SIEM

A cybersecurity tool

What is SIEM?
Security information and event management.
its a system that collects logfiles,security alerts and events in one place so security team can easily analyse the data.
It can also be said as a log management system specialized for security.

it collects all the information from other security systems like endpoint security, filewall, IDS email security etc.

offers powerful log search feature, the ability to trigger alerts using rules and reports that organizaiton can provide to auditors to demonstrate compliance with various regulation.

Later UEBA and SOAR was added to SIEM.

UEBA stands for User Entity behaviour analytics. It is an analytic slayer that tracks normal and abnormal behaviour for users and entities like database, servers and devices.
Mostly helps analytcis spot abnormal behaviours like logins from unusual locations or machine uploading large amount of information for the first time.

Basically, UEBA helps the analyst by highlighting the anomalous activity that they should look into.

SOAR stands for Security Orchestration Automation Response

SOAR automates what security analyst need to do to respond to security incidents.