

# Providing Information Security Using ArcSight SIEM in an Organization.

*Aamir Sohail*

M.Tech., Department of Computer Network and Information Security  
Manipal University  
Jaipur, India  
[aamirscw90@yahoo.com](mailto:aamirscw90@yahoo.com)

**Abstract**— In Today's world Data is very important and we are storing our confidential data using the latest technology like –Cloud, Virtualization and BYOD (Bring your own device i.e. Laptop, mobile etc.). We all are storing our confidential data over there .Even there is advancement in the thinking and behaviour of Hackers. Cyber Attack is also a big concern. To overcome all these problems we have ArcSight SIEM (Security Information and Event Management) Technology. Arcsight SIEM will collect, analyse and present information on security products, Operating System, Databases etc. Every data needs to be recorded. So it will monitor all the data coming from different devices and will give you the centralized view of logs.

**Keywords**-Information Security, ArcSight SIEM.

## I. Introduction

ArcSight SIEM will identify and mitigates business risks. It will protect us from external threats such as malware and hackers, internal threats such as data breaches and fraud. It will give us a real time analysis and historic view into external attacks, insider threats and compliance breaches. So that we can intelligently and effectively protect our environment .ArcSight Security Information and Event Management (SIEM) system is a centralized system for collecting data, analysing from any devices and also does a real time event correlation. We can make a report of the vulnerabilities. Even we can inform about the vulnerabilities and can respond also.

## II. ISSUES

There are so many organizations like RSA Security , Zappos .They all were using technologies like Cloud , Virtualization etc. to save confidential data over there .They lose millions of users, loss of billions of dollars, tinting of brand value of some of the biggest organizations that puts TODAY's

enterprise at a risk LARGER than ever before. Even Organization were being hacked and then at that moment they don't Know .They are also using Security Technology to fight against the hackers but there technology give the details of the hackers after that company would be bankrupt or going to be shut down .So we have the Technology ArcSight SIEM that will inform us who is on the network and what he is doing whether he is trying to hack it or not. If that guy is hacker then we would be informed on the same day only so that our organization won't be losing billions of dollars and won't get bankrupt like others.

## III. FUNCTIONAL PARTIONING OF PROJECT

### 1. Data collection

At this layer events from different devices would be forwarded to Smart connector by using push or pull function. They collect events from hundreds of devices in different format, and then they normalize it into a common event format (CEF). The Connectors collect locally and then send the normalized events to our logging and correlation

products in a guaranteed, secure, and bandwidth-efficient manner.

## 2. Data consolidation

At this layer all the data would be forwarded from smart connector to logging engine. Logger receives structured data in the form of normalized Common Event Format (CEF) events and unstructured data such as syslog events. Logger is a log management solution that is optimized for extremely

Date	Time	Event Name	Source IP	Device Name
21st nov 2013	12:01:00	Accept	65.65.65.5	Checkpoint

high event throughput, efficient long-term storage.

## 3. Data correlation

Correlation is a process that discovers the relationships between events, infers the significance of those relationships, prioritizes them and provides a framework for taking actions. ArcSight Enterprise Security Management (ArcSight ESM/Manager) is a software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation.

## 4. Data Collaboration

At this layer we can integrate ArcSight SIEM technology with existing security point solution (i.e. Global Threat Intelligence, Vulnerability Scanner, Application Code Scanner etc.) to provide additional layer of security to strengthen network security posture of the organization.

## IV. Three tier Architecture

By using three tier architecture how data would be collected from different devices and forwarded to Smart Connector and then forwarded to Manager. Finally we can see the events in Arcsight Console. The Arcsight Console is the administrative part where we can monitor dashboards, analysis of data and can inform about the hackers and through pattern also we can check the data monthly and can

inform about the threats .By monitoring we can identify who is on the network, what he is doing, where he is on the network .We can also respond to the vulnerabilities .We can protect our organization from Cyber Attack.

## V. Methodologies

Different Components that we are using under this.

