Splunk SIEM— Enterprise Security Monitoring & SOC Visibility

Project By: Unnati Pandya

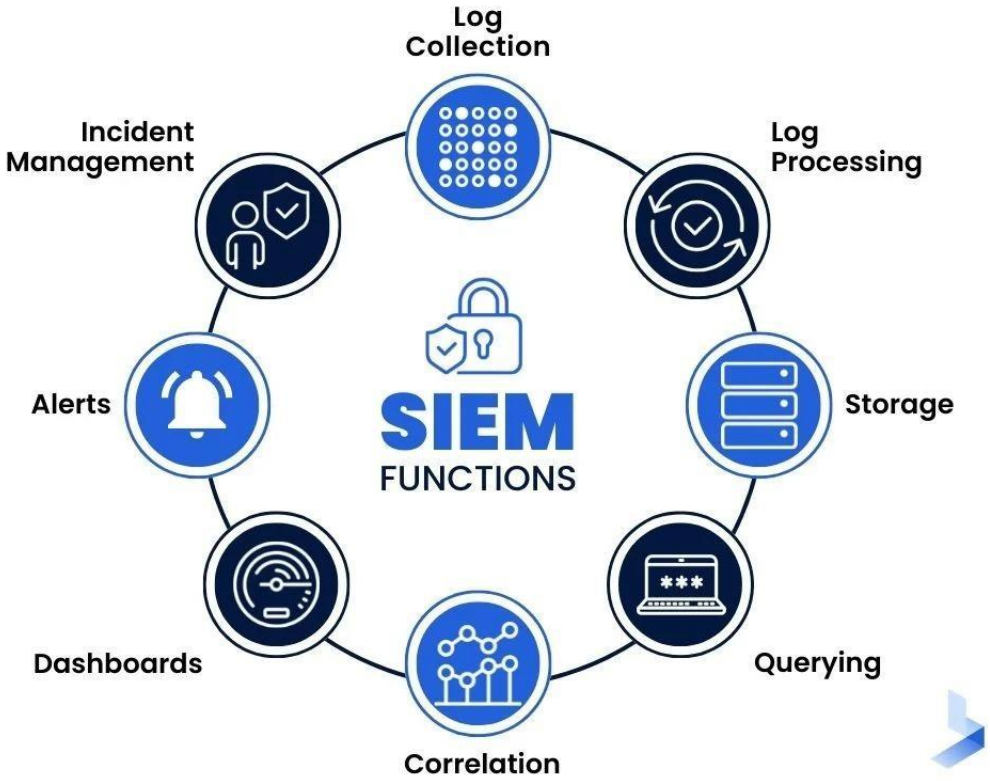
Role Focus:

