Информзащита
IZ:SOC

Секреты Active Directory
Разведка глазами SOC

Артём Цалпанов

Сунь-дзы. Искусство разведки

Неотъемлемая часть атак
на организации с доменной
инфраструктурой Windows

Большой объём информации
о действующих объектах
и ролях в домене

Широкие возможности
сокрытия своего присутствия
в локальной сети

Низкий порог вхождения
в реализацию атаки

Как следствие – сложность
в обнаружении вредоносной
активности средствами SOC

Определяет возможности
злоумышленника для дальнейшего
захвата контроля
над инфраструктурой предприятия

Вижу цель - не вижу препятствий

Требования

Учётные данные любого доменного пользователя

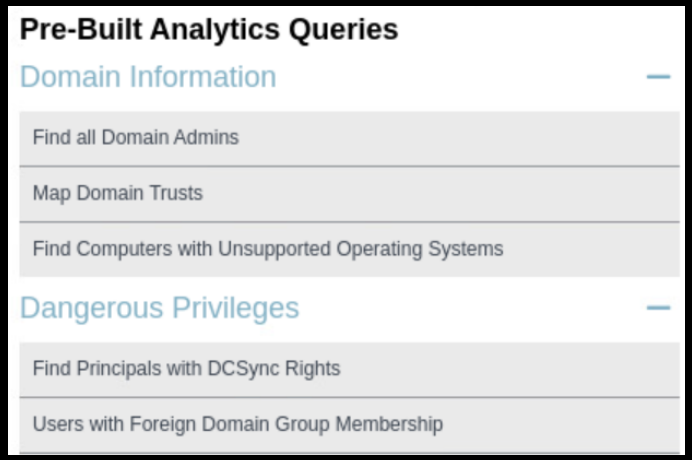
Результат

- Членство пользователей в привилегированных группах
- Векторы для дальнейшего продвижения в доменной сети
- Схема доменной сети
- Обнаружение уязвимых конфигураций объектов
- Доменные роли конечных узлов в локальной сети

Классика бессмертна

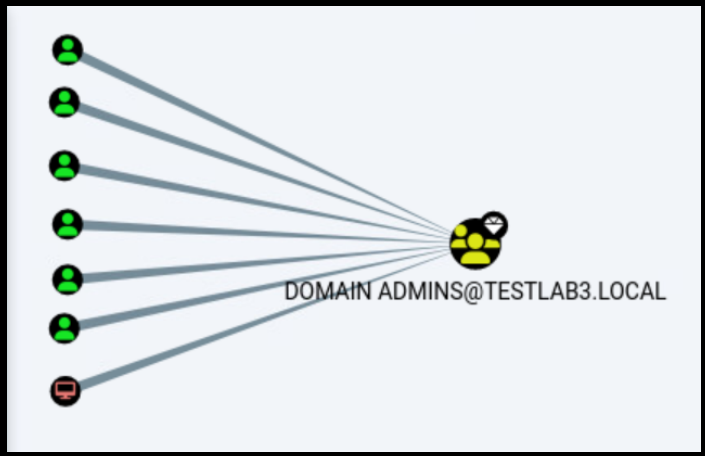
Ручное исследование объектов

- Модули ВПО
- Wmic.exe
- Powershell.exe
- Net.exe



Автоматизированные инструменты

- Bloodhound / Sharphound
- PingCastle
- AD Explorer
- LDAPDomainDump



Выбор есть всегда

SIEM

- Гибкая детектирующая логика
- Большой объём полезной информации по объектам AD
- Потенциально низкая чувствительность правил корреляции
- Сложность создания основы детектирующей логики на базе «шумных» событий аудита

Network Analyzer

- Сложность отладки конкретных сигнатур в сетевом трафике
- Потенциально высокая чувствительность правил корреляции
- Сложность атрибуции активности к паттернам разведки AD
- Большое покрытие сети детектирующей логикой

Редкий зверь «4662»

Событие аудита безопасности ОС Windows EventID **4662** (DS Access) – **An operation was performed on an object**

Необходимые для отслеживания доступы к объектам AD – **Read Property, READ_CONTROL**

