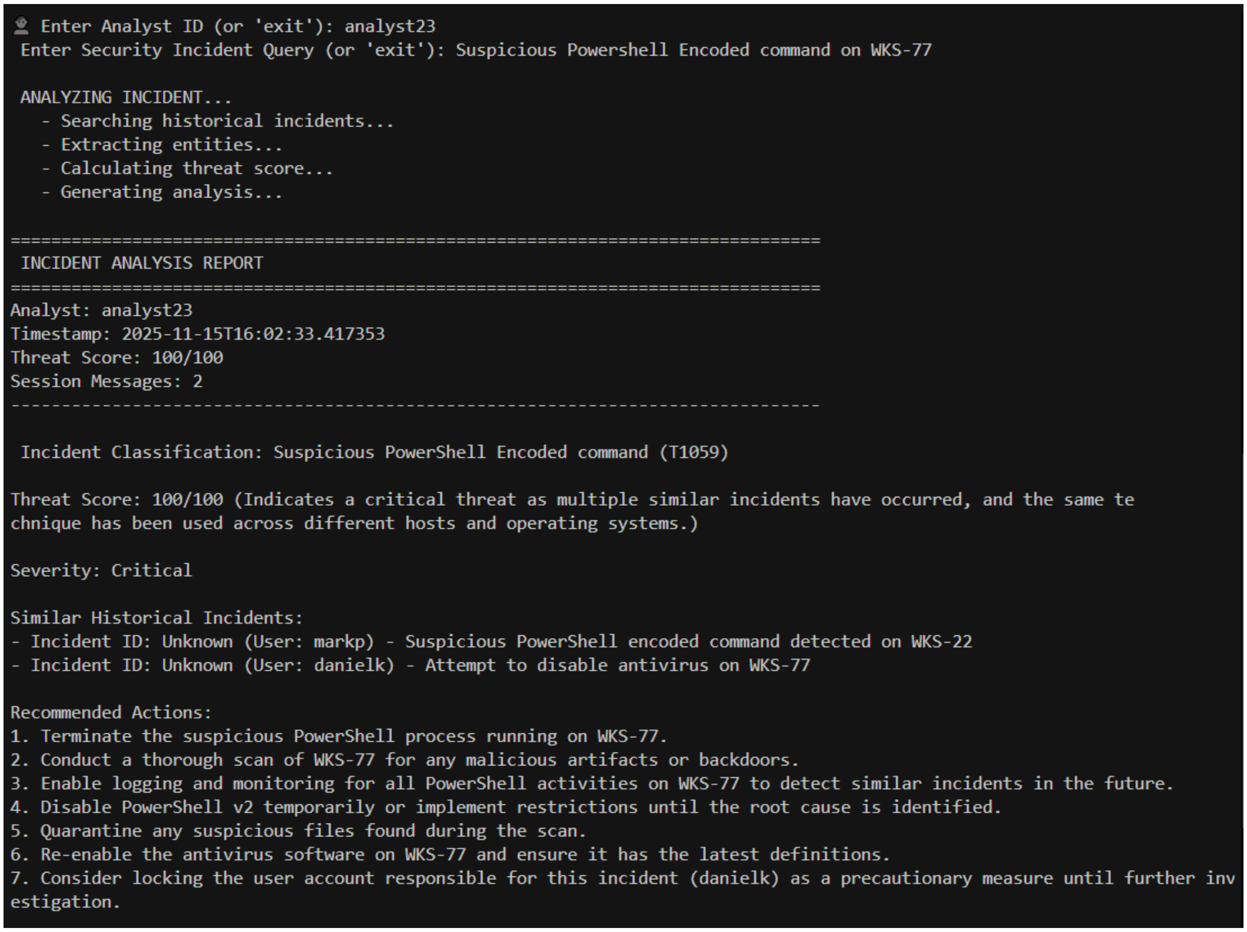
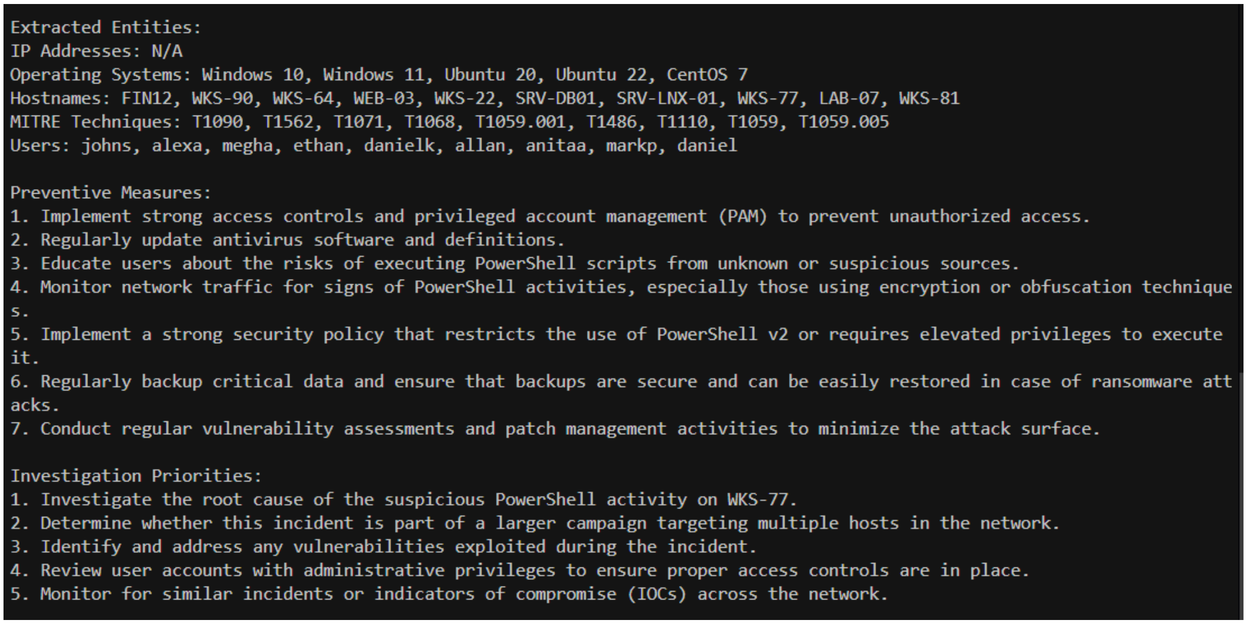


```
👤 Enter Analyst ID (or 'exit'): analyst23
 Enter Security Incident Query (or 'exit'): Suspicious Powershell Encoded command on WKS-77

 ANALYZING INCIDENT...
   - Searching historical incidents...
   - Extracting entities...
   - Calculating threat score...
   - Generating analysis...

================================================================================
 INCIDENT ANALYSIS REPORT
================================================================================
Analyst: analyst23
Timestamp: 2025-11-15T16:02:33.417353
Threat Score: 100/100
Session Messages: 2
--------------------------------------------------------------------------------

 Incident Classification: Suspicious PowerShell Encoded command (T1059)

Threat Score: 100/100 (Indicates a critical threat as multiple similar incidents have occurred, and the same te
chnique has been used across different hosts and operating systems.)

Severity: Critical

Similar Historical Incidents:
- Incident ID: Unknown (User: markp) - Suspicious PowerShell encoded command detected on WKS-22
- Incident ID: Unknown (User: danielk) - Attempt to disable antivirus on WKS-77

Recommended Actions:
1. Terminate the suspicious PowerShell process running on WKS-77.
2. Conduct a thorough scan of WKS-77 for any malicious artifacts or backdoors.
3. Enable logging and monitoring for all PowerShell activities on WKS-77 to detect similar incidents in the future.
4. Disable PowerShell v2 temporarily or implement restrictions until the root cause is identified.
5. Quarantine any suspicious files found during the scan.
6. Re-enable the antivirus software on WKS-77 and ensure it has the latest definitions.
