**SBA2**
**Secure Business Austria 2**
**Programme: COMET – Competence Centers for Excellent Technologies**
**Programme line: K1-Centres**
**COMET subproject, duration and type of project:**
**Systems & Software Security, 04/2014 – 03/2017, multi-firm**

## Data Cube: Nessus-Based Vulnerability Analysis

Vulnerability management includes repetitive scanning and analyzing of the gathered data and is therefore a cumbersome task. Various stakeholders demand different views on the data. SBA Research analyzed the requirements of each group and designed a data cube model to provide customized vulnerability information for each group. Hereby, the focus is on dynamic and customizable report generation. Our software covers the full stack – scanning, data collection, extract-transform-load (ETL) and reporting.

### Dynamic Nessus Reporting

Vulnerability Management contains the evaluation and presentation of recurring system and network scans (Nessus). Based on these reports further countermeasures are decided. Nessus scans are usually executed automatically and repetitively during a defined observation period. Various stakeholders analyze the collected data to assess the quality and security of their systems. However, Nessus does not provide suitable reports for all stakeholders. A CISO for instance needs shorthand views on the system, whereas a system administrator demands detailed information. SBA Research developed a software where Nessus scans are imported and further processed by state-of-the-art business intelligence systems. Sensitive data is provided and security in all areas is essential.

The first milestone of our research focused on data gathering from the Nessus API. Administrators configure Nessus metadata and data imports using a web application. A REST-client crawls the reports from the Nessus server and persists relevant information. The crawled data is fed into the extract-transform-load (ETL) process and finally stored in a data cube.

Users access the cube data via Excel Power Pivot. They have full flexibility and can build their own reports and aggregates. Additionally we provide templates for common use cases. The cube is flexible enough to analyze single Nessus scans or compare Nessus scans over time to observe the development of a system's quality. Future work may include automatic incident alerting based on user configurations and a pattern matching.
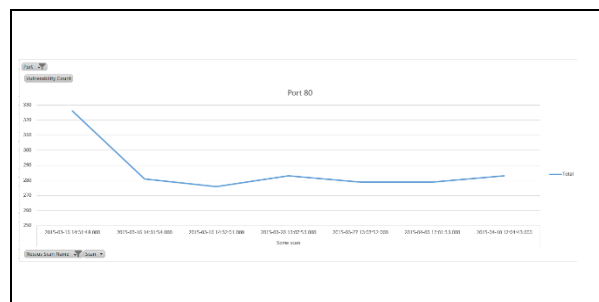


**Fig. 1: Report generated by Cube (Number of port 80 vulnerabilities over time)**

## Impact and effects

The developed software provides a flexible application for Nessus reporting capable of addressing various stakeholders. As a main benefit, users can analyze data with information filtered according to their business requirements. Another benefit is the central storage of dedicated Nessus reports which would otherwise be distributed on numerous Nessus instances and accounts.

**Contact and information**
K1-Centre SBA2

SBA Research gGmbH
Favoritenstr. 16, 1040 Vienna
T +43 1 505 36 88
E mklemen@sba-research.org, www.sba-research.org

**Project coordinator**
Mag. Markus Klemen

**Project partners**

| Organisation | Country |
| --- | --- |
| Anovis it-services and trading GmbH | Austria |
| ISCP GmbH | Austria |
| Raiffeisen Informatik GmbH | Austria |
| SEC Consult Unternehmensberatung GmbH | Austria |