



<https://t.me/learningnets>



PROJECT

ENG

PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project **ENG PRO**

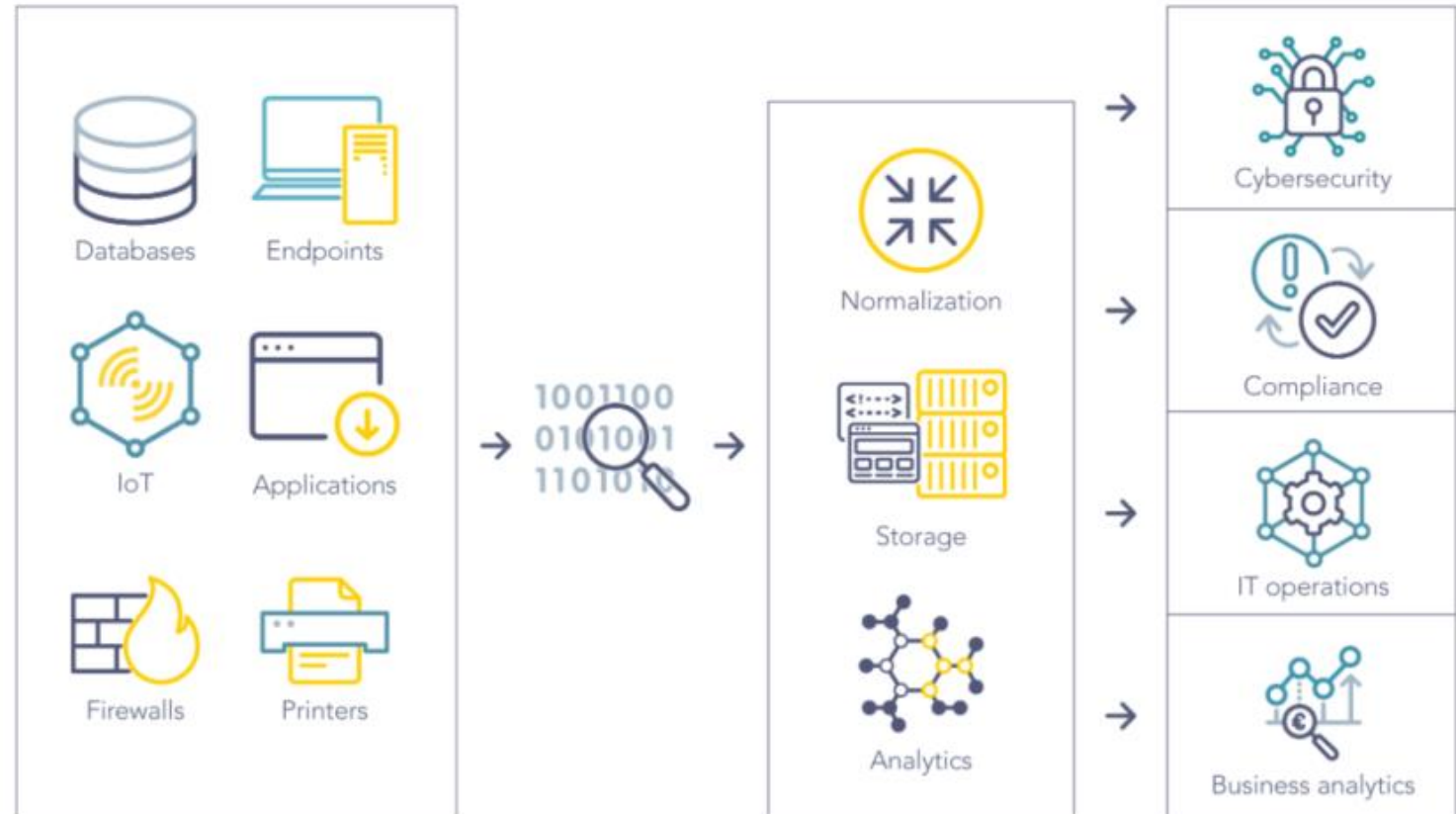


SIEM Solutions in Cybersecurity



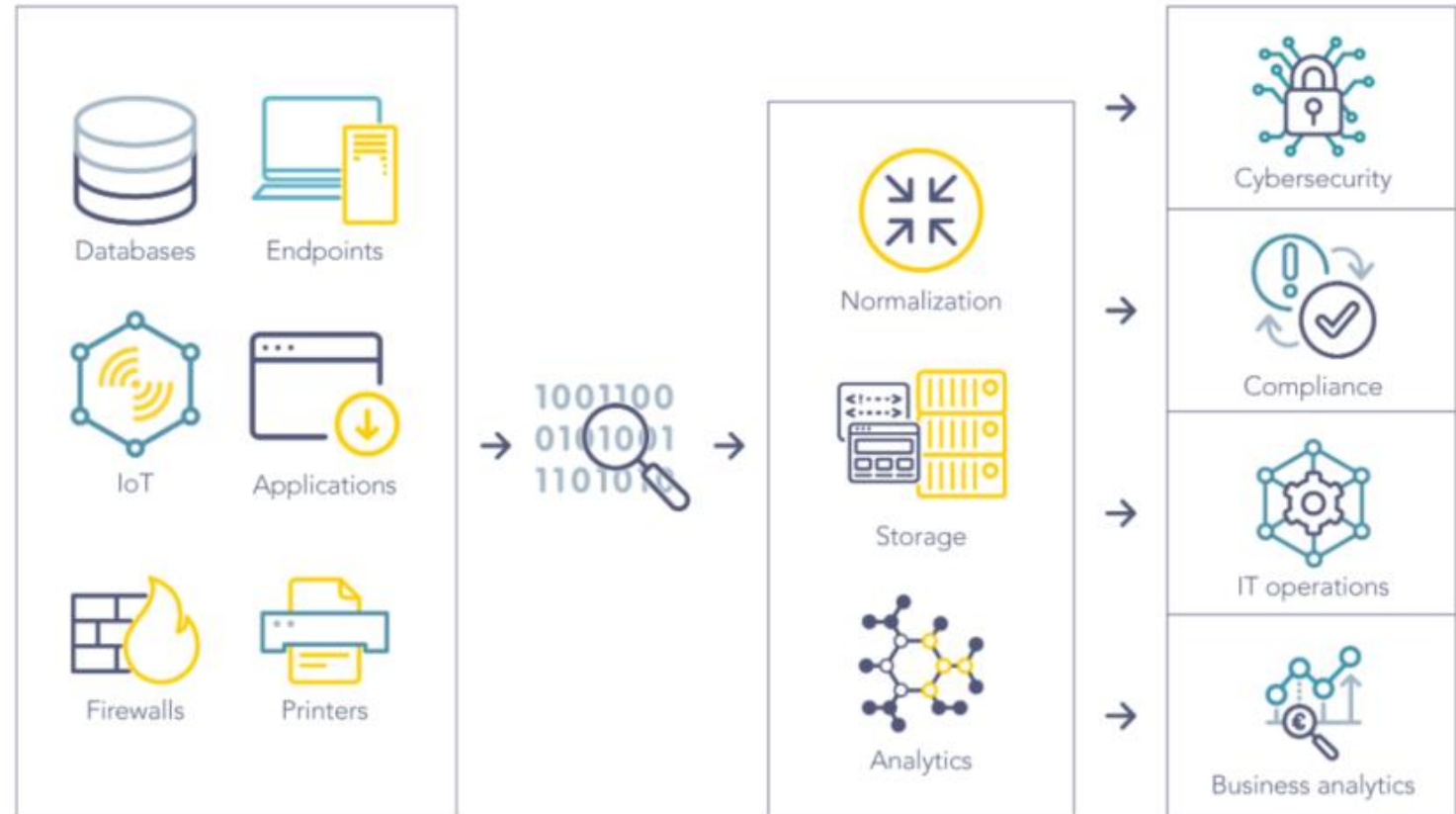
SIEM Introduction

