Security Information and Event Management – Capabilities, Challenges and Event Analysis in the Complex IT System

Mario Žgela
Croatian National Bank
Trg hrvatskih velikana 3, Zagreb, Croatia
Mario.Zgela@hnb.hr

Ivan Penga
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
Ivan.Penga@foi.hr

Abstract. *Important prerequisite for adequate data protection is to collect, monitor, analyse and react on different events in an IT system. Security Information and Event Management solutions (SIEM) advantage over traditional platform-centric log management is centralization of event data thus creating prerequisites for efficient correlation and incident management. Paper explains importance of SIEMs in modern IT environment, desirable characteristics, challenges and future development. Specific real world security events created in various IT platforms are collected, analysed, correlated and conclusions are drawn. In total 3.462.187 IT events from 10 platforms during 1,5 months period were gathered. It is clarified how events from different environments should be mutually related, understood and how possible incidents, anomalous or non-standard behaviour may be identified – all with the objective of information security improvement.*

Keywords. SIEM, security incidents, IT event monitoring, correlation of events

1 Introduction

Security Information and Event Management (SIEM) is a technology that enables detection of threats and security incidents as well as a prompt incident response by use of near real time event log collection and analysis of various, disparate event data. Very often, term SIEM is used interchangeably with SEM (Security Event Management) as noted in [What's the difference between SEM, SIM and SIEM?].

The main SIEM objective is to improve threat detection capabilities. Detection is possible only if IT events are gathered and appropriately analysed which is increasingly complex at least because:

a) variety of platforms, services, applications, users and solutions within the IT system environment,
b) consequently, as a result of a), number and type of events increases,
c) types of threats become very distinct, variable and hard to understand.

Contemporary threat detection solutions like intrusion detection systems, firewalls and intrusion prevention systems are potentially capable of detecting simple anomalies and attacks that are isolated on one platform. However, events that are mutually related and activated on different platforms will usually stay undetected unless solution for centralized events logging together with advanced correlation analysis is implemented.

In order to mitigate threats, SIEM solutions very often offer various capabilities:

a) agent or agentless event collection,
b) aggregation and normalization of events,
c) near real time event monitoring,
d) pre-defined engine for threat identification, with possibility of custom rule definition, and
e) searching and reporting on various threats.

Although modern SIEMs include advanced possibilities, there are numerous challenges and issues that should be taken care of during implementation. Also, there are still some open issues which should be resolved.

2 Purpose of a Paper

The main purpose of this research paper is to analyse and assess desirable characteristics, magnitude of challenges related to the use of SIEM solutions, to research how concrete security event data can be analysed and useful conclusion taken out. Numerous events are collected from bank's IT system and investigated in order to describe techniques for

detection of threats, breaches and anomalous behaviour in specific information system[1].

There is no organization fully resistant to security attacks. Additionally, with modern IT implementations, services and applications businesses and people get more IT bound and dependent. The painful consequence is that attacks, possible incidents and breaches pose even greater risk for organizations and individuals alike. Various technical reports, media news and individual experience show that as IT solutions enter more and more domains of business and activity in general, number and magnitude of attacks increases. Furthermore, attacks are becoming highly innovative and disparate (DBIR, p. 22). According to (DBIR, p. 4), in 2018 there were over 53.000 incidents and 2.216 confirmed data breaches in the world, counting only incidents and breaches in business organizations and excluding botnet attacks[2]. Tactics utilized for attack are various: 48% featured hacking, 30% malware, 17% of breaches were based on errors as a causal event, 17% social engineering, 12% privilege misuse and 11% involved physical actions. Breaches are noted in almost all business sectors, attackers were mostly outsiders with significant internal actors involved (Fig. 1).

