Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation

Ferda Özdemir Sönmez
CyDeS Cyber Defence and Security Laboratory
Department of Information Systems,
Informatics Institute
Middle East Technical University
Ankara, Turkey
ferdaozdemir@gmail.com

Banu Günel
CyDeS Cyber Defence and Security Laboratory
Department of Information Systems,
Informatics Institute
Middle East Technical University
Ankara, Turkey
bgunel@metu.edu.tr

***Abstract*—Security Information and Event Management Systems (SIEM) are generally very complex systems encapsulating a large number of functions with different behaviors. Visualization is a common way of data presentation in these systems along with other data presentation ways such as reporting, alerting, text messaging. However, generation of the visualization has different steps. If the data is in a custom format, rather than a predefined format which either obeys a standard or a known file structure, the generation of custom visualizations may not be straightforward. Evaluation information for these tools related to custom visualization generation capabilities may be useful for better decision making. This information can be used while designing visualizations through SIEM systems or purchasing the most useful SIEM system for an organization. In this study, six well-known SIEM systems are evaluated through a common scenario created by the authors to check custom visualization generation capabilities. The contributions include this unique scenario and the advantages and disadvantages regarding various steps of the provided scenario along with the difficulties experienced by the authors during the installation and configuration of these SIEM systems.**

Keywords—Security Information and Event Management, SIEM, Visualization, Splunk, AlienVault, Event Log Analyzer, Gartner, ArcSight, Rapid7

I. Introduction

Security Information and Event Management (SIEM) systems [1] is the current trend for the examination of big data related to cybersecurity or information security. The rapid evolution of big data technologies and the existence of a considerable amount of data sources resulted in the development of many SIEM systems.

SIEM systems commonly include the tasks of data collection, data aggregation, data normalization, event correlation, reporting, and alerting. A few of the SIEM systems have capabilities to give information related to compliance with well-known security standards.

Visualization is one efficient way of data analysis which may aim [2] data summary, comparison of values across groups, displaying connections/ relationships between variables, showing hierarchical or part to whole structures, illustrating change over time, and exhibiting data patterns.

SIEM systems commonly include built-in visualizations as part of reporting tasks. These visualizations ordinarily happen to be in dashboard formats. Some of the SIEM systems also allow visualization of custom data. Thus, the visualization capabilities of custom-made security visualization dashboard designs are commonly compared to other security-related dashboard designs prepared by using business intelligence (BI) tools such as Tableau [3] or dashboard designs encapsulated in the SIEM tools.

All three groups of tools have specific characteristics and pros and cons. Thus, lack of detailed examination of custom visualization generation capabilities of SIEM tools results in incorrect or missing perceptions. For instance, the capabilities of custom security visualization systems designed in dashboard format are perceived as lower than they are because they do not have other common SIEM features. Another example is the unnecessarily increasing expectations for the capabilities of designing custom visualizations using custom data in SIEM systems which may compete with visualization focused tools.

These drawbacks are the results of unique features served by business intelligence tools, custom-made security visualization solutions, and the SIEM tools. Some examples of these incomparable features are:

- advanced interactivity through drag and drop type of user actions for visualization generation and a large number of display types which exist commonly in visualization focused tools and BI tools,
- correlation analyses, easy enterprise integration, a large number of use-cases, and advanced data collection features which commonly exist in the SIEM tools,
- data or use-case specific design details which may exist in custom-made security visualization studies.

SIEM systems have many comparable features which may be used during the evaluation of these systems, such as the number of platforms supported, scalability, latency, number of built-in metrics, number of built-in dashboards, number of integration ways with third-party tools. In this paper, the evaluation is limited to current capabilities related to the generation of custom visualizations using popular SIEM systems.

978-1-7281-0472-0/18/$31.00 ©2018 IEEE

Since the ability to use the SIEM tools and achieving the correct results may be related to the experience and knowledge of the users, before starting the evaluation, it should be stated that the authors have more experience in business intelligence (BI) tools (specifically Tableau [3]) and visualization tools compared to SIEM systems. They are at an equal distance to all the SIEM systems and did not have formal education for any of them.

The rest of this paper is structured as follows. In Section 2, the methodology of the study will be described. Section 3 includes the results of the study. Section 4 and Section 5 are the discussion and the conclusions sections.

