iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VI **Month of publication:** June 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Vol. 2 Issue VI, June 2014
ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Be Secure with Analytics

Anu Taneja

Abstract: Once the data has been captured, monitored and analyzed properly, it can be used to understand security threats which enterprises were not able to detect earlier. Today every organization have security information and event management technology at the place which provides real time analysis of security alerts generated by network hardware and applications.
Keywords: SIEM- Security Information and Event Management, Network Security, Big Data, Security Analytics.

I. INTRODUCTION

The two biggest worries which have become nightmare for many CIOs or CISOs are big data and security. With ever changing technologies, IT teams can count on the amount of data which they have to manage, as it will continue to increase by leaps and bounds. Today leaders in every sector have to grapple with these implications.

II. WHY SECURITY ANALYTICS IS IMPORTANT?

Scope of big data analytics have been moved one step ahead towards security analytics. Once the data has been captured, monitored and analyzed properly, it can be used to understand security threats which enterprises were not able to detect earlier with their traditional SIEM approach. With the use of security, one can get clear understanding of what's going on within a company's network, but also how external data sources can help predict upcoming attacks. Some experts have sounded the death knell for SIEM, while others see the fusion of big data technologies and SIEM as the next evolution, taking security analytics to the next level.
It will help SOC team to quickly determine how an attack happened and it will reduce the 'attacker free time'- the time between attacker entering the environment and being detected in the infrastructure- and to put measures in place to prevent similar future attacks.

III. SECURITY ANALYTICS: A NEW HOPE TO DETECT THREAT.

Today every organization have security information and event management technology at the place which provides real time analysis of security alerts generated by network hardware and applications. Network, switches and routers are aware of the packets that are flowing through the network, but all the data exists in different repositories that are not integrated at all.

This conventional security focused largely on blocking attacks, but with security analytics, breach detection and response time prevention becomes easy. Security Analytics will pick up from where security information and event management have failed to meet enterprise needs in keeping up with the overwhelming amount of data and new sources of information that need to be analyzed. One should identify areas in which traditional SIEM and log management systems are failing and determine how big data tools and technologies can help to turn many disparate sources of information into actionable intelligence.

So in simple terms, security analytics is a collection of security data sets that are large and complex and difficult to process using on-hand database management tools or traditional security data processing applications. As the ESG demand-side data indicates, many enterprise organizations have already crossed this threshold as they collect but struggle to analyze multiple terabytes of security data.

"The security analytics market is not new but emerging requirements like scale, performance and analytics are making these products obsolete. For this reason security analytics will evolve and expand quickly in both real-time and asymmetric big data security analytics capabilities.
One has to differentiate big data and then to exemplify how big data is helping security in ways that other technology were not able to do previously.

IJRASET - ISSN: 2321-9653

IV. CHALLENGES IN IMPLEMENTING SECURITY ANALYTICS.

Today security is currently a widespread and growing concern that affects all areas of business. It is very important for enterprises to implement security controls.

A few challenges that we still face are:

a) Developing New Talent: To really get big data security analytics you need a deep understanding of technical elements like switching, routing, operating systems, logs, flows, IP packet meta data, DNS, DHCP and known threat vectors.

So we require workforce such as architects, statisticians and data scientists.

b) Finding a single vendor to read logs from every device: All vendors must prepare for enterprise challenges with the right services, communications, and education to help CIOs navigate through complex planning, deployment, and operations. They should act as single window.

V. BENEFITS

a) The biggest changes security can bring to SIEM will be better scalability and performance, the ability to include and analyze new types of data and an increased speed of analysis so that decisions can be made more quickly.

b) By collecting data on a large scale and analyzing historical trends, you would be able identify when an attack started and what were the steps that the attacker took to get a hold of your systems.

c) Even if you did not detect the original attack in your system and you can go back and do an historical correlation in your database and system to identify the attack. So long term historical analysis is one advantage.