### 1. Arcsight Smart Connector

Functions performed by Smart Connector:

#### Normalization

After receiving data from different devices it will collect the data and will normalize in a readable format .Example

Check Point: "14" "21Nov2005" "12:10:29" "eth-s1p4c0" "ip.of.firewall" "log" "accept" "www-http" "65.65.65.65" "10.10.10.10" "tcp" "4" "1355" "" "" "" "" "" "" "" "" "" "firewall" "Len 68" This is how data would be normalized.

#### Categorization

It will categorize the events received from different devices.

Example

Category	Description	Examples
Object	Object refers to the entity being targeted.	Application, Operating System
Behaviour	What is being done to the object	Authentication, modify

#### Filter

It will filter out the events that are not required. Filters applied at the Smart Connector select only events that match the conditions, and then forwarded to the Manager for processing. Non-matching events are not forwarded to the Manager. Basically there are two types of filters

##### A. Named Filter

In this filter is predefined for every event that is received from different devices. We don't have to create filter by specifying conditions for creating rules, reports every time.

##### B. Unnamed Filter

In this filter is not predefined. We have to create filter by specifying conditions for creating rules, reports etc.

## Aggregation

We can configure Connector to aggregate events that have the same values in a specified set of fields, either a specified number of times, OR within a specified time limit. Let's take an example

Suppose we have firewall device from which we have received around 10 events having same source IP, Destination IP etc. Then the aggregated event would be 1 and aggregated count would be 10. In this way volume of events sending to manager would also be reduced.

## Caching

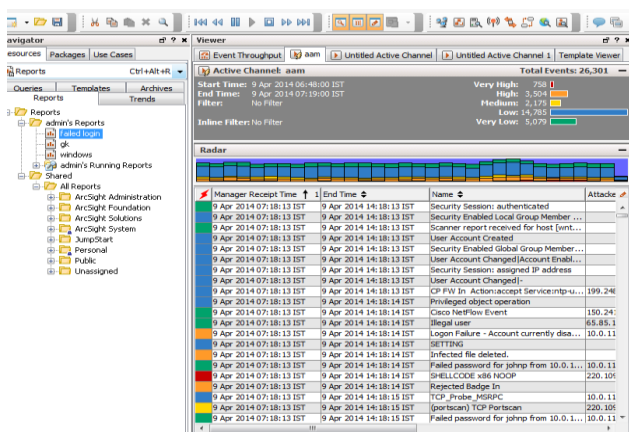
Suppose we lost the connection between connector and manager then at that moment all the data would be saved to caching.

## 2. ArcSight Logger

It's basically data storage where events would be stored. Analysis is also possible. We can see the vulnerabilities. But we can't respond to vulnerabilities. Some Organisations just want to use logger for Auditing purposes.

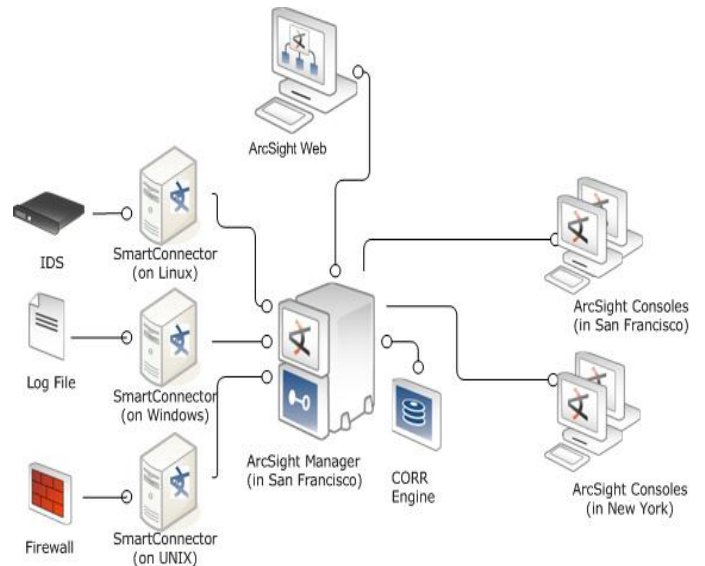
## 3. ArcSight ESM/MANAGER

ArcSight ESM is a Security Information and Event Management solution that collects and analyses security data from heterogeneous devices on network and provides us a central, real-time view of the security status .It will also give us notification on the console. We can respond through Workflow tools which includes Use Cases, Stages. On the right hand side we can see the Console. It has radar, graphs etc. It also has resources that includes filter, reports, active Channel. Through this we can analyse, notification on mobile, mail we can get.



