**Stage 3**

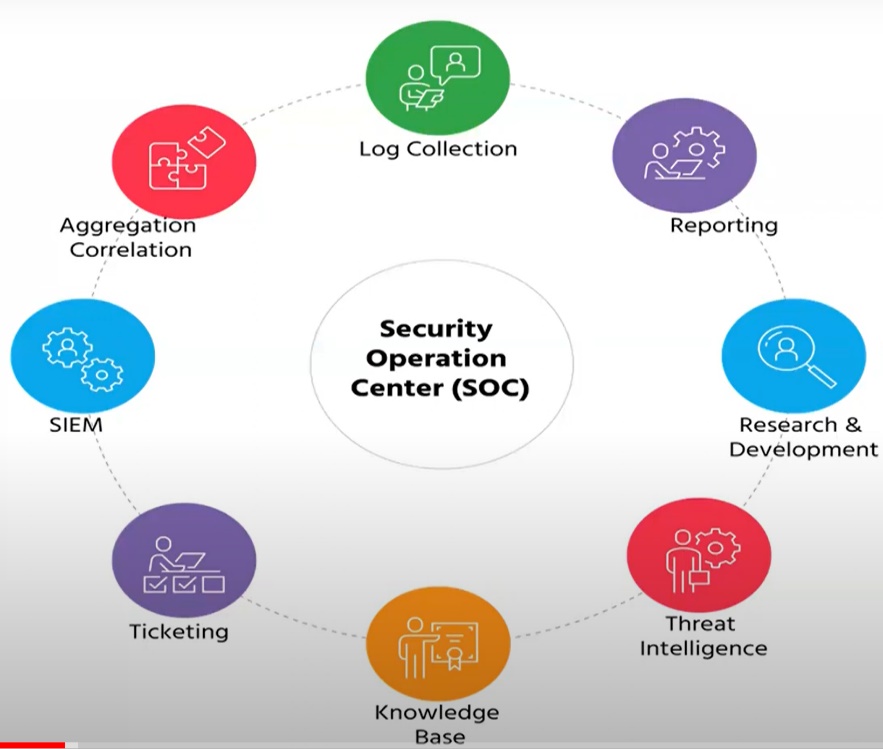
**Report**

**Title: Ability of SOC/SIEM**

* **SOC**

It is centralised unit within an organization that is responsible for monitoring, detecting and responding to cybersecurity incidents.It is the primary point of contact for security-related issues and typically includes a team of security analysts, incident responders, and other security personnel who work together to protect the organization's assets and data. SOCs may also be responsible for managing security technologies, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems, as well as developing and implementing security policies and procedures.

