ALERT CLASSIFICATION TABLE

The following table is a **basic mock template** that demonstrates how alerts can be classified and organized in a SOC environment. It shows how different factors—such as alert type, priority, CVSS score, MITRE ATT&CK mapping, and contextual details (IP addresses, affected hosts, status, and notes)—are combined to provide a structured view of security events. This is **not real data** but a simulated example created for practice purposes, to illustrate how analysts would approach alert triage and documentation. While simplified, it reflects the kind of structured thinking required in real-world SOC workflows.

Alert ID	Type	Priority	CVSS Score	MITRE Tactic	Source IP	Target Host	Status	Notes / Actions
001	Phishing	High	8.2	T1566 (Phishing)	203.0.113.10	User-PC-1	Open	User reported suspicious link, email quarantined
002	Brute-force	Medium	6.5	T1110 (Credential Access)	192.168.1.100	WebSrv-2	Open	Multiple failed SSH attempts, account locked
003	Malware	Critical	9.8	T1059 (Execution)	192.168.1.50	Server-X	Open	crypto_locker.exe detected, host isolated
004	Port Scan	Low	4.0	T1046 (Discovery)	10.10.10.5	Firewall	Closed	Nmap scan detected, IP blocked by firewall
005	Data Exfil	High	8.5	T1041 (Exfiltration)	198.51.100.20	DB-Srv-1	Open	Large outbound traffic detected, investigation ongoing