Security Operations | Threat Monitoring | Log Analytics

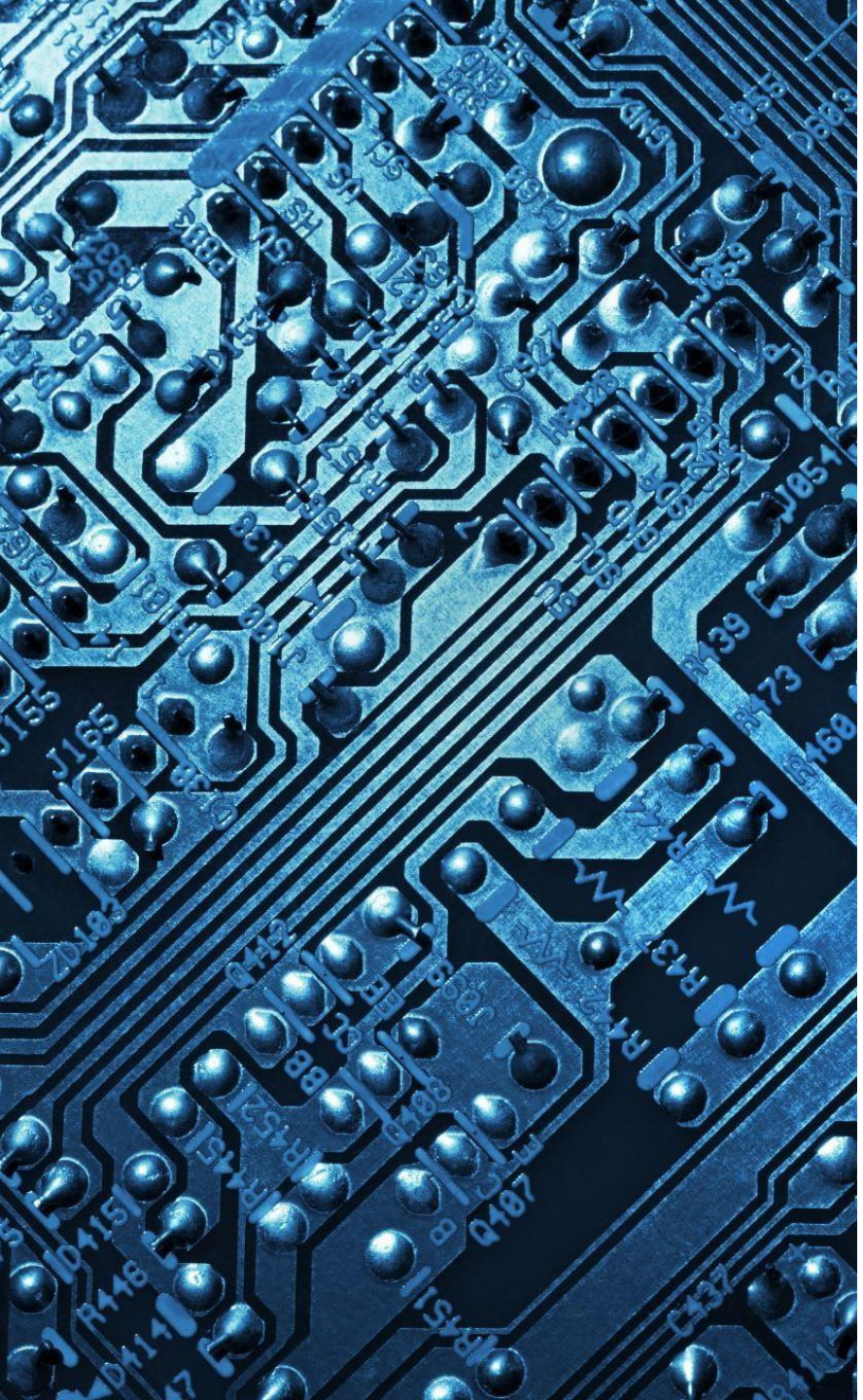
Introduction

What is SIEM in general?

- SIEM stands for “Security Information and Event Management”.
- It is a cybersecurity tool used by cyber security analyst which collects and analyzes the data from multiple origins such as different networks, applications, various end points such as, mobile phones, pc, IoT devices, virtual machines or containers.
- Basically, this tool helps detects and analyzes the cyber threats to any organization or company. It is an essential tool used by cybersecurity experts for threat detection.



SIEM has some key features because of why it is a crucial tool for cyber security specialist, and why is it useful?



1. ***Continuous monitoring and Threat Intelligence:*** SIEM tool provides continuous monitoring and is proactively analyzing and detecting the possible threats or some unusual activities taking place in an organization in real-time. It has quick incident response capability which makes easy for an organization or cyber security experts to catch the vulnerabilities. It scans and detects unauthorized user or activity entering the system or network.

2. ***Threat Detection and Incident Response:*** This technique includes to analyze the network flow, unusual behaviour and incidents. It keeps an eye on unauthorized incidents and identifies the malicious activity. Once potential threat is identified, it takes appropriate action to mitigate the risk by blocking the network flow and unusual traffic and prevents from exploitation which may lead to severe damage.

3. ***Alerting and Notification:*** This tool will notify you for all the threats detected and sends you an alarming notification that there may be some suspicious activity occurring. It will then provide recommendations on further steps to be taken from preventing further exploitation.

4. ***Forensic Investigations:*** SIEM will then investigate the threat incidents and conduct a forensic analysis, and will help organizations or cybersecurity analyst to implement the further necessary actions which will help them identify the root cause of where the threat came from, what were the risk mitigations , how it breached into the system or network and will take necessary measure.

5. ***Operational Efficiency:*** SIEM tool will improve system efficiency and will have a smoother operational workflow, it will create an automated response to mitigate risk and make the workflow and operation more easy and efficient.

- SIEM tool can be very handy and crucially important tool to have in any organization and for cybersecurity expertise.
- It *centralized* the *visibility* in our systems and *overall infrastructure*. Being reliable and its response capabilities to ensure regulatory observance.