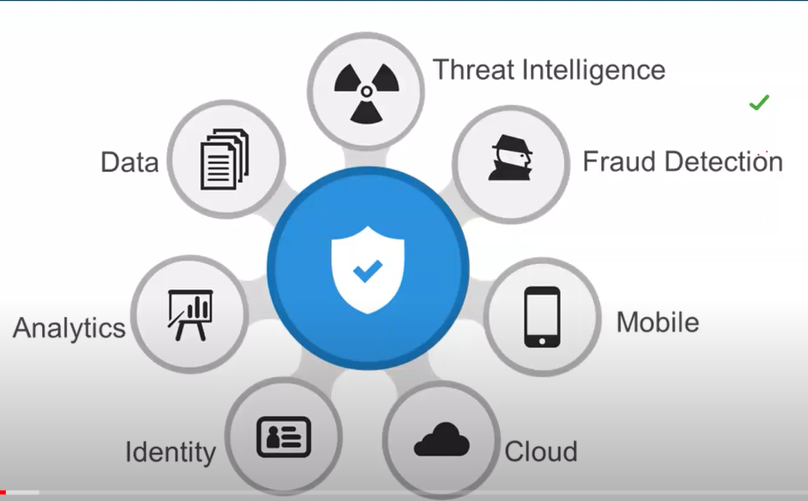
* **SOC Cycle**

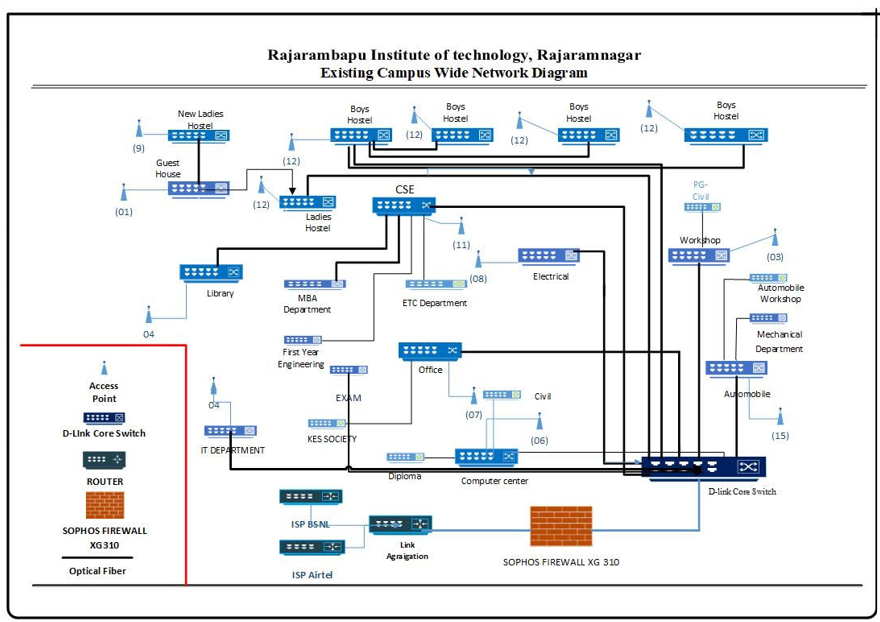
****

* **SIEM (Security Information and Event Management)**

SIEM systems continuously monitor various data sources, including logs, events, network traffic, and system activity, to gather information about the security posture of an organization's IT infrastructure. Monitoring involves the collection, analysis, and interpretation of security-related data to identify potential security incidents or anomalies.

* **SIEM Cycle**

****

* **MISP**
* **RIT College Network Information** 
* **Threat Intelligence**

****

* **Incident Response**

Incident response is the structured approach and set of procedures implemented by organizations to address and manage security incidents effectively. It involves detecting, analysing, containing, and mitigating the impact of security breaches or unauthorized activities on an organization's system, networks, data or assets.

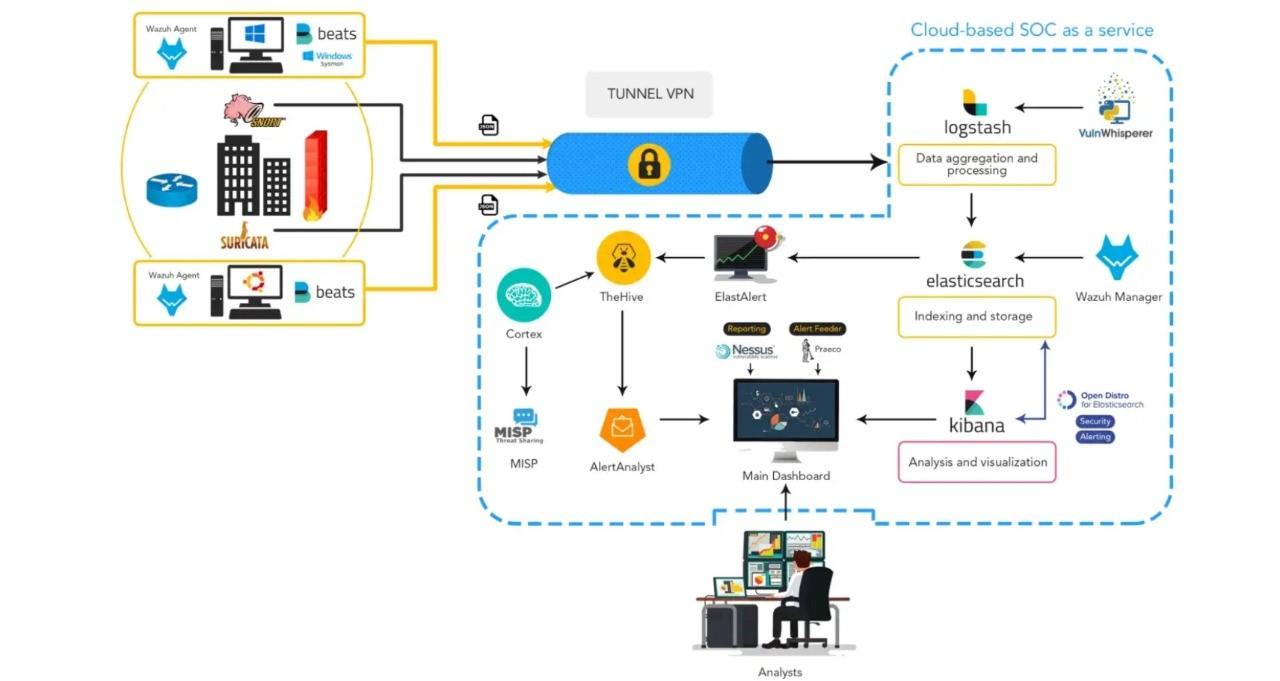
* **QRadar & Understanding about tool**

7:1

**Conclusion:**

**Intelligent Threat Detection And Response: AI Integration In Cybersecurity Frameworks**

A SOC, or Security Operations Center, is a centralized unit within an organization responsible for monitoring, detecting, and responding to security incidents. It is the primary point of contact for security-related issues and typically includes a team of security analysts, incident responders, and other security personnel who work together to protect the organization's assets and data. SOCs may also be responsible for managing security technologies, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems, as well as developing and implementing security policies and procedures.



* ENDPOINT
* SIEM
* MISP
* IR (incident Response)
* TI (Threat Intel)?
* Ticket/event Management
* IN an organization their will be many endpoints (sophos)?
* This will be monitored by soc analyst
* The organization every logs will be monitored through SIEM (Like firewall

,router, ips/ids, devices, cloud? LOGS), Think it as a L1– ? If it finds any different LOG? It will forwarded to L2 .

* It will do the elastic search?
* Then by using of shuffle it will give the alerts to the? teams to soc agents .
* HERE the hive logs will collect all the details of the log .
* And then , It will be send to cortex for scanning of the log details