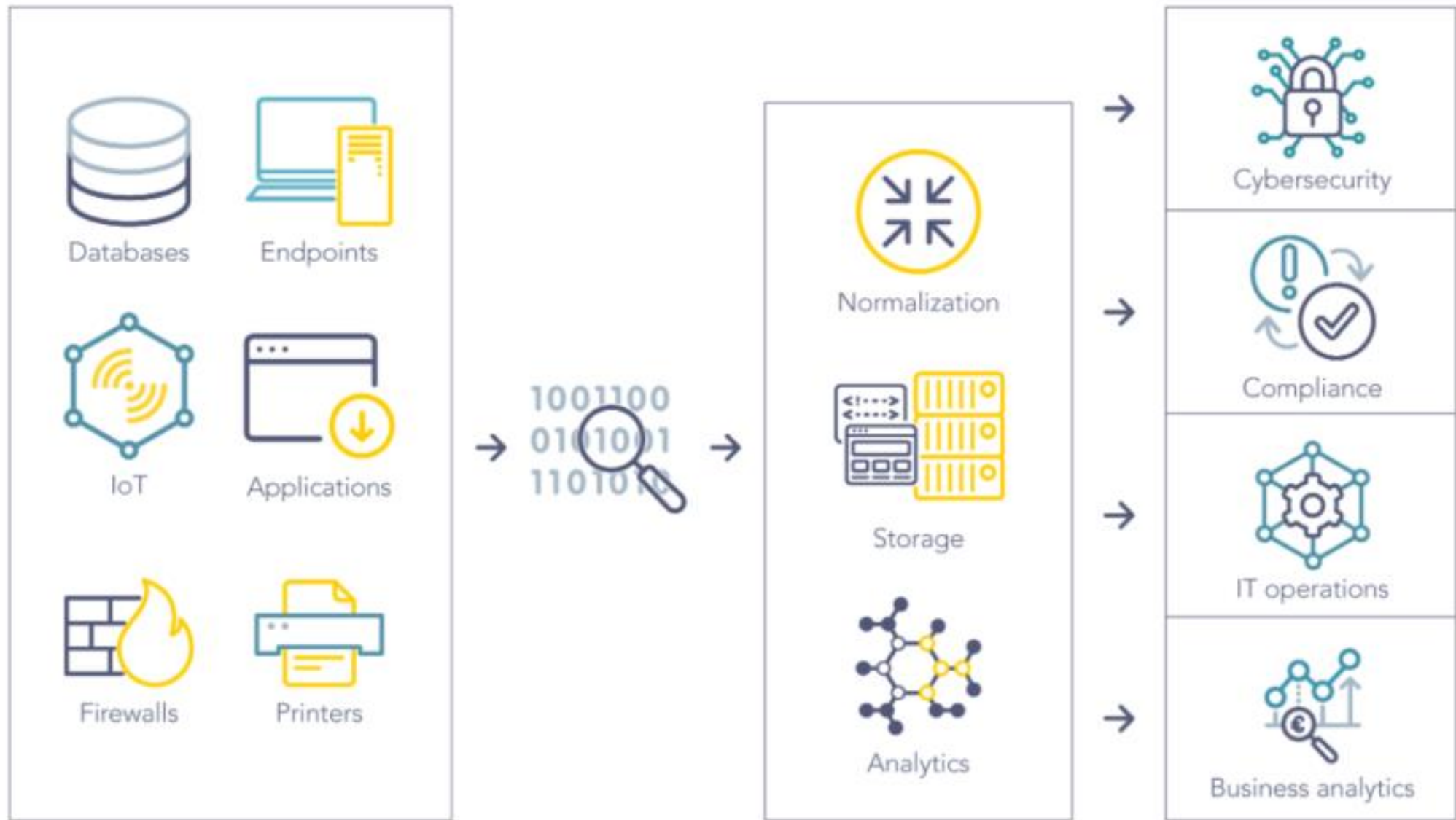
SIEM software collects and aggregates log data generated throughout the entire IT infrastructure, from cloud systems and applications to network and security devices, such as firewalls and antivirus.