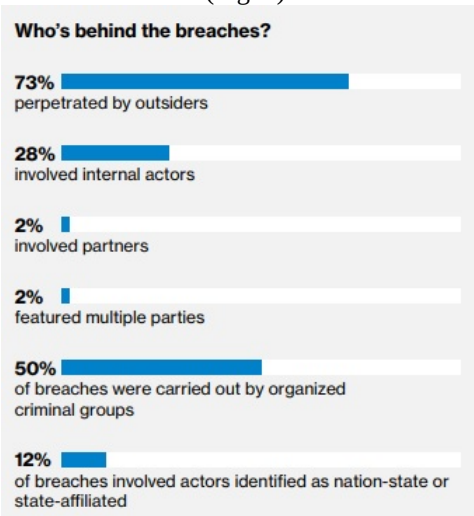

Figure 1. Structure of attackers (DBIR, p. 5)

Numbers show that despite IT investments, use of modern technology and advance security measures does not ensure safe and protected IT environment. Furthermore, while it is not possible to determine how much time is spent in intelligence gathering, the time from first action in an event chain to initial compromise of an IT platform is often measured in minutes. Breach discovery time is likelier to be weeks or even months (DBIR, p. 10). This proves that event monitoring and analysis is extremely important in realizing that attack is pending as well as understanding when incident and/or breach are accomplished. That is exactly where SIEM solutions can offer significant help.

The purpose of this paper is to:

a) explain imperative characteristics of contemporary SIEM solution,
b) indicate possibilities for SIEM improvement, and
c) analyse real world data collected within a banking IT system and indicate how SIEM can be used as a platform for complex event analysis and discovery of possible incidents.

3 SIEM Architecture and Capabilities

A notable model of SIEM architecture is explained in Fig. 2 (Swift, 2006, p. 18-19).

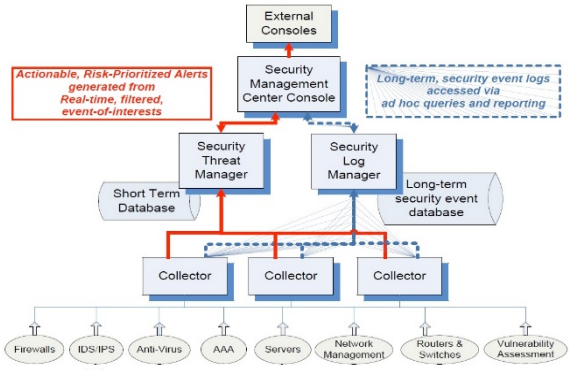

Figure 2. An example of SIEM architecture

On the bottom line, different platforms from which events must be gathered are displayed. Collector is a process which actually gathers data events and it can be in various forms – from agents that are resident on the monitored platform or agentless solutions to centralized logging process with abilities to split and accordingly format streamlined data. Agent is a software provided by a SIEM vendor which is capable of transferring and converting the log entries from the target system to a SIEM application collector. The key agent features are pre-filtering of log entries based on their severity or type and ability to normalize log entries so they can be more easily compared, comprehended and correlated to other events. Agents send log entries to SIEM application collector over secure connections. In agentless solutions platform sends log entries to a SIEM collector, thus mitigating the need for an agent to be installed on corresponding platform. Syslog, which may send log data directly to collector, is such example (Dorigo, 2012, p. 26).

However, there are numerous different platforms with different message standards, various types of data

[1] Data that is in the research focus was collected from Croatian National Bank's IT system. All data is depersonalized and masked in order to avoid eventual privacy and security threats and issues.

[2] Actually, number of botnet attacks was 43.000 (DBIR, 2018, p. 7).

and often converse semantics behind, for example Syslog, NetFlow, SNMP, jFlow, NCSA, ELF. Some platforms do not pass on the events data to SIEM, or any other, solution. In these cases, ready-made software agents or other customized software with pull capabilities must be implemented.

A threat manager component, detective and investigative – as noted in chapter 4, should process and correlate events gathered by the collectors in near real time and report detected threats and attacks to a security management console or another presentation layer solution (Swift, 2006, p. 19). Threat manager should store events generated in shorter period of time, typically 30 days, in order to quickly identify threats and thus prevent incidents.

Security log manager component comprehends compliance and regulatory obligations, policy management and everyday operations monitoring, as noted in chapter 4. It has to store vast amounts of data, may take either raw logs or filtered events of interest. Often, it is necessary to compress and index events data for a long-term forensic analysis and compliance reporting. Since log manager content is related to regulatory and compliance activities which are often connected to commercial, internal and regulatory (state) auditors capacity for storage of significantly more than 12 months of data may be required. Closing of books at the end of the business or fiscal year, audit performed and finalized are crucial for the definition of capacity and time span for events storage (Swift, 2006, p. 19).

