## Enhances efficiency by automating systems / procedures

## Common Tools:

Logs - Record of system events.

Security Information & Event management (SIEM) Tools - An application that collects and analyzes data from logs to monitor critical activities.

### Splunk:

Data analysis platform, the enterprise version provides SIEM solutions used to return, analyze, & search log data.

### Google Chronical:

Cloud native SIEM tool that stores data for search & analysis. Being cloud native, it allows for fast delivery of new features.

### Other Security tools:

Playbooks - Manual that provides detail about any operational action

Network Protocol Analyzer - A packet sniffer designed to capture & analyze data traffic within a network.

### Programming:

Specific set of instructions for a computer to execute tasks.

### Linux:

An open source operating system, it is usually used with CLI but now it uses a GUI for ease of use. Think of how Linux Mint uses a GUI similar to windows.

### Structured Query Language (SQL):

A programming language used to create and interact with. Also is used to request information from a database.

### Python:

Used for performing tasks that are repetitive and time consuming, that require a high level of detail accuracy.

### Operating System:

An interface between the user and the computer.

### Web Vulnerability:

A flaw in a web application which a threat actor can use to their advantage. Look at OWASP to stay up to date with these flaws.

### Antivirus Software:

Program used to detect and destroy malware.

### Intrusion detection System:

An IDS monitors activity and alerts for possible intrusion. It scans packets that may include theft and unauthorized access.

### Encryption:

Uses Cryptogram Encoding converting plaintext to ciphertext.

### Penetration Testing:

Also known as Pen testing. It is a participation in a simulated cyber attack.