Lateral movement in win logs

# Methods

## Experimental environment

Advanced Audit Policy was set to log both success and failure for every sub-category (auditpol /set /category:\* /success:enable /failure:enable); the resulting policy file is provided in the supplement.

[**Supplementary ZIP** Include auditpol\_backup.csv and audit\_enable.ps1.]

Sysmon Event ID 16 (configuration change) is forwarded to ELK and triggers a Grafana alert to ensure any tampering with the monitoring configuration is detected within one minute.