II. Methodology

A. *Selecting the SIEM Systems to be Evaluated*

Gartner Report 2017 [4] divided the SIEM products into four quadrants as shown in Figure 1; Leaders: IBM Q1 Labs [4], LogRhytm [5], Splunk [6], McAfee [7], Challengers: Micro Focus ArcSight [8], Dell RSA [9], Visionaries: Rapid7 [10], Exabeam [11], Securonix [12], and Niche Players: AlienVault [13], Micro Focus NetIQ [14], FireEye [15], FortiNet [16], VenusTech [17], Trustwave [18], EventTracker [19]. SolarWinds [20], ManageEngine [21], BlackStratus [22]. This categorization is based on two factors: the ability to execute and the completeness of vision. The ability to execute includes product/service properties, overall viability, sales execution and pricing, market responsiveness and record, market execution, customer experience, and operations factors. The completeness of vision includes market understanding, marketing strategy, sales strategy, product offering strategy, business model, vertical/industry strategy, innovation, and geographic strategy factors. See Gartner report for further explanation of the quadrants.

Due to limited time, and non-existence of trial versions for some SIEM systems, the authors decided to select one or two systems from each quadrant based on the count of systems in each quadrant.

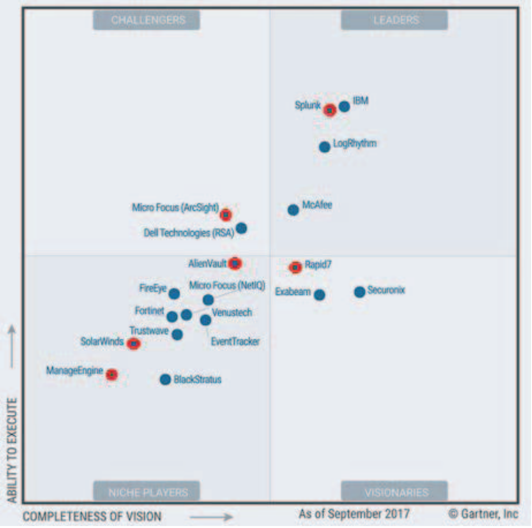

Fig. 1. Gartner magic quadrant for SIEM systems *(Adapted from Gartner 2017)* [4]. Systems marked in red color were included in the evaluation.

Accessibility of trial versions or existence of cloud demo platforms for evaluation also affected the selection. As a result, AlienVault, Micro Focus ArcSight, Manage Engine Event Log Analyzer, Splunk, Rapid7 InsightIDR, and Solar Winds Log and Event Manager were selected for evaluation, which are marked with red color in Figure 1.

B. *Evaluation Scenario*

The majority of the SIEM tools are very complex and would require specialized training to achieve complex tasks. In order to allow an interpretation of the capabilities and make a comparison with each other, a simple scenario is needed. This scenario should point out the steps required to build a custom visualization using custom data.

Each SIEM system eventually has its own predefined metrics and visualizations. However, the creation of custom visualization would require additional features and tasks. In order to provide a basis for the evaluation which mainly targets checking the availability of these necessary features and tasks on each SIEM, an evaluation scenario was selected. Figure 2 shows a stepwise description of the examination steps for the selected scenario. This scenario includes the examination of:

- predefined metrics for a selected use-case,
- data import options for suitable data for the use-case,
- the existence of built-in data structures which may be used to map the imported log files for the selected use-case,
- the ability to load custom data files,
- the ability to form custom searches,
- the abilities of data joining and data blending for visualizations combining multiple data sources,
- built-in visualization capabilities to display the selected data results.

