Analysis of Alternatives for a Security Information and Event Management Tool in a Virtualized Environment

Roy A. Sepúlveda Rodríguez
Master in Computer Science
Dr. Nelliud Torres Batista
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Security Information and Event Management is a software tool that increases the cyber-situational awareness of a system. Since many products are available in the market, there is a desire from companies and individuals to establish which candidate is the right one for their needs. This project dives into why it is necessary and recommended for an enterprise to deploy such a tool. It will produce a list of quantifiable metrics in which needs can be leveraged against. It also intends to present a sample attack methodology to test the desired product. To further explain the relation between metrics and needs, example user cases are generated to provide a satisfactory solution. It is intended for the interested party to understand all vectors that relate to the acquisition of a product, and by using the conclusions presented, reach a decision, or accelerate their selection process.*

Key Terms *— Analysis of alternatives, event manager, security information, virtualization*

INTRODUCTION

Computing systems require an array of tools to provide a safe and secure working environment. We trust that implementing them will be enough to protect a system. These tools will not necessarily provide a complete picture of the cyber-health of the system. Mechanisms to monitor, correlate, and aggregate the security logs and events are required.

A Security Information and Event Management (SIEM) tool is a software product that monitors a computing system for cyber security violations in real time. It fulfills this task by performing log management, compliance reporting, real-time monitoring, and incident management [1]. It can parse and correlate log information into human-readable events. Events are triggered when a security rule is being infringed, and it will display some type of alert. This type of functionality is often referred to as situational awareness.

These tasks are often facilitated by the use of a graphical user interface, which allows a user to see these events in real time, thus making it possible to mitigate a possible attack in progress or look at existing data to perform forensic studies and discover vulnerability vectors or patterns in a series of events. There are many open-source and commercial SIEM tools available, and it could prove difficult to choose the correct tool that will satisfy the interested group's needs.

MOTIVATION

There is always an inherent risk of being attacked when using a computing system. This affects work functions and data in a negative manner. As a member of the Cyber Security Workforce, it is imperative that I provide my customers with tools and solutions to help them complete their mission and keep their systems as safe as possible.

Performing cyber-forensics is not an easy task, but deploying a SIEM increases the rate of detecting anomalies and issues. My intention with this analysis of alternatives is to make users aware these tools exist and are trustworthy, and to help them decide which one will suit their needs.

PROBLEM STATEMENT

To reach a decision on which product to choose, the person or group needs to understand all the effects the acquisition will bring to the

interested party. There are more aspects to be evaluated than just which is the "best" tool. There are various views on what defines a tool as the "best." For some the best is often the fastest or the one with most added functionality, how well it performs or what added value can be provided on top of the plain SIEM component. Others will pick the most secure one, the one tool that meets most if not all security requirements posed by the GDPR and PCI DSS security requirements. There are, of course, those that need the cheapest solution possible, get some technical support, and deploy in one or more systems. To answer all these questions, a process called analysis of alternatives (AoA) is performed.

To conduct an analysis of alternatives is to inform a private user, enterprise, or agency on benefits they can gain by implementing a SIEM in their computing environment. It shows what standard security requirements it meets and how licensing and support will impact a program's budget. Additionally, other evaluation points include the type of resources it expects and uses while performing its functions, and whether or not it is actually able to detect and display event data. After examining four different SIEM candidates and performing all the necessary steps to conduct this analysis, a report will be delivered with the findings, effectively providing factual information, as well as some possibly biased opinions based on personal experience that may influence their decision to use the tool that better suits their needs.

One of the benefits of this investigation is to accelerate the fact-finding process of the interested party. Usually when someone is tasked to research what tools are available, there is a big impact on schedule and cost; deviating someone's man-hours to evaluate and test products can be very time-consuming and expensive. Ideally, by doing that "work" for them, the resulting report should at least cut their options extensively to one of the few that might be their best option, and hopefully leverage most if not all testing required.

