

### EDR Alert Details (Scan)

---

Endpoint Detection Alert

Generated: 2026-02-11 03:16:05

Host: WS-17 (Plant Floor)

User: operator1

Severity: HIGH

Detection: Suspicious PowerShell

Command: powershell -enc <base64-redacted>

Parent process: explorer.exe

Network: outbound connection observed

Destination IP: 185.77.88.12

Port: 443

Bytes sent (approx): 24,810,112

Recommended action: isolate host, collect memory dump

Note: full telemetry export referenced as EDR\_Report\_INC-2026-0211.pdf