RAZ-LEE

AUTHORITY INSPECTOR

Minimizing Threats Posed by Excessive User Authorities

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world’s leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee’s flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies’ technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva

IBM

McAfee™

Akamai

RSA®

SEA™ SOFTWARE ENGINEERING OF AMERICA

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

Authority Inspector

Minimizing Threats Posed by Excessive User Authorities

Excessive User Authorities

Sometimes IT Managers needs to provide a user enough rights to carry out a unique assignment that his security level rights normally doesn’t allow him to accomplish it.

- This leads to an excessive amount of Users with High Authority, which leads to a major risk, because usually this Authorities aren't disallowed over time.

- The iSecurity Authority Inspector is installed on a PC while processing data pulled off the IBM i. And identifies this security breaches.

Authority Distribution Strategies

There are various methods to confine authorities:

- Adopted authority
- Authorization lists
- Group Profiles

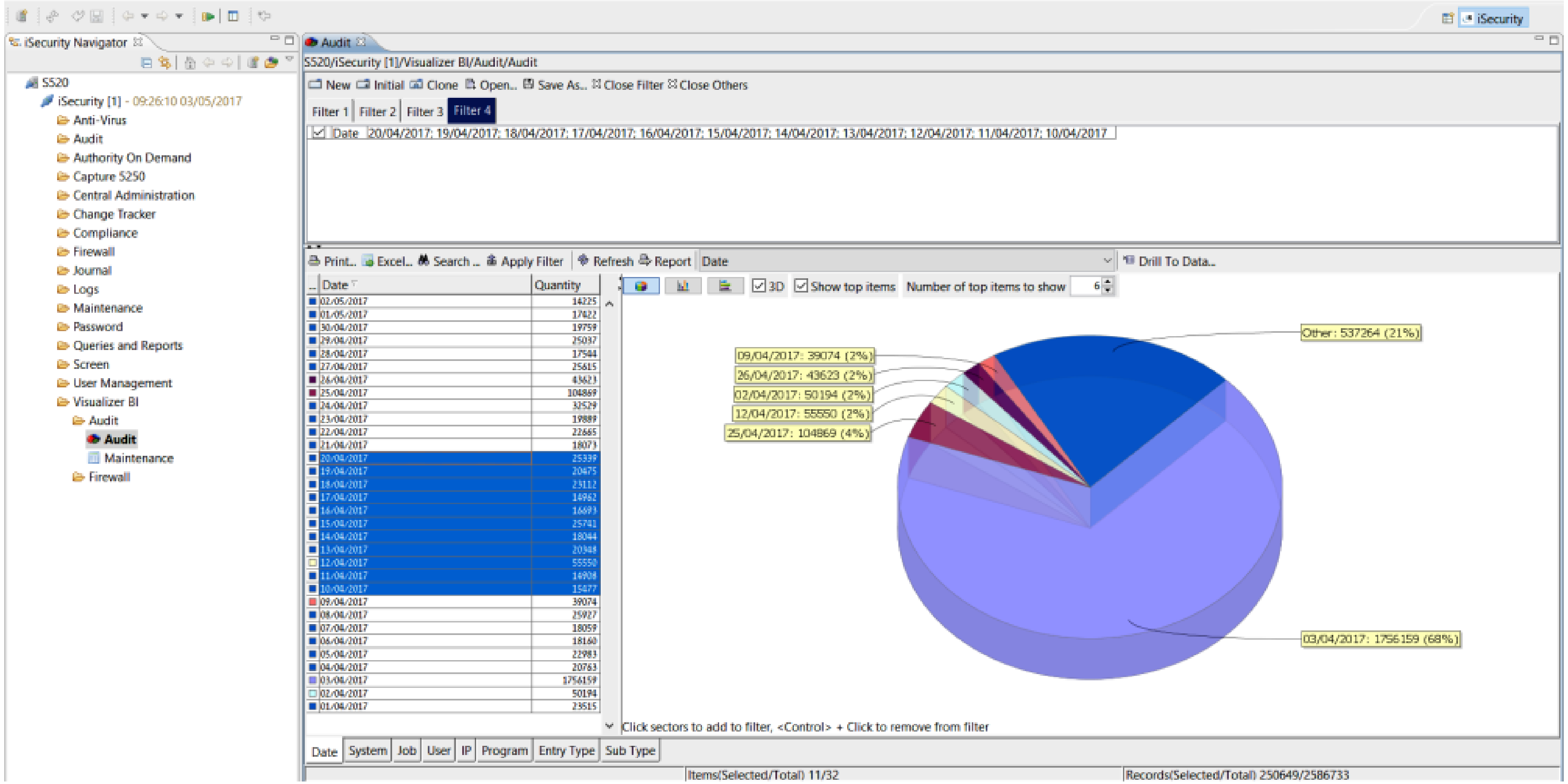
The Authority Inspector supports the user regardless of the specific method in use.

It enables comparison of utilized authority versus the required ones, and supports selection of the method.

Also provides information on the minimal authority to be given at each stage and the frequency of testing authorities.

Minimizing Threats by Excessive User Authorities

Works with IBM's Authority Collection data. It reads, summarizes and analyzes the data and presents it, with the analysis results, in graphs and tables. In some cases, the Authority Inspector presents the data in a more meaningful way to ease understanding.



S520/iSecurity [1]/Visualizer BI/Audit/Audit

☑ Date 20/04/2017; 19/04/2017; 18/04/2017; 17/04/2017; 16/04/2017; 15/04/2017; 14/04/2017; 13/04/2017; 12/04/2017; 11/04/2017; 10/04/2017

Date ▾

	Date	Quantity
■	02/05/2017	14225
■	01/05/2017	17422
■	30/04/2017	19759
■	29/04/2017	25037
■	28/04/2017	17544
■	27/04/2017	25615
■	26/04/2017	43623
■	25/04/2017	104869
■	24/04/2017	32529
■	23/04/2017	19889
■	22/04/2017	22665
■	21/04/2017	18073
■	20/04/2017	25339
■	19/04/2017	20475
■	18/04/2017	23112
■	17/04/2017	14962
■	16/04/2017	16693
■	15/04/2017	25741
■	14/04/2017	18044
■	13/04/2017	20348
□	12/04/2017	55550
■	11/04/2017	14908
■	10/04/2017	15477
■	09/04/2017	39074
■	08/04/2017	25927
■	07/04/2017	18059
■	06/04/2017	18160
■	05/04/2017	22983
■	04/04/2017	20763
■	03/04/2017	1756159
□	02/04/2017	50194
■	01/04/2017	23515

Click sectors to add to filter, <Control> + Click to remove from filter

Items(Selected/Total) 11/32

Records(Selected/Total) 250649/2586733

Authority Collection Commands

Authority Collection commands, introduced in OS400 Ver. 7.3

- Start Authority Collection (STRAUTCOL)
- End Authority Collection (ENDAUTCOL)
- Delete Authority Collection (DLTAUTCOL)

Are used to collect authority data during program run.

Now that authority data is available, Authority Inspector may be used to turn it into valuable information assisting the users in the mission of minimizing threats posed by excessive authorities.

iSecurity Authority Inspector Advantages

- Runs on a PC that processes data from the IBM i
- Automatically summarizes and analyzes the data
- Graphical User Interface
- Easy to use for non IBM i Users
- Advanced Filtering options to get accurate reports

RAZ-LEE

Thank You

For more information about our company and products please visit

www.razlee.com