RESEARCH QUESTIONS

What are the measurable cyber security benefits of implementing a SIEM in an enterprise network? How well do SIEM tools comply with industry standardized security requirements? Does the SIEM implementation actually provide the system with all the purported functions it offers? What evaluation metrics and methodologies can be implemented to properly compare alternative SIEM tools?

LITERATURE REVIEW

There is a strict need for implementing security measures in public and private computing environments. The deployment of cyber security tools helps increase the level of security and confidence we have in said environment. Still it is very important to manage and analyze the data that is created whenever ant event occurs. Introducing the SIEM as the log manager, real-time analysis and long-term storage, that need can be fulfilled. To identify what is a proper SIEM, we have to research what the current field of tools offers, and that information has to be leveraged on the specific needs and requirements of the enterprise.

To properly define the proper methodology for researching, testing, and choosing the correct SIEM for the occasion, many aspects of the tool need to be looked at. These include actual government regulations and industry standards such as the PCI DSS and GDPR [2]. These have led researchers to compile a list of criteria that a tool must meet in order to be considered as a potential solution. There are also industry studies that help define what a customer will expect from deploying any particular tool, such as the Gartner Magic Quadrant for Security Information and Event Management 2017. Other researchers have proven the need and possibility of actual acceptance testing for the verification of a tool's desired and expected functionality. "The complexity of computer network security management causes the necessity to develop powerful automated security analysis components." [3]

The primary focus of this research is making sure each tool is as compliant as possible with all mandated system security requirements. The United States government expects all industries and government agencies to keep track of their system log messages. This complies with the need to keep archived data in order to produce forensic analysis. This will be done on scheduled maintenance events based on policy and once an event happens, and all information regarding the event needs to be evaluated. This is why particular attention is paid to the PCI DSS and GDPR standards.

As per NIST's definition of what log management entails, and how a SIEM is a permissible solution for that need, we delve deeper into what other areas can be evaluated for picking a product. A list of criteria can be seen on the NIST [4] and Gartner [1] reports. Areas such as deployability, ease of use, functionality, performance, and licensing schemes must all be included in the analysis. It's difficult to perform quantitative analysis on some of these areas [5]. This means that some areas will be more biased based on the researched pool of knowledge and experience, but metric data can in fact be generated.

The user's requirements must also be properly understood. Their wants may not be the same as their needs. According to research, not only is SIEM used in government, but also in Olympic games, mobile money transfer systems, managed enterprise services, and critical infrastructure process control [6]. This allows us to understand different uses and what types of organizations apply to them to better identify different user case scenarios.

The fourth section of research involves the actual testing of a SIEM-enabled system. Research on attack methodologies has been done in the past. Having a sound strategy and the components to execute it will show just how effective, or ineffective, the SIEM is at performing its expected tasks. Performing these attacks gives an insight of the capacity of the SIEM at displaying alerts, and it is also necessary to study its performance and understand how a series of events can lead a user to reach the root cause of a security violation incident.

Many of the previous field studies have taken into account the main needs that must be addressed upon working with a SIEM. Primarily each study focuses on an individual aspect of the trifecta of security compliance, evaluation metric, and attack vectors. One gap found is that when a cyber-attack methodology is mentioned, no actual attack "steps" are provided to be emulated. This means that the actual commands or code used to perform these attacks are unavailable. This research will include the ones used on the Linux-based systems with the SIEM installed. Another gap is a failure to provide a metric rubric for evaluating several evaluation aspects. For example, the Gartner Magic Quadrant shows the type of metrics taken into account, but the actual mathematical data is internal to the organization. This research will include such a defined metric.

While there are many studies on the needs, expectations, testing, and deployment of SIEMs, there is still ground to reach new conclusions about the proper manner of selecting, evaluating, and utilizing them. It is intended for the user to use a system that will not only comply with laws and policies, but it has proven beneficial for its intended system. It is also very important to reiterate that everything is primarily based on the user's needs and available resources The intention of completing the research is to give yet another avenue for the user to compare the possible SIEM solutions.

