Intrusion Detection System (IDS) Logs (Palo Alto Threat Prevention)

2024-02-20T14:32:10Z PAN-IDS Alert: Source=192.168.1.100 Destination=10.0.0.5 Severity=High Type=SQL Injection Attempt Rule=Blocked
2024-02-20T14:45:55Z PAN-IDS Alert: Source=203.0.113.45 Destination=192.168.1.200 Severity=Critical Type=RDP Brute Force Rule=Blocked
...
2024-02-20T16:10:30Z PAN-IDS Alert: Source=172.16.4.50 Destination=192.168.5.20 Severity=Medium Type=Suspicious Network Activity Rule=Allowed

Security Information and Event Management (SIEM) Logs (Splunk Enterprise Security)

2024-02-20T14:35:45Z Event ID=4625 Source=WindowsServer10 User=Admin FailureReason=Invalid Credentials Action=LoginFailed
2024-02-20T14:55:21Z Event ID=5140 Source=FileServer User=JohnDoe FileAccessed=/secure/data Action=Unauthorized Access Attempt
...
2024-02-20T16:02:12Z Event ID=1102 Source=SecurityLog User=Unknown Action=Log Cleared Criticality=High

Firewall Logs (Fortinet FortiGate)

2024-02-20T14:40:22Z FortiGate Alert: Source=172.16.0.1 Destination=8.8.8.8 Port=443 Protocol=HTTPS Action=Allowed SuspiciousTraffic=Yes
2024-02-20T15:15:12Z FortiGate Alert: Source=10.0.3.5 Destination=192.168.4.100 Port=445 Protocol=SMB Action=Blocked Reason=Unauthorized Access Attempt
...
2024-02-20T16:10:50Z FortiGate Alert: Source=192.168.2.200 Destination=External_IP Port=53 Protocol=DNS Action=Blocked Reason=Possible DNS Tunneling