А вы знаете, что именно защищаете?

Опыт инвентаризации ИТ активов со стороны ИБ

Старостин Георгий

Директор по ИБ АО «СОГАЗ»

Кто живет в корпоративной сети?

согаз

А вы готовы ответить на вопросы по своей инфраструктуре?

Точное количество хостов и устройств в сети?

Какие пользователи (включая локальных) имеют доступ к системе?

Не поставил ли вчера администратор неразрешенное ПО на сервер?

Все ли параметры системы соответствуют политикам ИБ?

Какое реальное покрытие серверов средствами ИБ?

Какие и сколько из средств ИБ на конечных хостах штатно функционируют?

согаз

Различие ИТ и ИБ инвентаризации конечных устроств

Вопрос	ИТ	ИБ
Количество свободных ресурсов	✓	✗
Количество устройств	✓	+
Типы устройств	✓	✓
Соответствие настроек хостов требованиям ИБ	✗	✓
Соответствие настроек хостов требованиям ИТ	✓	+
Список пользователей на конкретном сервере	✗	✓
Точный список всего установленного ПО и версий	✗	✓
Список ключевого установленного ПО	✓	✓
Информация об открытых портах	✗	✓
Быстрая группировка устройств по произвольным параметрам	+	✓
Степень покрытия средствами ИБ	✗	✓

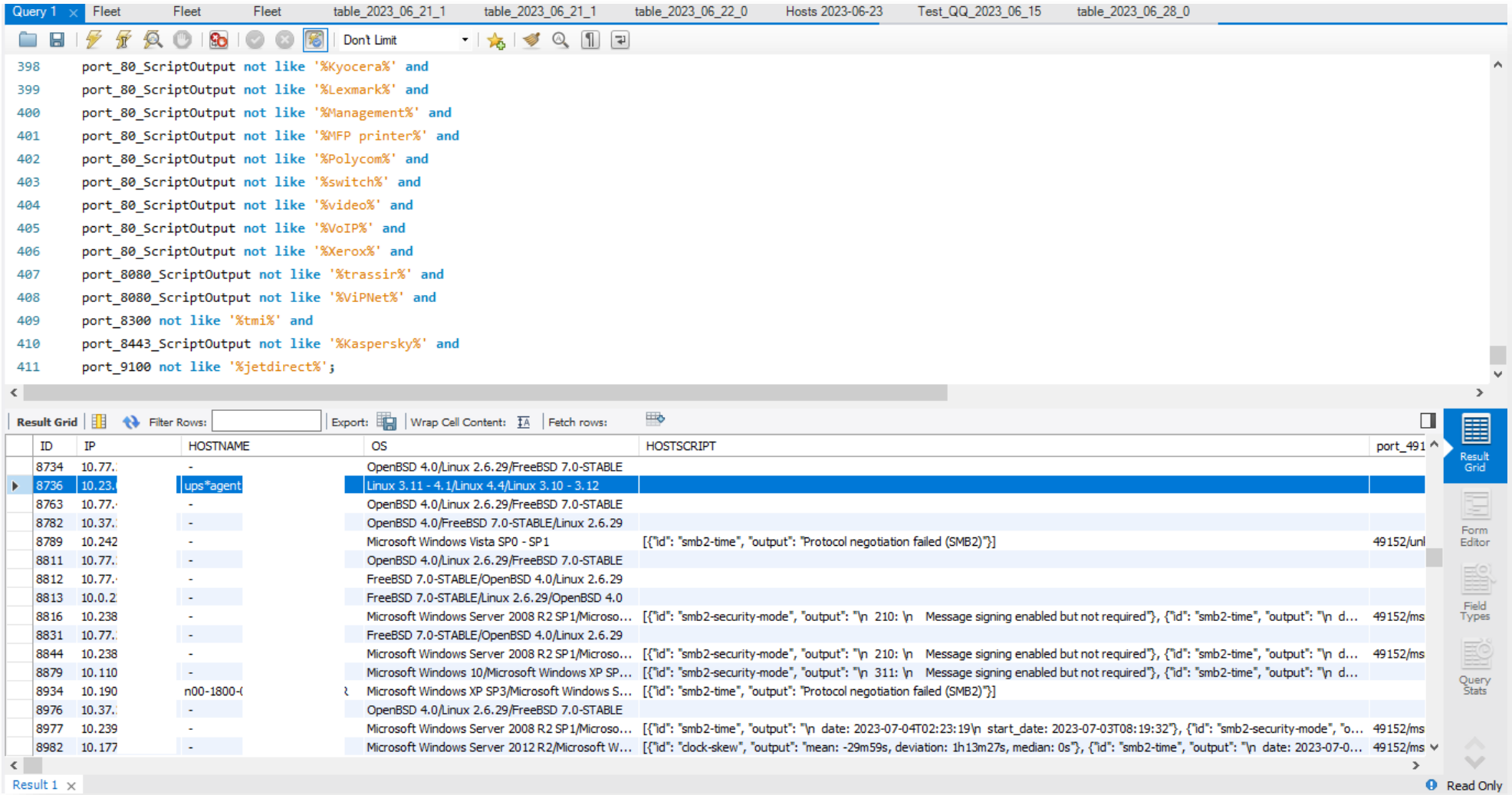
согаз

Описание компонентов

Компонент	Назначение
Nmap + Masscan	Сканирование активных хостов и портов, первичный фингерпринтинг ОС и сервисов на открытых портах
EyeWitness	Снятие скриншотов с Web сервисов
Fleet + Osquery	Мониторинг политик ИБ, мониторинг установленного ПО. Использование в качестве метки учета в ИБ инвентаризации
Парсер DNS записей	Сбор внешних DNS записей с DNS серверов компании
Парсер NetFlow	Выявление в сетевом трафике IP адресов, не найденных сетевым сканированием
Движок корреляции (самописный, Python)	Сопоставление данных из сканеров и баз знаний