SIEM Introduction

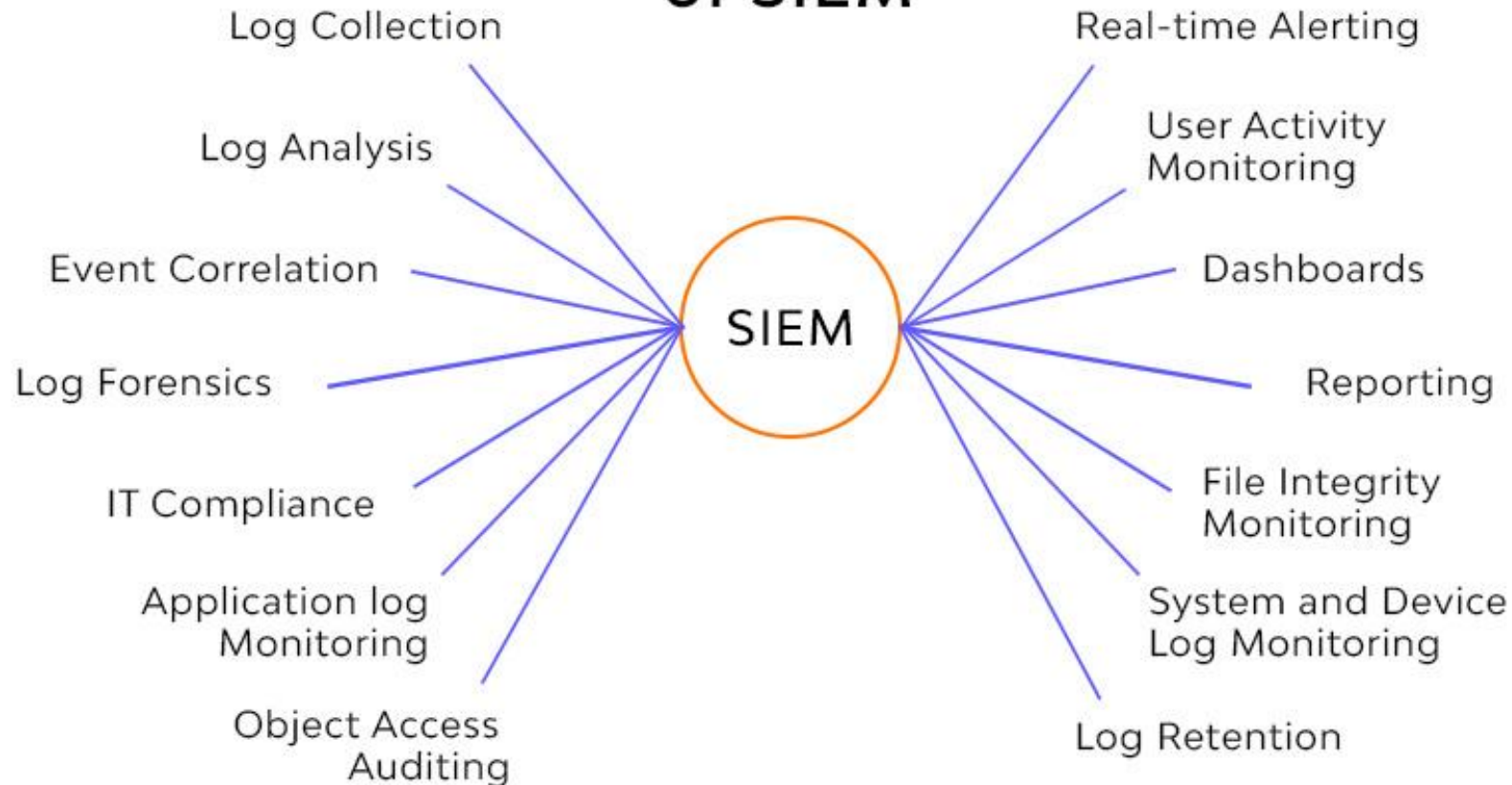
Enterprises must monitor and guard their data to protect themselves from increasingly advanced cyber threats in the digital economy. Companies have more data to collect and analyze than ever before.





