What types of data can be ingested into ELK?

🔷 **Types of Data ELK Can Ingest**

ELK is very flexible – it can handle **any kind of machine data**.

1. **Application Logs**
   - Errors, warnings, debug logs from apps (Java, Python, NodeJS, etc.).
   - Example: "500 Internal Server Error at /login."
2. **System Logs**
   - OS-level logs (Linux syslog, Windows Event Viewer).
   - Example: Failed SSH login attempts.
3. **Web/Server Logs**
   - Apache, Nginx, IIS access/error logs.
   - Example: "GET /index.html 200 OK."
4. **Database Logs**
   - MySQL, PostgreSQL, MongoDB slow query logs.
   - Example: Query taking >5 seconds.
5. **Network/Infrastructure Logs**
   - Firewall, load balancer, router logs.
   - Example: Dropped packets or unusual IP traffic.
6. **Cloud Service Logs** 🌩️
   - AWS CloudWatch, Azure Monitor, GCP logs.
   - Example: Lambda execution failures, S3 access logs.
7. **Metrics (numeric data)**
   - CPU, memory, disk usage, response times.
   - Example: CPU = 80%, Response latency = 300ms.
8. **Security & Audit Data** 🔒
   - Authentication attempts, policy violations.
   - Example: Multiple failed logins from same IP.
9. **Business/Event Data**
   - E-commerce orders, user clicks, IoT device data.
   - Example: "User added item X to cart at 10:15AM."

🔷 **Short Interview Answer**

ELK can ingest almost any machine data – application logs, system logs, web server logs, database logs, network/cloud logs, security events, even metrics and business events. This makes it powerful for troubleshooting, monitoring, and business analytics.

Which of the following is an example of *application logs* that can be ingested into ELK?
A) CPU usage = 75%
B) 500 Internal Server Error at /login
C) Dropped network packets
D) Failed SSH login attempt
✅ **Answer:** B) 500 Internal Server Error at /login

Which type of logs would capture "GET /index.html 200 OK" messages?
A) Database logs
B) Security logs
C) Web/Server logs (e.g., Apache, Nginx, IIS)
D) Business event logs
✅ **Answer:** C) Web/Server logs (e.g., Apache, Nginx, IIS)