® QRadar® SIEM software, gaining the ability to detect threats 15 times faster while facilitating compliance.

Alex Nivin
Security Solutions Leader
IBM Business Partner ScienceSoft

Results

Detects threats and suspicious behavior 15x faster
with real-time analysis of log data and network flows

Reduced false positives from 50 million to zero
by fine-tuning the system to filter out white noise

Saves up to 30% of security administrative time
using automated tools to detectdeviations and improve system performance

Unibank Commercial Bank Open Joint-Stock Co.

Detecting threats 15 times faster with a security intelligence platform

Headquartered in Baku, Azerbaijan, Unibank is one of the country's largest private banks, operating a network of more than 30 branches and 30 ATM end points. For nearly 950,000 private and retail customers, it offers a broad range of banking products and services, including savings deposits, credit and debit cards, consumer loans, mortgages, direct debit facilities, foreign currency products, derivative products, consulting and finance leasing activities. Unibank was founded in 2002 as the result of the merger of two private commercial banks: Mbank and Promtekhbank.

"If a bank is smart, it deploys the number one security system in the world: IBM QRadar. It's the best enterprise-grade solution for all industries and sectors."

—Alex Nivin, Security Solutions Leader, IBM Business Partner ScienceSoft

Share this

Defending against data breach attacks

According to the *2018 Cost of Data Breach Study: Global Overview* report released by IBM Security and Ponemon Institute, the average total cost of a data breach is equivalent to USD 3.86 million. What's more, it took organizations 196 days on average to detect them. Although the direct costs related to detecting, containing and remediating an attack can be high, the indirect costs—diminished customer trust, reputational damage and potential regulatory action—can be catastrophic.

Financial organizations are a primary target for attack because their information holds such tremendous value for cybercriminals. "The consequences of a breach can ruin your reputation and destroy your business," says Alex Nivin, Security Solutions Leader at ScienceSoft, which provides security operations and response expertise. "Today we need to focus on both offensive and defensive strategies when it comes to protecting assets."

Unibank holds more than AZN 3.5 billion in assets. "And yet," Nivin continues, "like all banks, one of its most important assets is information—everything from card numbers to employee data. All of this needs to be tracked, monitored and protected. The data is at risk all the time from both outside and inside sources."

The banking sector is also one of the most highly regulated, with the Payment Card Industry Data Security Standard (PCI DSS) among the most rigid. The mandate protects credit card holders' data and sets requirements for any organization that collects, processes, stores or transmits cardholder data.

"One of the PCI DSS requirements is that banks must track and monitor all access to network resources and cardholder data," says Nivin."Unibank processes three billion security events per month.They needed a system that could better protect their private and corporate clients.

"But they also wanted a solution that was fully compliant with PCI DSS. And that's QRadar. So Unibank reached out to us."

Gaining world-class threat protection

To provide Unibank with log monitoring and real-time visibility for threat protection, ScienceSoft designed and deployed an enterprise-grade, fully compliant SIEM system based on a suite of IBM QRadar SIEM software. The solution applies built-in analytics and custom correlation rules to detect threats, enabling the bank to spot anomalies, collect specific audit events and generate targeted reports for compliance mandates.

ScienceSoft also implemented the software's built-in IBM QRadar Risk Manager and IBM QRadar Vulnerability Manager offerings, which systematically scan assets for susceptibilities and assess network device configuration risks.

"If a bank is smart, it deploys the number one security system in the world: IBM QRadar," says Nivin. "It's the best enterprise-grade solution for all industries and sectors."

To assess the overall health, fine-tune and optimize the performance of its SIEM system, Unibank is also using a trial version of QLean technology, an IBM Validated Solution developed by ScienceSoft. "QLean is our own proprietary application," says Nivin. "About half a million lines of code went into it, and it gets its data from almost 50 different data sources within QRadar."

ScienceSoft rolled out the project in stages, starting with an evaluation of the bank's needs. "Every project starts with a requirements phase," says Nivin. "We gathered all of the needs and pain points and then designed the architecture based on the size of the network and total assets under protection. Science Soft deployed the IBM QRadar SIEM system in less than one week with 2,500 EPS [events per second] and provided its out-of-the-box configuration."