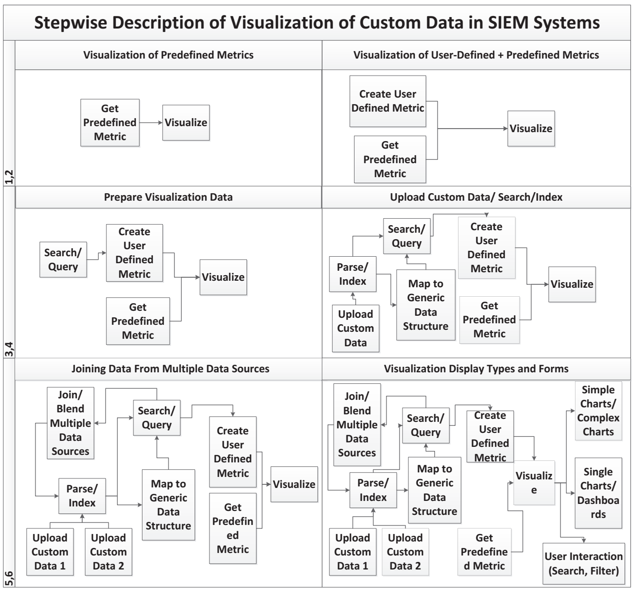
Stepwise Description of Visualization of Custom Data in SIEM Systems
Visualization of Predefined Metrics
Get Predefined Metric
Visualize
Visualization of User-Defined + Predefined Metrics
Create User Defined Metric
Get Predefined Metric
Visualize
1,2
Prepare Visualization Data
Search/ Query
Create User Defined Metric
Get Predefined Metric
Visualize
Upload Custom Data/ Search/Index
Search/ Query
Parse/ Index
Upload Custom Data
Map to Generic Data Structure
Create User Defined Metric
Get Predefined Metric
Visualize
3,4
Joining Data From Multiple Data Sources
Join/ Blend Multiple Data Sources
Search/ Query
Parse/ Index
Upload Custom Data 1
Upload Custom Data 2
Map to Generic Data Structure
Create User Defined Metric
Get Predefin ed Metric
Visualize
Visualization Display Types and Forms
Join/ Blend Multiple Data Sources
Search/ Query
Parse/ Index
Upload Custom Data 1
Upload Custom Data 2
Map to Generic Data Structure
Create User Defined Metric
Get Predefine d Metric
Visualiz e
Simple Charts/ Complex Charts
Single Charts/ Dashboa rds
User Interaction (Search, Filter)
5,6

Fig. 2. Stepwise description of visualization of custom data using SIEM tools

In the evaluation scenario, all the steps, except the first, are directly related to custom visualization generation. The first step, examination of predefined metrics, was included to help the researchers get accustomed with the SIEM systems before trying more complex steps.

As the target, the use-case "visualization of web application vulnerabilities" was selected by the authors due to its extensive usage and high recognition properties. Thus, during this examination, primarily the predefined metrics, existing log file types and data structures, and predefined visualizations related to the web application vulnerability scan results were investigated. However, other remarkable findings which are not directly related to the use-case, but which may be useful during visualization of other custom data, are also mentioned.

III. Results

In this section, first, the selected SIEM systems are introduced briefly. After the introduction, the evaluation platform is identified for each SIEM. Following this, each SIEM system is examined in seriatim using the evaluation scenario. Later, in the Discussion Section, overall comparison results are explained.

A. *Manage Engine Event Log Analyzer*

Manage Engine Event Log Analyzer stays in the Niche quadrant in 2017 report. The Event Log Analyzer free edition was installed as a desktop application for evaluation and the user guide was used to find out solutions for complicated tasks. Event Log Analyzer has a rich set of predefined metrics including application logs, operating systems logs, firewall logs, antivirus, and Hyperware management information. It does not include any predefined metric for web application vulnerability scan results, explicitly. Event Log Analyzer has built-in alert definitions, but these point out general purpose alerts not vulnerability scan related alerts. Built-in alert data structure does not include scan information but only alerts. The tool is undoubtedly prepared to have advantages to search for indicators, but using custom log files for different purposes has some usability issues. It allows loading custom files. It allows searching the log files through the use of search expressions which mainly consist of a series of search criteria groups (key value pairs). concatenated with AND and OR keywords. Field values can also be directly used as search criteria for a quick search experience. The authors could not manage to join multiple log files using the described type of search expressions. The application has a considerable amount of latency for basic search queries. Lastly, the authors observed the existence of visualizations of custom data through line chart, area chart, and vertical bar chart.

B. *Splunk*

Splunk stays in the Leaders quadrant in the 2017 report. In order to make an evaluation, Splunk server was installed in a Windows machine, and Splunk Universal Forwarder was installed in a Linux virtual machine. Both the server and the universal forwarder applications are easy to install, execute, and configure. Splunk base application does not come with predefined metrics. Splunk has a large number of add-ons called applications. These applications provide ways to integrate with other tools and include predefined metrics and visualizations for these integrations. The authors searched for an add-on specifically for web application vulnerability scans using “web application” search term, but could not associate any application with this topic. It has a large number of add-ons related to vulnerabilities, VulnDB is one of them.

