

# А вы знаете, что именно защищаете?

Опыт инвентаризации  
ИТ активов со стороны ИБ



Старостин Георгий

Директор по ИБ АО «СОГАЗ»

**СОГАЗ**



# Кто живет в корпоративной сети?



# 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?

# Различие ИТ и ИБ инвентаризации конечных устройств

| 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                           | ✗  | ✓  |

# 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.<br>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<br>(самописный, Python) | Сопоставление данных из сканеров и баз знаний  |

# Подход к инвентаризации сети



# Результаты сканирования и корреляции

Query 1 x Fleet Fleet Fleet table\_2023\_06\_21\_1 table\_2023\_06\_21\_1 table\_2023\_06\_22\_0 Hosts 2023-06-23 Test\_QQ\_2023\_06\_15 table\_2023\_06\_28\_0

```
398 port_80_ScriptOutput not like '%Kyocera%' and
399 port_80_ScriptOutput not like '%Lexmark%' and
400 port_80_ScriptOutput not like '%Management%' and
401 port_80_ScriptOutput not like '%MFP printer%' and
402 port_80_ScriptOutput not like '%Polycom%' and
403 port_80_ScriptOutput not like '%switch%' and
404 port_80_ScriptOutput not like '%video%' and
405 port_80_ScriptOutput not like '%VoIP%' and
406 port_80_ScriptOutput not like '%Xerox%' and
407 port_8080_ScriptOutput not like '%trassir%' and
408 port_8080_ScriptOutput not like '%ViPNet%' and
409 port_8300 not like '%tmi%' and
410 port_8443_ScriptOutput not like '%Kaspersky%' and
411 port_9100 not like '%jetdirect%';
```

Result Grid | Filter Rows: | Export: | Wrap Cell Content: | Fetch rows:

| ID   | IP     | HOSTNAME   | OS  | HOSTSCRIPT   | port_491  |
|------|--------|------------|---|--|-----------|
| 8734 | 10.77. | -          | OpenBSD 4.0/Linux 2.6.29/FreeBSD 7.0-STABLE     |  |           |
| 8736 | 10.23. | ups*agent  | Linux 3.11 - 4.1/Linux 4.4/Linux 3.10 - 3.12    |  |           |
| 8763 | 10.77. | -          | OpenBSD 4.0/Linux 2.6.29/FreeBSD 7.0-STABLE     |  |           |
| 8782 | 10.37. | -          | OpenBSD 4.0/FreeBSD 7.0-STABLE/Linux 2.6.29     |  |           |
| 8789 | 10.242 | -          | Microsoft Windows Vista SP0 - SP 1              | [[{"id": "smb2-time", "output": "Protocol negotiation failed (SMB2)"}]]  | 49152/unl |
| 8811 | 10.77. | -          | OpenBSD 4.0/Linux 2.6.29/FreeBSD 7.0-STABLE     |  |           |
| 8812 | 10.77. | -          | FreeBSD 7.0-STABLE/OpenBSD 4.0/Linux 2.6.29     |  |           |
| 8813 | 10.0.2 | -          | FreeBSD 7.0-STABLE/Linux 2.6.29/OpenBSD 4.0     |  |           |
| 8816 | 10.238 | -          | Microsoft Windows Server 2008 R2 SP1/Microso... | [[{"id": "smb2-security-mode", "output": "\n 210: \n Message signing enabled but not required"}, {"id": "smb2-time", "output": "\n d..."}]]  | 49152/ms  |
| 8831 | 10.77. | -          | FreeBSD 7.0-STABLE/OpenBSD 4.0/Linux 2.6.29     |  |           |
| 8844 | 10.238 | -          | Microsoft Windows Server 2008 R2 SP1/Microso... | [[{"id": "smb2-security-mode", "output": "\n 210: \n Message signing enabled but not required"}, {"id": "smb2-time", "output": "\n d..."}]]  | 49152/ms  |
| 8879 | 10.110 | -          | Microsoft Windows 10/Microsoft Windows XP SP... | [[{"id": "smb2-security-mode", "output": "\n 311: \n Message signing enabled but not required"}, {"id": "smb2-time", "output": "\n d..."}]]  |           |
| 8934 | 10.190 | n00-1800-( | Microsoft Windows XP SP3/Microsoft Windows S... | [[{"id": "smb2-time", "output": "Protocol negotiation failed (SMB2)"}]]  |           |
| 8976 | 10.37. | -          | OpenBSD 4.0/Linux 2.6.29/FreeBSD 7.0-STABLE     |  |           |
| 8977 | 10.239 | -          | Microsoft Windows Server 2008 R2 SP1/Microso... | [[{"id": "smb2-time", "output": "\n date: 2023-07-04T02:23:19\n start_date: 2023-07-03T08:19:32"}, {"id": "smb2-security-mode", "o..."}]]    | 49152/ms  |
| 8982 | 10.177 | -          | Microsoft Windows Server 2012 R2/Microsoft W... | [[{"id": "clock-skew", "output": "mean: -29m59s, deviation: 1h13m27s, median: 0s"}, {"id": "smb2-time", "output": "\n date: 2023-07-0..."}]] | 49152/ms  |

