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

One essential aspect of cybersecurity. It is a solution which collects log from various devices/services in a network and bring it to a central repository where analysis can be made. This enables real time threat detection, incident response and compliance monitoring.

**Components of SIEM:**

1. **Log collection** - Collects log from various components such as Databases, File Servers, Cloud environment.
2. **Parsing and Categorizing** – Once logs are collected from various components of the network, SIEM normalizes the data into structured format.

Parsing extracts useful data such as IP address, usernames etc.

Events are then categorized by type such as login attempts, authorization change etc. Which help in easy analysis.

1. **Correlation** – SIEM correlates different logs and events across multiple system to identify suspicious activities or patterns.
2. **Incident response and monitoring** – To detect threats early and minimize damage, SIEM solution monitors digital and on-premise system continuously. Analysis is displayed in a central dashboard and the SIEM solution will also send alerts to a centralized dashboard based on predefined rules.

**SOAR (Security, Orchestration, Automation, and Response)**

SOAR refers to security, orchestration, automation, and response, it is a security platform that integrated SIEM, Firewalls, and threat intelligence system to automate security operations and incident response features and simplify overall security operations.

**Components of SORE:**

1. **Security Orchestration** – It compiles various security solutions like SIEM, EDR and Threat intelligence feeds to present an end-to-end security solution
2. **Security Automation** – It automates repetitive task such as log correlation, threat investigation with the help of scripts, AI agents.

SOAR playbooks employ pre built response action to reduce or terminate threat with very little workload for SOC analyst.

1. **Security Response** – Automates blocking malicious IP, isolation of compromised devices on the network.

Reduces the effect of cyberattack by reducing the Mean Time to Detect (MTTD) and Mean Time to Response (MTTR).

**MTTR (Mean Time to Respond)**

Mean Time to Respond refers to the average time it takes for a team to begin responding to an incident after it has been detected. It is usually measured in minutes or hours, depending on the severity of the incidents and the responsiveness of the team.  
MTTR (Response) = Total Time to Respond to Incidents / Number of Incidents

**MTTD (Mean Time to Detect)**

It is the average time to detect a failure/issue after it has occurred. It reflects the efficiency of monitoring and alerting system in identifying the problem.

MTTD = Total Detection Time/ Number of Incidents

**Securonix**

Securonix is a top-tier, AI-first **security analytics platform** combining SIEM, SOAR, UEBA, and threat intelligence in a unified, cloud-native system. Its **Agentic AI**, **tiered data pipelines**, and strategic acquisitions place it at the forefront of efficient, intelligent, and affordable SecOps for enterprises and MSSPs worldwide.

**Torq**

Torq is a rapidly scaling, generative-AI-first security automation platform disrupting legacy SOAR with true hyperautomation. With industry-leading compliance, deep integrability, inventive AI agents like Socrates, and exceptional customer traction and growth—it's positioning itself as the backbone for modern autonomous SOCs.

**Radiant Security**

Radiant Security offers a next‑generation Adaptive AI SOC platform that automates triage, investigation, and response for every alert—from any tool or source—without manual intervention. With full AI transparency, one-click response workflows, unlimited log retention, and fixed pricing, Radiant elevates SOC efficiency while reducing both analyst burnout and costs.

**Hunters**

Hunters Security is a modern, AI-first SIEM solution tailored for lean teams craving powerful, automated security operations without the overhead of traditional SIEMs. Combining data lake flexibility, prebuilt detections, and expert services, it enables rapid threat detection, reduces alert fatigue, and offers enterprise-grade SOC capabilities at a predictable cost.

**Splunk SIEM**

**Introduction**

The video provides a beginner-friendly crash course on Splunk as a SIEM (Security Information and Event Management) solution. It teaches how to set up Splunk, ingest logs, use its search capabilities via SPL (Search Processing Language), and build visualizations and dashboards. The instructor also discusses how Splunk fits into the role of a SOC Analyst and how it helps monitor security events in real-time.

**Getting Started with Splunk**

The instructor begins by showing how to access the Splunk web interface, usually at http://localhost:8000. After logging in, the main area of work is the **Search & Reporting** app. This is where most queries and data exploration happen.

You are taught how to add data to Splunk by uploading a log file or monitoring a directory. Sample logs such as syslog files, Apache web logs, and internal log files are used for demonstrations. The instructor also mentions Splunk’s Universal Forwarder, which is a lightweight agent used in production environments to forward logs to Splunk.

**Basic Searching in Splunk**

The instructor explains the use of SPL, the Search Processing Language used by Splunk to query logs. A basic search looks like:

index=main sourcetype=syslog

This search filters logs based on the index and source type. Further filters can be added, for example:

host=webserver status=404

This retrieves logs where the host name contains “webserver” and the HTTP status code is 404.

**Working with SPL Commands**

Several SPL commands are demonstrated throughout the video.

1. **The stats command** is used for aggregation.

This gives the number of events grouped by each host.

1. **The timechart command** is used to build time-based line charts. For example:

| timechart span=1h count

This displays the number of events per hour.

1. **The eval command** is used to create new calculated fields. For example:

| eval risk=if(status>=500,"High","Low")

This adds a new field named “risk” based on the value of the status code.

1. **The rename command** helps rename fields:

| rename clientip AS source\_ip

1. **The dedup command** removes duplicate events:

| dedup session\_id

1. **The lookup command** is used to enrich logs with external data:

| lookup users’ user\_id OUTPUT full\_name role

This pulls full name and role from a lookup table for a given user ID.

1. **The convert command** can change the format of timestamps:

| convert ctime(\_time)

This makes Unix timestamps more human-readable.

1. **The where command** is used for post-processing filtering:

| where count > 100

This filter results to only include rows where the count is greater than 100.

**Field Extraction and Data Parsing**

The video briefly discusses how Splunk can extract fields automatically or using regular expressions. The instructor shows how to use the Field Extractor GUI to define patterns and extract custom fields.

Behind the scenes, files like props.conf and transforms.conf are responsible for data parsing and field extraction. These are more relevant in production or advanced setups using the Universal Forwarder or heavy forwarders.

**Creating Dashboards**

The instructor shows how to build dashboards using saved SPL queries. A new dashboard panel can be created using visual elements like pie charts, bar graphs, line charts, and tables.

An example panel might show the number of 404 errors over time, or the top source IPs accessing a server. Dashboards can include multiple panels for a real-time monitoring view.

**Installing Apps and Add-ons**

The video also covers how to enhance Splunk by installing apps and add-ons. One example shown is the "Splunk Security Essentials" app, which comes with prebuilt dashboards and sample searches for common security use cases.

These apps help beginners understand what real-world SOC monitoring looks like and how to replicate those capabilities

**Summary of Key Concepts**

By the end of the video, I learned how to ingest log data, perform basic and advanced searches, create calculated fields, enrich events with lookups, and build dashboards. The course emphasizes the importance of using Splunk in security operations and monitoring, making it suitable for beginners preparing for SOC roles or SIEM responsibilities.