ИНФЕРИТ ИТМЕН

МСВСфера

Linux vs Windows

в чем отличие сбора данных: пошаговый алгоритм

Василий Гурьев

Директор продукта «Инферит ИТМен»

Дмитрий Баранов

Директор продукта «ОС МСВСфера»

itman.ru

Приятный бонус для всех,
кто дослушает до конца

МСВСфера

Василий Гурьев

- Более 20 лет в ИТ
- 12 лет в разработке инфраструктурного ПО

Дмитрий Баранов

- Более 25 лет в ИТ
- 15 лет в сфере продаж инфраструктурного ПО

Объекты сбора данных

что собираем

Сетевые Устройства

Подключенное оборудование и конфигурация

Программы

Пользователи

Linux

Windows

Устройства

Места хранения

Linux

- Файлы,
  файловая система
- Ядро
- База
  пакетного менеджера

Windows

- Файлы,
  файловая система
- Реестр
- WMI
- Ядро

Устройства

- Прошивка

Внешние источники данных

Linux

- FreeIPA, Samba
- KVM
- VMware

Windows

- Active Directory
- Hyper-V
- VMware

Способы сбора данных

Linux

- Shell

Windows

- PowerShell
- WMI
- Реестр

Устройства

- IPMI
- SNMP

Устройства

Оборудование

Поиск и опрос сетевого интерфейса

- **Поиск устройств**
  Ping
  ARP сканирование
  Журналы DHCP
  Анализ FDB-таблиц коммутаторов
- **Проверка портов**
  80 - HTTP
  22 - SSH
  161 - SNMP

Конфигурация

Запросы к SNMP|IPMI

- **MiB**
  "Description": ["1.3.6.1.2.1.1.1.0"],
  "Name": ["iso.3.6.1.2.1.1.5.0"],
  "SerialNumber": ["1.3.6.1.4.1.14988.1.1.7.3.0"],
  "PrinterState": ["1.3.6.1.2.1.2.2.1.6.5"]
- **IPMI**

Linux

Оборудование/конфигурация

Запросы к ядру

- Команды (например)
  lsusb,
  lspci,
  lscpu,
  lshw
- dmidecode

Программы

Запросы к пакетному менеджеру

- Команды (например)
  dnf list installed
- flatpak list
  snap list

Пользователи/группы

Содержимое файлов

- Пользователи
  /etc/passwd
- Группы
  /etc/group

Windows

Оборудование/конфигурация

Запросы к ядру и ОС:

- Команды (например)
  Get-PnpDevice
  Get-WmiObject
  Get-CimInstance

Программы

Запросы к WMI

- Команды (например)
  Get-ComputerInfo
  Get-InstalledApps
  Microsoft.Win32.RegistryKey

Пользователи/группы

Запрос в реестре:

- Пользователи
  Get-ItemProperty
  -Path 'registry::HKEY_USERS

2 проблемы инвентаризации

Сбор данных

Очистка и обогащение данных

Нет полной картины данных

Думаем,
что понадобиться

До проекта

Базовые данные
об оборудовании и ПО

- **Процессор**
- **Базовая информация о устройстве**
- **Программное обеспечение**
- **Пользователи**
- **Операционная система**

Что действительно нужно –
безлимитный объем данных

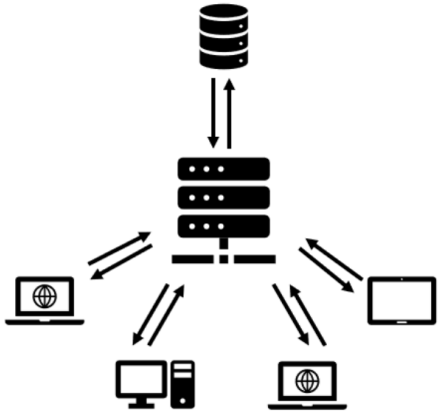
В процессе проекта

Детальные параметры
вплоть до версии самой защищенной ОС Astra

- **Процессор и его составляющие**
  (имя, марка, модель, потоки, семейство и т. д.).
- **Тип устройства и его расположение**
- **Цифровые сертификаты**
- **ПО и файлы**
  (изготовитель, наименование, версия, путь установки, файл или пакет, бесплатное или платное, категория и т.д.).
- **Операционная система**
  (имя, дата установки, серийный номер).