Log Management

Components and Capabilities of SIEM



Log Management's Broad Scope

SIEM's Analytical Power

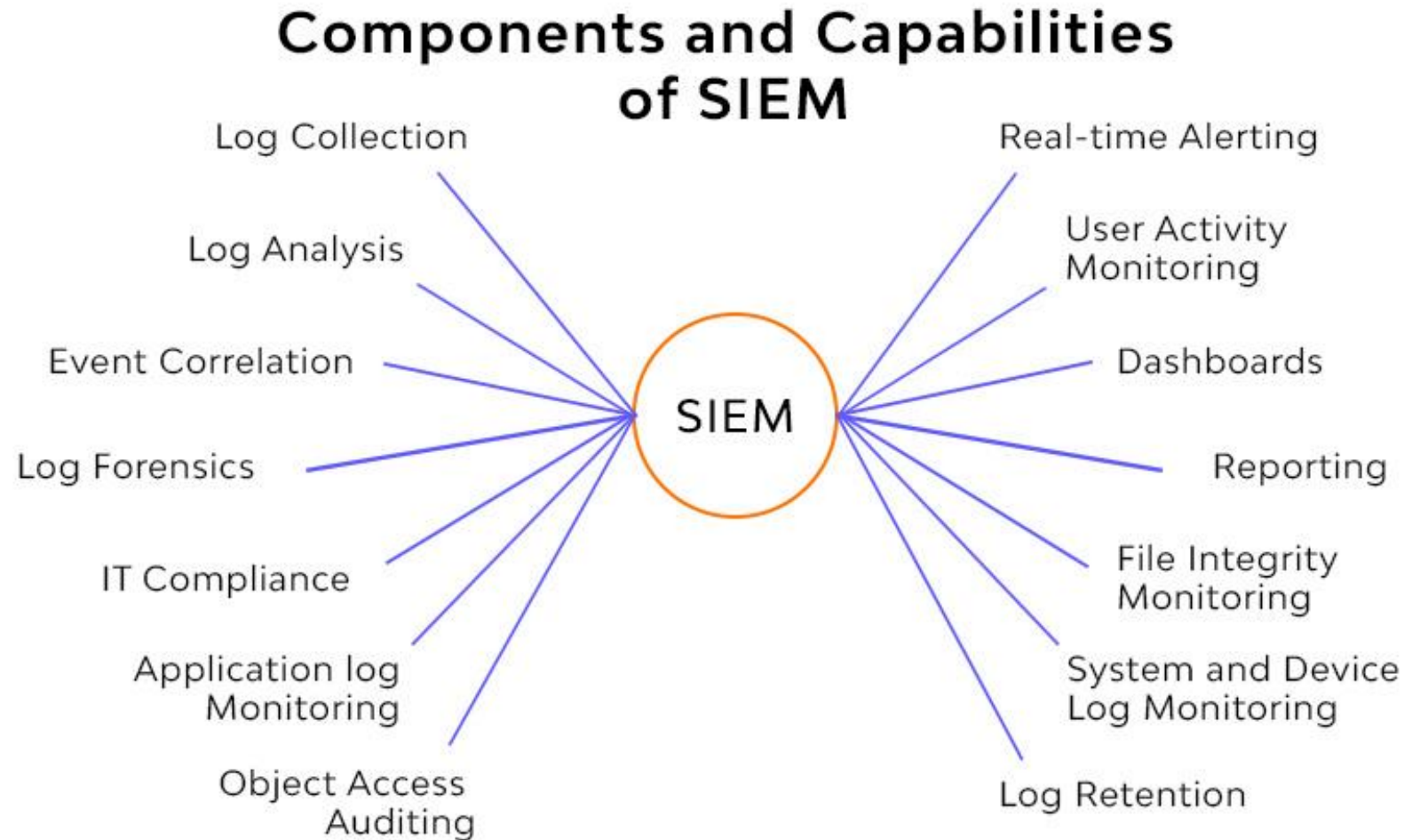
Centralized Insights

Alerting

Analyzing
Events

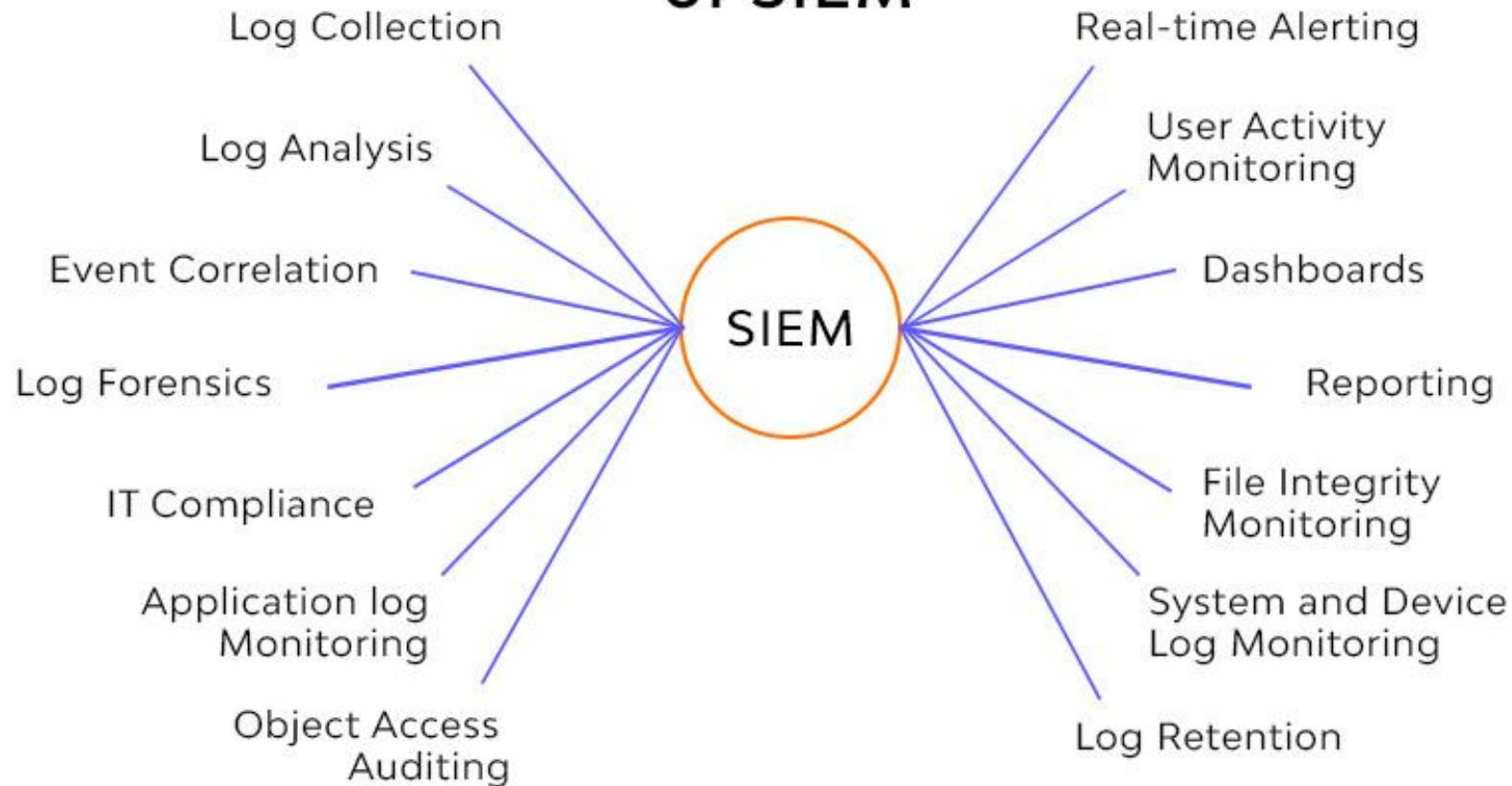
Escalating
Alerts

Notifying
Security Staff



Dashboards and Visualisation

Components and Capabilities of SIEM



**Dashboard
and
Visualization**

