Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-018-0936-7

ORIGINAL RESEARCH

Near-miss situation based visual analysis of SIEM rules for real time network security monitoring

Abdul Majeed[1] · Raihan ur Rasool[2] · Farooq Ahmad[3] · Masoom Alam[4] · Nadeem Javaid[4]

Received: 6 November 2017 / Accepted: 2 July 2018

Abstract

Security information and event management (SIEM) systems are generally used to monitor the network for malicious activities. These systems are capable of detecting a wide range of malicious activities in the network using built-in rules to generate alerts on malicious activities. Although SIEM systems provide comprehensive reports about each alert including relevant details such as, severity score, events, and events counts. However, a key limitation of SIEM systems is not presenting the rule's status in real time before an alert is raised. This paper presents a novel visual tool that enables security analyst to grasp visually, and in real time a complete overview of SIEM rules execution, and alert circumstances that may happen in advance based on near-miss situation. Apart from the real time rules analysis, it also enables security analysts to explore the reasoning behind the alerts in an organized and efficient manner via security questions. The essence of the approach is to evaluate and visualize the current status of each rule execution according to pre-compiled conditions in real time. We demonstrate the utility of our approach using IBM QRadar events data to support the informative analysis of different rules in real time, and security questions based insight about the rules via story page.

Keywords Malicious · SIEM systems · Near-miss situation · SIEM rules · Alerts · Informative analysis

1 Introduction

Cyber threat detection and mitigation remains an agenda of interest to governments, businesses, researchers etc. and not surprisingly this is a hotly studied research area. A recent media release (Clayton 2017) of the Chairman of the U.S. Securities and Exchange Commission (SEC) reported that:

> I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important. Malicious attacks and intrusion efforts are continuous and evolving, and in certain cases they have been successful at the most robust institutions and at the SEC itself. Cybersecurity efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery.

No single current protection approach alone can efficiently defeat emerging threats, and thus research efforts are required to further investigate this area (Choo and Dehghantanha 2018). For example, the capability to see and understand everything that is happening on the network could be extremely useful in securing an organizations network. This may not,

✉ Masoom Alam
masoom.alam@comsats.edu.pk

Abdul Majeed
abdulmajid09398@kau.kr

Raihan ur Rasool
raihan.rasool@live.vu.edu.au

Farooq Ahmad
hfahmad@kfu.edu.sa

Nadeem Javaid
nadeemjavaid@comsats.edu.pk

[1] School of Information and Electronics Engineering, Korea Aerospace University, Deogyang-gu, Goyang-si, Gyeonggi-do 412-791, South Korea

[2] Victoria University, Melbourne, Australia

[3] College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Kingdom of Saudi Arabia

[4] Department of Computer Science, COMSATS University Islamabad, Park Road, Islamabad 45550, Pakistan

Published online: 25 July 2018

however, be possible in practice. Different security controls such as, intrusion detection system (Rowland 2002), intrusion prevention system (Patil and Meshram 2012), honeypots (Kabiri and Ghorbani 2005), honeynets (Levine et al. 2003), firewalls (Cheswick et al. 2003) and SIEM systems [e.g., IBM QRadar (Fratto 2004), Splunk (Roberts 2013), Hp ArcSight (Product Brief 2008), LogRhythm (Villella and Peterse 2011)] are used to maintain the security of organizations. SIEM systems are mainly used as an all-in-one solution for the maintenance of security in organizations. These systems use different security rules to detect malicious activities in the network and provide incident statistics via generated reports. These systems collect logs, analyze and generate alerts on malicious activities. Although SIEM generate alerts on malicious activities, and provide incident details via textual report, a security analyst is unlikely to be able to observe the status of different rules in real-time (Huang et al. 2015). As the security analyst examining the report or incident does not have visibility of the current status of the rules and the entity details, it is challenging for the security analyst to effectively identify problematic activity which may occur again in the near future (Coudriau et al. 2016).

We observe that while both network security analysis and security data visualization are two active research areas, they are mostly treated as separate domains despite having overlapping challenges and characteristics [a similar observation between digital forensics and forensic data visualization was made by Tassone, Martini and Choo (Tassone et al. 2017; Choo et al. 2017)]. For example, both network security analysis and security visualization (Shabtai et al. 2006) focus on the monitoring of network activities from different viewpoints, performing of time-dependent data analytic, exploration of patterns and unusual behaviours in large datasets, etc. (Pronoza et al. 2016). Real-time security visualizations have become much demanding now for displaying high-level information about threats (Rohs and Essl 2006).

Considering the importance of visualizations and typical shortcomings of textual reports generated in SIEM systems, the need for real-time security analytics-based solution is becoming increasingly important, particularly in our Internet-connected society (Lu et al. 2017; Briesemeister et al. 2010; Mahmood and Afzal 2013; Pavlik et al. 2014; Constantinescu et al. 2016; Guimarães et al. 2017). The utility of SIEM systems can be enhanced significantly with the addition of security visualizations as a core component to view events in real-time (e.g., with features such as obtaining required information such as IP addresses associated with the respective rules and historical activity analysis of the respective IP addresses in real-time, without the need to read the lengthy and complex textual reports).

Although there are many visualization tools (Kotenko et al. 2013; Novikova et al. 2017; Chuvakin 2010; Nguyen et al. 2016; Shah et al. 2017; Langton and Baker 2013) designed for malicious activities detection, these tools lack the capability in providing a detailed (visual) insight into the internal workings of SIEM systems in the context of rules and alerts (also referred to as alarms in the literature). Thus, in this paper, we seek to provide near-miss situation analysis of different SIEM rules visually in real time, and rules details with the help of different security questions. Additionally, we provide different rule statistics to security analysts in real time to enhance activity monitoring in systematic way. Specifically, we identify different rule specific security questions which provides reasoning about the offense (if rule fires) and provide answer through different security visualizations to overcome the drawbacks of textual reports in SIEM systems. Finally, we present our findings about visualization tool in terms of the security objectives that our tool provides from different security aspects.

In the next section, we briefly describe SIEM systems and security data visualizations. Section 3 presents related literature. Section 4 describes the problem and presents the proposed near-miss situation visual analysis model. In Sect. 5, we use two case study examples to explain how the question-based rules exploration can be used. Section 6 discusses the pilot study and results. We conclude this paper in the last section.

2 Background

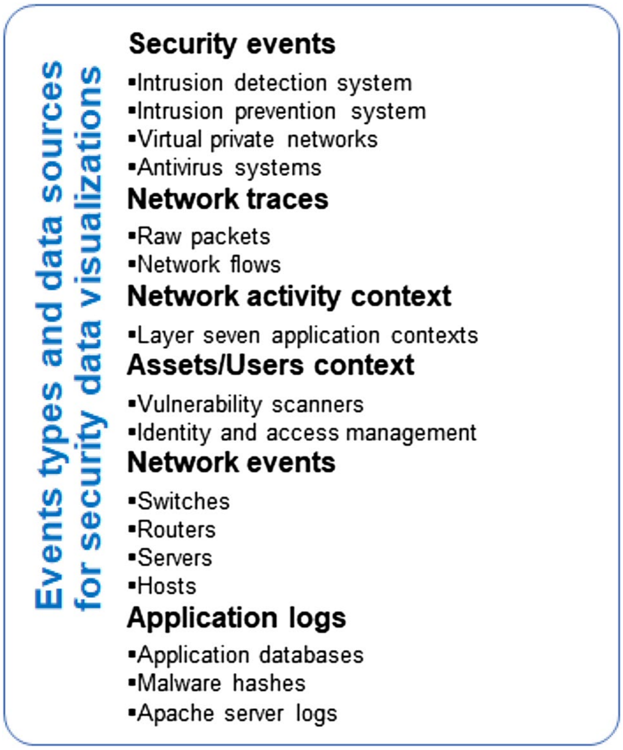
2.1 Security information and event management systems

Efficient monitoring of a network in real time to ensure its security is a global challenge. SIEM is a widely deployed enterprise solution, which has the ability to monitor large networks. SIEM combines SIM (Security Information Management) and SEM (Security Event Management) to function as one security management system. The integration of both these components strengthens the real-time network analysis by providing the capability to collect log data, perform trend analysis, and undertake automated reporting for compliance and centralized management (Conroy 2016). In other words, SIEM is used for threat identification, analysis, alerting, and compliance monitoring. SIEM also provides support for an organizations legal compliance (Azodi et al. 2013). Typically, in SIEM, multiple agents are deployed in a sophisticated manner to obtain security events from multiple devices. The collectors of each device collect logs, perform some sort of filtering, and then forward them to SIEM where analysis is carried out on the basis of certain conditions. SIEM uses certain built-in rules and statistical correlation engine to perform the required analysis. Apart from being expensive, SIEM solutions are also complex to manage and operate. While major industries such as Payment Card Industry Data Security Standard (PCI DSS) compliance has used SIEM driven solution to ensure the security of their infrastructure (Gupta 2017), the costs associated with SIEM may be out of reach for small-and-medium sized businesses.

2.2 Security data visualization

Security visualization allows the visual representation of security data, which can ease one's understanding of complex technical information, for example in terms of illustration, interpretation, storytelling, unlocking the sight, facilitating deep search in the data, exploration, pattern finding, extracting, details-on-demand etc. Security data visualizations also allow users to search for particular types of visualizations, appropriate visualizations methods, a graphical representation of the objects, classification of security data visualizations, and selection of appropriate visualization based on the data (DAmico et al. 2016; Lee et al. 2015), which allows us to fulfil the ever growing needs of network security monitoring. Management of SIEM can be eased if users have a visualization of rules and security data, which are helpful in real-time network monitoring and situational awareness (Sethi et al. 2016; Zhang et al. 2014; Mantere et al. 2013).

Visualization cannot be made without having data or information. Most of the existing visualization systems rely on single source of data. Looking at network events from multiple perspectives using different data sources into a system can provide an analyst with a richer insight into the underlying events and activities. Therefore, a comprehensive list of most widely used events types and data sources that are available to the research community and may be added in the design of network security visualization systems are given in Fig. 1. The decision about the type and number of data sources to be used is subject to security monitoring objectives because some data sources, e.g., network traces can contain thousands of features (Zander et al. 2005). The importance of selecting the most appropriate features, as a first step in designing a visualization system, has been extensively studied in the potential data sources for security visualizations (Bauernschmidt et al. 2004) in the fields of statistics, machine learning, pattern recognition, and data mining and the outputs are applied to the fields of artificial intelligence, text categorization, and also intrusion detection (Stein et al. 2005). Based on a particular problem whether it is an intrusion detection or activity monitoring researcher/security experts are facing, and the data sources available to him/her, a subset of features can be extracted and incrementally validated until a desired optimality or target concept is achieved. In this work, we used security events of the IBM QRadar to evaluate, and present the rules status and highlight the situation before it becomes worse. SIEM systems collect data from different security and network devices as mentioned in Fig. 3 in the form of raw logs, and transform the collected logs into events via normalization and parsers.