METHODOLOGY

This research will employ quantitative and qualitative methodologies. Industry standards, factual data, and compiled experiment data will attain numeric values or threshold values to establish which has the "most" points. Qualitative approach can be seen in areas of human experience, such as looking or handling the product. While some numeric values can also be applied to it, it is inferred that the expected value will be more biased by the experience of the researcher.

The methodology that will be implemented consists of four main parts:

- Compiling documentation and resources: The items to be gathered include installation, configuration, user guides, licensing schemes, and other relevant documents for each SIEM product. Other documentation will include the GDPR and PCI DSS to pull log monitoring tool security and functionality requirements.
- Forming an evaluation matrix for each testable aspect of the tools: This includes ease of use, installation, configuration functionality, performance, resource management, met requirements, and cost. They will be matrixes that give some boolean or numeric value while cross-referencing the tool with the evaluated aspect.
- Establishing the proper resources needed for optimal VMs to be created, then create said machine using the VirtualBox hypervisor. Installing and configuring each SIEM tool on its corresponding VM. Creating a fifth machine that will act as the "attacker." Loading or creating scripts that simulate simple and common attacks into that VM to test the SIEM product's functionality and performance.
- Conglomerating all data findings and producing a report that will include all conclusions reached based on several use cases. This intends to provide the relevant information for aiding a user to pick the optimal option.

Table 1 shows all metric values. The SIEMs that are going to be evaluated vary in terms of services offered, licensing schemes and costs, and other areas. The selected tools for the research are the following:

- Splunk's Enterprise Security
- CS's Prelude SIEM
- Elastic's Elastic Stack/Wazuh
- Alien Vault's Open Source Security Information Management

Finally, all filled data matrixes can be compared based on each one's rubric. Other visible results will also be drawn based on documentation needs. A set of four user cases will be generated. These will include the following:

- A regular user, in this case for his/her home computing system
- A small-sized company, in this case a mom-and-pop shop
- A large company, in this case a car parts manufacturer
- A large government joint project, in this case missile defense

Note that the user cases are decided based on their idea of resources and expectations. They are meant to simulate a real-world sample, but do not necessarily reflect the actual manner, processes, or information they use. This is primarily geared toward the government/military example; it is not supposed to inform of any type of actual ongoing government project.

FINDINGS

After completing all evaluations, the information will be presented in this format: a brief description of the company and its tool, a brief explanation of the acquired metrics, and the experience with the tool. After that, the actual captured metrics, and how we can pick a best SIEM for each category, will be presented and discussed. Then each hypothetical use case will be presented and a recommendation of a SIEM product will be offered.

Splunk

Splunk, Inc. is a cyber security and computing solutions corporation that specifies in SIEM software and other analytical tools, founded in 2003 and based in San Francisco, California. They offer the Splunk Enterprise SIEM (Table 1). Their standout approach is to include configuration items for other tools to be integrated into the SIEM via "app store." They are very popular in the government, banking, and manufacturing industries. They boast over 50 awards by different

organizations and publications, mostly about good employment practices and services.

Their licensing scheme follows a data ingested in system approach. This means that the more data is inserted and acted on, the costlier the licensing fees will be. The more data consumption threshold desired, the lower the cost. Its average cost is $50 per instance per day. The license does provide support, but highly encourages premium services to manage and configure the user's environment. They ask for a sizeable amount of RAM, even though it can work with a limited amount. It boasts most of the features expected from a SIEM, and they also include a machine-learning module, on top of the aforementioned "app store." It meets PCI DSS, HIPAA, NIST CSF, and GDPR standards.

Acquisition and deployment are very easy and quick, but require subscribing to a trial version. It was by far one of the easiest SIEMS to have running. Configuring it to understand data being forwarded took a little more work, since the GUI is not as intuitive as one would expect. One has to traverse some tabs and boxes and not necessarily be able to access other parts of the tool. It also clutters the screen a bit on the left side. It did catch all attacks and reported on them within seconds. The only "issue" was that one of the attacks took 7 seconds to show up; of course, 7 seconds is a short amount of time, but expected alerts average 4 seconds.