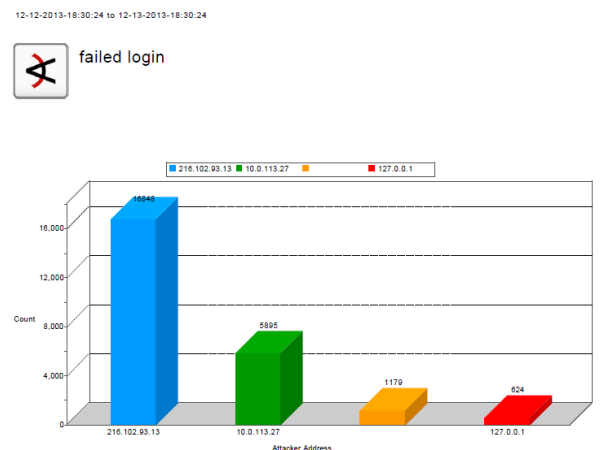
## VI. DEPLOYMENT SCENARIO

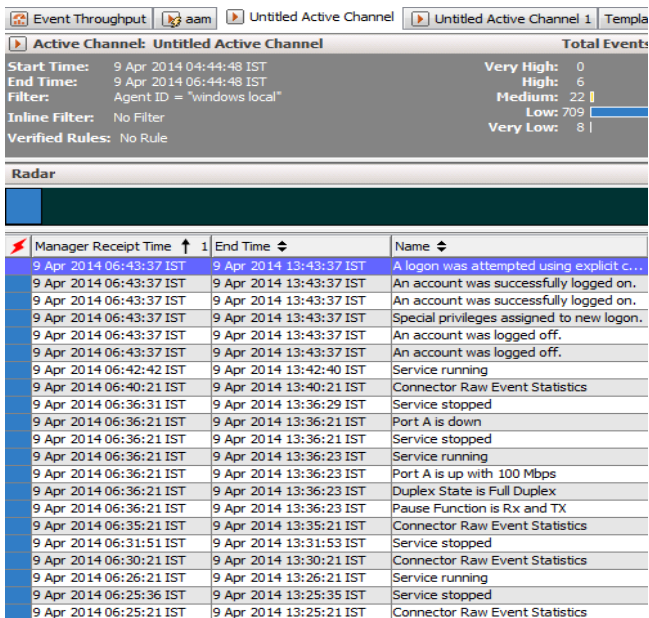
This is how I have deployed this ArcSight SIEM Technology to protect from Cyber Attack, Vulnerabilities. ArcSight Console, ArcSight Manager, and ArcSight Smart Connector communicates using HTTP (Hypertext Transfer Protocol) over SSL (Secure Sockets Layer), often referred to as HTTPS (Hypertext Transfer Protocol Secure). The HTTPS protocol provides for data encryption, data integrity verification, and authentication for both server and client.