SIEM software: SPLUNK

In our SIEM tool software, we choose ***SPLUNK!***

Firstly, what is Splunk? So, Splunk is a versatile big data platform which simplifies the task of collecting and gathering massive information and allows you to collect, search, index, analyze and visualize data from various sources like websites, applications, systems etc. Splunk enables predictive analysis and is a very reliable monitoring tool.

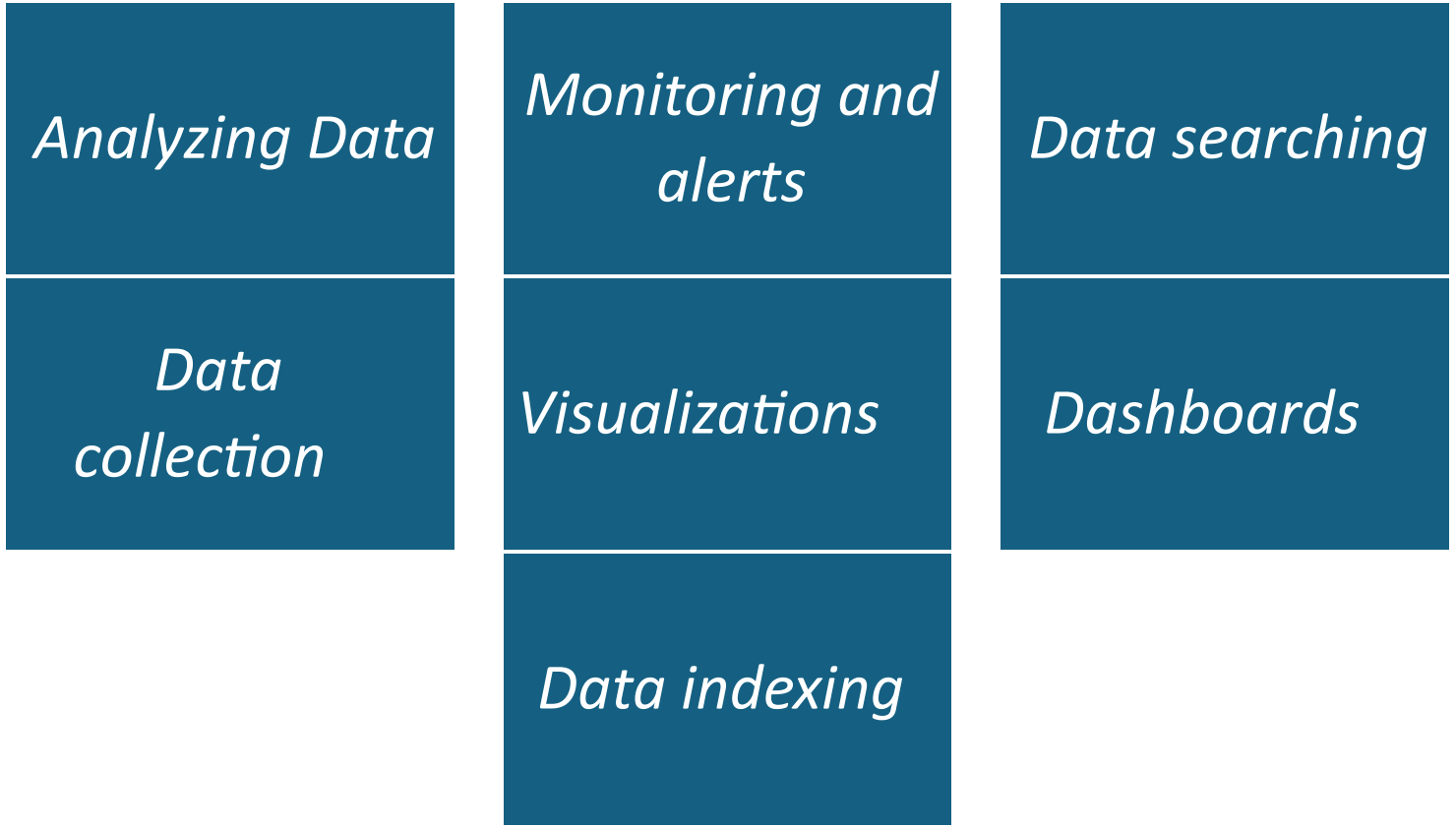
The reason we choose Splunk is because

- *It* ***instantly and accurately*** alerts the dynamic thresholds.