In stage 2, ScienceSoft's security consultants connected more than 50 log sources and assets in the bank's network to the platform. This included a set of firewalls, an intrusion detection system (IDS) and an intrusion prevention system (IPS) and a central authentication system. "What we do is protect the whole infrastructure," adds Nivin.

Stage 3 focused on fine-tuning the solution by building a network hierarchy, creating user role security profiles, configuring backup and restore and other procedures. "After you connect every log source in the network to the platform, you start fine-tuning—setting up and configuring those log sources for efficient work," explains Nivin.

During stage 4, ScienceSoft developed custom rules. "We developed and implemented over 100 different custom correlation rules, such as if a board member tries to access individual account information," remarks Nivin. "Why would a board member be looking at accounts? That's suspicious. It raises a flag. Within QRadar, we build modules to investigate offenses like that."

For the final stage of the project, ScienceSoft conducted four days of advanced training, during which the bank's security team investigated reported offenses on the bank's new QRadar technology-based platform. "A problem with the industry is that there's a huge skills shortage; people lack training and don't know how to use the tools," says Nivin. "They see something they think is an offense but when they go in and identify it, it's not an offense at all. So they end up skipping real offenses because they're tracking false positives.

"That's where we come in. Our solutions help remove white noise, false positives. Plus we make certain that the leaders and staff are educated and trained.

Detecting real threats faster, amidst the noise

Today, Unibank has a custom SIEM system that better secures its assets with around-the-clock, real-time advanced persistent threat (APT) protection and insider threat detection while meeting the requirements of PCI DSS for effective log monitoring. As the infrastructure expands, Unibank's security personnel preconfigures all newly commissioned servers, devices and applications with security policies and audit baselines for the SIEM solution, easing audit data analysis.

"Unibank didn't really have an enterprise-grade system before," adds Nivin. "We went in and implemented the best system in the world. It meets all of the requirements of the bank and its shareholders. QRadar is number one for a reason: it's a world-class system."

In fact, Nivin estimates that Unibank can detect threats at least 15 times faster now—an efficiency gain of 1,500 percent. During the fine-tuning phase, ScienceSoft reduced the number of unrecognized and unknown events from 50 million per week to zero.

"We built the whole system from scratch and fine-tuned it, making certain that an offense is an offense," says Nivin. "When the system fires an offense—an incident flagged by those correlation rules—it shows on the dashboard. White noise doesn't even show up on the dashboard."

The QLean tool helps Unibank save time and money by proactively detecting operational deviations and improving SIEM performance and maintenance. "There's a lot of raw data but it's very hard to get out," explains Nivin. "What we do is automate those analyses and metrics and use dashboards to visualize it. So QLean saves up to 30 percent of security administrators' time on a daily basis, not just when they're investigating offenses. That translates into a real dollar value."

Moving forward, Unibank continues to work with ScienceSoft to integrate additional business applications with the SIEM systems and develop and integrate customer-specific threat cases.

"There are many other phases of this project, so our work is ongoing," concludes Nivin. "The client is very satisfied with the SIEM deployment. They know they're working with the leaders—IBM in partnership with us, we in partnership with IBM. A lot of business came to us as a result of this one implementation, so we're very pleased."

Solution components

- IBM® QRadar® SIEM
- IBM QRadar Risk Manager
- IBM QRadar Vulnerability Manager
- ScienceSoft

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

About ScienceSoft

Headquartered in Texas in the US and with an office in Vantaa, Finland, IBM Business Partner ScienceSoft provides IT consulting services and custom software development to large and midsize companies in the healthcare, banking, retail and telecom industries, among others. The company's areas of expertise include customer relationship management, data analysis, collaboration and knowledge management, and information security. Customers include Walmart Inc., Nestlé S.A, eBay Inc and T-Mobile US, Inc. ScienceSoft was founded in 1989 and employs more than 500 IT professionals worldwide.

Please Recycle

89021989USEN-00