🔧 1. Servers & Operating Systems

Sources:

- Windows Event Logs
- Linux/Unix logs (/var/log, auditd, syslog)
- macOS system logs
- Mainframes (e.g., z/OS)

Splunk Mechanisms:

- **Universal Forwarder (UF)** – Installed on endpoints to collect logs
- **Heavy Forwarder (HF)** – For parsing at the edge
- **WMI Input** – For agentless Windows data collection
- **Modular Inputs / Custom Scripts** – For mainframe integration
- **Syslog to UF/HF** – For Unix systems using syslog

🌐 2. Network Devices

Sources:

- Firewalls (Palo Alto, Cisco ASA)
- Routers/Switches (Cisco, Juniper)
- Load Balancers (F5, Citrix NetScaler)
- Web Proxies (Blue Coat, Squid)

Splunk Mechanisms:

- **Syslog to UF/HF** – Devices send logs to a syslog server that's monitored by Splunk
- **HTTP Event Collector (HEC)** – For real-time data push
- **Splunk Connect for Syslog** – Modern scalable syslog framework
- **Cribl Stream** – For log parsing and routing from network sources

---

🖥️ 3. Security Tools

Sources:

- IDS/IPS (Snort, Suricata)
- EDR (CrowdStrike, SentinelOne)
- Antivirus (McAfee, Symantec, Windows Defender)
- Security Information Platforms

Splunk Mechanisms:

- **Syslog to UF/HF**
- **HEC** – Especially for CrowdStrike and SentinelOne
- **Modular Inputs** – Pull logs from vendor APIs (e.g., CrowdStrike API)
- **Splunkbase Apps/Add-ons** – For vendor-specific field extractions and dashboards
- **Cribl Stream** – Enrichment and filtering

☁️ **4. Cloud Platforms**

Sources:

- AWS (CloudTrail, CloudWatch, GuardDuty, S3)
- Azure (Monitor Logs, Activity Logs, Defender)
- Google Cloud Platform (GCP Audit Logs)

Splunk Mechanisms:

- **HTTP Event Collector (HEC)** – AWS Lambda, Azure Functions
- **Splunk Add-on for AWS / Azure / GCP** – Pulls logs via APIs
- **Cribl Stream/Cloud** – For S3 > Splunk pipeline
- **Terraform / Automation scripts** – For structured onboarding
- **Kinesis Firehose to HEC** – For streaming logs

📦 **5. Applications & Services**

Sources:

- Web Servers (Apache, NGINX, IIS)
- Databases (MySQL, PostgreSQL, SQL Server)
- Email Servers (Exchange, Postfix)
- Authentication Systems (Active Directory, LDAP)
- VPN logs

Splunk Mechanisms:

- **Universal Forwarder** – File monitoring
- **Splunk DB Connect** – JDBC-based access to databases
- **Modular Inputs / Scripts** – Pull logs from applications
- **Syslog** – Email/VPN server logs
- **HEC / Cribl** – API-based logs or file outputs

🔁 6. Log Aggregators & Message Queues

Sources:

- Syslog servers (rsyslog, syslog-ng)
- Kafka Streams
- Fluentd / Fluent Bit
- Logstash
- Cribl

Splunk Mechanisms:

- **Syslog to HF/UF**
- **Splunk Connect for Kafka**
- **HEC** – Fluentd, Fluent Bit, or Logstash can send to HEC
- **Cribl Stream** – Ideal for shaping/filtering before Splunk ingestion

---

📁 7. File-Based Sources

Sources:

- Log files (.log, .txt)
- CSV, JSON, XML
- Shared file systems

Splunk Mechanisms:

- **Universal Forwarder** – File monitoring via monitor stanza
- **Heavy Forwarder** – For parsing-heavy files
- **Modular Inputs** – Scripted parsing logic
- **Cribl Edge/Stream** – Pre-processing files before ingest
- **Batch Input** – For one-time ingests

🧰 8. Custom Scripts / APIs / SDKs

Sources:

- Python, PowerShell, Bash scripts
- REST API data
- SDK integrations (Java, Python, .NET)

Splunk Mechanisms:

- **Modular Inputs** – Custom scripts that run on a schedule
- **HTTP Event Collector (HEC)** – Scripts can POST directly to HEC
- **Splunk SDKs** – Used to build custom ingest pipelines
- **Cribl** – Can call APIs and reshape data before forwarding

---

📡 9. IoT & OT Devices

Sources:

- Sensors (via MQTT, OPC-UA)
- SCADA/ICS devices

- Building automation logs

Splunk Mechanisms:

- **HEC** – MQTT brokers can push data
- **Modular Inputs** – Polling device APIs
- **Syslog to UF/HF**
- **Cribl** – Great for edge processing in OT environments
- **Universal Forwarder** – Installed on a gateway/collector device

---

Let me know if you want this formatted into a table, spreadsheet, or slide deck for your team or