Splunk, SPL query language allows the joining of multiple data sources. However, forming any query with or without joining, requires specialized training and is much more complicated than using BI tools. Splunk has two types of join operations left join and inner join. The user typically makes a query from a data source and assigns a table name to the result using the SPL language and this table can be joined to another table which is formed in a similar way. The difference from normal SQL queries is, in SQL query the query fields, joins and constraints are designed all in once, in SPL they are like separate and sequential operations piped to each other. Both approaches may have its own pros and cons. Preparation of queries to build the dashboard with a large number of metrics may be an issue for a user who does not have experience with the SPL language.

Splunk is more successful in automatic field extraction; it even assigns new fields, such as index time. Splunk has good time facilities to investigate events.

Splunk has display options which are comparable to BI tools in look-and feel. The authors observed the existence of line, area, column, bar, pie, and scatter charts, and radial, filler and marker gauge type displays. Splunk add on applications may provide other display types, which have not been observed and tested in this study. However, the design phase of these displays is more complicated compared to BI tools due to the complexity of the search statements Other dashboard creation steps are straightforward. Each metric should be prepared as a table or as a visualization which should then be saved as dashboard panels for reuse. The created dashboards cannot be accessed via external applications. However, reports can be accessed. So, dashboards should run and be converted to a report before access from external applications.

C. *Rapid7 InsightIDR*

Rapid7 InsightIDR stays in the Visionaries section of the magic quadrant of Gartner 2017 report. Cloud Trial Platform was used for evaluation. Rapid7 InsightIDR Collector has been installed on a Windows machine for data collection. Rapid7 InsightIDR has predefined metrics for various subjects including firewall activity, ingress authentication, active directory admin activity, compliance, asset authentication, DNS queries, IDS alerts, virus alerts, and file access activity. It does not have predefined metrics for application vulnerability scan results.

It has built-in integration with Rapid7 Nexpose vulnerability scanner system, and thus built-in data structure is compatible with the Rapid7 Nexpose vulnerability scanner. It allows importing custom data. However, this process is not very straightforward. It requires that every source machine has a fully qualified domain name which may not be possible for all cases.

Rapid7 has a unique language, Log Entry Query Language (LEQL) for data query which follows SQL syntax. It allows building queries based on multiple data sources easily with the use of joins. Save of queries is possible. No information was found related to set operations.

It has good dashboard building features which resemble BI tools. Dashboards are designed as a composition of cards which may be either built-in cards or user-defined cards. The authors observed the availability of timeline area chart, horizontal bar chart, bar chart, calculated number, gauge chart, timeline line chart, timeline multi-area chart, horizontal multi-bar chart, multi-bar chart, timeline multi-line chart, pie chart, table data, in trial platform.

D. Solar Winds Log and Event Manager

SolarWinds Log and Event Manager (LEM) stays in the Niche quadrant of 2017 report. Log and Event Manager server application was installed as a virtual machine on VMWare, and SolarWinds reporting tool was installed on a Windows machine for evaluation. The server application is primarily responsible for data collection, data correlation, and alerting tasks. Reporting application has around 300 built-in reports encapsulating a large number of metrics. These metrics are related to agent status, authentication, change management, event summary, file audit, incident alert, machine audit, malicious code, network events, network traffic audit, registry audit, resource configuration, and tool maintenance. The authors did not find an existing data structure or a generic data structure suitable for application vulnerability scan imports.

SolarWinds has a number of connectors for various devices or formats. It does not have a generic connector which reads custom log files. The company offers that if the third party tools can be generated in Syslog format, then it may be indexed and searched using LEM. One other solution suggested in the user forums is forming a new user-defined connector. This suggestion depends on the fact that each connector is actually an XML file which defines the mapping of log file attributes to LEM items.

In SolarWinds, available built-in reports can be modified by the users by adding user-defined filters based on report attributes. These reports can then be saved in Crystal reporting format. SolarWinds uses “custom reports” term for these user-defined reports.

LEM reports application depends on Crystal Reports third-party visualization tool. Thus, it encapsulates various types of table and display formats available in crystal reports.

E. Micro Focus ArcSight

The authors made an effort to evaluate SIEM systems from all four quadrants. However, it was not possible to find and access an evaluation setup for some for the SIEM systems, either permanently due to test platform maintenance (RSA) or indefinitely (Microfocus ArcSight). Micro Focus ArcSight stays in the Challengers quadrant of 2017 Gartner report. No trial version was available at the time of evaluation. Thus, a series of workshop video tutorials and product documents have been used to understand the critical features related to custom visualization generation.