Security consoles cover presentation layer. They contain information about events, priorities, event correlation, threats, incidents, history logs in meaningful manner in order to improve organization's security and protection levels. In larger organizations, consoles may be arranged for a larger number of security experts and even giving certain subsets of information to each of them. E.g. antimalware expert should have insight in all antimalware platforms events as well as certain security devices (firewalls, network traffic analysers). However, it is important to define subsets in a manner such that entire sequence of all related events is not lost.

Log data collection is the focal point of any SIEM. Typically, greater the number of platforms included in log management, SIEM will have the greater effect. However, logged events collected on single platform rarely contain information necessary to understand them inside the context of IT system and related business activities. Furthermore, security personnel are not experts for each platform IT system relies on. That is why normalization, aggregation and correlation are immensely important. Often, SIEM solutions may include hundreds of different source platforms because these events provide the data needed for analysis of the status and security of IT system. In order to get a broad end-to-end view, everything what is collected must be consolidated on a single platform. Aggregation is the process of moving data and log files from disparate sources into a common repository. Collected data is placed into a homogenous data store, typically proprietary flat file repositories or relational databases where analysis, reporting, and forensics occur. The process of aggregation, compiling these dissimilar log data (event feeds) into a common repository, is fundamental to any useful SIEM solution. Perhaps most importantly, having all the data on a common platform allows for event correlation and data analysis, which are key to addressing the security challenges organizations are facing today (Lane, 2010, p. 1).

Normalization is the process of converting logs collected on each platform into a universal format, which will be used within the SIEM solution. Each IT platform generates specific events with different attributes (columns). E.g. firewall log usually contains data on source IP, destination IP, source port, destination port, action (deny or allow), username. During normalization process, handful of event attributes (columns) produced by certain platform are reduced to common event attributes. In order to get more information about event, very often additional data enrichment is performed. In its essence, enrichment is a process of adding data to event generated by an IT platform in order to improve analysis and forensics. Added data is related to context that is not included in the original event data sent by the source platform, such as a geolocation, email address, client operating system version, active application modules and services running on a client platform. During normalization process, events should also be categorized into certain event types such as "Regular http request", "Excessive administrator privileges used", "Configuration change", “Regular file access”, "Excessive file access privileges" and “Buffer overflow attack".

SIEM solution should automatically analyse and react on certain event patterns registered on various platforms. It should use other information in order to detect context and threats like user privileges, user status (e.g. user on a sick leave, holidays, remotely located), timestamp, period of the day (e.g. opening hours), physical location of a platform and user initiating the event. Set of events that represent potential security incidents are additionally validated against contextual information in order to make appropriate conclusions (Ganapathy, 2018, p. 4). For example, backup of a server file system which holds user documents and files is usually regular operation which should be performed in order to ensure availability of files in case of system malfunction or data corruption. However, if backup is executed out of regular time periods it may be marked as suspicious and checked against other contextual information. If backup is preceded by:

- set of few Remote Desktop Protocol (RDP) actions resulting in failure,
- successful RDP action,
- set of few unsuccessful logons to a file server,
- successful logon to a file server,

- intensive file search through various folders,

it may be proof of attack and such set of events should be marked as a highly possible incident. Correlation engine analyses all these events as a whole and alerts security experts through presentation layer (security console). Some characteristics of an event correlation engine are shown in Fig. 3.

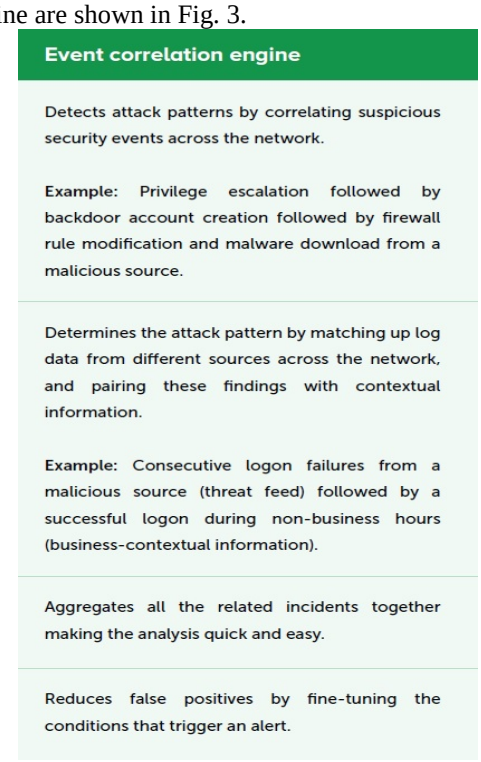

Figure 3. Event correlation and examples (Ganapathy, 2018, p. 5)

