Introduction to SIEM

## **Task 1 – Introduction**

Security Information and Event Management (SIEM) is a **security solution** that collects, normalizes, stores, and analyzes security-related data from multiple sources in real time.  
It enables **centralized logging**, **correlation of events**, and **alerting** to detect and respond to potential threats.

## **Task 2 – Core Functions of SIEM**

1. **Data Collection** – Gathers logs and events from various devices:
   * Firewalls
   * IDS/IPS
   * Servers
   * Applications
2. **Normalization** – Converts logs from different formats into a unified structure.
3. **Correlation** – Links related events across multiple sources to identify suspicious patterns.
4. **Alerting** – Sends notifications for critical or unusual activities.
5. **Reporting** – Generates compliance and security reports.
6. **Retention** – Stores historical logs for forensic analysis.

## **Task 3 – Benefits of SIEM**

* **Threat Detection** – Identifies malicious activity in real-time.
* **Incident Response** – Provides detailed logs to speed up investigation.
* **Compliance** – Helps meet regulatory requirements (e.g., PCI-DSS, HIPAA).
* **Visibility** – Centralized view of security across the network.
* **Forensics** – Enables post-incident investigation.

## **Task 4 – SIEM Architecture**

Typical SIEM consists of:

1. **Log Collection Layer** – Agents or syslog servers gather logs.
2. **Processing Layer** – Normalization and correlation engines.
3. **Storage Layer** – Database for storing logs and events.
4. **Presentation Layer** – Dashboards, alerts, and reports.

## **Task 5 – Examples of SIEM Tools**

* **Commercial**: Splunk, IBM QRadar, ArcSight
* **Open Source**: Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana), OSSIM

## **Task 6 – Limitations of SIEM**

* Can produce **false positives** if not tuned properly.
* Requires skilled analysts to interpret alerts.
* Resource-intensive (needs storage and processing power).

## **Task 7 – Conclusion**

SIEM is a critical component in modern cybersecurity operations.  
It enhances visibility, improves detection, and supports compliance, making it essential for both **enterprise security** and **incident response workflows**.