Result 1 x Read Only

# Примеры оповещений

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

По хосту нет (или недостаточно) данных в CMDB

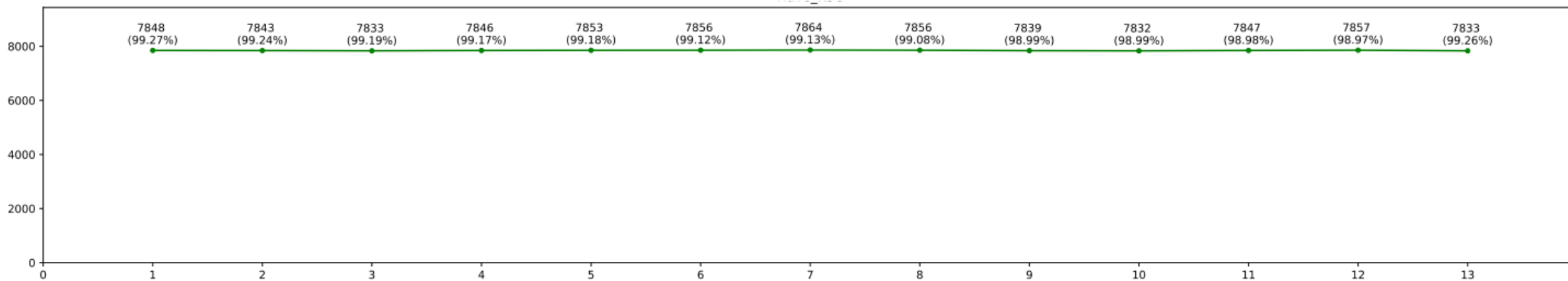
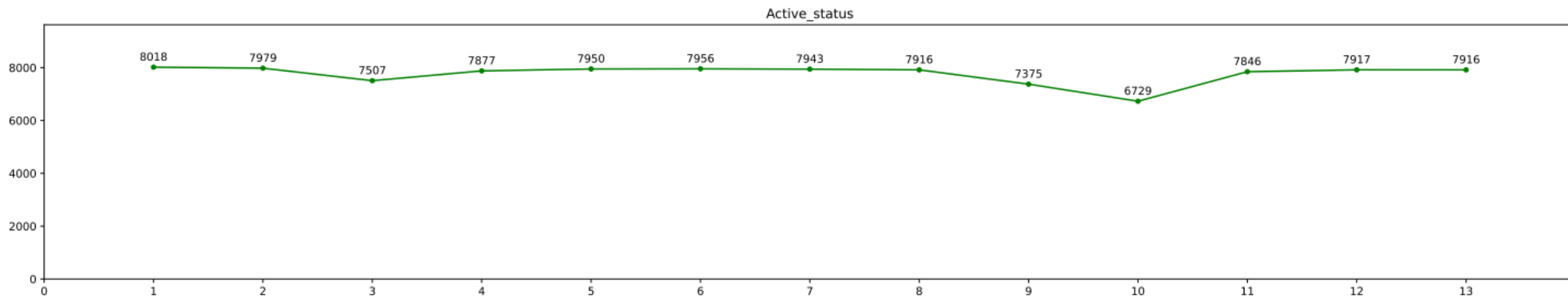
Отклонился любой параметр настройки серверов в части ИБ

На сервере появился пользователь, но на него нет заявки

Выключено любое ИБ средство на конечном хосте




# Контроль покрытия средствами ИБ



# 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
```

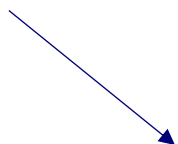
Compatible with:  macOS  Windows  Linux

Checks on:  macOS  Windows  Linux

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

Save

Run



| <input type="checkbox"/> | Name                            |  Yes |  No |
|--------------------------|---------------------------------|--|---|
| <input type="checkbox"/> | SMBv1 server disabled (Windows) | 7819 hosts   | 1285 hosts  |
| <input type="checkbox"/> | SSH keys encrypted              | 9391 hosts   | 351 hosts   |
| <input type="checkbox"/> | Suspicious autostart (Windows)  | 9108 hosts   | 0 hosts   |

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

