Log Sentinel Security Report
Host: MSI
Generated: 2026-05-13 11:48:46 UTC
Window: last 24h
Events analysed: 21
Findings: 15

Severity summary:
- Critical: 3
- High: 6
- Medium: 5
- Low: 1
- Info: 0

Plain-English next steps:
- Critical means stop and investigate now. Do not ignore it.
- High means fix soon. Check whether you recognize the activity.
- If unsure, disconnect from the internet and ask for help.

Findings:
1. [Critical] IOC match: mimikatz.exe (Credential dumper)
   Process 'mimikatz.exe' matched threat-intel database. Type: process Description: Credential dumper

2. [Critical] New service installed: 'WindowsUpdateHelper'
   Service 'WindowsUpdateHelper' installed from suspicious path: c:\users\public\svc.exe at 10:18:46.

3. [Critical] Security audit log cleared
   The audit log was cleared by 'hacker' at 2026-05-13 10:08:46. This is a strong indicator of an attacker covering tracks.

4. [High] Sensitive privileges granted to 'hacker'
   User 'hacker' was granted: SeDebugPrivilege, SeImpersonatePrivilege, SeTcbPrivilege at 10:43:46.

5. [High] Suspicious process: mimikatz
   Process 'c:\temp\mimikatz.exe' launched by 'hacker' with args: mimikatz.exe sekurlsa::logonpasswords

6. [High] Suspicious PowerShell script block detected
   PowerShell script contains: -enc. Snippet: powershell -enc sqbfafgaiaaoae4azqb3ac0atwbiagoaz
   qbjahqaiaboaguadaauafcazqbiaemababpaguabgb0acaalqbdag8abgbuaguaywb0afqaaqbtaguabwb1ahqaiaaxa
   daakqauagqabwb3ag4ababvageazabtahqacgbpag4azwaoaccaaab0ahqacaa=

7. [High] User added to privileged group 'Administrators'

’backdoor_user’ was added to group ’Administrators’ by ’hacker’.

8. [High] Brute-force login attempt on account ’Administrator’
   6 failed logins for ’Administrator’ within 5 minutes (first: 09:48:46).

9. [High] Brute-force from IP 185.220.101.45
   6 failed logins from 185.220.101.45 in 5 min.

10. [Medium] Account locked out: ’bob_smith’
    Account ’bob_smith’ was locked out (triggered from WORKSTATION-07). May indicate a brute-force attempt.

11. [Medium] Firewall rule added: ’Allow_Backdoor_4444’
    Firewall rule ’Allow_Backdoor_4444’ was added at 10:38:46. Unexpected changes may indicate an attacker disabling defenses.

12. [Medium] Scheduled task created: ’\Microsoft\Windows\SystemUpdateCheck’
    Task ’\Microsoft\Windows\SystemUpdateCheck’ was created by ’hacker’ at 10:33:46. Scheduled tasks are a common persistence technique.

13. [Medium] New local user account created: ’backdoor_user’
    Account ’backdoor_user’ was created by ’hacker’ at 2026-05-13 10:13:46.

14. [Medium] Unexpected system shutdown detected
    System experienced an unexpected shutdown at 2026-05-13 08:28:46. Could be hardware failure, crash, or forced power-off.

15. [Low] Off-hours logon: ’contractor_bob’
    User ’contractor_bob’ logged in at 03:15 UTC (outside 06:00?22:00 UTC).