4 SIEM Challenges and Future Development

One of the most important features of SIEM solution is the efficient management of great number of events, their correlation, automatic actions and response on threats and incidents. For example, incident management policy will automatically disable database user account if five unsuccessful login attempts are made within three minutes time span on specific database. These are simple, one-platform set of events, which are obvious, easy to understand, without any need to correlate them to any other events, context or status. But, if a user who is on a sick leave connects to a database which is not (or at least which should not be) accessible remotely, then it is probably security incident which is not so easy recognizable.

Some SIEMs include the ability to execute external scripts, shutdown compromised service or running process or automate rule additions to existing security devices or IT platforms. Let us consider following scenario:

1. users are accessing certain white listed web site,
2. few minutes after web access, antimalware software detected same type of malware on all endpoints accessing specific white listed web site.

It is highly probable that white listed web site included a malware that was discovered by existing http antimalware solution. So, it makes sense to automatically move web site address from white to black list in order to prohibit other users from accessing contaminated site. While in this scenario such reaction sounds desirable, it is sometimes impractical and human intervention by a trained professional is often more appropriate. Additionally, for a forensic reasons or business needs, a compromised system sometimes may have to stay online (Swift, 2006, p. 27).

Furthermore, types of attacks very often does not follow historically known pattern or set of events, but are becoming extremely inventive. Among those, zero day exploits pose significant risk to integrity, confidentiality and availability of IT system. So, sandboxing solutions should be tightly integrated with SIEM solutions in order to adequately mitigate risks.

False positives are one of the most significant challenges in every SIEM solution. False positives may pose enormous burden for security staff which is anyways very limited in number and capabilities especially when compared to increasing number and types of platforms which have to be included in event monitoring.

Artificial intelligence (AI) is one of key technologies that should be used in order to decrease number of false positives. It enables SIEM to learn from vast amount of data collected from different IT platforms - it can relate data and automate its system to detect new anomalies, outliers, potential threats and incidents. It may figure out significant hidden relationships between disparate data and thus predict future problems. While learning from the data and noticing mistakes in its conclusion engine, AI also reduces its error rate. AI and SIEM solutions make possible to increase IT security team efficiency through vulnerabilities, threats and cyber-attacks detection. This technology has improved to predict unknown threats attacks with minimal human analyst intervention. As already noted, AI within SIEM allows IT security team to reduce the frequency of false positives, which require human intervention. Doing so, SIEM analysts can redirect their attention and the time they invest in checking false positives to focus on higher priority threats and incidents. The integration of AI with SIEM solution offers following advantages (Rivas, 2018, p. 2):

- AI uses cognitive reasoning to determine the relationship between anomalies without human supervision.
- It changes focus from traditional reactive security systems to a new and proactive solution. It enables security teams to mitigate risks, eliminate threats and prevent incidents

rather than spending resources on incident resolution after they happened.
- Reduction of false positives allows IT security team to concentrate their intuition and creativity on higher priority events.
- AI optimizes UEBA module (User and Entity Behavioural Analytics) to detect irregular patterns in users' behaviour. For example, these patterns include changes in users' regular system logon time, entry schedule, frequencies of users' transaction generation and updates or connections from different geographical locations.

Massive number of file updates by certain users in file system folder can seem like inappropriate activity, and some SIEMs would declare such event as incident. However, such event may be a consequence of regular activity: for example, authorized user has obligation to perform massive file updates every last Friday in a month and it should not be concluded that event is the result of an incident. AI engine could recognize it as a regular and present it as such in a security console.

There are numerous examples of data loss and data theft. Very often, data is sent out of companies' premises over telecommunication networks without adequate analysis of its confidentiality. Furthermore, there are situations in which regular users with adequate privileges copy data on various storage media types. Consequence is that it is not possible to monitor the usage of such data. Here is where data loss prevention (DLP) processes may be taken into consideration. Merging SIEM solution with DLP becomes clear necessity and streaming various DLP events to SIEM could surely improve incident management. For example, shortly after bank's employee received an e-mail from a suspicious domain, he logged on database, performed search on personal current account data, exported them into text file and included the file into reply to a suspicious e-mail address. SIEM system should perceive that data loss is about to occur, and as a consequence, should change e-mail server configuration. Changes may result in preventing all outbound e-mails to suspicious domain or prohibit sending a particular attachment with current account data.