Prelude

CS, a cyber security and aerospace company founded in 1998 and based in France, offers cyber-solutions in the form of a SIEM. This SIEM is called Prelude SIEM (Table 1). Its approach is to provide both a fully featured SIEM tool and a free limited version for deployment. The French government highly recommends it and it is quite popular in other European countries. They don't publicly boast awards.

Prelude charges a flat cost per device added to the instance. The exact amount is not specified. This means that use and management of the tool is free, but a cost is applied to each computer that will be protected. Nonetheless, they offer limited functionality (mostly visualization and reporting, not detection) for free. They also offer premium services for additional fees. They do not specify required hardware, but it runs with a pretty basic setup. It meets PCI DSS, ISO 27001 IDMEF, and NIST CSF standards.

Acquisition and deployment are very easy. The steps to install are very easy to understand and follow, except that in one section it is not specified that one command must be run while a first one is running. That is the extent of any trouble. It configures automatically. Their free version is very barebones, which for the simplicity of the tool is actually good. By having only two tabs, traversal is very easy. The tool detected each attack in an average 1.75 seconds, making it the fastest of all evaluated tools.

Elastic/Wazuh

Elastic NV, operating since 2010 and based in Amsterdam, is a cyber security and services consulting company. They offer the Elastic Stack tool (Table 1), consisting of the sub-tools Elasticsearch Kibana, Wazuh, and others. The product's attractiveness lies in a fully functional SIEM that operates under an open-source license, making it free to deploy. They do offer to host and manage the system as a premium service. Social media, video streaming, and other service industries use this tool. They do not seem to publicly boast their accolades.

As stated, this is a free product. Its only resource demand is over 8 GB of RAM, but during testing, barely 4 GB sufficed to install and run the services. It includes all detection, visualization, and reporting features out of the box with proper installation. The documentation does not explicitly state it only complies with DGPR standards, but it mentions other military and government standards, such as DON Application and Database Management System, NIST 800-53, and US Air Force Certificate to Field.

Installing this tool was more complicated than the others. While instructions are simple to follow,

sometimes installation would fail for unknown reasons; attempts at reinstallation worked. A benefit is that a total installation is enough to configure the system. It is nice-looking and everything exists in a logical space. It took a lot of resources during the installation process and initialization, but the system always ran well afterwards. The tool captured all four attacks in a timely manner, averaging 2.75 seconds.

OSSIM

Alien Vault is a company operating since 2007 and based in California that works in providing open-source and commercial cyber security solutions. Their SIEM product is called OSSIM USM (Table 1). Their big item is the Open Threat Exchange, which includes data and updates on all cyber attacks from experts and other users, which is integrated in the SIEM itself. It is used mostly by service and goods industries. They showcase at least ten awards.

Their license charges a monthly flat rate of $1,095 for the standard edition per instance. Other extra services and dedicated support can raise the monthly rate to $2,500. It is the most resource-heavy of the solutions; they do need every bit of RAM and CPU they ask for. It includes all expected features in a SIEM and also the aforementioned Open Threat Exchange. It meets PCI DDS, ISO 27001, HIPAA, and NIST CSF standards.

Acquisition requires creating an account with Alien Vault, after which they give a VM appliance. It is the easiest to "install." Issues did arise during this process. I gave it 4 GB and it took over 4 hours to install; giving it more RAM halved installation and initialization times. It is the best organized and looking so far. It is fairly easy to use. It captured one of the attacks; the others are waivered, since the VM configuration itself does not allow the creation of additional users. It was also very quick in detecting the attacks.

GATHERED METRICS PER CATEGORY

Cost

Actual prices can be detailed if an actual implementation is going to be performed with each company sales department (Table 1). From what is shown, costs range from free in some cases to $13,000 annually. The cost of equipment and training is not taken into account. The cheapest solution is Elastic.