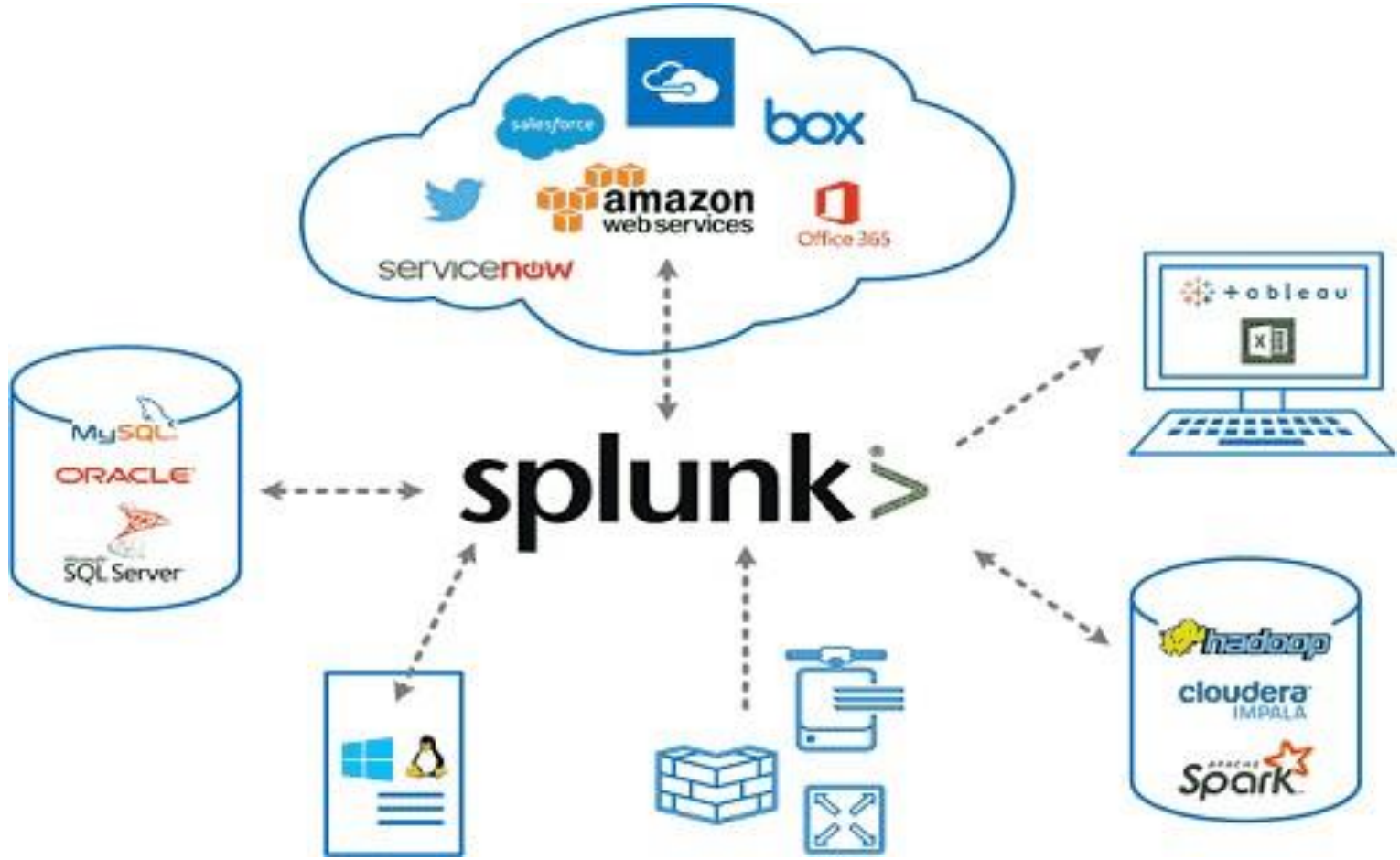
Why did to choose Splunk?

- Because of its ***user-friendly Interface*** and ***accurate search capabilities***.
- ***High scalability:*** Splunk can handle massive amount of data.
- ***Real-time monitoring feature***: Splunk offers real time monitoring
- ***Cloud deployment friendly:*** Splunk has a robust support for cloud environment. It offers both on-premises, Hybrid as well as multi cloud support. Offers flexible deployment.
- ***Customization and Integration:*** It's add on feature are unique which fulfills seamless integrations which allow users to utilize most of its benefits of Splunk software.

