# PROJECT #2

As machine data continues to grow, it is becoming increasingly difficult to manage. This is especially true for organizations that have not put in place the proper tools and infrastructure to handle the volume of data. In order to effectively manage machine data, organizations need to have a plan in place that includes the right tools and processes. Without the proper tools and processes, machine data will continue to grow unchecked, making it difficult to make sense of and use.

Organizations use Splunk to monitor and analyze machine data from any source to gain insights into their IT operations and business. By using Splunk, they are able to quickly and easily identify issues, troubleshoot problems, and gain operational intelligence. Additionally, Splunk can help organizations save time and money by reducing or eliminating the need for custom scripts or other manual processes to collect and analyze data.

The splunk can take data and add it to an searchable index, this would consider both structured and unstructured data. This would not only solve the application issues but also point to web security, user behavior, sales totals.

The heart of splunk is the index, this would contain the machine data from all the network devices and applications. These consist of different search results and these results can be changed to reports. The facility to transform knowledge to respective data models can also be performed using splunk.

Some of the main functions of spunk are -

- Index data
- Search and investigate
- Add knowledge

- monitor, and alert.
- Report and analyze
- Create alerts
- Create visualizations

The splunk offers a “splunk web” and application. There are different roles present in the system. These roles are used to see, perform and interact with different operations.

1. Admin- Web apps
2. Power: share knowledge objects and share
3. User - can see their own knowledge objects and view shared ones.

The use of search is very much recommended in the splunk. The search is used to retrieve and transform -

- Events
- Patterns
- Statistics
- visualizations

The configuration of exploiting different fields are present in the application. These events are returned chronological order. This would show the newest first.

Splunk also consists of a language called search processing language(SPL), here these would offer different commands to perform operations. Such as -

1.search terms

2. Commands;

3. Functions

4.Arguments

5. Clauses - how we want groups defined

Additionally, Splunk offers some best practices for carrying out tasks and achieving successful outcomes. This would make the process simple and offer users a wide range of features. The sensitivity of the situation and successful results are some of the best practices. This would make the process simple and offer users a wide range of features. One of the finest practices is to take the case's sensitivity into account. The host value replaces the values that are currently present in the Splunk fields, which are case-sensitive. This would comprise source type, host, source, and index. These are significant and merit consideration. It is advised to utilize "or" or "in" when searching in order to obtain the needed results much more quickly. It is important to observe how filtering instructions are used.

The knowledge objects are tools that help the user perform operations. Some of the operations that can be performed by using these objects are -

- Data interpretation
- Data classification
- Data enrichment
- Data models
- Data models

These are useful to save and reuse for multiple applications. Knowledge managers are people responsible for knowledge objects. They implement best practices by creating data models. Splunk also offers visualization. The option of generating maps uses geostatistics. It uses geostatistics with IP addresses.

It also used choropleth maps and a keyhole markup language file. Splunk's choropleth maps are a great way to visualize data sets that are geographically distributed. By using colors to represent different data ranges, choropleth maps make it easy to see patterns and trends in the data. Splunk's choropleth maps are interactive, so you can hover over a data point to see more information about it. And finally, security information and event management (SIEM) is a use of technology by blue teams to identify, detect, and respond to cyber threats. SIEM technology aggregates and analyzes data from multiple security tools and devices in real time. This data can include system logs, network traffic data, and security alerts from intrusion detection systems and firewall logs. By analyzing this data, blue teams can detect and respond to threats more quickly and effectively.