Security Intelligence Solutions and Services for Banking and Financial Services
ScienceSoft is an **IT service and software development company** headquartered in McKinney, TX, with offices in Europe and the Middle East.

- **Key Facts**
  - ISO 27001: Proven approach to customers' data safety
  - 18 years in Security, 16 years in Banking
  - 700 employees
  - ISO-27001-proven approach to customers' data safety
Our Clients
Security Challenges for Banking

A subject to wide regulatory oversight

The richest source of personal consumer data and monetary assets

Disparate internal users across numerous channels and applications

Strong compliance need

Top target for cybercrime

Place for internal fraud

Validate and comply with SOX, PCI, and GLBA incidents

Protect sensitive data and limit costs associated with a breach

Detect fraudulent activity among thousands of users
Fraudulent Activities Pointed at Banks

- Malicious access to confidential data
- Payment card fraud
- Money laundering
- ATM fraud
- Call-center fraud, banking service center fraud (with participation of banks employees)
Our Services

- Security Information and Event Management (SIEM)
- Identity and Access Management
- Penetration testing
SIEM Services

1. SIEM consulting
2. SIEM implementation
3. Support services
4. Migration to QRadar
QRadar Security Intelligence for Banking

- **Automate regulatory compliance** (PCI-DSS, GLBA) with collection, correlation and reporting
- **Full visibility** of network, application and user activity
- **Anti-fraud** solution
- Continuous **collection of log data** across all bank locations and channels
- **Real-time intelligent analysis** of collected security events
- **Deliver a manageable set** of prioritized security threats
- Highly-scalable long-term **data retention** for forensic investigations and reports
We identify over 40 fraud patterns through the monitoring of:

- Payment card hijacking
- Unauthorized software running on ATM
- Transaction from one payer to several accounts in different locations, and backwards
- Over-the-limit transactions
- PAN key entries
- Unsuccessful authentication access, user activity outside office hours
- Repeated payments, etc.
SIEM Consulting

Detection of **insider** and **external threats**

Selection of essential **log sources**

Full technical **assessment** of the existing **IT environment**

Validation of **critical security components**

---

Detailed **recommendations** on all aspects of the architecture

---

**QRadar workshops and trainings**
SIEM Integration

We integrate QRadar with the Customer’s devices and applications using:

- **Out-of-the-box** log source extensions
- **Custom** log source extensions

We have developed **over 100 custom LSXs**
We develop LSXs to collect information from extensive data sources:

- Security devices and applications
- Configuration info
- Server activity
- Network activity
- Online activity
- Data activity
- Application activity
- User activity

We perform deep analysis to create correlation rules:

- Event correlation
- Activity baselining & anomaly detection
- Fine-tuning

You get actionable and accurate security insight

Fraud detection

True offense

Suspected incidents
Support Services

IBM-certified consultants

- IBM Certified Associate
  Security Qradar
- IBM Certified Deployment Professional
  Security QRadar

24/7 support services

Remotely or on-site
Proof of Concept

For the visual argument in favor of our SIEM solution we are delighted to offer a free proof of concept demonstration. With an open POC you can:

1. Develop a sampling of the system and try real user interface
2. Review event correlation and connect your specific event sources
3. Exercise response management process and reports
4. Work through specific banking challenges and evaluate real attack
What You Get

Data collection from **all possible sources**

- Banking **fraud protection**
- Distinguishability between **true threats** and false alarms
- **Automation** that allows you to better monitor, analyze and act
- **Retention** and **compliance** capabilities
- **Time to value** - ability to get up quickly in your environment
- **Monitoring** of all bank locations and infrastructure (data centers, branch offices, ATMs, online infrastructure, call centers, etc.)

- **One-console security** and unmatched **scalability**
- **Ease of use** and ongoing **ease of maintenance**
Why ScienceSoft

- **Silver level accreditation** in IBM Security QRadar SIEM
- IBM-certified **SIEM consultants**
- **Comprehensive expertise** in SIEM implementation
- Experience in **Banking IT**
- **Deep knowledge** of the QRadar architecture
- **Carrying out** of 100% projects
- **Customers’ convenience** as a core aim
Identity and Access Management

- Automated management of user identities
- Role-based access management
- Secure access to web, mobile and cloud applications
- Protection of sensitive enterprise data
- User activity monitoring
Penetration Testing

We test:

- Network services
- Web applications
- Remote access
- Client side
- Employee behavior *

* Social engineering testing
IBM SIEM Solution for Eurasian Bank

Customer:
Eurasian Bank, a universal commercial Kazakhstan bank with over 850,000 customers and $3.6 bn in assets

Solution:
High-level tuning of an IBM QRadar SIEM solution. ScienceSoft developed custom LSXs to integrate log data from 12 business apps and created 94 correlation rules for threat cases across 5 critical apps

Tools & Technologies:
IBM Security QRadar SIEM, Python, Regex, Linux Shell
IBM SIEM Configuration for a Middle East Bank

Customer

An international bank with headquarters in Middle East, operation centers in EMEA and $11+ bn in assets

Solution

ScienceSoft reviewed the QRadar’s initial deployment, created the Customer’s network hierarchy, configured out-of-the-box features and developed custom LSXs to fix security vulnerabilities

Tools & Technologies

IBM Security QRadar SIEM, QRadar API, Python, Regex, PostgreSQL, Linux, Shell
IBM SIEM Solution for Home Credit Bank

Customer

A branch of the international holding Home Credit B.V. with 44 offices and over 3100 sales outlets across the country

Solution

Deployment and high-level tuning of an IBM security QRadar SIEM solution. ScienceSoft developed 10 LSXs to integrate the Customer’s applications and a set of 60 correlation rules

Tools & Technologies

IBM Security QRadar SIEM, Python, Regex, Linux Shell
Penetration Testing for a Payment Services Company

**Customer**
A North American provider of services and products for financial institutions with offices in more than 30 cities across US and Canada

**Solution**
ScienceSoft performed black box penetration testing of the Customer's website and webserver in an extremely short timeframe of just one week and revealed the most critical vulnerabilities

**Tools & Technologies**
Nmap, sqlmap, metasploit, OpenVAS, w3af, BurpSuite, fierce, manual testing
Let’s Keep in Touch!

<table>
<thead>
<tr>
<th>The United States</th>
<th>Europe</th>
<th>The Nordics</th>
<th>Gulf Cooperation Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters</td>
<td>Latvia</td>
<td>Finland</td>
<td>The UAE</td>
</tr>
<tr>
<td>+1 214 306 68 37</td>
<td>+371 2569 2767</td>
<td>+358 92 316 30 70</td>
<td>+971 585 73 84 33</td>
</tr>
<tr>
<td><a href="mailto:contact@scnsoft.com">contact@scnsoft.com</a></td>
<td><a href="mailto:eu@scnsoft.com">eu@scnsoft.com</a></td>
<td><a href="mailto:nordics@scnsoft.com">nordics@scnsoft.com</a></td>
<td><a href="mailto:gulf@scnsoft.com">gulf@scnsoft.com</a></td>
</tr>
</tbody>
</table>