Resources

It should be mentioned that official documentation was not excellent in detailing exactly what type of hardware and amount of resources are required. From what was gathered, the most varying minimum is the RAM; each tool asks for different amounts (Table 1). In terms of processors and cores, the more the better. Compared to the actual environment, we see most of them can work with lower specs than the "recommended" (Table 1), except for OSSIM, which needs more RAM. Splunk and Prelude need the least resources in general.

Features

In both trial and licensed versions, all SIEMs contain the required features, such as detection, correlation, aggregation, log management, etc. (Table 1). OSSIM and Prelude's trials lack additional visualizations and reporting functions available in their full versions. OSSIM stands out for its threat intelligence feature. Also, Splunk and Elastic offer machine-learning modules. All SIEMs have all required features.

Standards

Not one SIEM tried in this study meets all the expected industry standards. Still all of them meet four out of the six, with the exception of Elastic (Table 1). This does not mean Elastic is a worse product, since they claim compliance with other standards, in which there might be overlap. Since PCI DSS and HIPAA require great levels of

compliance and scrutiny, Splunk and OSSIM are the most compliable SIEMs.

Deployability

Acquiring all softwares was relatively easy. Each tool had a different approach to configuring and installing (Table 1). OSSIM is a VM; Splunk only requires extraction of some files, while Prelude and Elastic require some command line steps. Manual installations vary in times depending on familiarity with instructions, environments, and experience. Therefore, subsequent installations should take less time and effort. The easiest tool to install was OSSIM, due to both required complexity and interaction. Still it was the slowest and most resource-heavy. Elastic is prone to random breakages during installation. The tools with the least amount of configuration needed are Prelude and Elastic, as they come "preconfigured."

Usage

Usage is mostly based on personal taste and preferences (Table 1). Splunk is the most confusing tool, as it has many buttons and clickable items at any time; also it is hard to understand where one is at times. All other tools had clearer features. Prelude is very simple, which works in its favor. The best SIEM in terms of understanding and traversal is Prelude. The best SIEM in terms of visual appeal is OSSIM.

Functionality

The idea behind functionality was to see if the tools were properly configured and initialized to catch cyber events. They all did (Table 1). OSSIM was a special case, since its OS did not allow the creation of sub-users, rendering ssh and logging as another user to then get root privileges moot. It still captured ssh as root efficiently. All SIEMs function as expected.

Performance

Data was gathered for all attacks and all SIEM captures of the data (Table 1). The start time of the attack is compared to the tools' event registry. While no exact number is given to what the actual response time of an event should be, we could compare them with each other. Splunk took 7 seconds in one of the attacks, which is the slowest response in the suite. Still if compared with their other results, this might have been sort of a fluke. In general, Splunk and Prelude were the fastest to display the occurrence of a cyber event. Prelude had the quickest average response time.

BUSINESS USE CASES

The following are the business use cases. A list containing hypothetical resources and needs is presented in Table 1. Based on those needs, we will discuss primary requirements briefly and will recommend the best possible SIEM solution.

Regular User

We define a regular user as someone who wants to put a SIEM on their home computer, but has little to no money to invest in hardware or licensing costs. Still we believe this user to be confident enough to follow instructions to install the tool and learn how to use it by themselves. They will not need fancy support or features. In this case, a free license solution would be a better suit. If the intention is to just be able to monitor the system, Prelude OSS, the free version of Prelude, is recommended. If the user can trade a bit of hardware resources in order to have visualization features, Elastic is recommended.

Small Company

We define a small company as a mom-and-pop shop. Even small local businesses are required some compliance with industry standards. They could be using up to three or four devices in their operations. They are expected to be able to invest some money in their computing system. A decent server that deploys agents to other systems could be within reason. Since mom and pop only care about their day-to-day functions, they may not necessarily care or know how to implement or use the SIEM; therefore, a simple installation or management support agreement could come in handy. Unable to

afford the Prelude SIEM per-device license, if they can afford a license, OSSIM is recommended. It may require a bit more hardware resources, but the flat monthly fee is less expensive than Splunk's. Otherwise, they should go with Elastic, and perhaps hire someone to manage their system from time to time with the money they save on licensing.