Необходимые для отслеживания объекты AD – **User, Computer, Group, OU**

Для включения аудита необходимо также настроить **SACL**

DeviceCustomString1	Read Property
DeviceCustomString1Label	Access List
DeviceCustomString2	bf967a86-0de6-11d0-a285-00aa003049e2
DeviceCustomString2Label	Object Type
DeviceCustomString3	833a18d7-f214-40f6-b284-26455041b5bb
DeviceCustomString3Label	Object Name
DeviceCustomString4	0x83961bac
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Object Access
DeviceCustomString5Label	Operation Type
DeviceCustomString6	{bf967a86-0de6-11d0-a285-00aa003049e2} {e48d0154-bcf8-11d1-8702-00c04fb96050} {bf9679e5-0de6-11d0-a285-00aa003049e2} {bf96793f-0de6-11d0-a285-00aa003049e2} {bf9679e4-0de6-11d0-a285-00aa003049e2} {bf9679e7-0de6-11d0-a285-00aa003049e2} {771727b1-31b8-4cdf-ae62-4fe39fadf89e} {bf96798f-0de6-11d0-a285-00aa003049e2} {888eedd6-ce04-df40-b462-b8a50e41ba38} {4c164200-20c0-11d0-a768-00aa006e0529} {bf967a68-0de6-11d0-a285-00aa003049e2} {59ba2f42-79a2-11d0-9020-00c04fc2d3cf} {bf967a00-0de6-11d0-a285-00aa003049e2} {bf9679e8-0de6-11d0-a285-00aa003049e2} {3e0abfd0-126a-11d0-a060-00aa006c33ed} {6e7b626c-64f2-11d0-afd2-00c04fd930c9} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {bc0ac240-79a9-11d0-9020-00c04fc2d4cf} {bf9679c0-0de6-11d0-a285-00aa003049e2}
DeviceCustomString6Label	Properties

Баланс – эталон гармонии. Пользователь

Объект: **User**

Часто запрашиваемые атрибуты в рамках разведки AD:

- **UserAccountControl**
- **User-Account-Restrictions**
- **General-Information**
- **SAM-Account-Type**
- **Public-Information**
- **Default property set**

DeviceCustomString1	Read Property
DeviceCustomString1Label	Access List
DeviceCustomString2	bf967aba-0de6-11d0-a285-00aa003049e2
DeviceCustomString2Label	Object Type
DeviceCustomString3	6df44d51-c501-4639-9803-8528decc2a41
DeviceCustomString3Label	Object Name
DeviceCustomString4	0x8376b7c2
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Object Access
DeviceCustomString5Label	Operation Type
DeviceCustomString6	{bf967aba-0de6-11d0-a285-00aa003049e2} {e48d0154-bcf8-11d1-8702-00c04fb96050} {bf9679e5-0de6-11d0-a285-00aa003049e2} {bf96793f-0de6-11d0-a285-00aa003049e2} {bf9679e4-0de6-11d0-a285-00aa003049e2} {bf9679e7-0de6-11d0-a285-00aa003049e2} {771727b1-31b8-4cdf-ae62-4fe39fadf89e} {bf96798f-0de6-11d0-a285-00aa003049e2} {888eedd6-ce04-df40-b462-b8a50e41ba38} {4c164200-20c0-11d0-a768-00aa006e0529} {bf967a68-0de6-11d0-a285-00aa003049e2} {59ba2f42-79a2-11d0-9020-00c04fc2d3cf} {bf967a00-0de6-11d0-a285-00aa003049e2} {bf9679e8-0de6-11d0-a285-00aa003049e2} {3e0abfd0-126a-11d0-a060-00aa006c33ed} {6e7b626c-64f2-11d0-afd2-00c04fd930c9} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {bc0ac240-79a9-11d0-9020-00c04fc2d4cf} {bf9679c0-0de6-11d0-a285-00aa003049e2}
DeviceCustomString6Label	Properties

Баланс – эталон гармонии. Пользователь

UserAccountControl	and	User-Account-Restrictions
General-Information	and	SAM-Account-Type
	and	
Public-Information	or	Default property set