Events types and data sources for security data visualizations

Security events
- Intrusion detection system
- Intrusion prevention system
- Virtual private networks
- Antivirus systems

Network traces
- Raw packets
- Network flows

Network activity context
- Layer seven application contexts

Assets/Users context
- Vulnerability scanners
- Identity and access management

Network events
- Switches
- Routers
- Servers
- Hosts

Application logs
- Application databases
- Malware hashes
- Apache server logs

Fig. 1 Events and data sources for security visualizations

Once the required data is available, the next step is to decide about how to visually represent the data. Deciding the appropriate visualization for the data is very tricky since it needs the understanding of what we want to analyze, and what information is encoded in the data. Many types of graphs/charts can be used to visualize data. Each graph has its own features and is suited for a specific analysis scenario. Some graphs are great at visualizing large amounts of data; others are better suited for highlighting variations and trends in the data. A comprehensive overview of the security data visualizations grouped into three categories of static network visualization, network flow visualization and security visualizations is shown in Fig. 2.

Each of these visualizations has different capabilities and emphasizes specific aspects of the security data. The graphs facilitate the analysis of the distribution of values in a single dimension or the relationship between two or more dimensions in the data (i.e., time versus events count). The static network visualization includes simple visualizations such as, pie, bar, line and scatter plots etc. which are mainly used to show the distribution of values as proportions or percentages of the whole. For example, the proportion of the applications protocols, number of bytes transferred, number of blocked connection per day, and number of failed logins over the period of one day. These types of visualizations are mainly used to plot two-dimensional data and to show the properties of the static data. Network flow visualizations are the dynamic visualizations that show variations, and trends in the data (e.g., number of users connected to the network which keep updating time to time). These visualizations show more relationships in the data and covers broad aspects of the data. Network flow visualizations are used to show the peak traffic and low traffic, number of connections and data transmission etc. Link graph is mainly used to analyse the communication of the hosts with local and global systems. However, in some cases, static network visualizations are also used for the network flow visualization purposes. Security data visualization includes all types of the visualization and enable us to communicate a large amount of information to viewers. Security visualization gained the popularity since they offer several benefits over textual analysis of network data which is large and complex. Security data visualizations help identifying the attacks and their patterns with ease. The selection of the appropriate visualization type primarily depends upon the following three things, (1) what we want to understand (e.g., distribution, relationships, comparisons, and trends), (2) how many dimensions of the data are (e.g., 1D, 2D, 3D, …), (3) type of data (e.g., categorical, numerical, and combined). In this paper, we used security visualization of more than twenty distinct types including simple charts and D3 library visualization for presenting SIEM rules and their details.

3 Related literature

Designing visualization for network infrastructure is an established research topic (see Marty 2009; McKenna et al. 2015), but remains a topic of ongoing interest (e.g., there are conferences and journals dedicated to cyber security visualization such as the IEEE Symposium on Visualization for Cyber Security). Marty (2009), for example, described the key tasks associated with visualization (e.g., data reporting, monitoring, historical analysis) and presented a visualization taxonomy for security data. A sophisticated tool for monitoring network flow via security visualization, NVisionIP, was presented in Lakkaraju et al. (2005). NVisionIP is designed to display a wide range of network characteristics (i.e. works with network data from different devices, with different attributes such as IP address, source port, destination port, start time, end time of each flow, protocol used for the flow, and the volume of traffic), and present aggregated traffic between two systems. NVisionIP can be used to inspect network traffic visually and conduct investigation about anomalies and threats. However, NVisionIP does not provide details of all activities and user experience. Lakkaraju et al. (2004) and Ohnof et al. (2005) proposed a framework which uses scatter plot to show communication analysis between

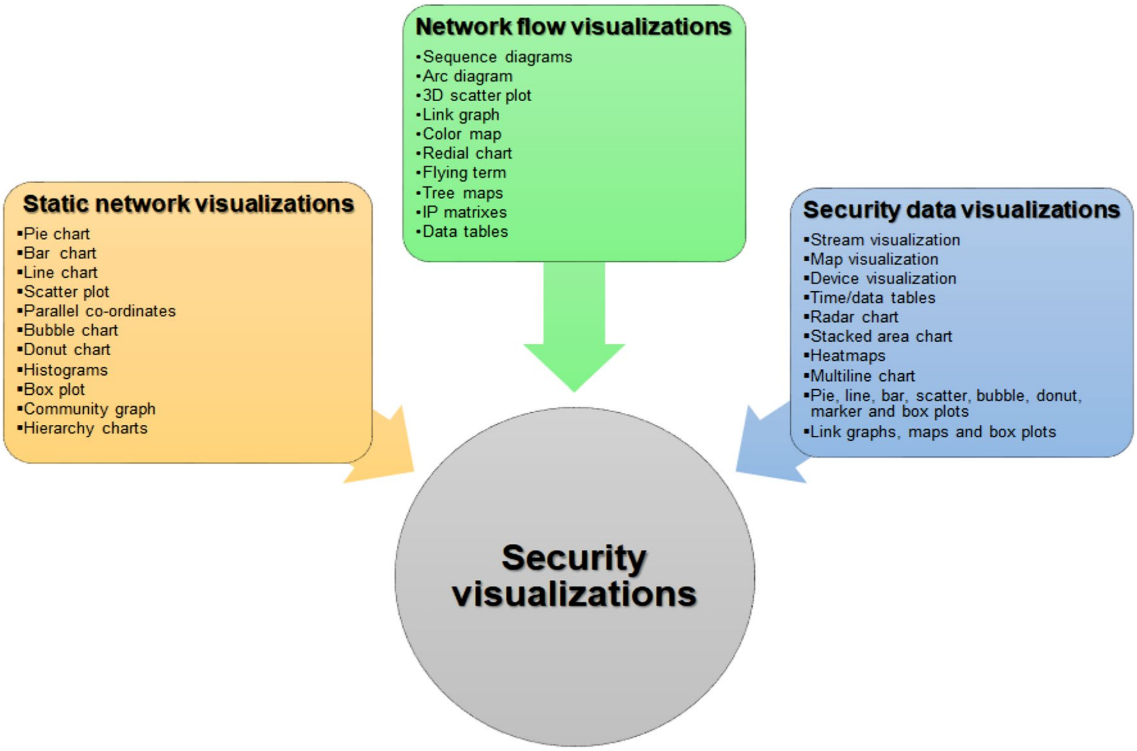


Fig. 2 Types of security data visualizations

different hosts. The flow is represented with dots and the visualization assists in tracing the spread of network worms and investigating devices vulnerable to that worm. In both research, a logical view of the security visualization is provided. However, both tools lack the capability to monitor other security activities like congestion, flows, and traffic spikes. A similar representation, but with the addition of a third dimension (i.e. map), is presented in Hideshima and Koike (2006). A limitation with the latter tool is the lack of detailed information of the attack source.

In Alsaleh et al. (2008) and Attipoe et al. (2016), the authors proposed using nodes of a graph to represent hosts and arrange using protocol distribution. These visualizations can facilitate attack detection and provide the identification of higher level entities and anomalies in the network (Azodi et al. 2016). However, the approaches are not sufficiently comprehensive, in terms of attack coverage, since additional details are not presented for any activity. In Sun et al. (2011), the authors used adjacency matrix clustering to identify attacks evolution in the network. Specifically, they identified and prioritized discrete steps on victim machines visually and showed the attacker origin using visualizations. The visualization tool is helpful in security monitoring, threats identification and classification. There are also a number of open source security tools, but several of these tools are limited in predicting future types of attacks/incidents. A number of tools also allow the visualization of a small number known attacks such as information flows, data packets injection, resynchronization, data injection code, packet latencies, sniffing and denial of service, but these tools are again limited in terms of forecasting and finding of patterns (Hinze et al. 2013). Spinning Cube of Potential Doom (Sun and Overbye 2004) is a very popular security tool that visualizes TCP connection attempts as points on scatter plot. It uses two IP address axes and a port number axis to display network activity in the form of three-dimensional cube. However, it has limited features in monitoring network security from multiple perspectives.

A related review of the literature on SIEM based framework was offered by Montesino et al. (2012), Holik et al. (2015), Coppolino et al. (2011) and Li and Yan (2017). They draw attention to comprehensive reporting, internal security and management monitoring access resources to the greatest extent possible with the integration of small scale frameworks with SIEM systems to enhance the security of organizations. By implementing the proposed framework provided by the authors one can automate as many security controls as possible, and ultimately organizations will achieve more efficiency in information security management. The proposed frameworks assist in reducing the complexity of overall process (i.e., log collection, transforming logs to events, event rules correlation, alerting and reporting). These research findings may also be useful for SIEM vendors, in order to include more functionality to their products and provide a maximum of security controls automation within existing SIEM platforms. However, the main weakness of their studies is that they make no attempt to consider the SIEM rules working, and modification in rules execution in terms of security monitoring.

Recently, the evolution of big data and threat intelligence about the security attacks have gained popularity (Ring 2014; Qamar et al. 2017; Brewer 2015). However, this requires the identification and modelling of security threats based on the attacks organizations are facing. Likewise, increasing dependence on digital technology (e.g., sophistication in technology due to which it has become more complex) (Oseku-Afful 2016), the underlying organizational policies (Flynn et al. 2012), and the need of quick network data processing (Balabine and Velednitsky 2018), may affect security. However, such types of threats have been overlooked in previous work except some efforts like collaborative approach given by the authors (Aguirre and Alonso 2012) to mitigate attacks. They improve the management, and analysis of generated alerts in which a set of partners from different domains share information about detected attacks with SIEMs systems. Several attempts from both industry and academia have been made to compile and relate the concepts of alarms, events, attacks, vulnerabilities, and devices etc. Hence, there is a pressing need to formalize either a standard method or a formal ground to unequivocally represent knowledge on attacks (Cheung et al. 2003). Recent work from The MITRE Corporation (Barnum 2008) has addressed the necessity of an ontology architecture describing the automatic and semantic interoperability within the SIEM lifecycle (Parmelee 2010). In particular, a novel specification has been proposed namely Common Event Expression (CEE) to semi-automate the SIEM process.