Large Company

We exemplify a large company as a car parts manufacturer. We infer they have hundreds of employees, different computing environments, and proprietary data, so they need a somewhat more secure and supportable solution. We would assume they have the monetary resources to bulk the hardware resources of systems that will carry the SIEM tool, and could, to some degree, afford some ongoing service with a company. A good feature for this environment is machine learning, helping detection and mitigation of common events. They have employees capable of implementing and using any of the tools. Still they could pay Elastic to host and monitor such a large-scale environment and save on licensing fees. Such a huge amount of data would skyrocket the cost of Splunk, and the volume of devices is too big to pay per device with Prelude. In this case, OSSIM USM is recommended.

Military

We established Military as a large joint operation for a missile defense project. In this type of venture, money and hardware are almost never an issue, since lives will hang on the line based on the integrity and availability of the system. The military is very confident they can acquire or train personnel to install, configure, manage, and monitor their systems. Still, on an enclave that manages such mission-critical hardware, only a few computers exist in it. They still may need a very specific type of dashboard suited for the mission, which Splunk is really good at. They will need a license for tech support; a system failure is risky and a prompt response could save lives. The threat intelligence feature of OSSIM is very attractive to military environment. If the military can support ongoing funding, the recommendation is Splunk, although the cap on data could be a very serious risk. Otherwise, OSSIM USM is recommended.

Table 1
Complete List of Evaluated Metrics

AREA	METRIC		TOOLS / RESULTS		
		SPLUNK	PRELUDE	ELASTIC/WAZUH	OSSIM
COST FACTORS	DOES TEST VERSION HAVE ALL FEATURES AND SERVICES	NO	NO	YES	NO
	IS TEST VERSION DEPLOYABLE AS A SOLUTION	YES VERY LIMITED	YES	YES	NO 14 DAY TRIAL
	CAVEATS TO USING TEST VERSION	CAP ON DATA 500 MB	OTHER FEATURES NOT ENABLED	N/A	NOT ALL FEATURES ENABLED, LIMITED TRIAL
	LICENSING SCHEME	CHARGED DAILY BASED ON CAP DATA AMOUNT INGESTED BY SIEM. THE MORE DATA DESIRED THE CHEAPER THE PRICE.	CHARGED BY EACH DEVICE CONNECTED TO THE OSSIM SERVER	FREE	FIXED PER INSTANCE, MONTHLY PAYMENTS START AT 1095
	GENERAL COST BASED ON LICENSING	50 PER 100GB DAILY	N/A FREE	FREE	1095 BASIC MO
	RENEWAL OF LICENSING	CAN BE PERPETUAL OR FIXED ON TERMS	PERPETUAL, FREE	N/A	N/A
	ARE SECURITY PATCHES AND BUG FIXES SUPPORT INCLUDED IN LICENSING DEAL	YES	YES ON PAID, NO ON FREE	SOME	YES
	ARE THERE ADDITIONAL COSTS RELATED TO AQQUISITION	N/A	NO	N/A	N/A
	SUPPORT	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES PRICE GOES UP TO 2600
RESOURCE FACTORS EXPECTED	NUMBER OF CPUS	2	N/A	N/A	N/A
	NUMBER OF CORES PER CPU	6	N/A	2	4
	CPU SPEED	2 Ghz	N/A	N/A	N/A
	RAM MEMORY	12 GB	N/A	8 GB	4 GB
	FREE HDD SPACE	5 GB	N/A	N/A	500 GB
	STORAGE	N/A	N/A	N/A	N/A
RESOURCE FACTORS ACTUALLY USED	NUMBER OF CPUS	2 CPU	2 CPU	2 CPU	2 CPU
	NUMBER OF CORES PER CPU	N/A	N/A	N/A	N/A
	CPU SPEED	N/A	N/A	N/A	N/A
	RAM MEMORY	2 GB	2 GB	4 GB	6 GB
	FREE HDD SPACE	4 GB	4.5 GB	5 GB	8.5 GB
	STORAGE	20 GB	20 GB	20 GB	30 GB

