

Data Analysis and Visualization Services

September 2011

Service Summary

- **Log Analysis and Visualization Workshops:** Custom trainings in the areas of log analysis; from data collection and processing to SIEM architectures. Visualization principles, concepts, tools, and libraries, best practices and security use-cases. All accompanied by hands-on exercises.
- **Data Analysis and Visualization:** Analysis of customer provided data sets and producing visual representations.
- **Data Visualization Development:** This service covers custom tools based on dynamic queries and linked views, as well as real-time dashboards.
- **Data Collection Architecture:** Defining an infrastructure that supports a customer's data analysis use-cases. Data routing, filtering, aggregation, and data source configurations are part of the engagement.
- **Data Analysis Processes:** Data analysis tasks need to be repeated periodically. We architect those processes to turn data into tangible actions.
- **Dashboard Development:** Implementation of a custom dashboard for customer defined metrics.
- **Forensic Investigation:** We assist in a forensic investigation to document the path of abuse and the data flows.
- **Compliance:** We define a data collection architecture and analysis processes for applicable regulations and mandates. Visualization is used as a key component to making all of the data accessible and actionable.
- **SIEM Application Development:** We help you build content for your SIEM or log management solution based on your exact use-cases.

Detailed Service Descriptions

Log Analysis and Visualization Workshops

These workshops can be tailored to the needs of the customer. Customized to the needs of, for example developers, security analysts, or managers. On the log analysis side, we cover anything from data sources to data processing. Log management tools and SIEMs, what are the differences, strengths, weaknesses. Education for developers on how to write effective log records. The data visualization parts cover anything from visualization theory with perception, how to generate meaningful and easy to read charts. It covers the different types of charts and graphs that can be used and when to use them. A number of visualization tools and libraries are introduced and hands-on exercises will deepen the knowledge. A number of security visualization examples then show how these principles work in the real world. From perimeter threat analysis to compliance and insider threat visualization.

Data Analysis and Visualization

Our core competency lies in the in-depth understanding of IT data and how to turn it into actionable visual representations. The customer provides a data set that needs to be visualized. We will work with the customer to understand the use-cases and then develop a visual representation of the data that is suited for the task at hand. The customer will be given the tools to repeat this process on the same type of data at any later point in time.

Data Visualization Development

The knowledge and experience with IT data puts us into unique position to deliver custom-built visualization tools. Many use-cases demand the development of custom tools that support, for example dynamic queries or linked views.

Data Collection Architecture

Data analysis and visualization requires readily available data. Ideally all the data is centrally collected. However, the data is rarely generated at one location. It is therefore necessary to define a collection architecture that brings the data from possibly remote location into once central repository. In addition, applications and devices need to be configured to output the necessary messages for the use-cases at hand.

This service focuses on the definition of use-cases together with the customer. Based on the use-cases, we will identify the data source necessary to address them. This will result in a recommendation for the configuration of various applications and devices in the environment. The next step is to define a *data collection architecture* to centrally collect all of this data. Data routing and filtering, as well as bandwidth and storage estimations are part of this engagement.

The customer will be left with a detailed plan on how to implement a data collection architecture.

Data Analysis Processes

Data centralization and accessibility is the first step to turn knowledge into actionable results. This service defines processes, roles, and assigns responsibilities in order to turn the collected data into tangible actions. The service starts with an inventory of the available data and an assessment of the data collection architecture. The next step is the definition of use-cases. They will be the basis for the processes developed. The service delivers data flow processes to address the use-cases. What data is collected where, who is looking at the data and how, what tools are they using, what are the escalation paths, how is data triaged and how is it prioritized? For each of the use-cases we will then also define, together with the customer, what the correct responses are. The final processes are heavily focused on knowledge capture and repeatability. This will help ensure that knowledge from working with the tools is captured and made available to other users of the processes.

Dashboard development

Dashboards are a common way of visualizing either real-time data or regular snapshots of a data set. We will define the use-cases with the customer, define the personas that need insight into a specific process or environment, and then develop the dashboard and data adaptors to continuously update the dashboard. Often this involves the definition of metrics. Those metrics are then displayed in the dashboard. We will identify metrics with the customer. The dashboard is also designed together with the customer. The engagement can include the data acquisition, centralization, normalization, and processing. The dashboard is implemented in a Web interface to visualize the metrics identified and address the use-cases.

Forensic Investigation

We will assist in a forensic investigation to document the path of abuse and the data flows. This generally involves social network analysis via email and IM logs, Web access analysis, document tracking, and traffic flow analysis. All of these tasks are supported by visuals to ease the investigation, as well as to document it in an easy consumable way.

Compliance

All of the compliance mandates, such as federal ones (Sarbanes Oxley (SOX), Federal Information System Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA)) and industry mandates, such as the Payment Card Industry (PCI) digital security standard (DSS) have specific requirements with regards to data collection (often called logging) and data analysis. We help making sense of the regulations and will work with the customer to identify regulatory important data sources. We define the data collection architecture, define retention policies, and security requirements. We then define analysis processes that address the regulations at minimal cost. Visualization plays a key role in unlocking the information contained in the data and providing a cost-effective solution.

SIEM Application Development

None of the SIEM or log management products will just work in your environment out of the box. Configuration and fine tuning is needed to make the product know about your environment and policies, as well as processes. We will help you gather your policies, define processes, and implement them in your SIEM or log management product.