SIEM AI SECURITY REPORT

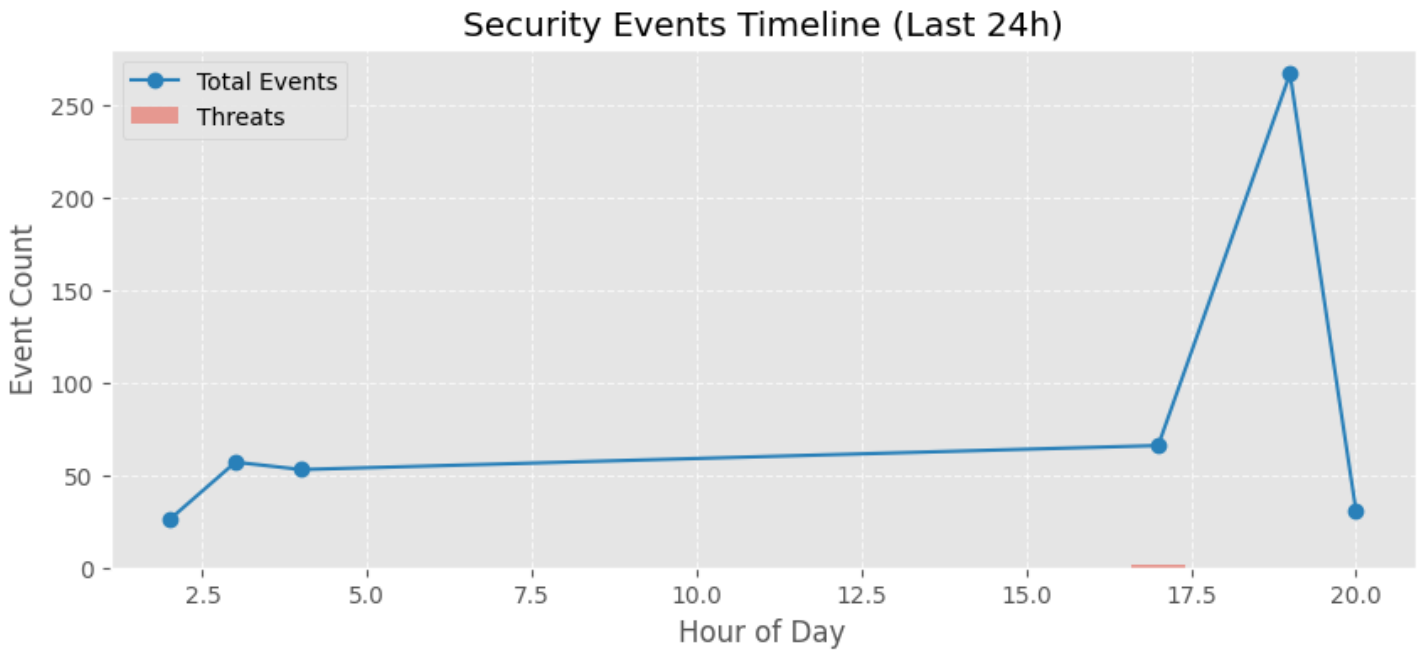
1. System Metadata

Report ID:	RPT-20251124-0649
Target Environment:	Wazuh Lab (Production)
Total Agents:	2 Active Agents
Log Volume:	500 events processed
Detection Engine:	AI Engine v3.0 (XGBoost + NLP)

2. Incident Narrative & Analysis

At 2025-11-23T17:42:15.844+0000, the agent 'win' generated a high-severity alert (Level 15). The system detected 'Executable file dropped in folder commonly used by malware'. Investigation reveals that process 'C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe' was involved. This usage of system administration tools is indicative of 'Living off the Land' (LotL) tactics. This is considered a CRITICAL incident requiring immediate containment.

3. Threat Timeline



4. Top Threat Processes

Process / Executable	Count	Avg Level	Severity

dows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe	1	15.0	CRITICAL
C:\\Windows\\system32\\cleanmgr.exe	**1**	**15.0**	CRITICAL

5. MITRE ATT&CK Matrix

Tactic	Technique ID	Description
Execution	T1059.001	PowerShell Usage
Persistence	T1078	Valid Accounts
Defense Evasion	T1027	Obfuscated Files

Appendix A: Raw Log Samples

```
[2025-11-23T17:42:15.844+0000] win | Lvl:15 | ...
```

```
[2025-11-23T17:29:31.674+0000] win | Lvl:15 | ...
```