Table 1

Complete List of Evaluated Metrics (continued)

AREA	METRIC	TOOLS / RESULTS			
		SPLUNK	PRELUDE	ELASTIC/WAZUH	OSSIM
FEATURES FULLY LICENSED TOOLS	SECURITY	YES	YES	YES	YES
	CENTRALIZATION	YES	YES	YES	YES
	LOG MANAGEMENT	YES	YES	YES	YES
	DETECTION	YES	YES	YES	YES
	NORMALIZATION	YES	YES	YES	YES
	CORRELATION	YES	YES	YES	YES
	AGGREGATION	YES	YES	YES	YES
	ALERTING	YES	YES	YES	YES
	DATA VISUALIZATION	YES	YES	YES	YES
	METRICS	YES	YES	YES	YES
	REPORTING	YES	YES	YES	YES
	MONITORING	YES	NO	YES	YES
	MACHINE LEARNING	YES	NO	YES	NO
	THREAT INTELLIGENCE	NO	NO	NO	YES
FEATURES TRIAL VERSION TOOLS	SECURITY	YES	YES	YES	YES
	CENTRALIZATION	YES	YES	YES	YES
	LOG MANAGEMENT	YES	YES	YES	YES
	DETECTION	YES	YES	YES	YES
	NORMALIZATION	YES	YES	YES	YES
	CORRELATION	YES	YES	YES	YES
	AGGREGATION	YES	YES	YES	YES
	ALERTING	YES	NO	YES	NO
	DATA VISUALIZATION	YES	NO	YES	NO
	METRICS	YES	YES	YES	YES
	REPORTING	YES	NO	YES	YES
	MONITORING	YES	NO	YES	NO
	MACHINE LEARNING	YES	NO	YES	NO
	THREAT INTELLIGENCE	NO	NO	NO	YES
STANDARDS	PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)	YES	YES	NO	YES
	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 27001 (ISO 27001)	NO	YES	NO	YES
	GENERAL DATA PROTECTION REGULATION (GDPR)	YES	NO	YES	NO
	HEALTH INSURANCE PORTABILITY ACT AND ACCOUNTABILITY ACT (HIPAA)	YES	NO	NO	YES
	INTTRUSION DETECTION MESSAGE EXCHANGE FORMAT (IDMEF)	NO	YES	NO	NO
	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBER SECURITY FRAMEWORK (NIST CSF)	YES	YES	NO	YES
DEPLOYABILITY	ACQUISITION COMPLEXITY STEPS	2 STEPS	2 STEPS	2 STEPS	2 STEPS
	AQQUISITION METHODOLOGY	SIGN UP AND DOWNLOAD	RPM YUM INSTALL	RPM YUM INSTALL	SIGN UP AND DOWNLOAD
	INSTALLATION COMPLEXITY STEPS	4 STEPS	22 STEPS	24 STEPS	4 STEPS
	INSTALLATION COMPLEXITY UNDE	VERY EASY	EASY/STANDARD	EASY	VERY EASY
	INSTALLATION TIME	30 MINUTES	60 MINUTES	75 MINUTES	120 MINUTES
	CONFIGURATION COMPLEXITY STE	8 STEPS	N/A	N/A	5 STEPS
	CONFIGURATION COMPLEXITY UNI	VERY EASY	N/A	N/A	VERY EASY
USAGE	EASE OF ACCESS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS
	EASE OF TRAVERSAL	3 TO 5 STEPS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS
	VISUALY PLEASING	OK	GOOD	GOOD	GREAT
	UNDERSTANDABLE INTERFACE	OK	GREAT	GOOD	GOOD
FUNCTIONALITY	FAILED SSH ATTEMPT REGULAR US	YES	YES	YES	N/A
	SUCESSFUL SSH ATTEMPT REGULAI	YES	YES	YES	N/A
	FAILED ROOT ESCALATION	YES	YES	YES	N/A
	SUCCESFUL SSH ATTEMPT ROOT US	YES	YES	YES	YES
PERFORMANCE	FAILED SSH ATTEMPT REGULAR US	5 SECONDS	5 SECONDS	8 SECONDS	N/A
	SUCESSFUL SSH ATTEMPT REGULAI	2 SECONDS	1 SECOND	<1 SECOND	N/A
	FAILED ROOT ESCALATION	7 SECONDS	1 SECOND	2 SECONDS	N/A
	SUCCESFUL SSH ATTEMPT ROOT US	<1 SECOND	<1 SECOND	1 SECOND	2 SECONDS

