Python

Python is a powerful, beginner-friendly programming language widely used in cybersecurity for **automation**, **log parsing**, and **scripting**.

Why It's Useful:

- Automate repetitive tasks (e.g., scanning logs, sending alerts)
- Parse and analyze logs (e.g., JSON, CSV, syslog)
- Interact with APIs (e.g., threat intel platforms)
- Build detection scripts or small tools

Example Use Cases:

- Extract suspicious IPs from logs
- Automate VirusTotal lookups
- Write Sigma rule generators
- Create dashboards or reports

Libraries to Learn:

- pandas – for data analysis
- requests – for web/API calls
- re – for regex and pattern matching
- json – for parsing structured logs

Bash (Linux Shell Scripting)

Bash is a command-line language used in Linux environments to automate tasks and manage systems.

Why It's Useful:

- Navigate and manage Linux systems (common in SOCs and servers)
- Automate log collection and parsing
- Schedule tasks (e.g., cron jobs)
- Chain commands for quick analysis

Example Use Cases:

- Search logs with grep, awk, sed
- Monitor system activity (top, netstat, ps)
- Automate backups or script alerts
- Write scripts to clean up or extract data

How They Work Together:

You might use **Bash** to collect logs and **Python** to analyze them. For example:

- Bash script pulls logs from /var/log
- Python script parses those logs and flags anomalies