ArcSight comes with a standard structure which involves a series of coordinated resources. This structure involves built-in metrics and dashboards related to configuration monitoring such as undesired actions to systems, devices, and applications, intrusion monitoring, network monitoring, incident response tracking and ArcSight system monitoring.

ArcSight uses ArcSight Common Event Format data structure. Thus, even a custom log file can be loaded to the system. Then,the data attributes which are identified after parsing can be mapped to Common Event Format Data Fields by the user. This mapping is done as a continuation of the Regex definition for the particular file.

ArcSight has a large number of Flex Connectors. ArcSight Regex connector is one of them. ArcSight Regex connector allows making a definition of the log file by using Regex format. Using regex format allows parsing and indexing of complex log files. ArcSight Regex connector breaks the log statement into tokens using the declared Regex statement. The system provides a helper tool, ArcSight Regex Tester, which can be used to generate the necessary Regex statement to parse the custom file.

ArcSight has viewer panels which can include HTML based reports and several charts. Although the product includes other chart types, such as hierarchy maps (treemaps), custom query results can be visualized as a table, pie chart, bar chart and horizontal bar chart according to user documents in ArcSight.

F. AlienVault

AlienVault stays in the Niche quadrant of Gartner 2017 report. The tool cannot be installed on Windows OS directly. It is designed to be installed on VirtualBox. Since the authors had some problems with this installation, the AlienVault online demo version was examined for evaluation.

The online version has a number of prebuilt dashboards encapsulating a large set of metrics. However, it does not have a specific dashboard for web application vulnerabilities scan results.

The authors examined generic vulnerabilities dashboard which is designed to be used by various assets including software programs. Generic vulnerabilities dashboard has very few metrics which includes more vulnerable assets, mostly detected vulnerabilities, vulnerabilities by type, and a number of scan jobs.

The online demo version did not allow uploading custom data due to restrictions. However, the authors contacted the customer support and found out that this restriction is only applied to the online demo version.

The querying mechanism of AlienVault is based on search strings consisting of key-value pairs. These keys can be both built-in fields such as IP, src_port and user-defined fields. The filename can also be used as a search parameter which shows that data source specific search can be made using file names. It looks like there is no straightforward method to join multiple data files. However, AlienVault has connectivity to several databases and allows complex database queries including joining of multiple tables

The authors observed the creation of visualization using simple charts including line chart, area chart, and vertical bar chart in this tool.

IV. Discussion

SIEM systems are generally expensive systems, which require specific installation platforms to be installed. For this reason, the authors think that the majority of the SIEM users are familiar with only a few of these systems. Independent evaluations, such as this study, would help to get familiar with these systems. This familiarity would eventually help to make better selections in the long term. Table I contains information related to the configuration of the selected SIEM systems in this study. There may be multiple interfaces for a few of the SIEM systems. For example, ArcSight has Console, Web, and Command Center interfaces. The table includes the access type which was evaluated during this review. A few of the SIEM systems are suitable to be installed on different operating systems. The data connectors or data collectors have different mechanisms with the same purpose, gathering data for the SIEM systems. The SIEM systems may have various type of data collectors. The collectors listed in the table are the ones which are tested during this study. It is important to note that this table is prepared based on authors' own experiences and limited with the configurations tested in this study.

TABLE I. SIEM CONFIGURATION INFORMATION

	Quadrant	Inst. Platform	Data Collector/Connect or App.	Reporting App.	Access Type
Manage Engine Event Log Analyzer	Niche	Windows machine	-	-	Web Based Access
Splunk	Leaders	Windows machine, Universal Forwarder - Linux machine	Universal Forwarder	-	Web Based Access
Rapid7 InsightIDR	Visionaries	Cloud Trial Platform, Rapid7 InsightIDR Collector-Windows machine	Rapid7 InsightIDR Collector	-	Web Based Access
Solar Winds Log and Event Manager	Niche	Server App - VMWare Virtual Machine, SolarWinds Reporting App -Windows machine	-	SolarWinds Reporting Tool	Web Based Access
Micro Focus ArcSight	Challengers	-	ArcSight Regex Connector	-	Web Based Access
AlienVault	Niche	VirtualBox, Online Demo Version	-	-	Cloud Access

SIEM systems are focused on threat capture, gathering network intelligence and detecting malicious activities. In general, they have very advanced features to accomplish these targets. Although most of the SIEM tools are very handy and have useful features, when the objective is working on custom log files, they have different approaches which result in several difficulties.