A number of studies have explored a closely-related method used in enhancing the traditional SIEM process as a whole, especially focusing on event correlation via bioinspired, and adaptive learning system based on Artificial Immune System (AIS) (Suarez-Tangil et al. 2014). The proposed work facilitates an automatic correlation of attacks and improve the attack detection efficiency. However, most of the current SIEM systems lack of an efficient mechanism to generate correlation rules and cannot adaptively predict novel attacks either (Anuar et al. 2010). Due to the popularity of SIEM system in cloud computing, a comprehensive work which discuss requirements and concerns related to implementation of SIEM as a service is provided by Wenge et al. (2014). We refer the interested reader to Nicolett and Kavanagh (2011) for a comprehensive evaluation of current SIEM products. However, since current SIEM systems are highly dependent on the alerts reports which are obtained after the alarm has raised, a visual tool to consistently present the relevant security situation is required. It is clear from the literature review that there is a need for an automated tool with visual analytics capabilities to facilitate real-time analysis of SIEM rules and highlight the malicious activities in an efficient manner before they convert into an alarm.

4 Problem description and proposed model

4.1 Problem definition

We seek to address the following problem in this paper: At a specific time, how do we determine which rule has most number of events, and how to pinpoint rules that are about to generate an alert soon. In other words, how do we accurately monitor different rules execution status according to pre-compiled condition in real time, and insight about the rules based on security questions such as, who, when, from where, and against which device a malicious attempt was made.

4.2 Proposed near-miss situation analysis model

The significant increase in the types, volume, and sophistication in security threats and limited capabilities of visual analytics tools for providing SIEM rules status necessitate a unified and near-miss situation aware visual tool, in order to present the rule status in real time. This will facilitate users (and organizations) in responding to malicious activities. This section presents the conceptual overview of the proposed near-miss situation aware visual analysis of the SIEM rules and outlines its procedural steps as shown in Fig. 3.

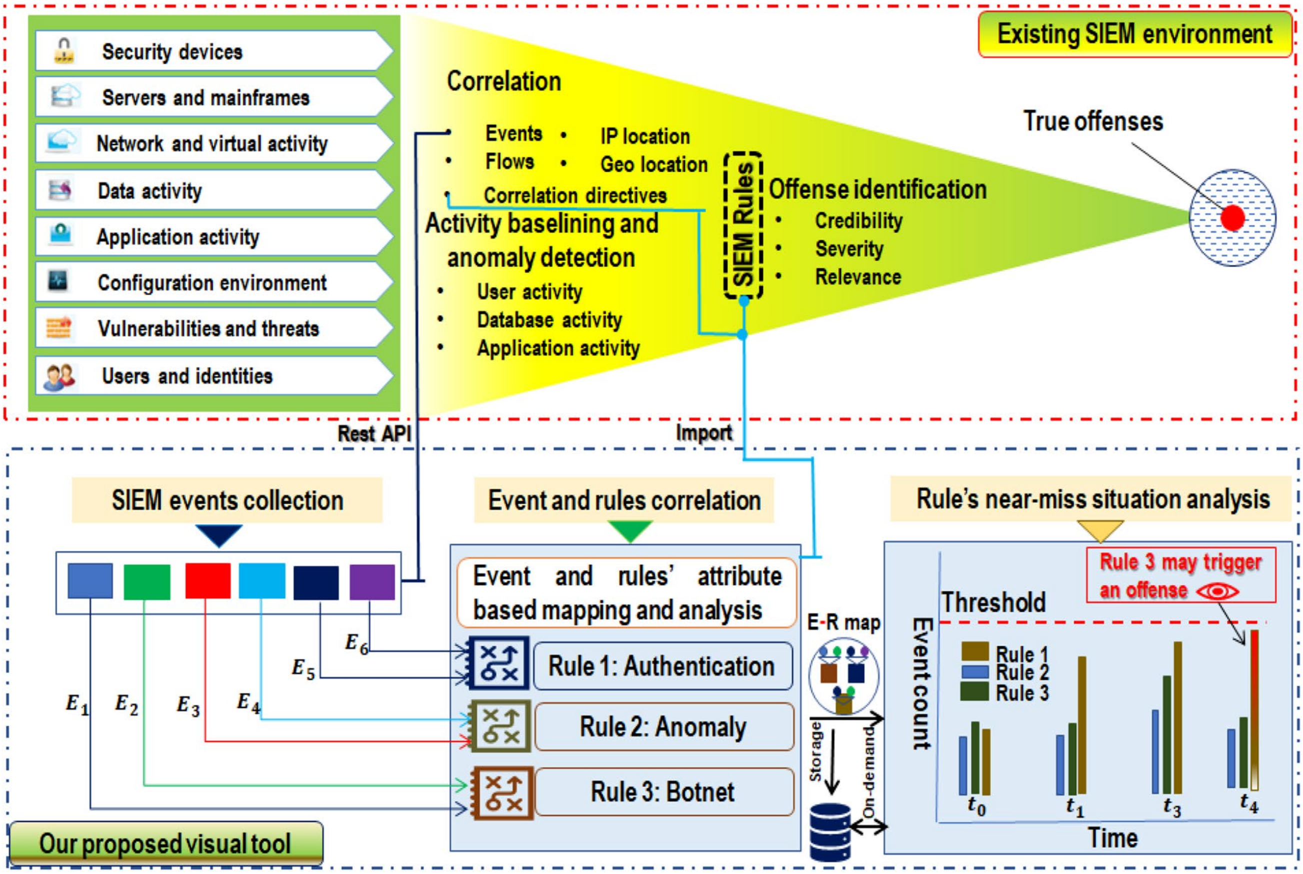


Fig. 3 Conceptual overview of the proposed near-miss situation analysis model

Generally, the term real time is used to describe computer systems/frameworks that update information approximately at the same rate as they receive data. In our work, by real-time we mean that proposed tool provides up-to-date information about rules execution status based on newly detected security events with the help of robust visualizations that display fresh data as it comes. For example, if a particular rule *X* has *n* events at time *t*, and in next interval $t + 1$ of time $2n$ more events are received for the same rule, then event count will become $3n$ of rule *X*. The same process is observed for all rules which are supported by our tool. By means of the real time rules analysis, the security analyst can always have the awareness about rules execution status. Meanwhile, SIEM systems are still, typically, a tool-driven approach that requires heavy customization. When it comes to taking more and more real time information into account for the security monitoring, they show limitations regarding their scalability. In our proposed tool, we fetch only events data in periodic intervals, therefore, scalability, and delay issues are resolved up to great extent possible. Meanwhile, sometime with no or fewer events, this would consume a substantial amount of unnecessary resources. Events collection from the SIEM system is done through polling with high frequency, and polling frequency can be adjusted according to the security monitoring objectives. The first time that we run the polling script for fetching events from SIEM system, there is an expected delay of at least one minute. Despite this, on the real time performance test (i.e., bringing potential malicious activities into the knowledge of security analyst) with even very high event rate the events collection, processing, and analysis is faster as compared to the actual SIEM systems.

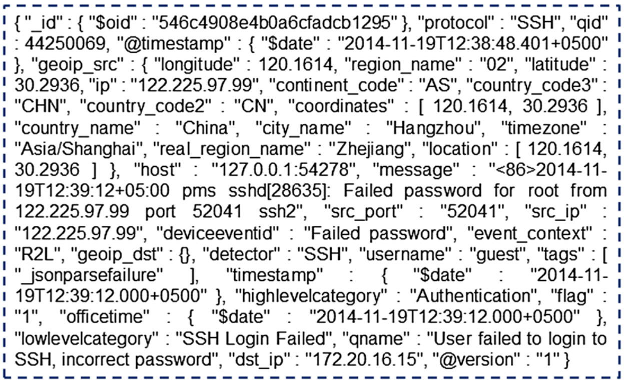
The proposed near-miss situation model provides a complete rule analysis, event-rules ($\mathrm{E} \mapsto \mathrm{R}$) mapping, indication of malicious activities (rules which may turn into an “offense”), and interface for security question based exploration of rules. It is a multilevel model, which collects different SIEM system events via application program interface (API) and maps these events to rules based on categories present in the events. After mapping, the status of each rule is updated in the corresponding visualization. The security analyst can view the rule status as well as critical rules which can cause an offense in real time. Specifically, our model allows the monitoring of events across multiple information spaces using event rules correlation within a network for better detection of the threats and monitoring of network on the basis of events via a single dashboard. This layered dashboard eases the monitoring of malicious activities on critical resources in real time and provides insight about each offense. Thus, a security analyst can have up-to-date knowledge of each rules status.

It is viable to flag near-miss situation before the actual triggering of an alarm, which allow us to undertake the necessary preventive measures (Yin et al. 2004). Near-miss situation can be explained using an example such as, if an alarm triggers on the hundredth failure attempt from a single IP address, then the desired threshold using organization specific intelligence can be set for the indication of may happen situation, say 70. When this threshold is met by any rule, it will be highlighted visually. This draws the attention of the security analyst to examine the incident before it becomes a more severe issue later on if left unchecked.

To facilitate predicting of future network attacks using historical and current states, our proposed tool abstract view shows the status of different rules in real time, and the story page of any associated alarm. The story page provides complete details of each rule with the relevant questions, such as: what is current status of a specific rule? What is the traffic analysis of the network now? What changes have been made on the network before and after an alert? What is the most likely time of the attacks? What is the status of other rules at the same time? This allows one to answer the who, what, when, how, etc. (Ab Rahman and Choo 2015; Ab Rahman et al. 2017). Specifically, the current status of all rules is displayed on one dashboard with a click-and-go functionality. Brief details of the principal components with data formats, conditions, and procedures are as follows.

