Security Intelligence Solutions and Services
Key Facts

18 years in Security, 32 years in IT consulting

700 employees

150+ projects in Security consulting

ScienceSoft is an IBM Silver Business Partner that has been working in the Security Intelligence area since 2003 and has over 150 information security projects behind its belt
Our Customers in Security

- IBM
- Robert Half
- NASA JPL
- The Housing Bank for Trade & Finance
- RBC Royal Bank
- M&T Bank
- Alfa-Bank
- Eurasian Bank
- tieto
- TELEKOM AUSTRIA GROUP
Industry Competencies

- Banking
- Telecom
- Healthcare

- Retail
- Oil & Gas
- Public Sector
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
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 Implementation

Solution **integration**

Correlation rule **creation**

Solution **deployment**

Solution **configuration**
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**
Correlation Rule Creation

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

Offense identification

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
Identity and Access Management

Full-cycle IAM services:

- Consulting
- Deployment and configuration
- Maintenance and support
- Migration
Identity and Access Management

Automated management of user identities

Role-based access management

User activity monitoring

Protection of sensitive enterprise data

Secure access to web, mobile and cloud applications
Penetration Testing

We test:

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

* Social engineering testing
Success Story

IBM SIEM Solution for a 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
Success Story

TSIEM for a Healthcare Organization

Customer

A large US healthcare organization with more than 4,000 employees

Solution

SIEM solution to collect information from 5 healthcare applications and convert it for further processing (as much as 700,000 medical transaction events per day)

Tools & Technologies

TSIEM, DB2, WAS, TDI, VMWare, GSL, GML, GEM, W7, GVS, RegExp, SQL, Batch, Shell, Python

www.scnsoft.com © 2021 ScienceSoft ®
IAM Solution for a Public Organization

Customer

A governmental organization

Solution

Custom solution for role-based access control to manage access rights of thousands of employees according to their job roles

Tools & Technologies

IBM Security Identity Manager
Success Story

Penetration Testing for a Mobile Operator

Customer

Mobile operator with over 5 mln subscribers and almost 2,000 employees

Solution

ScienceSoft assessed the Customer’s security level (5 selected public web applications and 5 selected elements of the network perimeter) and revealed serious vulnerabilities

Tools & Technologies

Acunetix, Burp Suite, Immunity Debugger, Metasploit, Nmap, OpenVAS, Skipfish, sqlmap, XSpider, w3af, Wfuzz, ZAProxy
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>