Comparison of these systems is also challenging due to the existence of different data flows as a result of different sequence of actions which end up with user interfaces that are difficult to compare.

The authors could not complete some steps of generating visualization for each SIEM, such as importing custom data, joining multiple data sources, building a visualization encapsulating multiple displays, designing a visualization by a drag and drop type user interactivity. These difficulties or inabilities are interpreted as either not having this feature or not having a straightforward way to achieve this step by the authors.

Although each SIEM system has its own outstanding features, one obvious result of this examination is, it was not possible to complete the planned scenario for the majority of the selected SIEMs. This result points out the known differences in BI tools and SIEM tools.

Installation and file upload difficulties were the most common difficulties during this study. Different ways of mapping the available custom data to the product fields have different results. Some tools make an automatic mapping of provided custom data to an available standard data structure. While this automatic mapping is faster and less tedious, the authors felt that mapping the fields manually as in the ArcSight example allows more correct mappings of the fields and helps to manage the data better in subsequent sections such as search and display. Otherwise, the tool has all the control, and the user may end up with visualizations that he/she did not plan. The background of the user is also important. Having prior knowledge on some technologies such as Regex syntax makes things easier. Otherwise, a long preprocessing step for some tools may be a burden for some users.

The authors think that, it was prudent to choose visualization of web application vulnerability scanner results as the custom use-case. The reason is it never existed in a built-in manner in the evaluated tools. Otherwise, the comparison would be biased, and the target of generation of custom visualization would have been strayed by the authors, unintentionally.

The observations described in this evaluation study apply only to the custom data visualization. In general, the tools behave entirely differently in data parsing, indexing, and querying and even in data display tasks for a data source which has a familiar data structure such as sys log or built-in integrator with the SIEM. In that condition, most of the manual tasks may turn into automatic tasks, and the displays are generated quickly in real time with the data occasionally. The known data structure will also cause other tasks such as automatic correlation of data with other data sources, automatic threat/vulnerability detection with known metrics, automatic display of prebuilt dashboards. Table II provides a summary of the comparisons of the selected SIEM systems.

The vendors for the majority of the evaluated products have other security analyzer tools along with SIEM systems. A few of those products may be more suitable for custom log file visualizations.

One significant contribution of this study is better decision making. The authors aim that the potential users of SIEM systems may benefit from this study when choosing a SIEM for their needs and when designing their custom log management systems.

TABLE II. EVALUATION SUMMARY

	Visualization of Predefined Metrics	**Creation of User Defined Metrics**	**Search/Query Mechanism**	**Upload Custom Data**	**Join/Blend Multiple Custom Data**	**Display Types**
Manage Engine Event Log Analyzer	Yes	Yes	Key-value paired search expressions	Hard	No	Line, area, and vertical bar charts
Splunk	Yes	Yes	Search Processing Language (SPL)	Very Easy	Yes	Line, area, column, bar, pie, scatter charts and radial, filler and marker gauges
Rapid7 InsightIDR	Yes	Yes	Log Entry Query Language (LEQL)	Hard	Yes	Timeline area, horizontal bar, bar, gauge, timeline line, timeline multi-area, horizontal multi-bar, multi-bar, timeline multi-line, and pie charts, table data, and calculated number
Solar Winds Log and Event Manager	Yes	No	Update Built-in Reports	Hard	No	Display formats available in crystal reports
Micro Focus ArcSight	Yes	Yes	Regex Based Query	Easy	Yes	Table data, and pie, bar and horizontal bar charts
AlienVault	Yes	Yes	Search strings consisting of key-value pairs	Neutral	No	Line, area, and vertical bar charts

V. CONCLUSIONS

This paper presents the evaluation results for SIEM systems focused on the creation of custom visualizations. The evaluation results demonstrated custom visualization generation related features/functions which are powerful or open for improvement for six well-known SIEM systems.

The provided evaluation method points out a practical scenario to test the effectiveness of SIEM tools regarding the targeted objectives. This scenario may as well be used for other use-cases which may have other impressive results.

Generally, these SIEM systems are compared according to their feature lists. The authors claim that scenario based comparisons as in the provided case would provide better information for these SIEM systems.

The SIEM systems which stay in different quadrants of the Gartner report change annually due to changes in the SIEM systems. Related to this issue, the results achieved during this study would eventually be affected as existing features are modified and new features are added to the current SIEM systems. Thus, this kind of scenario based evaluations should be repeated in short periods.