Enrichment of event data should also adequately reviewed and considered. Data enrichment designates adding information or context to the data present in the platform logs as they are collected in order to increase the analytical value. It contains events sent by the monitored platform of interest with context data not in the original event, such as an email address, phone number, host location information, identities across multiple platforms, behavioural information, application runtime version, browser type initiating action, application data etc. Application data may be particularly interesting and usually focuses on application module, function or procedure initiating the event, specific data being processed by application, data about evasion of DLP rules, active window, tracking asset ownership, performance and utilization characteristics, associating users, end points and activities etc. This enriched data becomes part of the parsed event and is stored with the event just like the original fields. A number of platforms generate additional data, i.e. offers data enrichment property. Those data supplement gathered log data about event to improve analysis, incident management and risk mitigation.

Event correlation requires knowledge about the context, which is relevant in order to assess if set of events is important for further analysis. Without the context, analysis is usually meaningless. Furthermore, analysis of individual event without correlation in specific context is highly ineffective and leads to wrong conclusion, a number of false positives and false negatives. Context contains the information on what data event represents and what is its relevance. There are different types of context advanced SIEMs should recognize:

a) asset context – defines the platform on which event happened. Additionally, SIEM must take into account vulnerabilities that exist for a specific platform, and act accordingly. Attack history (local, or on larger scale) on certain platform also helps in definition of a context. Asset criticality is extremely important in risk assessment of an event, because not the same level of incident importance is defined on critical and regular or testing environment. For example, unavailability of a test database is not of a same criticality as unavailability of production payment system database.
b) user context – defines user business roles, user attributes and their translation into platform privileges through user accounts. Usually, there are a number of user accounts in the certain IT system. That contributes to a complexity of user context. A special attention needs to be given to privileged user accounts, like administrators, root or super users. User business roles should clearly define what is a function of a user within a business and, consequently, IT system and platforms. Specifically, segregation of duties should be carefully set and analysed within a SIEM. While performing event correlation, SIEM must take into account user attributes, like out of office, on a leave, office location, usual and outlier behaviour. For example, user who is on a holidays usually should not create payment message in a SWIFT system. If not correlated with user attributes ("user on a holidays"), this could go unnoticed because technically, this event is perfectly allowed.
c) temporal context – defines specific time or time period in which event(s) is generated. Certain event in specific time may be regular and allowed while in some other exact time may be very suspicious and deserve

classification as critical. For example, log on on internal payment system application at 23:30 probably denotes an incident while log on at 10:00 is regular event.

d) location context – denotes physical or logical location of platform on which event is triggered. If access to the application is allowed only from internal IP address space, and user is accessing the application from IP address which corresponds to public network, it is obviously sign of rule avoidance and a security incident.

Modern SIEMs must analyse various combinations of all above mentioned contexts.

5 Event Analysis Within the Complex IT System

SIEM stored events collected from various IT platforms in the period from 1st February 2019 to 15th March 2019 were thoroughly analysed and conclusions are being made and presented in this chapter. In total, there are 3.462.187 events, gathered from the following platforms: active directory domain, firewall, email server, production database, application server, client application, collaboration tool, server file system, endpoint antivirus/antimalware, firewall antivirus/antimalware (inspection of http and e-mail protocols). Typically, following data are collected and centrally stored in the SIEM: platform, timestamp, action performed, object referenced by action, user, source IP address, destination IP address, machine name, physical location. Data are furtherly normalized in order to convert disparate input log structures into unique data structure with common meaning. Some data are enriched with context with the aim to improve analytical capabilities of a threat assessment process.

Analysis was focused on eventual breaches of segregation of duty and possible avoidance of organizational policies, data management and DLP, behavioural change and malware identification. Four types of performed correlation event analysis are briefly explained in the following chapters.