**Pattern
Identification**

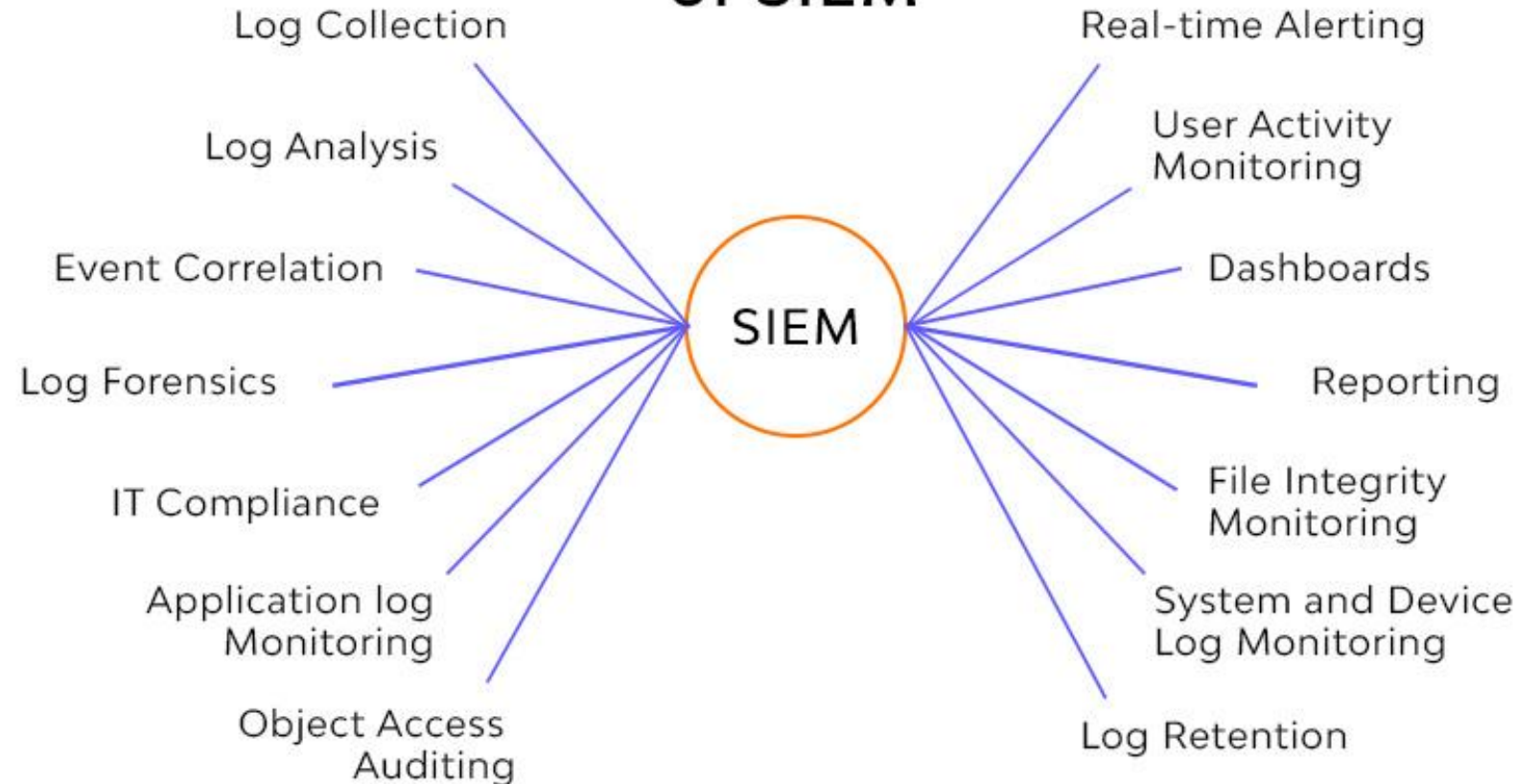
**Data
Retention**

Date Retention

Storing
Historical
Data

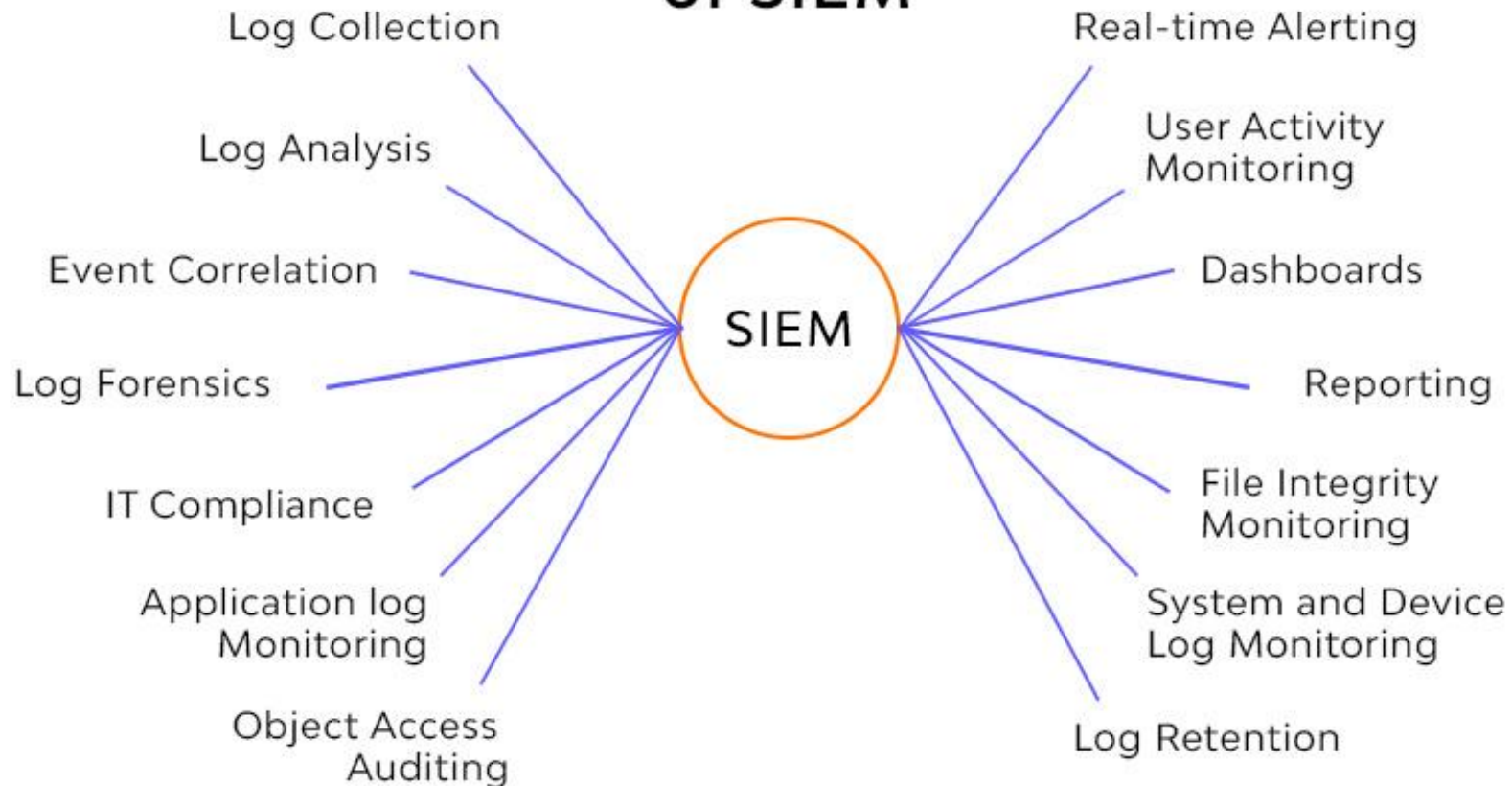
Supporting
Forensic
Investigations

Components and Capabilities of SIEM



Threat Hunting

Components and Capabilities of SIEM



**Proactive
Threat
Hunting**

**Manual or
Automated**

**Query and
Analysis**