Баланс – эталон гармонии. Группа

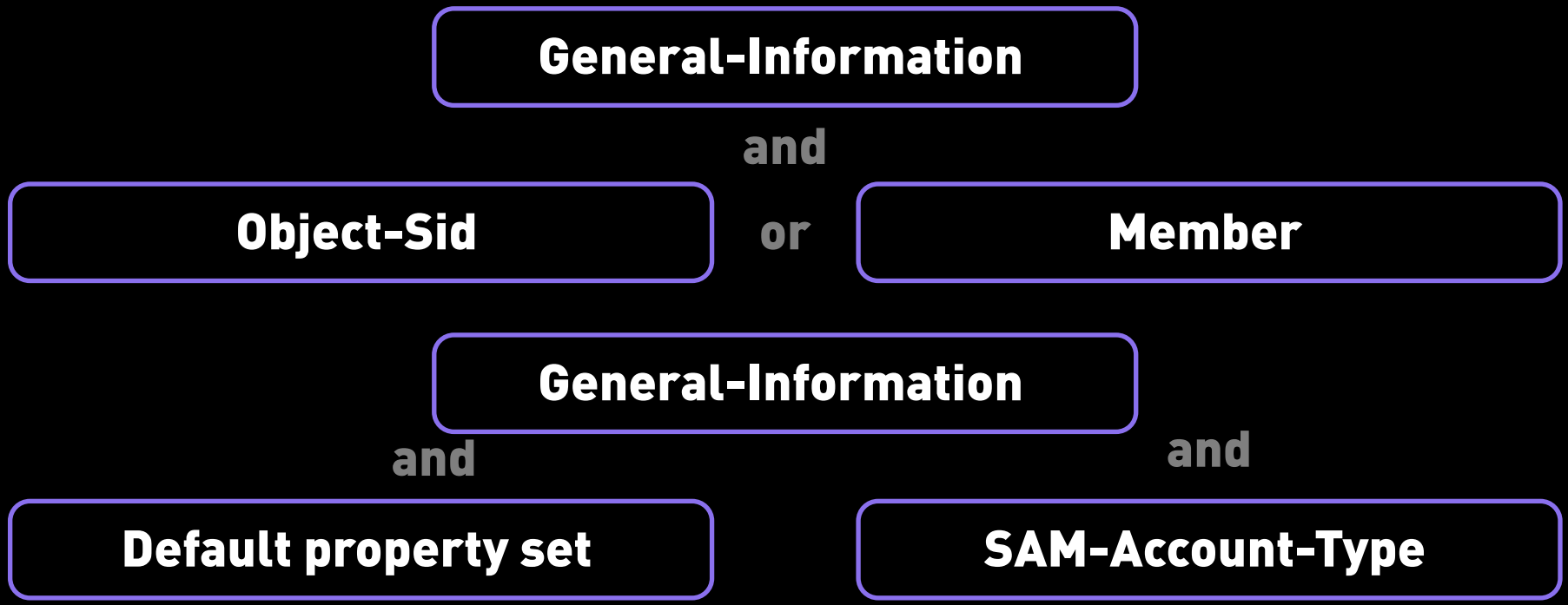
Объект: **Group**

Часто запрашиваемые атрибуты в рамках разведки AD:

- **General-Information**
- **Object-Sid**
- **Member**
- **SAM-Account-Type**
- **Default property set**

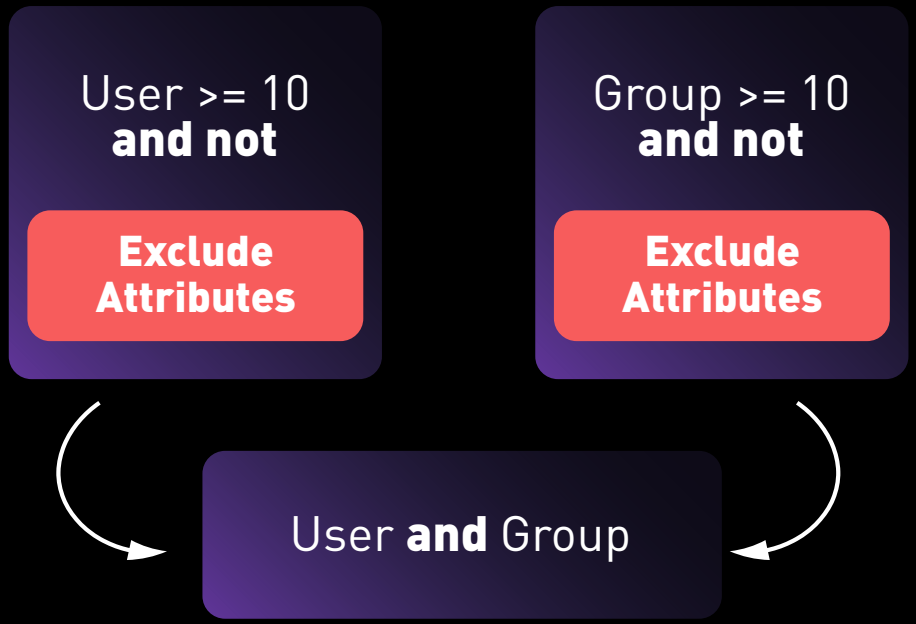
DeviceCustomString1	Read Property
DeviceCustomString1Label	Access List
DeviceCustomString2	bf967a9c-0de6-11d0-a285-00aa003049e2
DeviceCustomString2Label	Object Type
DeviceCustomString3	6a8192d4-3a58-4e62-b117-5d2620d15460
DeviceCustomString3Label	Object Name
DeviceCustomString4	0x83961bac
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Object Access
DeviceCustomString5Label	Operation Type
DeviceCustomString6	{bf967a9c-0de6-11d0-a285-00aa003049e2} {e48d0154-bcf8-11d1-8702-00c04fb96050} {bf9679e5-0de6-11d0-a285-00aa003049e2} {bf96793f-0de6-11d0-a285-00aa003049e2} {bf9679e4-0de6-11d0-a285-00aa003049e2} {bf9679e7-0de6-11d0-a285-00aa003049e2} {771727b1-31b8-4cdf-ae62-4fe39fadf89e} {bf96798f-0de6-11d0-a285-00aa003049e2} {888eedd6-ce04-df40-b462-b8a50e41ba38} {4c164200-20c0-11d0-a768-00aa006e0529} {bf967a68-0de6-11d0-a285-00aa003049e2} {59ba2f42-79a2-11d0-9020-00c04fc2d3cf} {bf967a00-0de6-11d0-a285-00aa003049e2} {bf9679e8-0de6-11d0-a285-00aa003049e2} {3e0abfd0-126a-11d0-a060-00aa006c33ed} {6e7b626c-64f2-11d0-afd2-00c04fd930c9} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {bc0ac240-79a9-11d0-9020-00c04fc2d4cf} {bf9679c0-0de6-11d0-a285-00aa003049e2}
DeviceCustomString6Label	Properties

Баланс – эталон гармонии. Группа



«Комбинаторика – моя стихия»

- Повышение точности срабатывания правила
- Адаптация логики под действия злоумышленника
- Улучшение качества анализа активности сотрудниками SOC
- Исключение заведомо ложных паттернов легитимных LDAP-запросов
- Увеличение покрытия мониторингом правила корреляции



Я есть LDAP

LogSource: **DC**

▼

EventID: **4624**

▼

Logon Type: **3**

▼

AuthPackage: **Kerberos OR NTLM**

▼

SourceAddress: **not 127.0.0.1**

DeviceCustomNumber1	3
DeviceCustomNumber1Label	Logon Type
DeviceCustomString1	0x0
DeviceCustomString1Label	Process ID
DeviceCustomString2	Kerberos
DeviceCustomString2Label	Authentication Package Name
DeviceCustomString3	0x0
DeviceCustomString3Label	Source Logon ID
DeviceCustomString4	0x8376b7c2
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Yes
DeviceCustomString5Label	Elevated Token
DeviceCustomString6	Kerberos
DeviceCustomString6Label	Logon Process Name

