opentext™ | Cybersecurity

Case Study

National Bank of Georgia

ArcSight streamlines and automates security operations, resulting in significant time savings and full compliance.

Who is National Bank of Georgia?

Price stability and efficient monetary policy are the ultimate objectives of the National Bank of Georgia. It uses inflation forecasts and general in-house designed macroeconomic models of the Georgian economy to achieve these goals. The National Bank of Georgia ensures the stability and transparency of the financial system and promotes sustainable economic growth while maintaining price stability.

"The ArcSight SOAR capabilities are one of the most important features when we think about Micro Focus CyberRes. We estimate that SOAR will give us the equivalent of an additional headcount. Considering how hard it is in Georgia to recruit quality cyber security staff, this is a major benefit for us."

Nino Simonishvili
Head of Cyber Security
National Bank of Georgia

Compliance with International Standards Requires Sophisticated SIEM

One of the bank's roles is to monitor payment transaction activities in the Georgian commercial banks. Business-critical applications are in use with constant real-time data exchange between the commercial banks and the national bank.

Nino Simonishvili, Head of Cyber Security with National Bank of Georgia, explains further: "Cyber security is a relatively new area in Georgia. As a result, we have a small team and need to work as effectively as we can. Compliance with international standards requires us to document and parse our security event logs accurately. Log parsing is the process of splitting data into chunks of information that are easier to manipulate and store. When we started looking into providers that could help it was clear we needed a Security Information and Event Management (SIEM) solution to simplify our log management. We compared ArcSight Enterprise Security Manager (ESM) by OpenText with market alternatives and were impressed with ArcSight's log parsing capabilities. Combined with a more cost-effective and flexible licensing model than other vendors we evaluated, this made the decision easy for us."

საქართველოს ეროვნული ბანკი
National Bank of Georgia

At a Glance

Industry

Finance

Location

Georgia

Challenge

Comply with reporting and security log parsing regulations while managing cyber security resource constraints

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Security Orchestration Automation and Response (SOAR)

Success Highlights

- 3 hours per day current time saving
- Effective security log parsing
- Full Standard compliance
- Cost-effective and flexible licensing model

> **"Every day we would spend up to three hours to manually identify and block malicious IP addresses. ArcSight has automated this process and reports back to us every 12 hours with a list of blocked IP addresses."**

Nino Simonishvili
Head of Cyber Security
National Bank of Georgia

Connect with Us
www.opentext.com

Local Expertise Resulted in Significant Time Saving through Automation

Local OpenText™ CyberSecurity experts worked with Nino and the team to implement ArcSight. "We cannot stress enough how important it is to have local support," comments Nino. "Any questions we had were answered swiftly and, when necessary, we could meet to sort out any issues. When I compare that with other vendors where we could sometimes wait for weeks to get feedback, I realize how helpful the local presence was for us. In fact, having a local presence is now included as a key factor in our procurement process for any future vendor relationships."

ArcSight ESM was implemented with mainly out-of-the-box functionality, focused on automating manual activities, and providing the team with a real-time overview and visibility into its security status. Security-focused visualizations help National Bank of Georgia to quickly identify threats, with insights into top threat intelligence alerts, targeted nodes, risky websites, MITRE Tactics, Active Lists, and much more. Although the implementation is still developing, with new data sources added regularly, the benefits are already clear to Nino: "Every day we would spend up to three hours to manually identify and block malicious IP addresses. ArcSight has automated this process and reports back to us every 12 hours with a list of blocked IP addresses. We all know that a human manual process is fallible and the ArcSight detection skills are far superior, so we feel safe in the knowledge that any threats are rapidly responded to."

ArcSight SOAR Promises Timely Action Against Cyber Threats

National Bank of Georgia is very interested in ArcSight Security Orchestration Automation and Response (SOAR) by OpenText and its potential to further automate security operations. ArcSight SOAR's automated orchestration helps automate all time-consuming, mundane work, prioritize incidents, and take timely action against cyber threats. "We estimate that SOAR will give us the equivalent of an additional headcount. Considering how hard it is in Georgia to recruit quality cyber security staff, this is a major benefit for us."

She concludes: "Many of our commercial bank partners look to us as an example of a cyber security framework. We are pleased that ArcSight has given us a sophisticated security operations model to support our compliance with standards and automate and streamline our threat hunting and vulnerability management. We look forward to continuing this journey with Micro Focus CyberRes and expanding our cyber security capabilities with ArcSight."

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.