4.2.1 SIEM events collection

We used security events of the IBM QRadar originally collected from different devices within a network to provide rules status in real time and highlight the situation visually before it becomes worse. Events are collected from the SIEM system correlation module via polling in regular intervals using rest API.To obtain the events and integrate our visual tool with SIEM system, server properties such as, IP address of the system where IBM QRadar is deployed, security token in the form of hash, and locations of the reference datasets are included in the configuration files. An overview of the events related to authentication which is collected in our system is shown in Fig. 4.



```
{ "_id" : { "$oid" : "546c4908e4b0a6cfadcb1295" }, "protocol" : "SSH", "qid"
: 44250069, "@timestamp" : { "$date" : "2014-11-19T12:38:48.401+0500"
}, "geoip_src" : { "longitude" : 120.1614, "region_name" : "02", "latitude" :
30.2936, "ip" : "122.225.97.99", "continent_code" : "AS", "country_code3" :
"CHN", "country_code2" : "CN", "coordinates" : [ 120.1614, 30.2936 ],
"country_name" : "China", "city_name" : "Hangzhou", "timezone" :
"Asia/Shanghai", "real_region_name" : "Zhejiang", "location" : [ 120.1614,
30.2936 ] }, "host" : "127.0.0.1:54278", "message" : "<86>2014-11-
19T12:39:12+05:00 pms sshd[28635]: Failed password for root from
122.225.97.99 port 52041 ssh2", "src_port" : "52041", "src_ip" :
"122.225.97.99", "deviceeventid" : "Failed password", "event_context" :
"R2L", "geoip_dst" : {}, "detector" : "SSH", "username" : "guest", "tags" : [
"_jsonparsefailure" ], "timestamp" : { "$date" : "2014-11-
19T12:39:12.000+0500" }, "highlevelcategory" : "Authentication", "flag" :
"1", "officetime" : { "$date" : "2014-11-19T12:39:12.000+0500" },
"lowlevelcategory" : "SSH Login Failed", "qname" : "User failed to login to
SSH, incorrect password", "dst_ip" : "172.20.16.15", "@version" : "1" }
```

Fig. 4 Events format

Events are collected in the form of key value pair, where key represents the attribute name and value represents the actual value of the attribute (i.e., *key*, IP : *value*, 122.225.97.99). There are variable number of attributes in each event which we collect and process accordingly. All common fields of an events are: Source IP address, destination IP address, time-stamp, high-level category, low-level category, device id, and context etc. These fields are used for mapping each event with the corresponding rule. Understanding of each event characteristics is important in classifying the attacks as internal or external.

The enrichment is also carried out to add the organization and region-specific details in the events for acquiring the intelligence about the attacks which will help to devise the new rules and policies for securing the critical assets. Meanwhile, the format (e.g., time-stamp) conversion is being done to convert values into standard formats.

4.2.2 Events and rules correlation

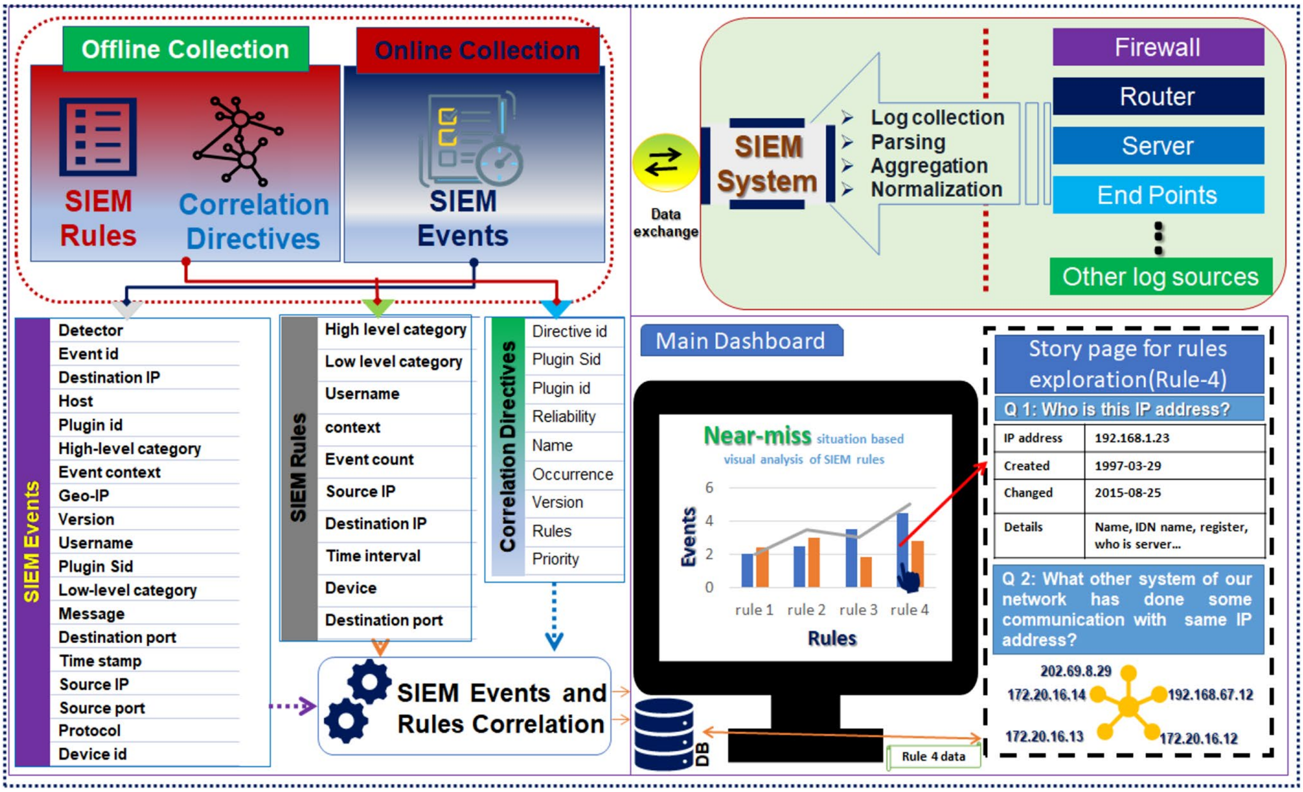
To provide the real time rules status in a fine-grained manner, the collected SIEM events are mapped to the rules based on the attributes present in the events with if/then logic statements. The essence of our approach is to analyze the conditions for triggering the rules of the SIEM-system, to evaluate and visualize the current level of rule execution according to pre-compiled conditions in real time. In this work, we selected ten rules of SIEM mainly from the categories of authentication and anomaly. The abstract information with title about the two categories is explained as, Anomaly (i.e., devices with high event rates, excessive database connections, and excessive firewall accepts from multiple sources to a single destination) and authentication (i.e., login failure attempt to disabled account, login failure to expired account, and multiple login failures for single username). An overview of the all selected SIEM rules characteristics is provided in Table 1.

In Table 1, context is shown via local and foreign and are respectively abbreviated as L and F. Time duration is in minutes, and count shows the total number of events required to trigger the rule. Some rules need single event to fire such as, outbound connection to a foreign computer or outbound connection from a foreign computer on local computer. Meanwhile, some rules need multiple events to raise alerts. It is also possible that one event can map to two different rules at the same time. However, the overlapping is minimized by applying nested conditions in mapping process.

Apart from the common characteristics details provided in Table 1, different high level and low-level categories are also part of the rules which assist in mapping of events on rules. Due to the nature of the different categories and subcategories, it is difficult to have a generic syntax of the SIEMs rule. Every rules has main category (e.g., authentication) and many subcategories like, host login failed, login with username/password defaults failed, mail service login failed, misc login failed, password change failed, privilege escalation failed, remote access login failed, samba login failed, ssh login failed, telnet login failed, VoIP login failed, web service login failed, database login failed, IKE authentication failed, RADIUS authentication failed, TACACS authentication failed, user login failure, and station authentication failed etc. Meanwhile, each rule possesses certain common characteristics and computation is performed on the basis of these characteristics. These characteristics are distinct for each rule and may overlap in more than one rule. Thus, a comprehensive overview of all rules specific conditions is important. Therefore, a detailed analysis of different rules characteristics is provided in Table 1 and Fig. 5.

Table 1 Different characteristics of SIEM rules

Rule no.	Source	Destination	Time	Count	Single event	Multiple events
1	F	L	5	= 100	–	Yes
2	F	L	5	= 100	–	Yes
3	L	F	–	–	Yes	–
4	F	L	–	–	Yes	–
5	F and L	L	5	–	–	Yes
6	F and L	L	–	–	Yes	Yes
7	F and L	L	–	–	Yes	Yes
8	F and L	L	–	–	Yes	Yes
9	F and L	L	5	= 10	–	Yes
10	F and L	L	5	= 10	–	Yes



IP address	192.168.1.23
Created	1997-03-29
Changed	2015-08-25
Details	Name, IDN name, register, who is server...

Fig. 5 System architecture of SIEM rules near-miss situation analysis based on the data acquired from SIEM systems

SIEM directives correlate network attacks using event sequences generated by malicious activity. SIEM directives typically consider a pattern of activity from a single user to increase the reliability of alerts, and do not consider whether the actions of multiple users have collectively achieved a malicious goal. A detailed system architecture based on the data collected from SIEM systems and its service delivery (e.g., rules execution in real time, and exploration) is presented in the Fig. 5. We select SIEM rules, explore their necessary characteristics as described in Table 1, and events data as shown in Fig. 4 which is obtained from the SIEM systems using java program and rest API with ariel query language (AQL) support. This computed data, and events-rules mapping results after correlation are forwarded for the near-miss situation analysis, and are cached in database for exploration purposes simultaneously. The rules and events statistics are visualized later with the help of different security visualizations.

4.2.3 Near-miss situation analysis of SIEM rules

Near-miss situation analysis is performed to visually analyse the events data in real time for monitoring of the current security state using SIEM-systems. This direction is also called visual correlation. Generally, we select SIEM rules and present their status on the basis of the events count in real time and near-miss situation analysis (i.e., whether a particular rule can trigger in fraction of time or not?) which is provided with the help of gradient change. Business logic is implemented at the client side and visualization module updates data at the controllers on continuous polling. This subsystem has support for both near-miss situation and rules specific investigation including attack source, target, malicious activities, insights about the attacks from multiple perspectives and resource misuse. A threshold value is used to determine the near-miss situation.

The desired threshold using organization specific intelligence can be set for the indication of the worse situations. However, lowering the indication threshold results in more frequent warnings which may increase number of candidates rules and complexity of the system. Therefore, events count, frequency of rules triggering, subjective judgement of the security analyst, and organization policies are taken into account while determining the near-miss situation threshold. The frequency of rule triggering(FRT) and event counts(EC) are calculated using Eqs. (1) and (2) respectively.

$$FRT = frq(R_i)/T \tag{1}$$

Table 2 Questions about alarm's insight

Q. no	Question statement
1.	Who is this IP address? From where it belongs?
2.	Show me route information of an IP address?
3.	Which hosts it has connected in last month, last week and last two days?
4.	Any other alarm by the same IP address in past?
5.	Which of our hosts has done some communication with that source IP address?
6.	Does any IP addresses from the same block of source IP address have done some communication with our network?
7.	At what time this connection was established?
8.	What was network behaviour during this activity?
9.	How many users were active before and after attack?
10.	Which application was accessed and for how long?
11.	Which ports are opened at victim's side? What other attacks can be launched on victim machine?
12.	Does the local machine have established connection in past or not?
13.	What other machines from different countries have established connections with that victim machine?
14.	What other escalation privileges has occurred as a result of this connection?
15.	Attempts made by source IP address per minute, per second, and per two minutes?
16.	Does the attacker succeeded in causing breach or not?
17.	Which protocol and port combination is used by the attacker while launching an attack?
18.	Any attempt on some active accounts of our network by the same attacker?
19.	Has the same IP address accessed some other resources of our network?
20.	Summary visualization i.e., attempts on any PC of our network in last 2 weeks, last week or last month?
21.	Which authentication method was tried (SSH, Telnet, FTP)?
22.	What was the event status of the other rules at the time of this activity?
23.	What are the average daily, weekly or monthly login failure attempts made on our network as well as per machine?
24.	Is any other IP address also involved in causing an alarm?
25.	After how much time of the disabling particular account an attempt of failure was made?
26.	What was the behaviour of destination machine during this activity?
27.	Attempt on some disabled account by other attacker?
28.	Activity of that source IP address in our network over the period of one month?
29.	What other machines were communicating with same machine on which failure attempts were made?
30.	Any failure attempt from local system on that machine?

where R_i is a specific rule, T is the total number of rules and frq represents the frequency of rule's firing.

$$EC = N/t \tag{2}$$

where N is the number of total events, t is the time interval in seconds.

Adaptive thresholding often assists in generating new and modifying the existing rules that reduce the number of false alerts that cyber analysts have to respond to Franklin et al. (2017). Meanwhile, this threshold value can be adjusted according to the protection level, organizations policies, and objectives of the security monitoring. Apart from the near-miss situation analysis only the proposed tool enables security analyst to explore the reasoning behind alarms.

This is done by means of the security questions as explained in Table 2. These questions are not covering all security aspects concerning SIEM systems, but they provide the comprehensive details about selected rules. We set questions manually within the developed tool considering rules properties. These questions enable security analyst to understand the attacks sources, attack patterns, and entities involved in the attacks.

5 Case study examples

Similar to the approach in Gray et al. (2015), the proposed tool comprises of two sections, namely: rules visualizations and story page visualizations (i.e. rule specific security questions based exploration). Rule visualization is basically a high-level (i.e., abstract) representation of each rule in term of events (as discussed in examples 1 and 2) of the rule while story page visualizations provide the detailed view of specific rule in terms of the attacker, attacker tactics, and activities etc. in the past as suggested in Hao et al. (2013).

5.1 Abstract view (Rule's visualizations)

This section uses two examples to demonstrate the utility of the near-miss situation based rules analysis. We demonstrate the utility of our approach using the IBM QRadar events, directives and rules data.

5.2 Example 1

In this example, we described the status of the 'Anomaly: Excessive Firewall Denies from Single Source' rule, where the *x*-axis in Fig. 6 represents time and the *y*-axis number of failures. Threshold level indicates the near-miss situation on the specific interval of time. An increase in line magnitude indicates the may happen situation. Figure 6 facilitates the identifying of different source IPs and their attempts on our systems. The legend shows the different source IPs associated with failure attempts. Normally, an upward trend in these lines indicates a malicious situation. Thus, such a visualization not only helps to view the status of the current rule but also the different IPs associated with malicious activities. Moreover, this detailed view of the malicious activities happening on the network would certainly help administrator to pinpoint malicious activities in seconds. The addition of such visualizations on the single dashboard can provide the bird eye view and detailed view of all malicious activities in the network. Each visualization is equipped with click and go functionality which provide detailed insight about activities.

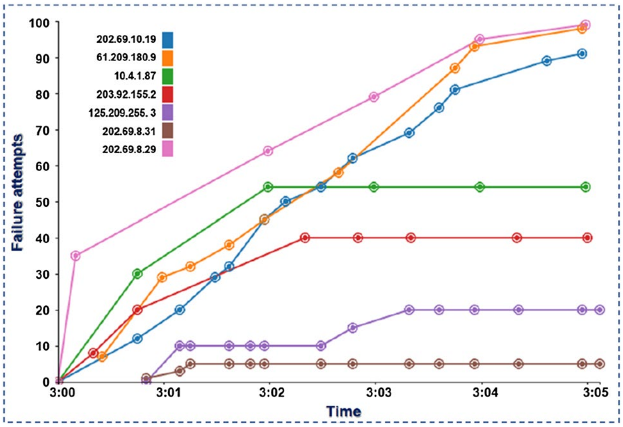


Fig. 6 Anomaly: excessive firewall denies from a single source

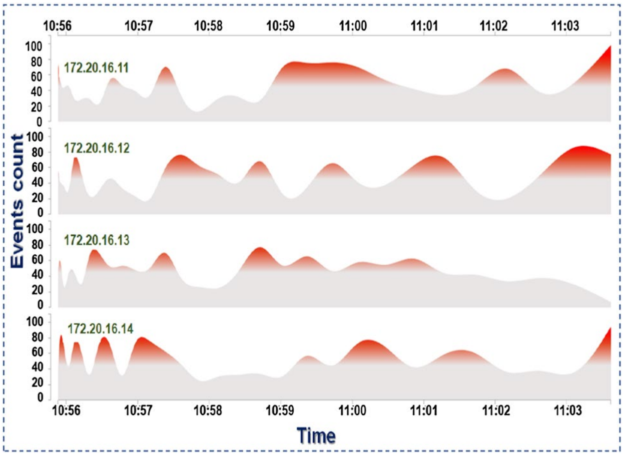


Fig. 7 Anomaly: excessive firewall accepts across multiple hosts

5.3 Example 2

In this example, we described the real time status of the 'Anomaly: Excessive Firewall Accepts across Multiple Hosts and Anomaly: Excessive Firewall Accepts from Multiple Sources to a Single Destination' rules visually. Figure 7 shows the detail of different IPs, event counts of each IP and time, etc. where normal and critical situations are illustrated via gradient change.

This visual analysis of the rules assists security analyst in identifying the malicious activities in advance. In this rule, the visualization *x*-axis represents time and the *y*-axis represents events counts. Threshold level indicates the near-miss situation on the specific interval of time. The threshold between 0 and 50 represents normal situation, the threshold between 50 to 75 represents just the build-up of a benign activity, and 75 onward threshold indicates the may happen situation that may result in a security breach.

5.4 Detailed view (story page visualizations)

Let us suppose that a specific rule has recently generated an alarm and the security analyst is interested to perform security question-based search. If the security administrator wishes to know the reasoning behind the alarm in more detail, the abstract view visualizations (rules visualizations) allow navigation to story page and present the rule details using security questions. The proposed framework uses *D*3 visualizations to present answers of different questions based on SIEM rules data. If the security analyst wishes to examine the network activities, then this visual tool is able to answer the questions being asked by a security analyst. A security analyst can explore every activity detail to the

Table 3 Rules insight: security questions and visualizations

Rule no.	Security questions	Security visualizations
1, 2	$q_1, q_2, q_3, q_4, q_5, q_6$	Data table, map plot, dot plot, bar chart, sequence chart, pie chart
3, 4	$q_1, q_2, q_5, q_6, q_7, q_8, q_9, q_{10}, q_{11}, q_{12}, q_{13}, q_{14}$	Data table, map plot, sequence chart, pie chart, stacked bar chart, dot plot, bar plot, link graph, bubble chart, list, dendrogram, marker plot
5, 6	$q_1, q_2, q_4, q_5, q_7, q_8, q_{15}, q_{17}, q_{16}, q_{19}, q_{22}$	Data table, map plot, dot plot, bar chart, stacked bar chart, bubble plot, sequence chart, timeline, link graph, line chart, tree maps
7, 8	$q_1, q_4, q_9, q_{15}, q_{18}, q_{20}, q_{21}, q_{25}, q_{27}$	Data table, bar chart, stacked bar chart, bubble plot, sequence chart, timeline, link graph, line chart, box plot
9, 10	$q_1, q_6, q_8, q_{12}, q_{14}, q_{15}, q_{16}, q_{21}, q_{23}, q_{26}, q_{28}, q_{29}, q_{30}$	Data table, pie chart, dot plot, list, marker plot, bubble plot, timeline, link graph, stacked pie chart, stacked bar plot, stacked line chart, dendrogram, box plot

required target and gain deeper insight about the activities. We categorize the questions used for exploration in five sets. Each set of questions is used for specific rules with set of visualizations. The detailed overview of the rules, security questions, and visualizations supported by proposed tool are shown in Table 3.

These questions lay foundation of the security monitoring from various aspects and help security analyst to gain insight about the attacks that may happen soon or already have happened. These questions help in conducting the detailed analysis of attacks from various perspectives. The questions for the analyzed event with visual answers are shown below.

1. Which are the top attacking countries based on attack counts?

This question can be answered visually—see Fig. 8.

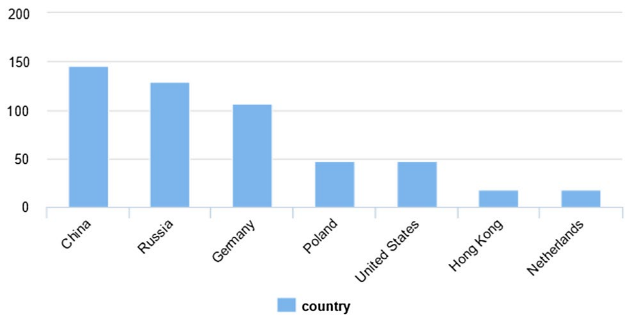


Fig. 8 Top attacking countries based on attack counts

2. What are the ports most commonly used by attackers?

A list of commonly used ports by attackers is described in Fig. 9. Similarly, security analyst can explore IP, ports and other related activities as well which are happening in the network back and forth.

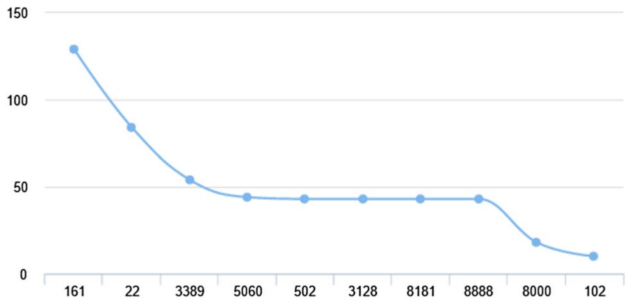


Fig. 9 Mostly used ports while performing attacks

3. What are the most used usernames in attacks?

Figure 10 presents a list of the most used usernames by the attackers while doing SSH attempts.

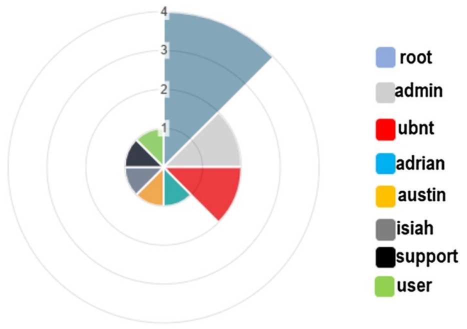


Fig. 10 What are the most used usernames in SSH attempts

4. What are the most used passwords by attackers?

Figure 11 presents a list of the most used passwords by attackers.

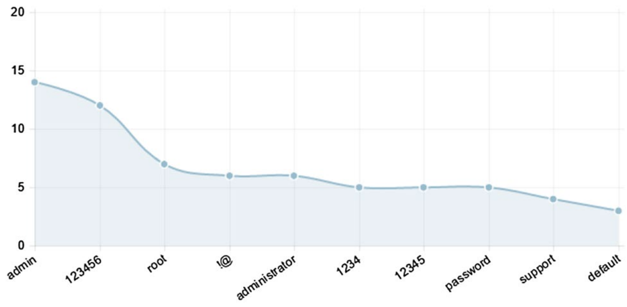


Fig. 11 Most used passwords in attacks

5. Which IP addresses have the most number of failure attempts over a specified period?

Figure 12 lists the IP addresses with the highest failure attempts over a specified period.

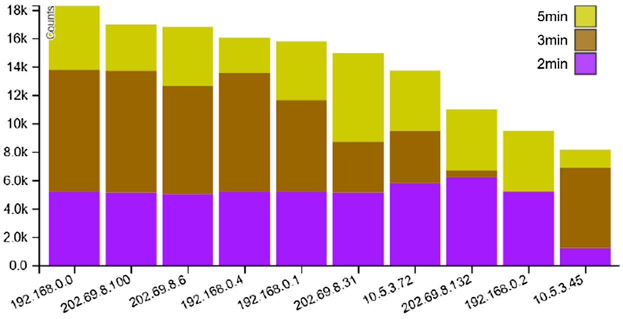


Fig. 12 IP addresses with the highest failure attempts

6. What are the top attacking IP addresses?

A list of top attacking IP addresses is shown in Fig. 13.

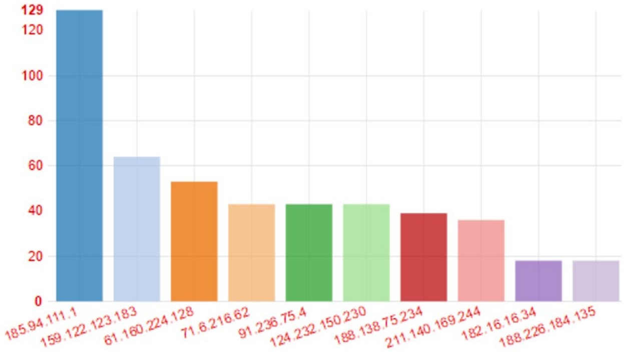


Fig. 13 Top attacking IP addresses

7. How many failure attempts had been made?

A security analyst can examine failure attempts at a country level, which may be useful in formulating future security measures—see Fig. 14.

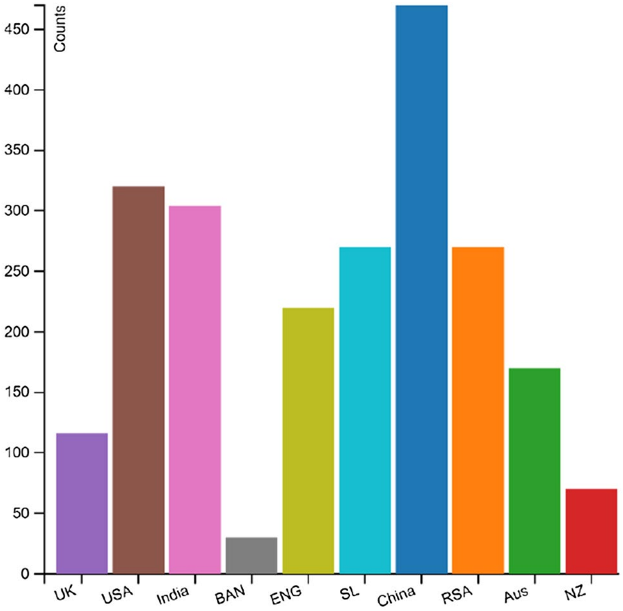


Fig. 14 Failure attempts from different countries on our network

8. How many times an attacker was successful in launching an attack detected by our system?

As we collect more information at both the infrastructure level, as well as the application level, it is important to develop organization specific intelligence based actionable tools. One specific visual analysis could be how successful an attacker is (see Fig. 15). In Fig. 15, the red colour indicates that attacker was successful in causing a breach (i.e., an alarm was raised), yellow colour indicates that attacker met the near-miss threshold, and green colour shows that few events were received from the attacker. The proposed tool provides such statistics about the attacks insights from the events and rules data.

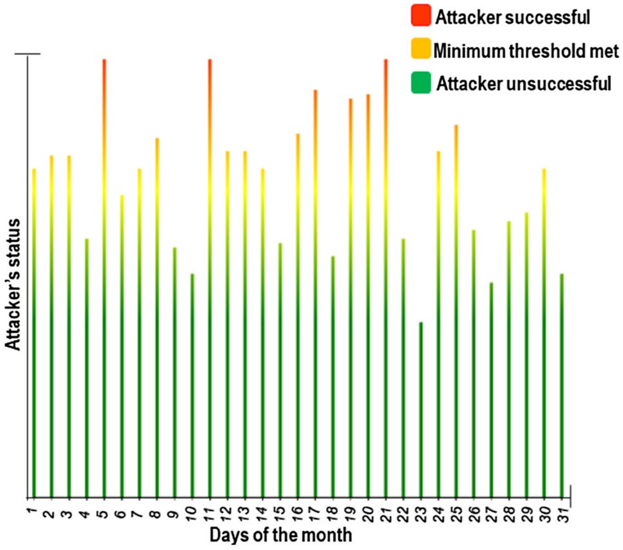


Fig. 15 Attacker failure vs. success analysis on our network

9. What other resources in our network are being accessed by attackers?

Security analyst can also determine resource mis-used, in order to develop more effective defensive solutions (see Fig. 16).

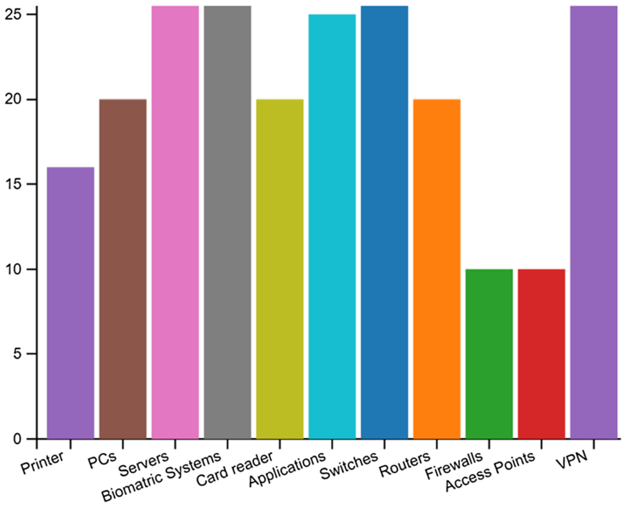


Fig. 16 Other network resources accessed by attackers

10. What failure attempts were made on specific destinations?

This question assists security analyst in carrying out specific destination analysis by studying the failure attempts (see Fig. 17). This relation highlights the association between systems and attacks launched on the particular system. This relation is useful to study the reasons of compromises and security controls enables on the systems.

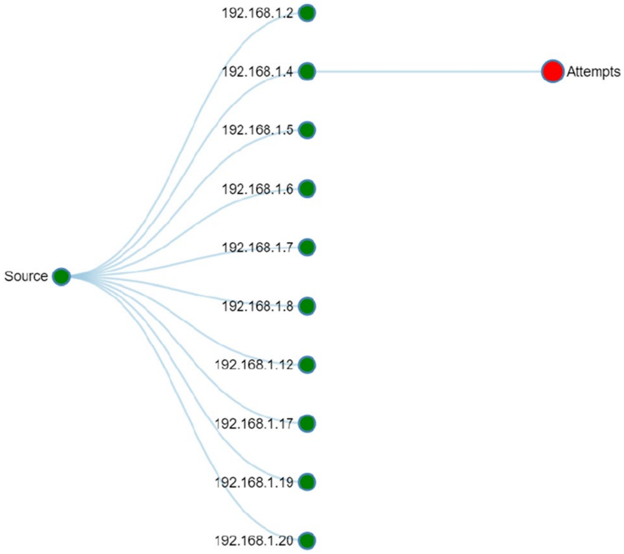


Fig. 17 Failure attempt analysis on specific destinations

11. Any other alarm raised by the same IP address in past?

Security analyst can also explore alarm history of the IPs, in order to develop more sophisticated defensive solutions. This analysis helps in getting detailed knowledge about insider and outsider attacks as well as the attacks frequency. After all, the security analyst can categorize the most active and frequent attacker as potential indicators of compromise (particularly at an early stage). The complete alarms history of an IP address, 172.20.16.11 is shown in Fig. 18.

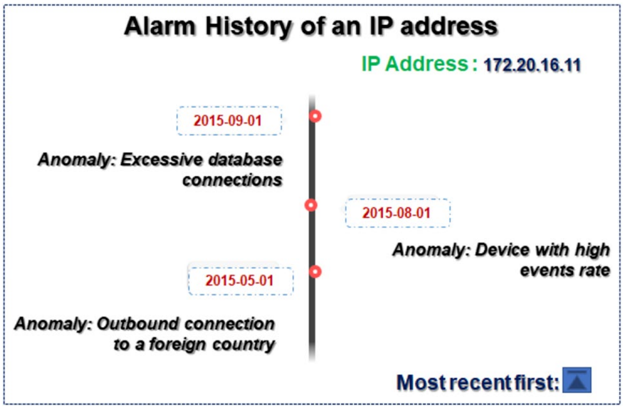

Alarm History of an IP address
IP Address: 172.20.16.11
2015-09-01
Anomaly: Excessive database connections
2015-08-01
Anomaly: Device with high events rate
2015-05-01
Anomaly: Outbound connection to a foreign country
Most recent first:

Fig. 18 Complete alarm history of an IP address

12. What is the overall status of all rules?

At any time, security analyst can also determine the overall status of all rules. This overall rule status helps in getting detailed knowledge about the event rate of the network. The overall status of ten selected rules in terms of their cumulative events is shown in Fig. 19.

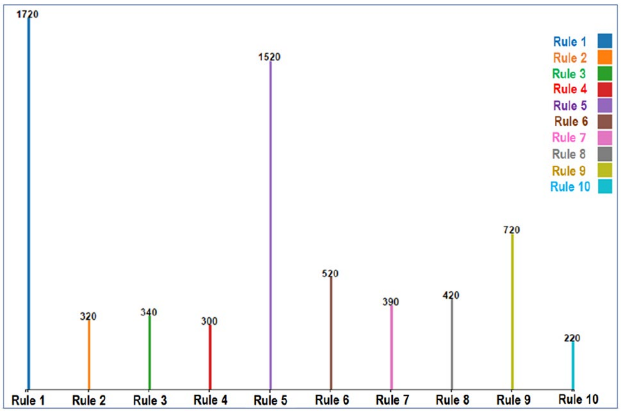


Fig. 19 Overall status of rules

All the questions explained above are extremely important to advance cyber defence mechanisms, and to enhance overall next generation cyber defence architectures. The security questions based intelligence analytics is very much helpful to overcome the advanced threats. For example, if security analyst can determine that which ports, usernames, and passwords are mostly used by the attackers based on the analytics using analyzed events would help to reduce overall attacks. Apart from the advance defence, organizations could even benefit by collaborating and sharing security analytics information with each other (Zuech et al. 2015). These questions provide improved situational awareness and are helpful in integrating SIEM capabilities to how business intelligence is traditionally applied. They also extend SIEM functionality in novel ways as such information can be leveraged for ensuring several protection measures for critical assets and devising new policies against infrastructure. These story page questions and visualizations are helpful in making attack repositories which are helpful in accessing the attack patterns, trends and evolving attacks. Even though there have been other papers on the situational awareness for network monitoring, log analysis, event rules mapping, and alerts analysis, our paper is unique compared to these prior papers in terms of real time rules execution analysis, and forensics. Furthermore, the proposed work uses visualizations rather than textual reports which require several hours to find the facts about the attacks.

6 Evaluation

We surveyed 20 security professionals based in Malaysia, Pakistan, South Korea, and Saudi Arabia after demonstrating the working of visual tool. We provided them twelve security questions and recorded their feedback through five-point scales response criteria: excellent, very good, good, average and poor. We determined the usefulness of our proposed tool that incorporates the near-miss situation and covers various aspects of security concerning SIEM rules by asking the following set of questions from participants:

1. Does the framework help in identifying source and destination of attacks?
2. Does it provide information and monitoring of different attacks?
3. Does it reduce false positives as compared to SIEM reports?
4. Does it provide a sense of real time security monitoring?
5. Does it reduce the complexity associated with the management of SIEM?
6. Does it provide enough support to protect assets (Situational Awareness)?
7. How do you find the historic data analysis about the network activities?
8. Is our framework easy to use in term of navigation and hardware selection?
9. Is the color scheme correct?
10. Does it helpful in attack pattern determination?
11. Does it helpful in understanding of the different breaches?
12. Is the overall information architecture of the application effective?

These professionals have an average of 6 ~ 10 years of industry experience using SIEM, and their responses to the twelve questions were reported in Fig. 20. The missing bar for any category has zero counts.

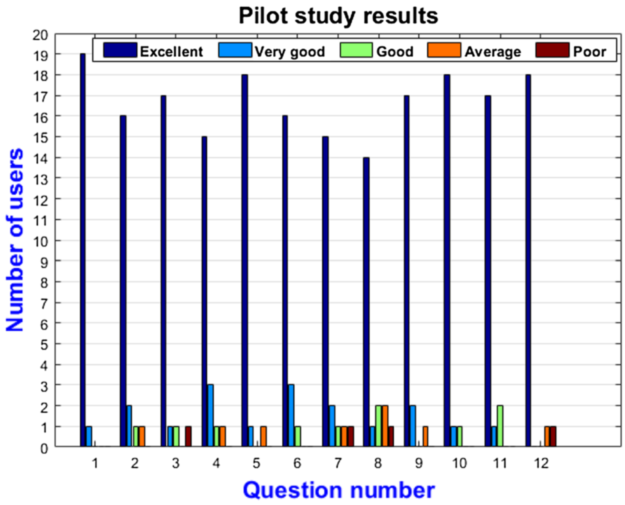


Fig. 20 Pilot study results: cumulative user responses per question

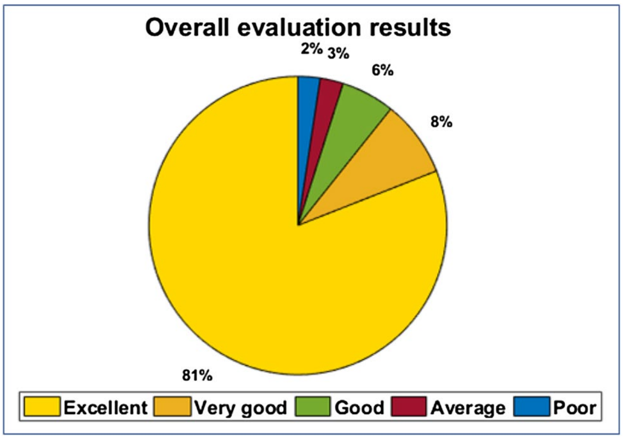


Fig. 21 Pilot study results: overall evaluation

The cumulative responses obtained from the pilot study are shown in Fig. 21. From the results it's clear that the proposed visual tool has above 90% acceptance in fulfilling the security objectives. These results emphasize the validity of the proposed tool with respect to identifying malicious activities timely, improved situational awareness about different rules, and exploring the security situation from different aspects. This study provides additional support for may happen situation as compared to current state of the art SIEM systems. The findings appear to be well substantiated for both real time rules analysis, and rules exploration via security questions.

The proposed visual tool performs well by providing SIEM rules status in real time, and presenting malicious activities details visually for forensics purposes.

7 Conclusions and future work

Cyber security attacks are a trend that is unlikely to fade anytime soon, and while cyber security is a topic that has been widely studied, there are a number of challenges that need to be addressed. One such challenge is limitations underpinning existing SIEM systems. For example, such systems generally are not capable of presenting the rule's status in real time before an alert is raised. Thus, in this paper, we presented a visualization tool for near-miss situation analysis of the SIEM rules and security question-based exploration about different rules. The proposed tool provides security analyst the capability to view status of the many different rules in real time, inspect vulnerable rules, and perform exploration using security questions. In other words, a security analyst could benefit by focusing only on the rules that may trigger an alarm.

We have implemented most of the system functionalities such as rules execution analysis in real time, rules and events status overview, notification components about alert circumstances based on near-miss situation, security questions based exploration, and also a WebGL based interface. However, the system is still in an early development stage, future research includes implementing more advanced functions specifically the custom rules creation from interface, adaptive near-miss threshold selection, interactive visualizations, and machine learning algorithm integration with visual tool for inspecting historical data more and more for various security monitoring scenarios (e.g., anomaly detection and advanced persistent threat). Additionally, we plan to add more number of questions for the exploration, and empowering security analyst to create questions for the forensics goals. We got positive feedback of security professionals regarding both near-miss situation based SIEM rules visual analysis and security questions based visual exploration of rules as approaches for improving cybersecurity incident management. We have high hopes that our unified and near-miss situation aware visual tool will enable analysts to respond to future threats more agilely. Finally, we plan to fine-tune the prototype more for real-world deployments.

References

Ab Rahman NH, Cahyani NDW, Choo KKR (2017) Cloud incident handling and forensic-by-design: cloud storage as a case study. Concurr Comp Pract Exp 29(14):e3868

Ab Rahman NH, Choo K-KR (2015) A survey of information security incident handling in the cloud. Comput Secur 49:45–69

Aguirre I, Alonso S (2012) Improving the automation of security information management: a collaborative approach. IEEE Secur Priv 10(1):55–59

Alsaleh M, Barrera D, van Oorschot PC (2008) Improving security visualization with exposure map filtering. In: Computer security applications conference, 2008. ACSAC 2008. Annual, IEEE, pp 205–214

Anuar NB, Papadaki M, Furnell S, Clarke N (2010) An investigation and survey of response options for intrusion response systems (irss). In: Information security for South Africa (ISSA), 2010, IEEE, pp 1–8

Attipoe AE, Yan J, Turner C, Richards D (2016) Visualization tools for network security. Electron Imaging 1:1–8

Azodi A, Cheng F, Meinel C (2016) Towards better attack path visualizations based on deep normalization of host/network ids alerts. In: 2016 IEEE 30th international conference on advanced information networking and applications (AINA), IEEE, pp 1064–1071

Azodi A, Jaeger D, Cheng F, Meinel C (2013) A new approach to building a multi-tier direct access knowledgebase for IDS/SIEM systems. In: 2013 IEEE 11th international conference on dependable, autonomic and secure computing (DASC), IEEE, pp 118–123

Balabine I, Velednitsky A (2018) Streaming method and system for processing network metadata. U.S. Patent No. 9,860,154. U.S. Patent and Trademark Office, Washington, DC

Barnum S (2008) Common attack pattern enumeration and classification (capec) schema description. Cigital Inc, http://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1 (**3**)

Bauernschmidt B, Schuck J, Webb N (2004) Method and system for visualizing data from multiple, cached data sources with user defined treemap reports. U.S. Patent Application No. 10/371,638

Brewer R (2015) Cyber threats: reducing the time to detection and response. Netw Secur 5:5–8

Briesemeister L, Cheung S, Lindqvist U, Valdes A (2010) Detection, correlation, and visualization of attacks against critical infrastructure systems. In: 2010 eighth annual international conference on privacy security and trust (PST), IEEE, pp 15–22

Cheswick WR, Bellovin SM, Rubin AD (2003) Firewalls and Internet security: repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc, Boston

Cheung S, Lindqvist U, Fong MW (2003) Modeling multistep cyber attacks for scenario recognition, In: DARPA information survivability conference and exposition, 2003. Proceedings, vol 1, IEEE, pp 284–292

Choo K-KR, Dehghantanha A (2018) Introduction to the minitrack on cyber threat intelligence and analytics. In: Proceedings of the 51st Hawaii international conference on system sciences

Choo K-KR, Esposito C, Castiglione A (2017) Evidence and forensics in the cloud: challenges and future research directions. IEEE Cloud Comput 4(3):14–19

Chuvakin A (2010) Siem: moving beyond compliance. White Paper for RSA

Clayton J (2017) Statement on cybersecurity. Last Accessed 5 Feb 2018

Conroy D (2016) Forensic data analysis challenges in large scale systems, In: Intelligent distributed computing IX, Springer, Berlin, pp 451–457