5.1 Complex Set of Events – Potential Violation of Segregation of Duties

Thorough investigation of SIEM stored events revealed the case of user A performed active directory domain (ADD – platform ADdom1) login and e-mail account, while simultaneously user B executed logon to database. Furthermore, user B exported data related to commercial bank balance sheet from database tables (labelled as "DB") to XML file and store it on File Share disc (labelled as "Fshare"). Consequently, user A connected to collaboration tool and copied XML file to collaboration tool (labelled as "Coll") folder. All activities were initiated on the same endpoint (machine name). Both user A and B had all required privileges for all mentioned activities. However, the fact that two users were performing subsets of the activities from the same endpoint rose the curiosity of security staff.

Table 1. User A and B actions on particular machine name (endpoint)

user	platform	action	Actobj	time
A	ADdom1	Logon		5/3/19 8:12:03
A	Email	Auth		5/3/19 8:13:45
B	DB	Logon		5/3/19 10:41:28
B	DB	Select	Select...	5/3/19 10:50:31
B	DB	Export	Select...	5/3/19 10:51:59
B	Fshare	Create	File.xml	5/3/19 10:52:49
A	Coll	Logon		5/3/19 10:55:41
A	Fshare	Copy	File.xml	5/3/19 10:56:07
A	Coll	Create	File.xml	5/3/19 10:56:28

IT security staff and business function minutely investigated process in order to draw more conclusions whether some delicate violation of segregation of duties was performed. Investigation revealed that whole set of events can be approved as justifiable: two users with appropriate set of privileges used the same machine interchangeably. XML exported balance sheet data was exchanged via collaboration tool with the bank which is owner of those data meaning data confidentiality was preserved. Although both users had the appropriate access rights (i.e. granted privileges were not violated), internal process was changed in order to prohibit such behaviour in the future. Also, complex set of IT rules was created in order to prevent future similar activities within the IT system.

5.2 E-mail&Cloud Services – Data management and DLP

SIEM detected occasional accesses to external mail services accounts, simple e-mail correspondence between external and Bank's e-mail servers, upload and download of files to/from cloud drive services (e.g. Google drive). Internal check-ups proved users had appropriate privileges and no confidential information was transferred to third party services. Anyways, such setup could be potentially exploited by the attackers, disgruntled employees as well as by the security unaware employees.

Table 2. Usage of external e-mail and cloud drive services

user	Platform	action	Actobj	time
C	FW	inbound	Gdrive	13/2/19 9:05:32
C	FW	Outbound	Gdrive	13/2/19 9:09:19
	...	...	...	
D	FW	Outbound	Dbox	19/2/19 11:21:07
	...	...	...	
E	FW	Logon	Gmail	21/2/19 14:45:11
E	FW	Send	Gmail	21/2/19 18:51:28

As a consequence, DLP system was upgraded and reconfigured in order to check up data in transit to external e-mail services. If some confidential data is identified, either in the body or e-mail attachments, transfer is forbidden. All traffic from and to external drive services is prohibited and disabled for all Bank's users.

5.3 Domain Authentication – Behavioural Change

All domain authentication procedures (logons) are audited and s tored in both platform and central (SIEM) logs. Temporal, user, asset and location context were analysed aiming at all logons of the same user occasionally originating from unusual IP addresses or endpoints. While these actions may be a part of regular activities, they may indicate successful social engineering resulting in misuse of authentication credentials by unprivileged users. During observed period, it was discovered that user X always connects and disconnects (43 logons and logoffs in total) to ADD from IP address 10.170.202.17 until 8th of March when he performed logon from different IP address (10.170.202.161). IP address range 10.170.202.1 to 10.170.202.60 is dedicated to building A, while range 10.170.202.100 to 10.170.202.200 is dedicated to endpoints located in building B. No DHCP (Dynamic Host Configuration Protocol) is implemented on networks and endpoints on either location.