7. Consider locking the user account responsible for this incident (danielk) as a precautionary measure until further inv
estigation.
```



```
Extracted Entities:
IP Addresses: N/A
Operating Systems: Windows 10, Windows 11, Ubuntu 20, Ubuntu 22, CentOS 7
Hostnames: FIN12, WKS-90, WKS-64, WEB-03, WKS-22, SRV-DB01, SRV-LNX-01, WKS-77, LAB-07, WKS-81
MITRE Techniques: T1090, T1562, T1071, T1068, T1059.001, T1486, T1110, T1059, T1059.005
Users: johns, alexa, megha, ethan, danielk, allan, anitaa, markp, daniel

Preventive Measures:
1. Implement strong access controls and privileged account management (PAM) to prevent unauthorized access.
2. Regularly update antivirus software and definitions.
3. Educate users about the risks of executing PowerShell scripts from unknown or suspicious sources.
4. Monitor network traffic for signs of PowerShell activities, especially those using encryption or obfuscation technique
s.
5. Implement a strong security policy that restricts the use of PowerShell v2 or requires elevated privileges to execute
it.
6. Regularly backup critical data and ensure that backups are secure and can be easily restored in case of ransomware att
acks.
7. Conduct regular vulnerability assessments and patch management activities to minimize the attack surface.

Investigation Priorities:
1. Investigate the root cause of the suspicious PowerShell activity on WKS-77.
2. Determine whether this incident is part of a larger campaign targeting multiple hosts in the network.
3. Identify and address any vulnerabilities exploited during the incident.
4. Review user accounts with administrative privileges to ensure proper access controls are in place.
5. Monitor for similar incidents or indicators of compromise (IOCs) across the network.
```