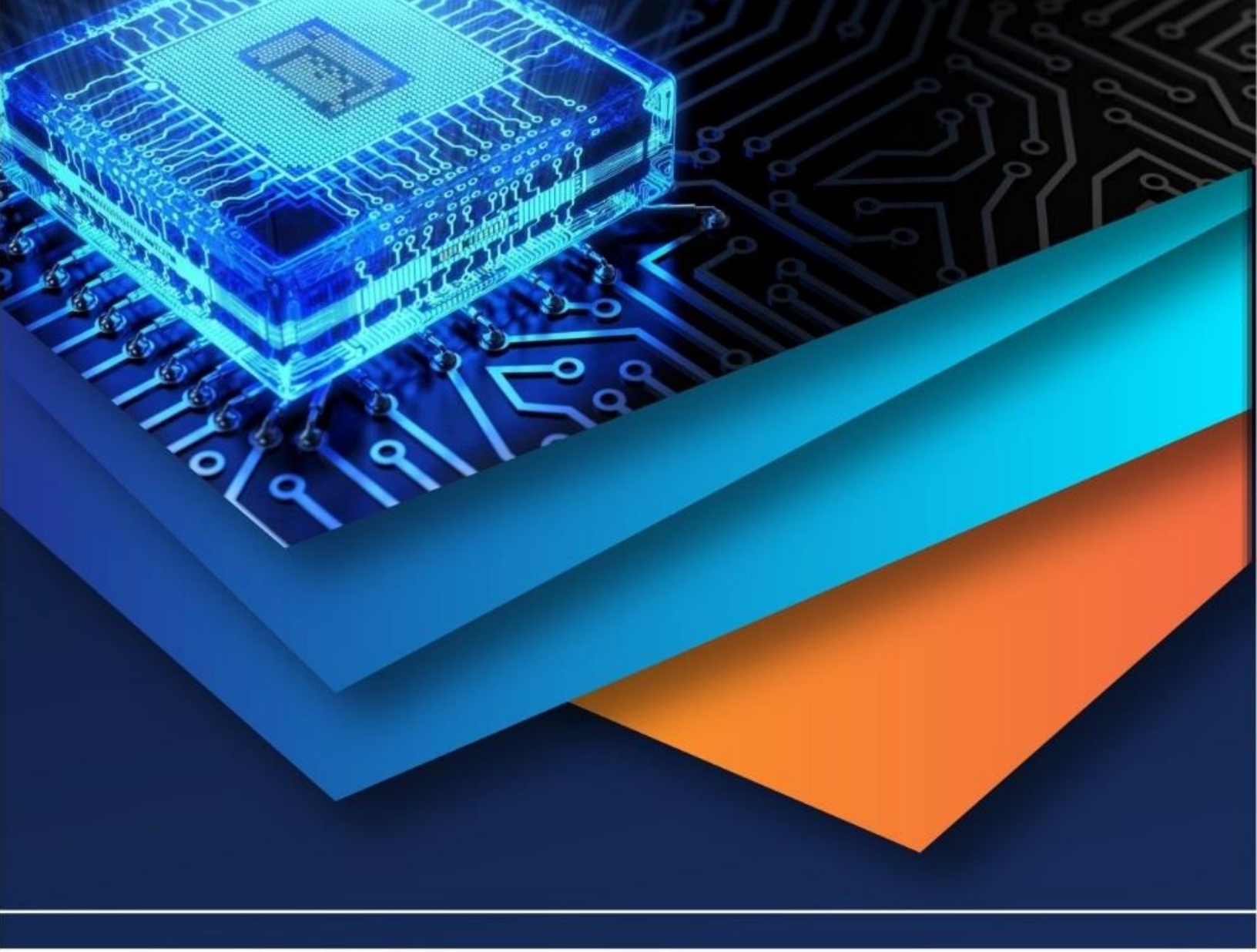
VI. CONCLUSION

To understand and detect new threats like targeted attacks, it is important to correlate all the logs and generate meaningful reports. This can only be possible with security analytics. Otherwise CSO will be flooded with data and it would be very difficult to identify and mitigate the risks. So security analytics plays a big role in the security model.

VII. REFERENCES

1. http://www.emc.com/collateral/analyst-reports/security-analytics-esg-ar
2. https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence

IJRASET: ISSN: 2321-9653



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)