1. Настройка расширенной политики аудита Windows:

Локальная настройка политик аудита производится через оснастки:

- gpedit.msc,
- secpol.msc,

или с помощью утилиты

- auditpol.exe.

Настройка в домене производится через

- gpms.msc.

Рекомендации по настройке аудита приводятся для следующих сущностей:

- Контроллеры домена
- Серверы
- Рабочие станции

Используем Best Practise:

- Microsoft Audit Policy Recommendations;
- Malware Archaeology;
- CIS Microsoft Windows Server Benchmark;
- CIS Microsoft Windows Desktop Benchmark;
- blue-resources/Windows_MITRE_Data_Source_Mapping.xlsx

2. Настройка логирования командной строки.

Для настройки логирования командной строки включается следующий параметр: **Конфигурация компьютера** – **Административные шаблоны** – **Система** – **Аудит создания процессов** – **Включать командную строку в события создания процесса** – **Включено**.

При включении командной строки в события создания процесса, сведения командной строки для каждого процесса будут регистрироваться в виде обычного текста в событии 4688.

3. Настройка списков управления доступом к объектам SACL.

При включении подкатегорий аудита: Аудит файловой системы и Аудит реестра необходимо настроить SACL для критичных ветвей реестра и системных директорий.

Аудит лучше настраивать для всех пользователей (Everyone) и выбирать тип Успеха. Разрешения необходимо настроить в зависимости от сценариев мониторинга.

4. Настройка PowerShell

Для настройки аудита Powershell включаются следующие параметры:

- **Конфигурация компьютера** – **Административные шаблоны** – **Компоненты Windows** – **Windows PowerShell** – Включить ведение журнала модулей. Для **Имен модулей** необходимо указать ***.
- **Конфигурация компьютера** – **Административные шаблоны** – **Компоненты Windows** – **Windows PowerShell** – Включить регистрацию блоков сценариев PowerShell.

5. Настройка Sysmon

Скачайте Sysmon - https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon

Создайте/скачайте/адаптируйте конфигурационный файл Sysmon:

- https://github.com/ion-storm/sysmon-config
- https://github.com/olafhartong/sysmon-modular
- https://github.com/MHaggis/sysmon-dfir

Установить Sysmon: sysmon -accepteula -i config.xml

Обновить Sysmon с новым конфигом: sysmon -c config.xml