Alert Priority Levels - SOC Notes

Alert Priority Levels - SOC Notes

Priority Definitions:
- Critical: Active ransomware, major data breach, or CVSS 9.0+ (e.g., Log4Shell CVE-2021-44228).
- High: Unauthorized admin access or lateral movement.
- Medium: Brute-force attempts or malware detected with no execution.
- Low: Recon activity like port scanning.

Assignment Criteria:
- Asset criticality (Production server > Test VM).
- Exploit likelihood (public exploit available).
- Business impact (financial loss, downtime).

Scoring Systems:
- CVSS: Use base, temporal, and environmental metrics.
- SOC Tools: Splunk Risk Scoring, Wazuh severity levels.

Example:
Log4Shell (CVE-2021-44228) -> CVSS 9.8 = Critical.