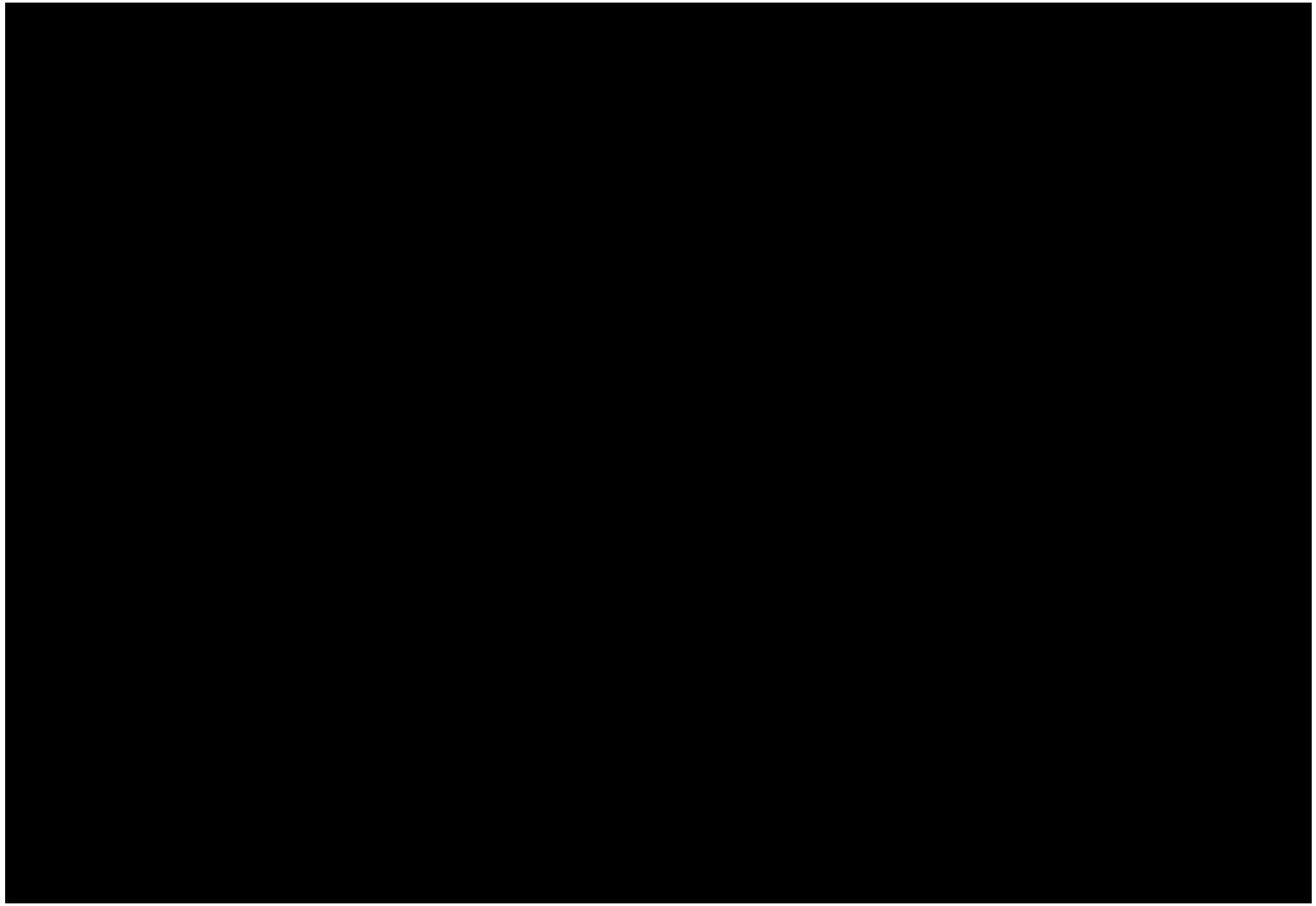
How splunk works


Analyzing Data
Monitoring and alerts
Data searching
Data collection
Visualizations
Dashboards
Data indexing