Подход к инвентаризации сети

Результаты сканирования и корреляции



Примеры оповещений

Если найден новый хост без агента osquery и его нет в исключениях

По хосту нет (или недостаточно) данных в CMDB

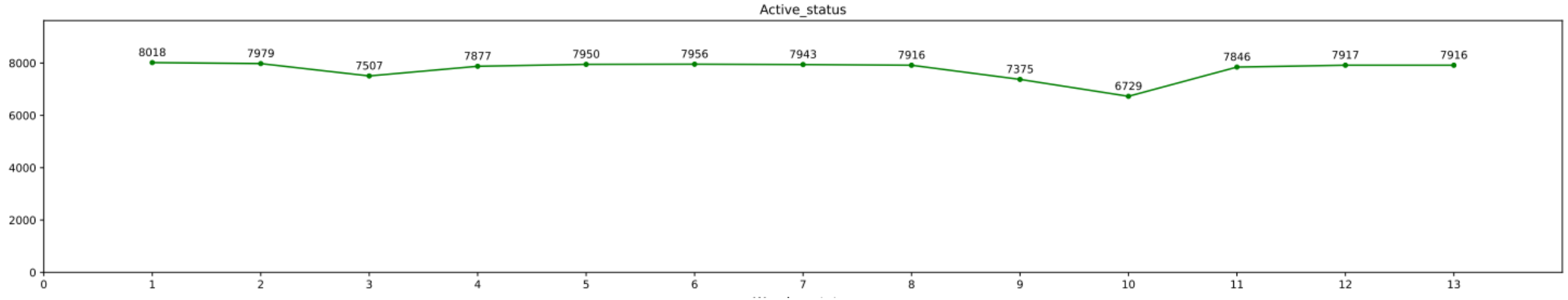
Отклонился любой параметр настройки серверов в части ИБ

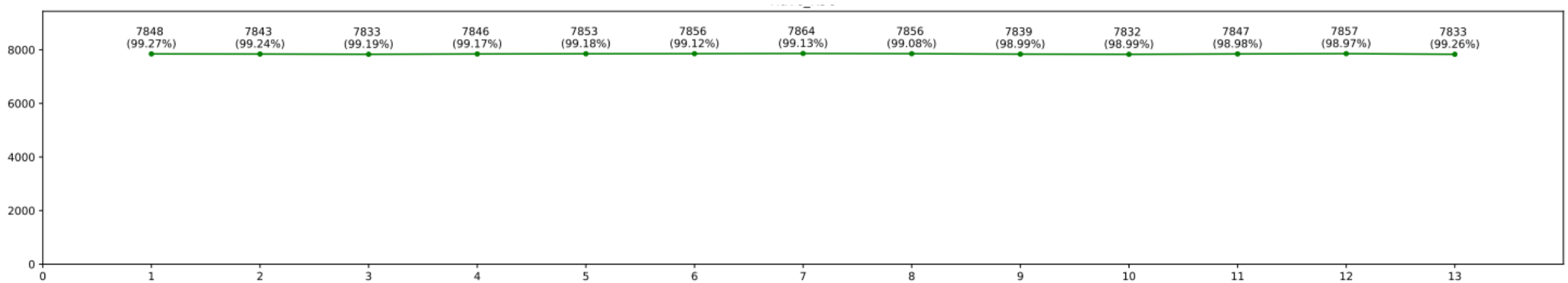
На сервере появился пользователь, но на него нет заявки

Выключено любое ИБ средство на конечном хосте

согаз

Контроль покрытия средствами ИБ





согаз

Наблюдение за требованиями ИБ

SMBv1 server disabled (Windows)

Checks that the SMBv1 server is disabled.

Resolve:
Contact your IT administrator to discuss disabling SMBv1 on your system.

Query

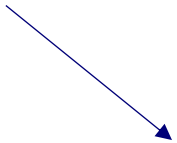
```
1  SELECT 1 FROM windows_optional_features WHERE name = 'SMB1Protocol-Server' AND state != 1
```

Compatible with: ✕ macOS ✓ Windows ✕ Linux

Checks on: ☐ macOS ☑ Windows ☐ Linux

Your policy will only be checked on the selected platform(s).

Save Run



Name	Yes	No
SMBv1 server disabled (Windows)	7819 hosts	1285 hosts
SSH keys encrypted	9391 hosts	351 hosts
Suspicious autostart (Windows)	9108 hosts	0 hosts

согаз

Приятный бонус

Максимально быстрый поиск системных данных по всей инфраструктуре

Query

```
1  SELECT * FROM deb_packages where name like '%log4j%';
```

Compatible with: ✕ macOS ✕ Windows ✓ Linux

~ 1 минута

8 results

Host	admindir	arch	maintainer	name	priority	revision
s00-0000-dt06	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	10+deb11u1
s00-0001-sp21	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	8+deb10u2
s00-0000-nx01	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	7+deb9u2
s00-0000-ab01	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	10+deb11u1
s00-0000-dt24	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	10+deb11u1
s00-0000-tc03	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	7+deb9u2
s00-0000-gl02	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	10+deb11u1
s00-0000-il08	/var/lib/dpkg	all	Debian Java Maintainers <pkg-java-maintainers@lists.alioth.debian.org>	liblog4j1.2-java	optional	7+deb9u1

Что дальше?

Добавить корреляцию с системой виртуализации

Добавить корреляцию с Docker/Kubernetes

Разработать единые дашборды

Спасибо
за внимание!

Старостин Георгий

Директор по ИБ АО «СОГАЗ»