4. ALERT TRIAGE WITH THREAT INTELLIGENCE – FINAL SUBMISSION

Step 1 — Identify the Alert in Wazuh

Navigated to:
Wazuh Dashboard → Security Events → PowerShell Events

The alert details displayed:

- Command line execution via PowerShell
- Non-standard arguments
- Source IP communication associated with the event

Step 2 — Document the Alert

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	192.168.1.101	High	Open

Step 3 — Initial Triage Evaluation

- PowerShell activity is frequently used in attacks for payload execution.
- Priority is marked High due to suspicious behavior.
- The source IP 192.168.1.101 requires IOC validation.
- Next step is to verify whether the IP or related file hashes appear in threat intelligence feeds.

Summary (50 words)

The PowerShell execution alert was triaged as high priority, but IOC validation showed no malicious reputation for the associated IP 192.168.1.101 on OTX. No pulses or detections referenced the indicator. The activity appears contained and likely benign, though further monitoring of PowerShell usage is recommended to confirm legitimacy.