Incident Response

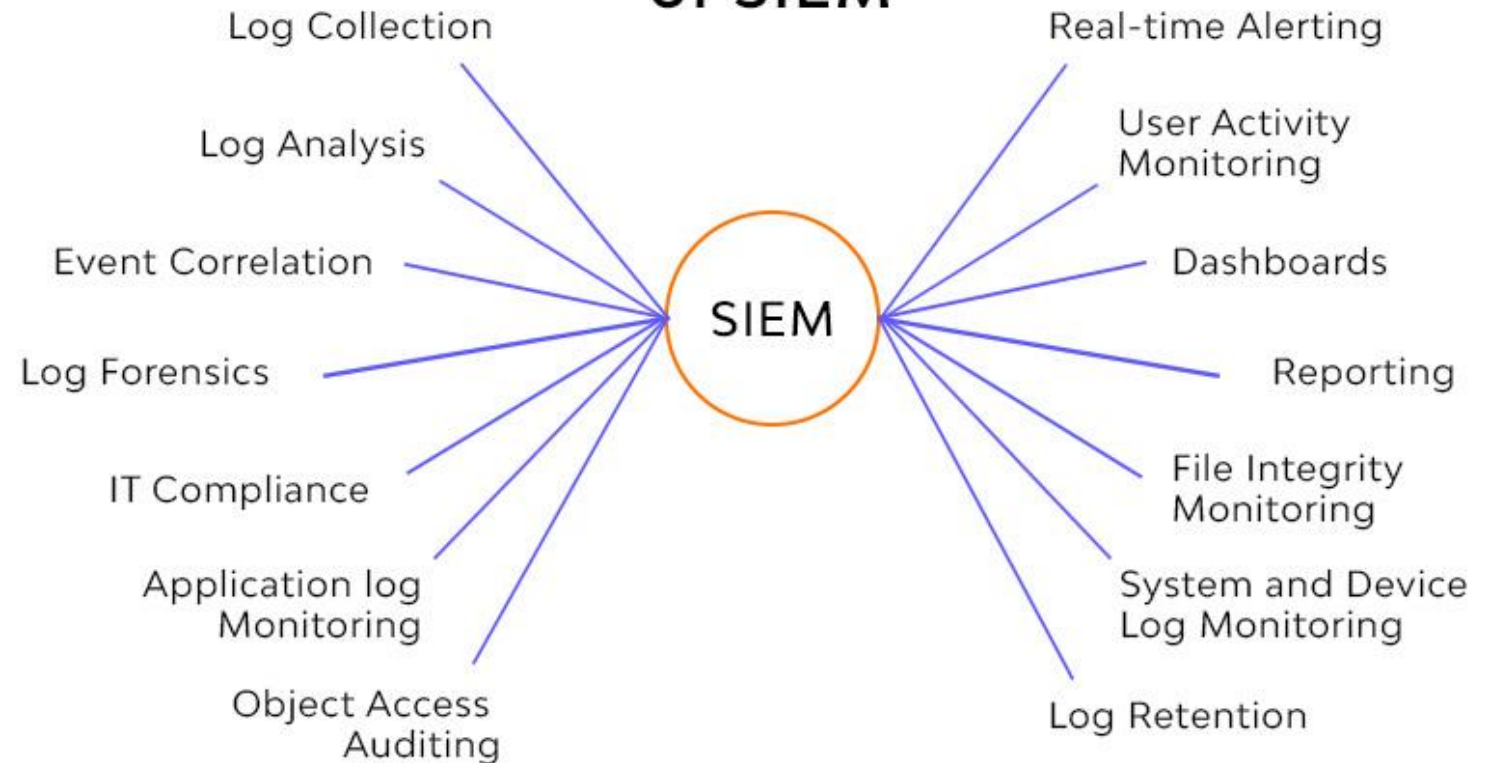
Case Management and Collaboration

Knowledge Sharing

Integration with Ticketing Solutions

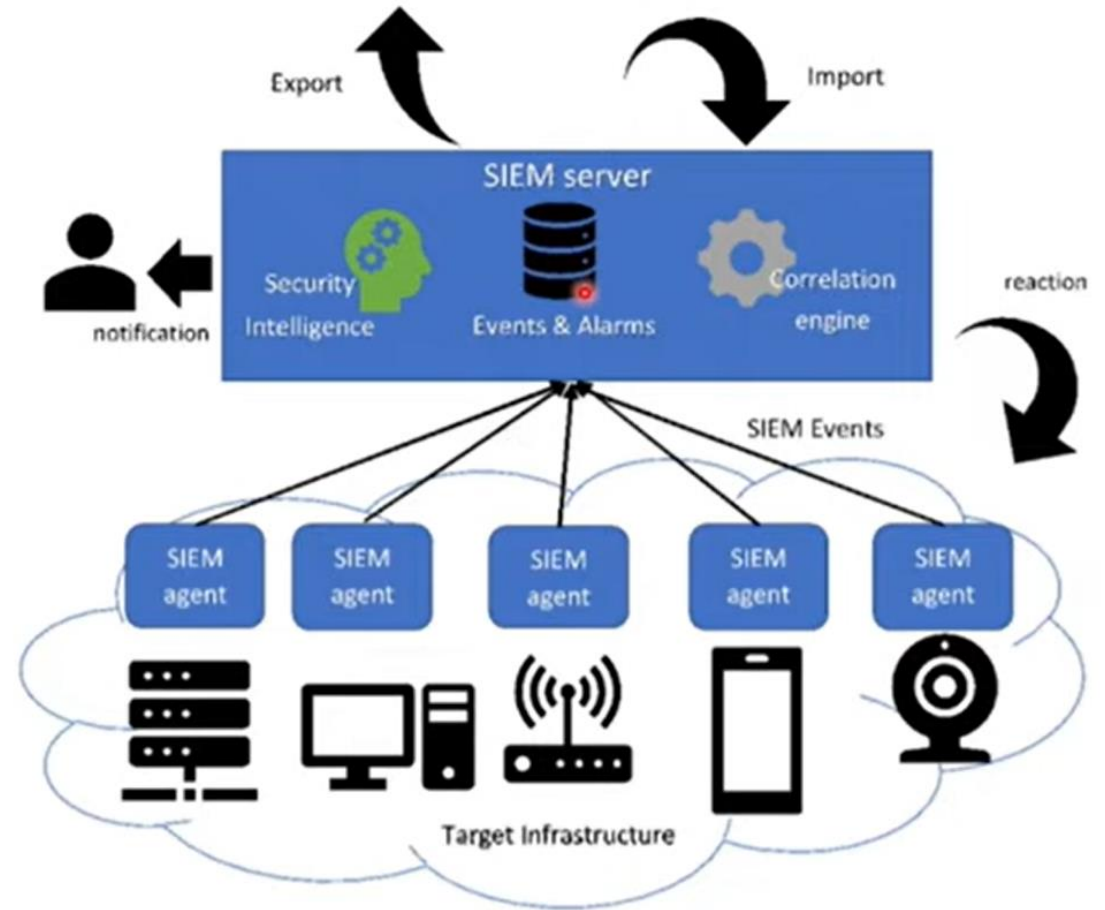
Communication Tool

Components and Capabilities of SIEM

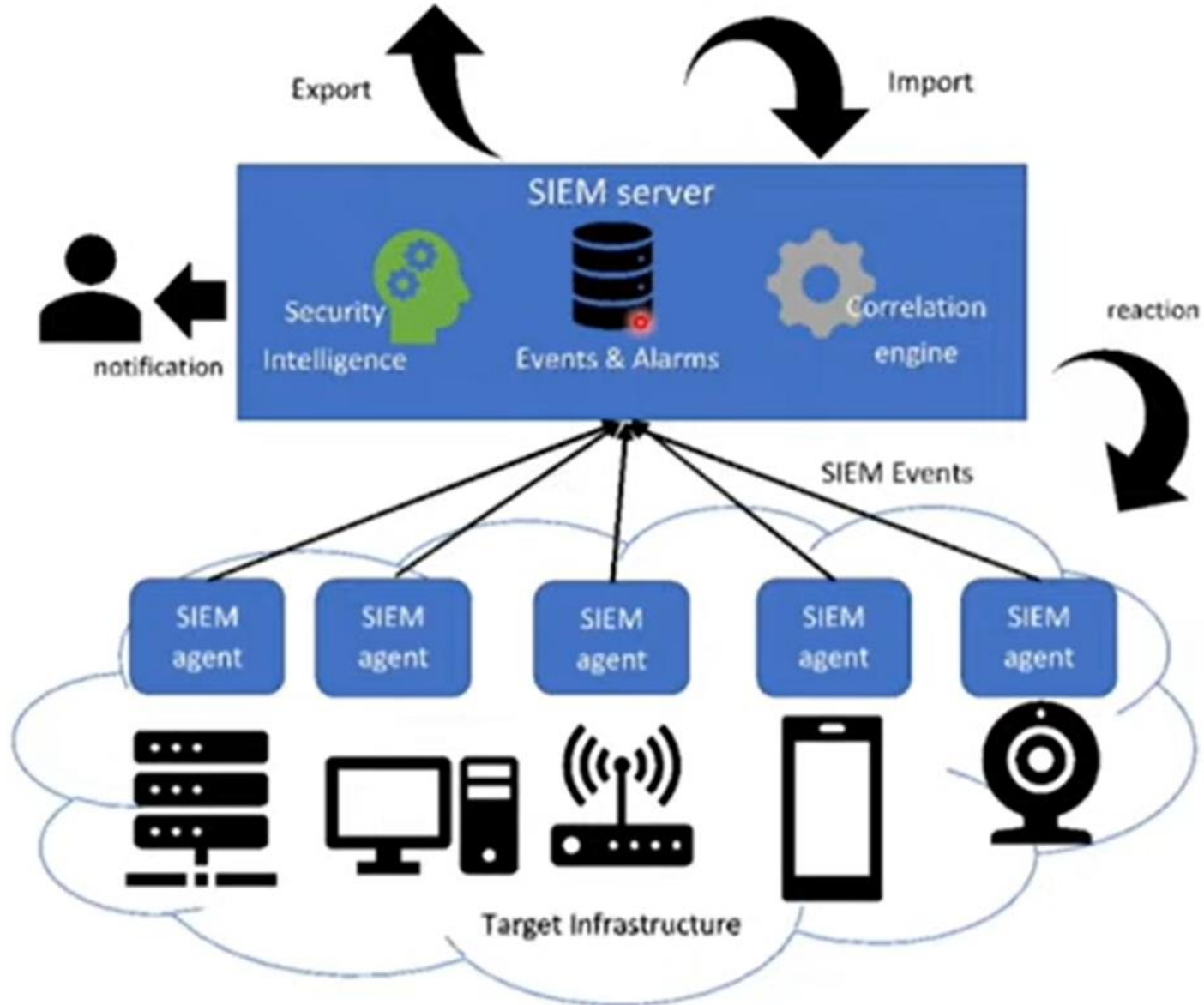


SIEM Solutions

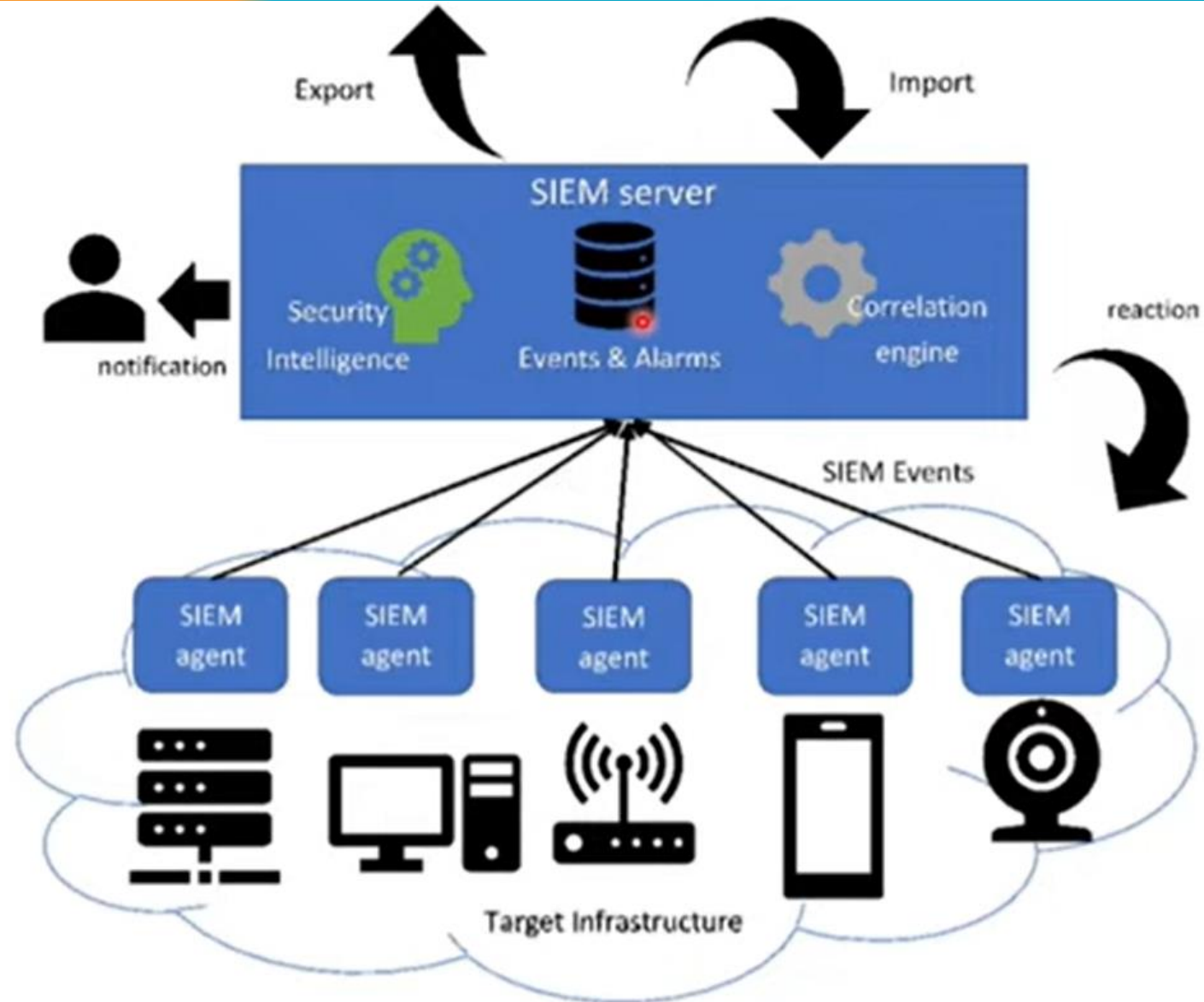