REFERENCES

[1] K. Dimitrios, "Security Information and Event Management Systems: Benefits and Inefficiencies," University of Piraeus, Piraeus, Greece, 2014.

[2] E. F. Sinar, "Data Visualization: Get Visual to Drive HR’s Impact and Influence," Society for Human Resource Management (SHRM)-Society for Industrial Organizational Psychology (SIOP) Science of HR White Paper Series. , Bowling Green, OH, USA, 2018.

[3] Tableau, "Make your data make an impact," 12 6 2018. [Online]. Available: https://www.tableau.com.

[4] M. Nicolett and K. M. Kavanagh, "Magic Quadrant for Security Information and Event Management," Gartner, Stamford, CT, USA, 2013.

[5] IBM, "IBM QRadar SIEM," 17 9 2018. [Online]. Available: https://www.ibm.com/tr-tr/marketplace/ibm-qradar-siem.

[6] Microfocus, "Microfocus," 17 0 2018. [Online]. Available: https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview.

[7] McAfee, "McAfee," 17 9 2018. [Online]. Available: https://www.mcafee.com/enterprise/en-us/products/siem-products.html.

[8] EventTracker, "Event Tracker," EventTracker, 17 9 2018. [Online]. Available: https://www.eventtracker.com/. [Accessed 17 9 2018].

[9] Splunk, "Splunk and AWS provides visibility into U.S. stock and options market transactions," Splunk, 17 9 2018. [Online]. Available: https://www.splunk.com/. [Accessed 17 9 2018].

[10] LogRhythm, "LogRhythm Security Made Smarter," 17 9 2018. [Online]. Available: https://logrhythm.com/. [Accessed 17 9 2018].

[11] K. Kavanagh and T. Bussa, "Magic Quadrant for Security Information and Event Management," Gartner, Stamford, CT, USA, 2017.

[12] MicroFocus, "ArcSight Enterprise Security Manager," MicroFocus, 19 9 2018. [Online]. Available: https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview. [Accessed 19 9 2018].

[13] Dell, "RSA At a Glance," Dell, 19 9 2018. [Online]. Available: https://www.rsa.com/en-us/customers/dell-technologies. [Accessed 18 9 2018].

[14] Rapid7, "InsightIDR," Rapid7, 19 9 2018. [Online]. Available: https://www.rapid7.com/products/InsightIDR. [Accessed 19 9 2018].

[15] Exabeam, "The Exabeam Security Management Platform," Exabeam, 19 9 2018. [Online]. Available: https://www.exabeam.com/product/. [Accessed 19 9 2018].

[16] "Most Visionary Next-Gen SIEM Platform," Securonix, 19 9 2018. [Online]. Available: https://www.securonix.com/. [Accessed 19 9 2018].

[17] AlienVault, "AlienVault Unified Security Management," AlienVault, 19 9 2018. [Online]. Available: https://www.alienvault.com/products. [Accessed 19 9 2018].

[18] MicroFocus, "NetIQ," MicroFocus, 19 9 2018. [Online]. Available: https://www.netiq.com/. [Accessed 18 9 2018].

[19] FireEye, "FireEye Leading The Way," FireEye, 19 9 2018. [Online]. Available: https://www.fireeye.com/. [Accessed 19 9 2018].

[20] Fortinet, "Forninet Featured Security Insights & Information," Forninet , 19 9 2018. [Online]. Available: https://www.fortinet.com/. [Accessed 19 9 2018].

[21] Venustech, "Venusense UTM," Venustech, 19 9 2018. [Online]. Available: http://www.venusense.com/product/view/11168.html. [Accessed 19 9 2018].

[22] "Trustwave: Smart Security On Demand," Trustwave, 19 9 2019. [Online]. Available: https://www.trustwave.com/home/. [Accessed 19 9 2019].

[23] Solarwinds, "Solve your toughest IT management problem, today," Solarwinds, 19 9 2018. [Online]. Available: https://www.solarwinds.com/. [Accessed 19 9 2018].

[24] ManageEngine, "ManageEngine," ManageEngine, 19 9 2018. [Online]. Available: https://www.manageengine.com/. [Accessed 19 9 2018].

[25] BlackStratus, "BlackStratus Managed Security Services," BlackStratus, 19 9 2018. [Online]. Available: https://www.blackstratus.com/. [Accessed 19 9 2018].