Всё ещё достоин

SharpHound.exe -c Group -d testlab3.local

DeviceCustomString1	Read Property
DeviceCustomString1Label	Access List
DeviceCustomString2	bf967aba-0de6-11d0-a285-00aa003049e2
DeviceCustomString2Label	Object Type
DeviceCustomString3	49c42d40-29af-49eb-bd34-cebc14b69fea
DeviceCustomString3Label	Object Name
DeviceCustomString4	0x83961bac
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Object Access
DeviceCustomString5Label	Operation Type
DeviceCustomString6	{bf967aba-0de6-11d0-a285-00aa003049e2} {e48d0154-bcf8-11d1-8702-00c04fb96050} {bf9679e5-0de6-11d0-a285-00aa003049e2} {bf96793f-0de6-11d0-a285-00aa003049e2} {bf9679e4-0de6-11d0-a285-00aa003049e2} {bf9679e7-0de6-11d0-a285-00aa003049e2} {771727b1-31b8-4cdf-ae62-4fe39fadf89e} {bf96798f-0de6-11d0-a285-00aa003049e2} {888eedd6-ce04-df40-b462-b8a50e41ba38} {4c164200-20c0-11d0-a768-00aa006e0529} {bf967a68-0de6-11d0-a285-00aa003049e2} {59ba2f42-79a2-11d0-9020-00c04fc2d3cf} {bf967a00-0de6-11d0-a285-00aa003049e2} {bf9679e8-0de6-11d0-a285-00aa003049e2} {3e0abfd0-126a-11d0-a060-00aa006c33ed} {6e7b626c-64f2-11d0-afd2-00c04fd930c9} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {bc0ac240-79a9-11d0-9020-00c04fc2d4cf} {bf9679c0-0de6-11d0-a285-00aa003049e2}
DeviceCustomString6Label	Properties

DeviceCustomString1	Read Property
DeviceCustomString1Label	Access List
DeviceCustomString2	bf967a9c-0de6-11d0-a285-00aa003049e2
DeviceCustomString2Label	Object Type
DeviceCustomString3	6a8192d4-3a58-4e62-b117-5d2620d15460
DeviceCustomString3Label	Object Name
DeviceCustomString4	0x83961bac
DeviceCustomString4Label	Destination Logon ID
DeviceCustomString5	Object Access
DeviceCustomString5Label	Operation Type
DeviceCustomString6	{bf967a9c-0de6-11d0-a285-00aa003049e2} {e48d0154-bcf8-11d1-8702-00c04fb96050} {bf9679e5-0de6-11d0-a285-00aa003049e2} {bf96793f-0de6-11d0-a285-00aa003049e2} {bf9679e4-0de6-11d0-a285-00aa003049e2} {bf9679e7-0de6-11d0-a285-00aa003049e2} {771727b1-31b8-4cdf-ae62-4fe39fadf89e} {bf96798f-0de6-11d0-a285-00aa003049e2} {888eedd6-ce04-df40-b462-b8a50e41ba38} {4c164200-20c0-11d0-a768-00aa006e0529} {bf967a68-0de6-11d0-a285-00aa003049e2} {59ba2f42-79a2-11d0-9020-00c04fc2d3cf} {bf967a00-0de6-11d0-a285-00aa003049e2} {bf9679e8-0de6-11d0-a285-00aa003049e2} {3e0abfd0-126a-11d0-a060-00aa006c33ed} {6e7b626c-64f2-11d0-afd2-00c04fd930c9} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {72e39547-7b18-11d1-adef-00c04fd8d5cd} {bc0ac240-79a9-11d0-9020-00c04fc2d4cf} {bf9679c0-0de6-11d0-a285-00aa003049e2}
DeviceCustomString6Label	Properties

Информзащита
IZ:SOC

Информационная безопасность

24x7x365

Центр противодействия кибератакам IZ:SOC

+7 495 980 23 45

izsoc@infosec.ru

www.izsoc.ru

Системный интегратор

+7 495 980 23 45

market@infosec.ru

www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Пресс-служба

pr@infosec.ru

Сервисный центр

+7 495 981 92 22

support@itsoc.ru

www.itsoc.ru