CONCLUSION

Through the research and testing of this proposal, it has been made clear that the inherent threat of a cyber-attack is real, and many talented and smart people have come together to define common forms of understanding and detecting said events. The implementation of SIEM tools definitely improves the visibility and standing of a computing environment. There are many options to choose from, and this paper only deals with Linux-based tools, but choosing one is not as easy as brand recognition. Further studies need to be done in order to select a tool; while this paper used attacks over the network, other threat vectors such as malware and file integrity checking implementation should be tested. Also, playing in a bigger sandbox with more resources can yield better performance data on ongoing attacks.

The results point to OSSIM as one of the best solutions, yet it requires heavy resources and a significant amount of money. For less heavy usage, Prelude OSS is a very good choice: free, simple, and fast.

As a third and final option, there is Elastic, still quite intuitive and also free, with all features readily available. Splunk is not a bad tool, but the licensing scheme is a bit steep money-wise to deploy. However, the four are popular and used by industries all over the world, which gives confidence on their ongoing effort to provide such solutions.

The most important piece of advice I can produce based on this paper is safeguard your system, monitor your system. Just installing a tool is never enough to protect a computer, and while there are bad people out there, there are also good people who work hard to help everyone in the cyberspace. Moreover, these software companies are willing and happy to help, but they are businesses, and their main goal is to make a profit. Selecting a company for licensing should not only be based on the test facts presented and its tool's good reputation, but also on its reputation as a company that treats its employees well, with a good moral compass, and that provides amicable, noteworthy services. We members of the cyber security workforce strive to make cyberspace safe for everyone; we will help you, but you can also help us by helping yourselves.

REFERENCES

[1] M. Nicolett and K. M. Kavanagh, "Magic Quadrant for Security Information and Event Management," *Gartner RAS Core Reasearch Note*, G00212454, May, pp. 1, 2011.

[2] V. K. Reynoso Vásquez. "Events Centralization and Correlation at a Finance Entity," M. S. thesis, Universitat Politècnica de Catalunya, Catalonia, Spain, 2009.

[3] I. Kotenko and A. Chechulin, "Attack Modeling and Security Evaluation in SIEM Systems," *International Transactions on Systems Science and Applications*, vol. 8, December, pp. 129-147, 2012.

[4] K. Kent and M. Souppaya, "Guide to Computer Security Log Management," *NIST*, Sept. 13, 2006. [Online]. Available: https://www.nist.gov/publications/guide-computer-security-log-management. [Accessed Feb. 11, 2019].

[5] LeanKanban, *How to Measure Anything: An Introduction from the Author - Douglas Hubbard*, Feb. 5, 2014. [Video file]. Available: https://www.youtube.com/watch?v=w4fHGTsZZD8 [Accessed Feb. 11, 2019].

[6] R. Rieke, L. Coppolino, A. Hutchison, E. Prieto, and C. Gaber, "Security and Reliability Requirements for Advanced Security Event Management," presented at 6th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, St. Petersburg, Russia, October 2012.