Constantinescu Z, Vlădoiu M, Moise G (2016) Viznetdynamic visualization of networks and internet of things. In: RoEduNet conference: networking in education and research, 2016 15th, IEEE, pp 1–6

Coppolino L, DAntonio S, Formicola V, Romano L (2011) Integration of a system for critical infrastructure protection with the ossim siem platform: a dam case study. In: International conference on computer safety, reliability, and security. Springer, Berlin, pp 199–212

Coudriau M, Lahmadi A, François J (2016) Topological analysis and visualisation of network monitoring data: Darknet case study. In: 2016 IEEE international workshop on information forensics and security (WIFS), IEEE, pp 1–6

DAmico A, Buchanan L, Kirkpatrick D, Walczak P (2016) Cyber operator perspectives on security visualization, In: Advances in Human Factors in Cybersecurity, Springer, pp 69–81

Flynn L, Huth C, Trzeciak R, Buttles P (2012) Best practices against insider threats for all nations. In: Cybersecurity Summit (WCS), 2012 Third Worldwide, IEEE, pp 1–8

Franklin L, Pirrung M, Blaha L, Dowling M, Feng M (2017) Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. In: 2017 IEEE symposium on visualization for cyber security (VizSec), IEEE, pp 1–8

Fratto M (2004) Sneak previews-anomaly detection gets better-q1 labs qradar 3.0 provides comprehensive network behavior anomaly detection with its graphical views of all network traffic. Netw Comput Niles 15(11):32–33

Gray CC, Ritsos PD, Roberts JC (2015) Contextual network navigation to provide situational awareness for network administrators. In: 2015 IEEE symposium on visualization for cyber security (VizSec), IEEE, pp 1–8

Guimarães VT, Rendon OMC, dos Santos GL, da Cunha Rodrigues G, Freitas CMDS., Tarouco LMR, Granville LZ (2017) A reuse-based approach to promote the adoption of visualizations for network management tasks. In: 2017 IEEE 31st international conference on advanced information networking and applications (AINA), IEEE, pp 712–719

Gupta A (2017) Review on big data promises for information security. J Data Min Manage 1(2):1–8

Hao L, Healey CG, Hutchinson SE (2013) Flexible web visualization for alert-based network security analytics. In: Proceedings of the tenth workshop on visualization for cyber security, ACM, pp 33–40

Hideshima, Y, Koike H (2006) Starmine: A visualization system for cyber attacks. In: Proceedings of the 2006 Asia-Pacific symposium on information visualisation, vol 60. Australian Computer Society, Inc., pp 131–138

Hinze SR, Rapp DN, Williamson VM, Shultz MJ, Deslongchamps G, Williamson KC (2013) Beyond ball-and-stick: Students' processing of novel stem visualizations. Learn Instr 26:12–21

Holik F, Horalek J, Neradova S, Zitta S, Marik O (2015) The deployment of security information and event management in cloud infrastructure. In: 2015 25th international conference on Radioelektronika (RADIOELEKTRONIKA), IEEE, pp 399–404

Huang Z, Shen C-C, Doshi S, Thomas N, Duong H (2015) Cognitive task analysis based training for cyber situation awareness. In: IFIP World conference on information security education. Springer, Berlin, pp 27–40

Kabiri P, Ghorbani AA (2005) Research on intrusion detection and response: a survey. IJ Netw Secur 1(2):84–102

Kotenko I, Polubelova O, Saenko I, Doynikova E (2013) The ontology of metrics for security evaluation and decision support in SIEM systems. In: 2013 eighth international conference on availability, reliability and security (ARES), IEEE, pp 638–645

Lakkaraju K, Yurcik W, Lee AJ (2004) Nvisionip: netflow visualizations of system state for security situational awareness. In: Proceedings of the 2004 ACM workshop on visualization and data mining for computer security, ACM, pp 65–72

Lakkaraju K, Bearavolu R, Slagell A, Yurcik W, North S (2005) Closing-the-loop in nvisionip: Integrating discovery and search in security visualizations. In: IEEE workshop on visualization for computer security, 2005 (VizSEC 05), IEEE, pp 75–82

Langton JT, Baker A (2013) Information visualization metrics and methods for cyber security evaluation. In: 2013 IEEE international conference on intelligence and security informatics (ISI), IEEE, pp 292–294

Lee D-G, Kim HK, Kim E (2015) Study on security log visualization and security threat detection using rgb palette. J Korea Inst Inf Secur Cryptol 25(1):61–73

Levine J, LaBella R, Owen H, Contis D, Culver B (2003) The use of honeynets to detect exploited systems across large enterprise networks, In: Information assurance workshop, 2003. IEEE systems, man and cybernetics society, IEEE, pp 92–99

Li T, Yan L (2017) Siem based on big data analysis. In: International conference on cloud computing and security. Springer, Berlin, pp 167–175

Lu M, Chen S, Lai C, Lin L, Yuan X (2017) Frontier of information visualization and visual analytics in 2016. J Vis 20(4):667–686

Mahmood T, Afzal U (2013) Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In: 2013 2nd national conference on information assurance (NCIA), IEEE, pp 129–134

Mantere M, Sailio M, Noponen S (2013) Network traffic features for anomaly detection in specific industrial control system network. Future Internet 5(4):460–473

Marty R (2009) Applied security visualization. Addison-Wesley Upper Saddle River, Boston

McKenna S, Staheli D, Meyer M (2015) Unlocking user-centered design methods for building cyber security visualizations. In: 2015 IEEE symposium on visualization for cyber security (VizSec), IEEE, pp 1–8

Montesino R, Fenz S, Baluja W (2012) Siem-based framework for security controls automation. Inf Manag Comput Secur 20(4):248–263

Nguyen HT, Tran AVT, Nguyen TAT, Vo LT, Tran PV (2016) Multivariate cube for representing multivariable data in visual analytics. In: International conference on context-aware systems and applications. Springer, Berlin, pp 91–100

Nicolett M, Kavanagh KM (2011) Magic quadrant for security information and event management. Gartner RAS Core Reasearch Note (May 2009)

Novikova ES, Bekeneva YA, Shorov AV (2017) Towards visual analytics tasks for the security information and event management. In: 2017 international conference quality management, transport and information security, information technologies (IT&QM&IS), IEEE, pp 90–93

Oseku-Afful T (2016) The use of big data analytics to protect critical information infrastructures from cyber-attacks

Parmelee MC (2010) Toward the semantic interoperability of the security information and event management lifecycle. In: Working Notes for the 2010 AAAI workshop on intelligent security (SecArt), Citeseer, pp 18

Patil S, Meshram BB (2012) Intrusion prevention system. Int J Emerg Trends Eng Dev 4(2)

Pavlik J, Komarek A, Sobeslav V (2014) Security information and event management in the cloud computing infrastructure. In: 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), IEEE, pp 209–214

Product Brief (2008) ArcSight Logger, Simplifying Log Collection, Storage and Analysis, ArcSight

Pronoza AA, Chechulin AA, Kotenko IV (2016) Mathematical models of visualization in siem systems. Trudy SPIIRAN 46:90–107

Qamar S, Anwar Z, Rahman MA, Al-Shaer E, Chu B-T (2017) Data-driven analytics for cyber-threat intelligence and information sharing. Comput Secur 67:35–58

Ring T (2014) Threat intelligence: why people don't share. Comput Fraud Secur 3:5–9

Roberts C (2013) Discovering security events of interest using splunk. SANS Institute

Rohs M, Essl G (2006) Which one is better? Information navigation techniques for spatially aware handheld displays. In: Proceedings of the 8th international conference on multimodal interfaces. ACM, pp 100–107

Rowland CH (2002) Intrusion detection system. U.S. Patent No. 6,405,318. U.S. Patent and Trademark Office, Washington, DC

Sethi A, Paci F, Wills G (2016) Eevi-framework for evaluating the effectiveness of visualization in cyber-security. In: 2016 11th international conference for internet technology and secured transactions (ICITST), IEEE, pp 340–345

Shabtai A, Klimov D, Shahar Y, Elovici Y (2006) An intelligent, interactive tool for exploration and visualization of time-oriented security data. In: Proceedings of the 3rd international workshop on visualization for computer security. ACM, pp 15–22

Shah A, Abualhaol I, Gad M, Weiss M (2017) Combining exploratory analysis and automated analysis for anomaly detection in real-time data streams. Technol Innov Manag Rev 7(4):25–31

Ohnof K, Koikef H, Koizumi K (2005) Ipmatrix: an effective visualization framework for cyber threat monitoring, pp 678–685

Stein G, Chen B, Wu AS, Hua KA (2005) Decision tree classifier for network intrusion detection with ga-based feature selection. In: Proceedings of the 43rd annual Southeast regional conference, vol 2. ACM, pp 136–141

Suarez-Tangil G, Palomar E, Ribagorda A, Zhang Y (2014) Towards an intelligent security event information management system. http://www.seg.inf.uc3m.es/papers/2013nova-AIS-SIEM.pdf

Sun K, Jajodia S, Li J, Cheng Y, Tang W, Singhal A (2011) Automatic security analysis using security metrics. In: Military communications conference, 2011-Milcom 2011, IEEE, pp 1207–1212

Sun Y, Overbye TJ (2004) Visualizations for power system contingency analysis data. IEEE Trans Power Syst 19(4):1859–1866

Tassone CF, Martini B, Choo K-KR (2017) Visualizing digital forensic datasets: a proof of concept. J Forensic Sci 62(5):1197–1204

Villella P, Petersen C (2011) Log collection, structuring and processing. U.S. Patent No. 8,032,489. U.S. Patent and Trademark Office, Washington, DC

Wenge O, Lampe U, Rensing C, Steinmetz R (2014) Security information and event monitoring as a service: a survey on current concerns and solutions. PIK-Praxis der Informationsverarbeitung und Kommunikation 37(2):163–170

Yin X, Yurcik W, Treaster M, Li Y, Lakkaraju K (2004) Visflowconnect: netflow visualizations of link relationships for security situational awareness, In: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. ACM, pp 26–34

Zander S, Nguyen T, Armitage G (2005) Automated traffic classification and application identification using machine learning, In: The IEEE conference on local computer networks, 2005. 30th Anniversary, IEEE, pp 250–257

Zhang T, Liao Q, Shi L, Dong W (2014) Analyzing spatiotemporal anomalies through interactive visualization. In: Informatics, vol 1. Multidisciplinary Digital Publishing Institute, pp 100–125

Zuech R, Khoshgoftaar TM, Wald R (2015) Intrusion detection and big heterogeneous data: a survey. J Big Data 2(1):3