## VII. ANALYSIS

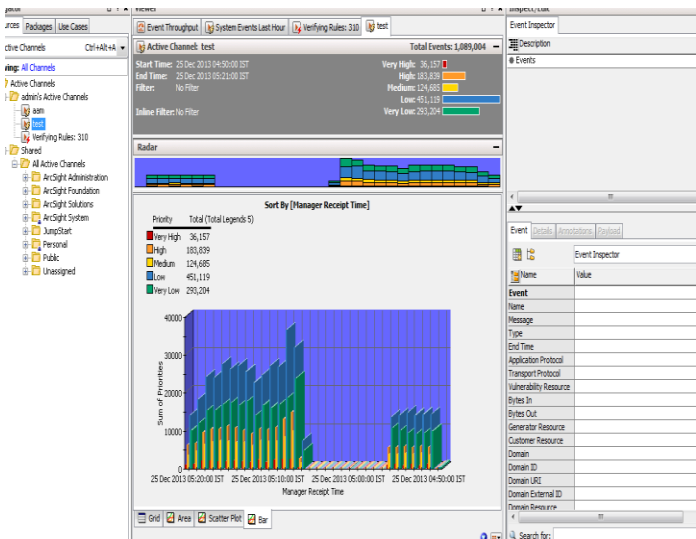
After implementing this technology I have got windows failed logins and notified through mail, and also I have made a report for the failed logon. I have also investigated the failed logins. The failed logins gives the details of Attacker Address and which Target Address the Attacker was targeting to .Even I had deployed this in my laptop to know if someone tries to get false login attempt to my computer .So I will flash out the details of windows failed logins.





Attacker Address	Target Address	Priority	Device Vendor	Device Product
127.0.0.1	192.168.1.6	3	Microsoft	Microsoft Windows
127.0.0.1	192.168.1.6	4	Microsoft	Microsoft Windows
127.0.0.1	192.168.1.6	4	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	ArcSight	ArcSight
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	ArcSight	ArcSight
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	ArcSight	ArcSight
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	Microsoft	Microsoft Windows
	192.168.1.6	3	ArcSight	ArcSight

I have captured the details of the false login attempt and I have made a report in different charts as shown above and below.



### VIII. CONCLUSION

In this paper I have shown that how we can monitor after collecting the data from different sources like security devices –firewall, IPS etc., Databases-MY SQL, Oracle etc. and would be informed about the hackers when we would be going to be hacked or being hacked .Implementing this technology will help us identify and prioritize threats. Fraud detection and forensic analysis can also be done by using this technology .I can say that by using this technology we can be relaxed as we would be getting notification either through mail or Text message on the registered number. Even if third person tries to modify the data then we would be informed .I am still working on to strengthen our security by integrating ArcSight SIEM with an existing security, Databases etc. of an organization.

### IX. REFERENCES

- [1.] J.H. Allen, “CERT System and Network Security Practices,” Proc.Fifth Nat’l Colloquium Information Systems Security Education, 2001.
- [2.] Common Criteria Sponsoring Organizations, “Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Rev 1,” Nat’l Inst. Standards and Technology CCMB-2006-09-003, Sept. 2006.
- [3.] A.I. Anto’n and J.B. Earp, “Strategies for Developing Policies and Requirements for Secure E-Commerce Systems,” E-Commerce Security and Privacy, vol. 2, Advances In Information Security, A.K. Ghosh, eds., pp. 29-46, Kluwer Academic, 2001.
- [4.] Common Criteria Sponsoring Organizations, “Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Rev 1,” Nat’l Inst. Of Standards and Technology CCMB-2006-09-001, Sept. 2006.
- [5.] ISO/IEC, “Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 3: Security Assurance Requirements,” ISO/IEC, Geneva, Switzerland, Int’l Standard 15408-3, Dec. 1999.
- [6.] C.L. Heitmeyer, “Applying “Practical” Formal Methods to the Specification and Analysis of Security Properties,” Proc. Int’l Workshop Information Assurance in Computer

Networks: Methods, Models, and Architectures for Network Computer Security, pp. 84-89, 2001.

[7.] O. Tettero, D.J. Out, H.M. Franken, and J. Schot, "Information Security Embedded in the Design of Telematics Systems," Computers and Security, vol. 16, no. 2, pp. 145-164, 1997.

[8.] L. Liu, E. Yu, and J. Mylopoulos, "Security and Privacy Requirements Analysis within a Social Setting," Proc. 11th IEEE Int'l Requirements Eng. Conf., pp. 151-161, 2003.