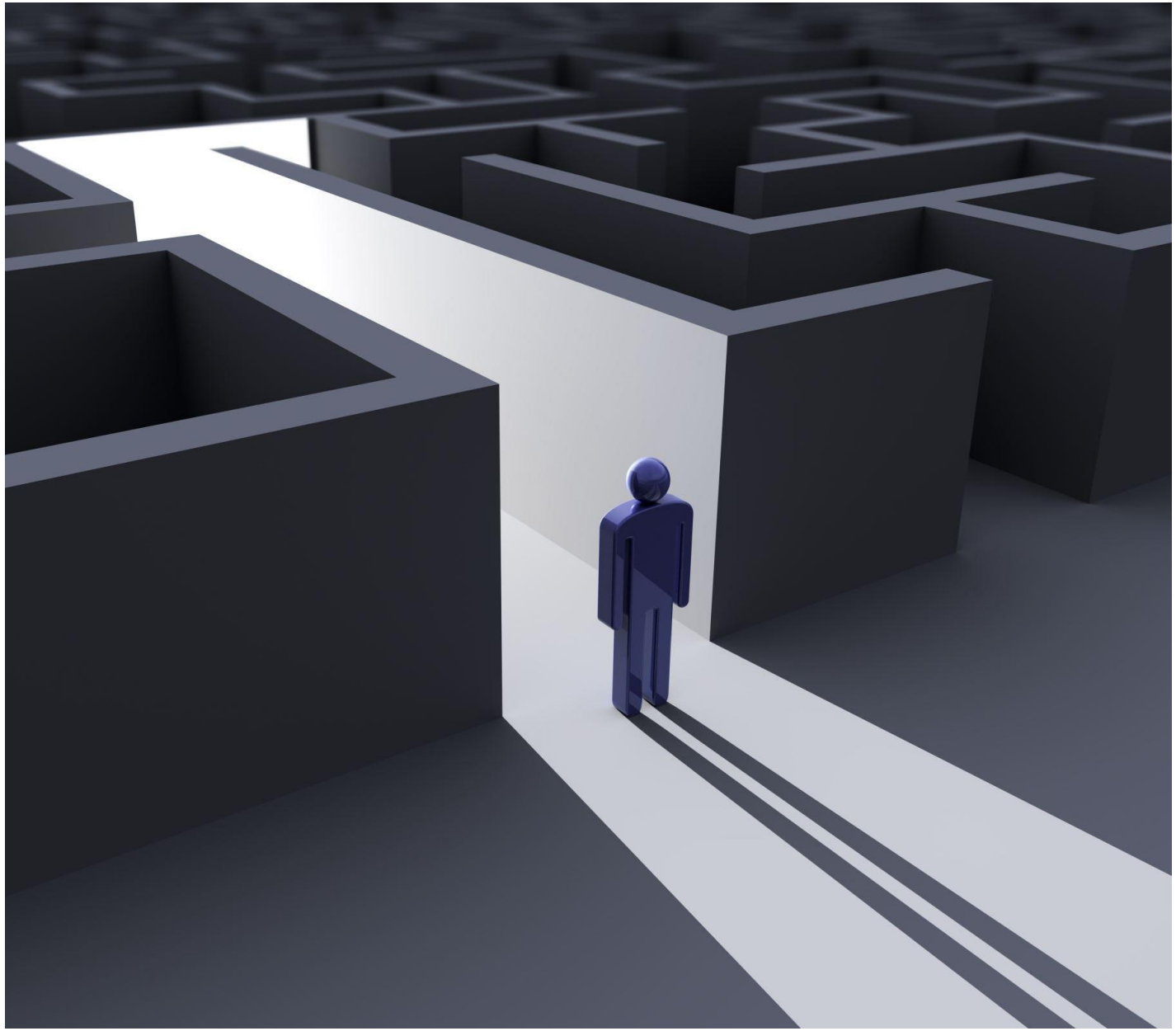
Explain how does it works and what will it do?


salesforce
box
amazon
web services
Office 365
servicenow
MySQL
ORACLE
SQL Server
splunk>
tableau
hadoop
cloudera
IMPALA
Spark

How to install (The Installation part)

