Analysis using Analytics in Cybersecurity

In the modern-day world, multiple technologies have evolved & its application has been implemented in various industries. The major reason seems to be the modern-day cyber attacks and the attackers approach. Modern day attacks have become more advanced & complicated than before which demands for a better technology and its use to prevent against such attacks.

Cyber security is the field which changes every day. New attacks, new vulnerabilities, new exploits get reflected on a regular basis. Multiple technologies such as Big data, Machine learning, AI are being used in the cyber security space to help cyber security professionals to prevent the organizations from any cyber attacks.

Let's understand how analytics is being used in cyber security and how to perform analysis using the analytical output:-

What is Analytics?

Analytics is nothing but generating some kind of pattern from data. Analytics can be Stack counting, Machine learning and much more. So, it involves input, processing and output. Input data will be the data of which you need some meaningful output. The processing part involves some kind of algorithm, formulas which can be applied on the input data. And the output is the actual use of analytics which will be used for any further analysis. Analytics makes the life of a cybersecurity professional a bit easy as it will be impossible for human to analyze huge amount of data.

What is Cyber security Analytics?

In the field of Cyber security, Cyber Security Analytics is the process of applying analytics to millions to logs which are collected from various IT infrastructure devices to identify any kind of unusual behavior or threat. Traditionally, for the purpose of security monitoring, SIEM has been used but SIEM doesn't fulfill the

requirements for detecting/preventing modern day attacks/APT's. SIEM works on an alert-based approach but we need something which can be a data-driven approach. Hence, multiple security vendors are incorporating Cyber analytics in their product functioning which will address the modern threats to organization.

In Cyber analytics, we apply some kind of formula/analytic to large amount of data and generate output which plays an important role in detecting threats. Output can be in the form of graphs, pie charts, etc. Anomalies, outliers can be detected using analytical approach. The data which is required for cyber analytics can be collected in various forms such as:-

- Endpoint logs
- User and entity data
- Network Traffic
- Cloud resources
- Identity & access management
- Threat Intelligence feeds

Need for Analytics:-

Analytics will be data-driven and it involves huge amount of data to be available at the input end to apply any kind of analytics. For a SOC professional, it involves looking out for alerts on a regular basis to detect/prevent any kind of malicious behavior but what if the logs are in millions. In such scenario, even alerts might miss lot of things and there needs to be a way out to analyze millions of logs. In such scenario, analytics comes into picture ad provides us with meaningful data out of those logs.

Machine learning is one such technology which provides us with analytical capabilities. Machine learning consists of various algorithms which can be applied to data and output can be generated based on the type of algorithm used. Mostly classification and clustering algorithms are used in Cyber security. It involves training set and test set wherein we initially train our data based on the training

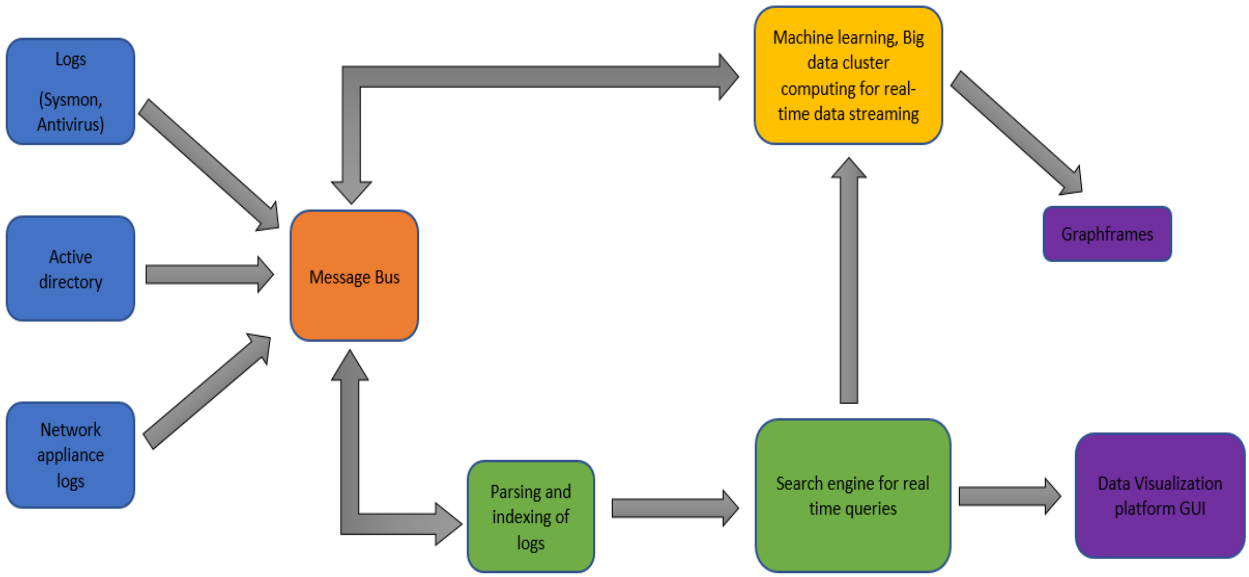
set and once, the algorithm has learned our data, we used new set of data or test set to generate output based on the algorithm.

Analyzing using Analytics:-

Various platforms are available to perform Cyber security analytics such as Securonix, RANK Vasa etc. The analytics work is done by the solution algorithms but the most important thing is the analysis part, once we have the meaningful output. The human element is always involved even if the Machine leaning and automation is applied.

“Proper Analysis using Analytics is the need of hour”

We can also build an analytical solution on our own using open source tools. Let’s understand how we can do that-



Above design can help us build our own cyber security analytical solution. Various open source tools can be used to perform the same.

1. Logs collection from various devices – BEATS from ELK stack.
2. Message Bus – Apache Kafka
3. Parsing and indexing of logs – Logstash from ELK stack.

4. Logs processing and search engine - Elasticsearch from ELK stack.
5. Real time data streaming and processing, Machine learning – Apache Spark
6. Data Visualization platform – Kibana from ELK stack.

Cyber Security Analytics Use cases:-

Cyber analytics has multiple use cases including network anomalies, UEBA etc. Please find the below mentioned few use cases:-

1. UEBA Abnormal user and entity behavior analysis
2. Real time Threat hunting
3. Detecting insider threats
4. Detecting data exfiltration
5. Network traffic anomaly detection
6. Abnormal processes making unusual connections
7. Compromised system/account/user analysis

& many more which you can think of.

In this way, cyber analytics should be adopted by every organization as it will not only reduce the work of the Cyber security professional but it will also provide you with an effective output. Various commercial vendors have already implemented analytical capabilities. We can also build our own analytical solution based on open source tools.

Before analyzing any solution, we need to understand whether its really required for the organization. Proper plan should be defined and data is of utmost important in this analytical solutions. Hence, **PLAN & IMPLEMENT**.

Cyber analytics, if possible & required, should be implemented by every blue teamer and it should be utilized in a proper and effective way i.e. **Proper Analysis using Analytics**

Happy analysis using analytics!!!