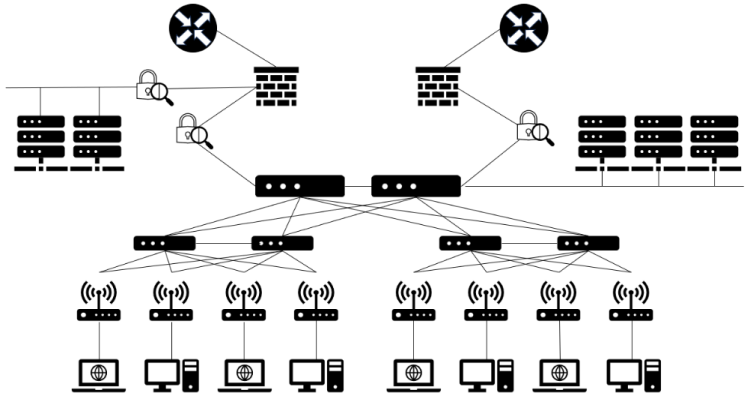
Прежние подходы к сбору данных не соответствуют актуальным требованиям ИБ

До проекта



Клиент-серверная

После всех запретов



Хабовая

Проблема чистоты инвентарных данных

До обработки

20 000

дублей

3 атрибута

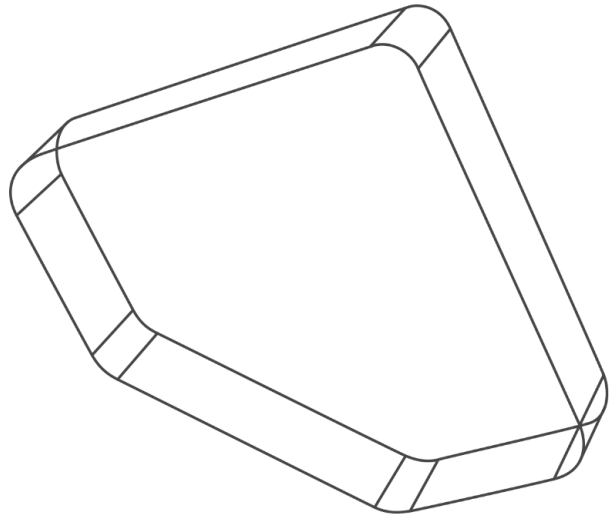
После

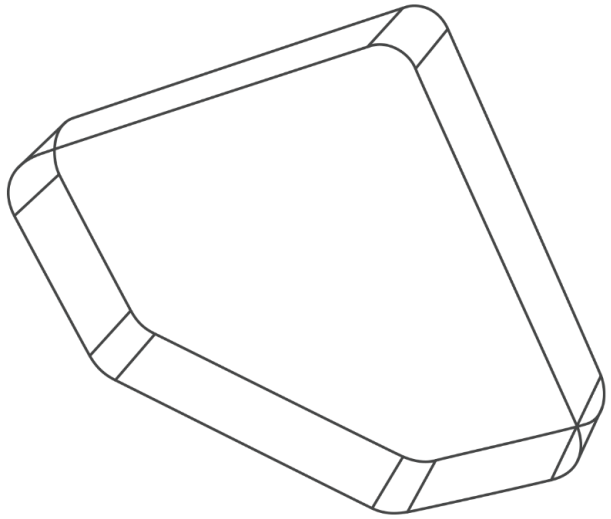
5 000

номенклатурных единиц

Дополнительные классы, категории и типы

Практика





Будем рады обратной связи

Оцените наш вебинар