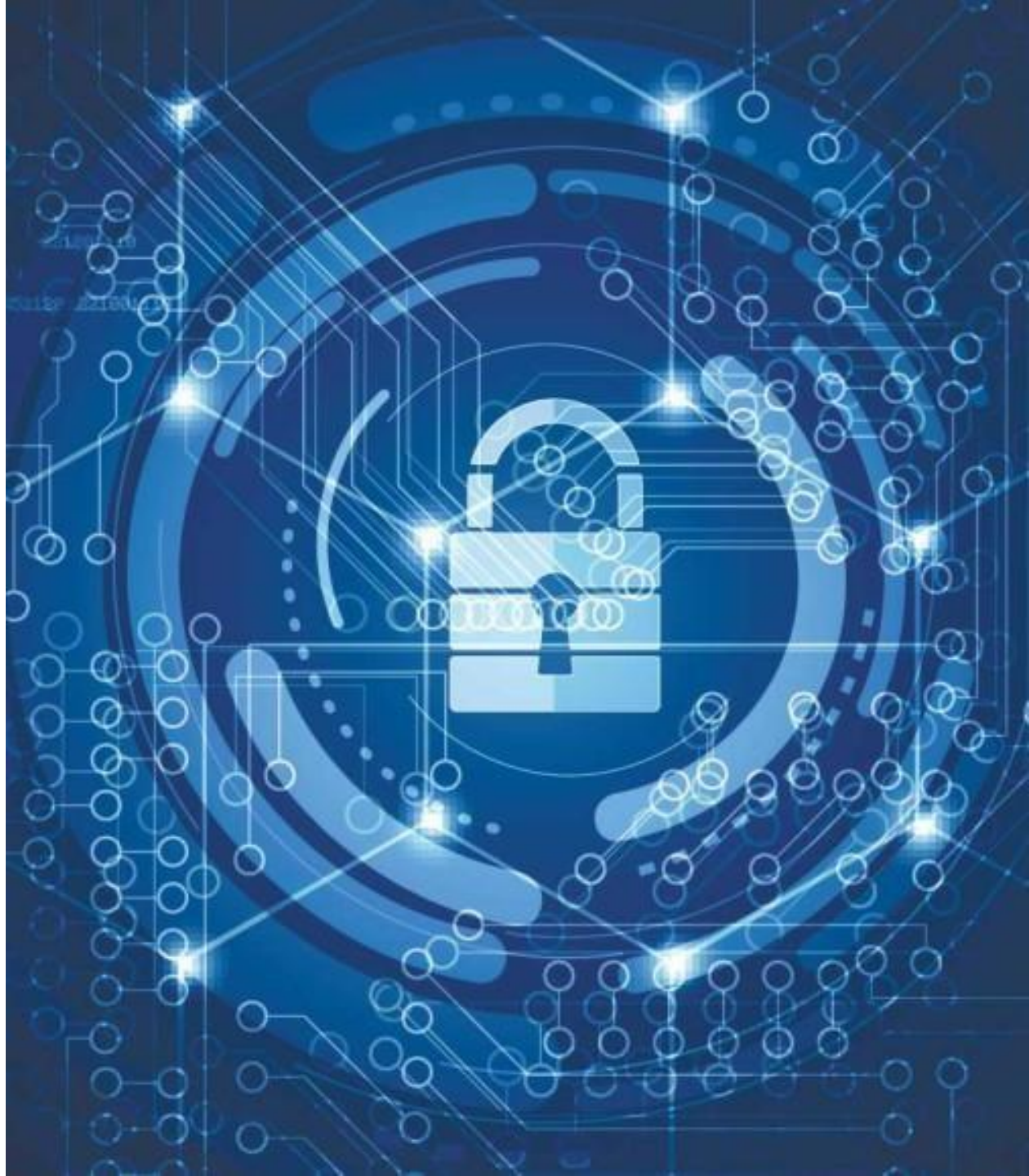


List any Pitfalls and Difficulties you faced



How can SIEM assist SOC?

- It plays major role in enhancing the overall security in any enterprise.
- It provides visibility to an organization in terms of security operations.
- In terms of security operations, it also minimizes the risk of potential threats occurring by proactively monitoring the flow and enhance overall security operations.



CONCLUSION

Was this useful?
Do you think this will help gathering all security related events?
Can this help discover abnormalities?

- Splunk is a versatile solution for enterprises wanting to reduce the risk of data breaches and cyber attacks.
- Its operational intelligence capabilities make a Splunk crucial to have.
- In conclusion, Splunk is valuable and crucial asset for any Organization. willing to enhance its security. It is powerful tool for maintaining robust security operations ensuring visibility, reliability, and safeguarding our enterprise overall.

What we Learn

- SIEM role in SOC in enhancing the overall security in any enterprise.
- Using the Splunk tool from security point of View.
- In security operations, Role of Monitoring and Analyzing the data and that even Raw data is important to organization when it comes for Cybersecurity.

THANK YOU

UNNATI PANDYA