There's a variety of SIEM (Security Information and Event Management) solutions available in the market, including Splunk, Exabeam, LogRhythm, FortiSIEM, IBM QRadar, Secureworks, and even Elasticsearch with SIEM capabilities.

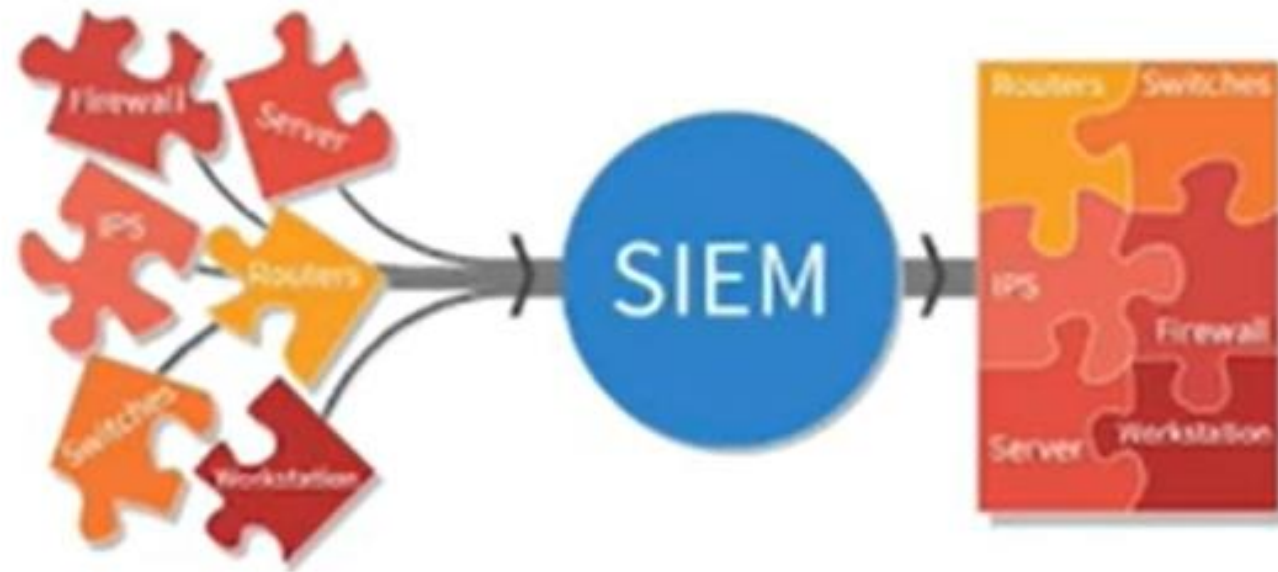


SIEM Solutions Deployment



SIEM Solutions Functional Components





Wrap Up



SIEM stands for Security Information and Event Management.

SIEM is a powerful cybersecurity tool that collects, manages, and analyzes log data.

It offers features like alerting, visualization, and long-term data retention.

SIEM aids in threat hunting and incident response.

SIEM systems can be deployed with or without agents.

Active monitoring and a dedicated security team are essential for maximizing SIEM effectiveness.



<https://t.me/learningnets>