Table 3. User X ADD logon/logoff events

platform	action	IPaddr	location	time
ADdom1	logon	10...17	A	11/2/19 8:24:10
ADdom1	logoff	10...17	A	11/2/19 16:58:31
ADdom1	logon	10...17	A	12/2/19 8:10:23
40 more logons – location A				
ADdom1	logon	10...161	B	8/3/19 11:24:43
ADdom1	logoff	10...161	B	8/3/19 12:33:03
ADdom1	Logon	10...17	A	8/3/19 13:12:31

It may be concluded that typical behaviour pattern shows that user X authenticates from location A using endpoint with the IP address 10.170.202.17. However, on 8th of March user X suddenly performs login from location B, logs off from the same location and after brief period logs on from hers/his "standard" IP address on location A. This denotes a significant behavioural change indicating:

- threat or incident stemming from social engineering or other successful attack, or
- regular temporary change caused by justifiable business reasons

Additionally, user X is granted privileges to run and use certain business applications. Further investigation performed by security professionals indicated that user X did not authenticate to business application with his credentials while authenticated to ADD from endpoint on location B. However, during that period of time user Y was connected to business application from the same endpoint (i.e. the same IP address: 10...161) which is also not regular, usual behaviour. Regular set of events includes username which logs on to ADD and business application by the same IP address on the unique location. This set of events was not strictly required and technically enforced on the IT infrastructure within the observed business entity. In this particular case, variation in behavioural pattern was clearly justified by business functions and internal control policies, which concluded further investigation[3].

5.4 Security – Malware Identification

SIEM identified that users F, G and H visited specific internet web site which was not black listed by a proxy or a firewall. Shortly after, SIEM noticed that client antimalware registered malware code (file Djsp – as noted in column Actobj) on machines belonging to users F, G and H. Since security configuration is very advanced, malware was prevented from execution harmful code on endpoints so no damage was done. Notification about three consecutive malware appearances was sent to security staff immediately after potentially harmful events were correlated. Security staff undertook further steps in order to

[3] User X logged on to ADD from location B because of a simple yet justifiable reason: she/he presented some data stored on network file system for which user X access rights were needed, while simultaneously user Y logged on to business application in order to compare two data sets.

minimize threat – in this case, specified web site was black listed.

Table 4. Web access and endpoint malware detection

user	platform	action	Actobj	time
F	FW	http	w.x.y.z	18/2/19 8:17:18
F	FW	MW detect	Djsp	18/2/19 8:17:29
	...	...	...	
G	FW	http	w.x.y.z	18/2/19 8:24:23
G	FW	MW detect	Djsp	18/2/19 8:24:37
	...	...	...	
H	FW	http	w.x.y.z	18/2/19 8:38:44
H	FW	MW detect	Djsp	18/2/19 8:38:59

It may be clearly understood that events of visiting certain web site and getting a virus on initiating endpoint are related and so defined within SIEM. There is temporal condition that was applied in order to relate two sets of events – visiting web site and AV alert on endpoints in short time span. However, this is a proof that antimalware on firewall is not appropriately efficient or configured because it did not recognize malware code passing through http protocol, thus allowing download of malware code on endpoint. In order to prevent malware download on endpoint, security assessment was done in order to improve antimalware configuration. Additional actions were performed and http antimalware scanning process altered which ended up with more efficient firewall malware analysis.

6 Conclusion

Practically, without centralized event management it is not feasible to adequately manage incidents, mitigate threats and ensure desirable level of IT security. SIEMs, if appropriately configured, applied and operated, can be very important security solution and primary tool in any security operation centre.

Some important features that should be implemented in SIEM solution in order to improve IT security are event correlation within different types of context, data enrichment, reduction in number of false positives, proactive reaction and automatic rule changes on security devices and IT platforms, integration of AI capabilities, integration with DLP solutions.

This paper gives overview of necessary characteristics, explains importance, challenges and future development in the area of SIEM solutions. Paper explains a few types of real-world case scenarios and shows how analyses can be performed. It provides solid basis for further theoretical research and practical improvements as well.

References

Dorigo, S. (2012). Security Information and Event Management. Radboud University, Nijmegen.

Ganapathy, S. (2018). *The Absolute Guide to SIEM*. Retrieved from https://download.manageengine.com/log-management/the-absolute-guide-to-siem.pdf

Lane, A. (2010). Understanding and Selecting SIEM/LM: Aggregation, Normalization and Enrichment. Retrieved from https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen

Rivas, G. (2018). AI and SIEM: Increase the efficiency of your IT security team. Retrieved from https://www.gb-advisors.com/ai-and-siem/

Swift, D. (2006). A Practical Application of SIM/SEM/SIEM Automating Threat Identification. SANS Institute.

2018 Data Breach Investigations Report (2018). Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

What's the difference between SEM, SIM and SIEM?, Retrieved from https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem