Яндекс

Яндекс

splunk>

Splunk based network access control (NAC)

Игорь Гоц
Группа инфраструктурной безопасности

Среда

01 Более 7 000 рабочих мест

02 Более 95% рабочих мест мобильные или удаленные

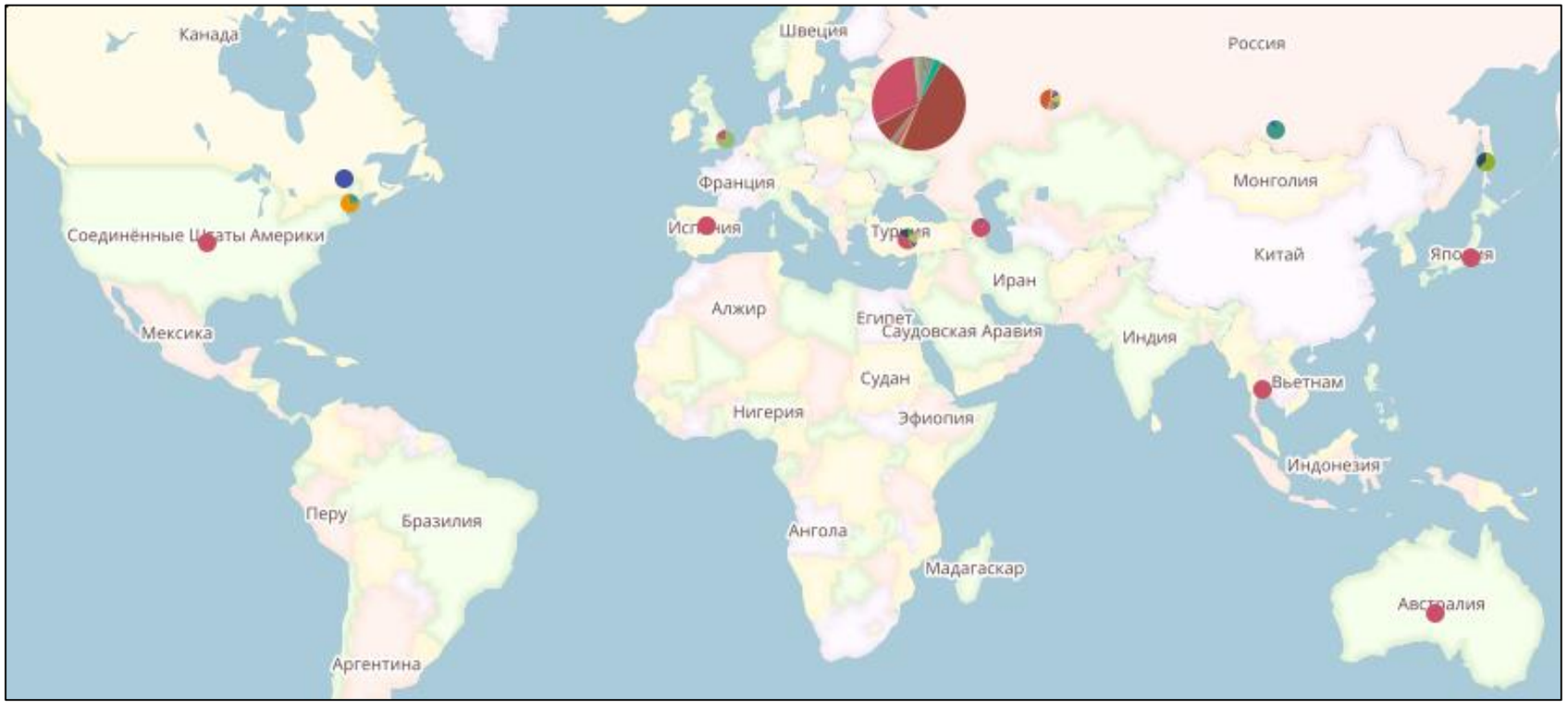
03 Более 30 версий операционных систем (Windows, MacOS, *nix)

04 Ежедневное изменение инфраструктуры

05 Разработчики и тестировщики \ локальные администраторы

06 Отсутствие средств фильтрации трафика

Среда


Канада
Швеция
Россия
Франция
Монголия
Соединённые Штаты Америки
Испания
Турция
Китай
Иран
Алжир
Египет
Саудовская Аравия
Индия
Мексика
Судан
Вьетнам
Нигерия
Эфиопия
Индонезия
Перу
Бразилия
Ангола
Мадагаскар
Австралия
Аргентина

Варианты клиентов NAC

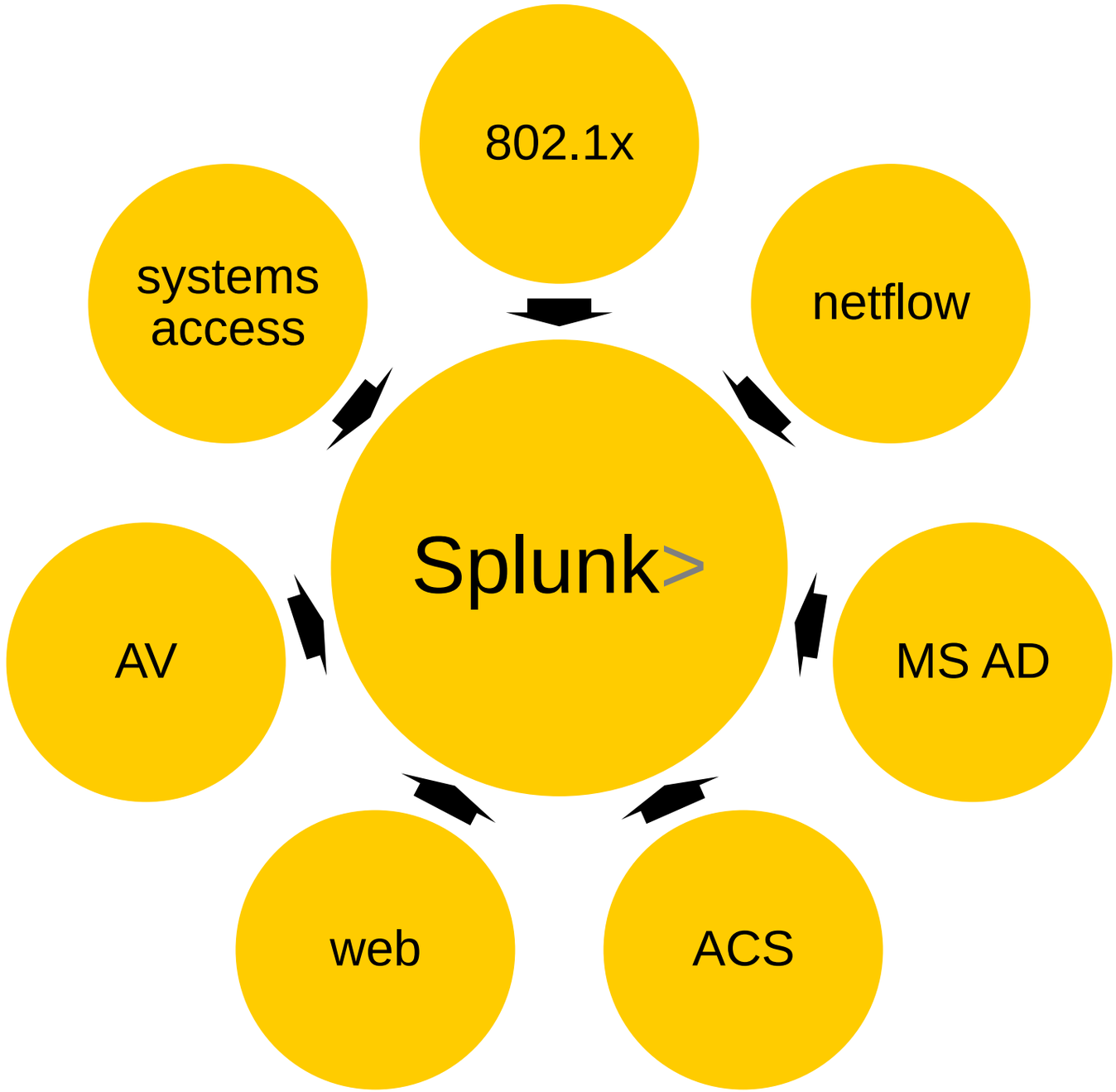
01	Установленный агент	✗
02	Скачиваемый агент	✗
03	Удаленный вызов процедур (RPC)	✗
04	Сканер уязвимостей	✗
05	Мониторинг	✓

Варианты клиентов NAC

Критерии

01	Профиль пользователя	• ОС • Браузер • Пароль • Статус
02	Профиль компьютера	• Сертификат • Имя компьютера • ОС • MAC-адрес
03	Антивирус	• Наличие • Статус
04	Сертификат 802.1x	• Время • Место
05	Обновление ПО	• Microsoft SCCM • Casper Suite • osquery

Критерии



Особенности

01 Полнота журнала

02 Скорость доставки журнала

03 Скорость индексации в splunk

04 Скорость появления событий в выдаче

05 Порядок выборок

06 Скорость выборки

Принципы применения политик

01	Мягкое уведомление	• Письмо • Тикет
02	Жесткое уведомление	• Письмо • Тикет • Сотрудник HD • Руководитель
03	Блокировка	• Карантинный VLAN • Доступ до email • Обращение в HD

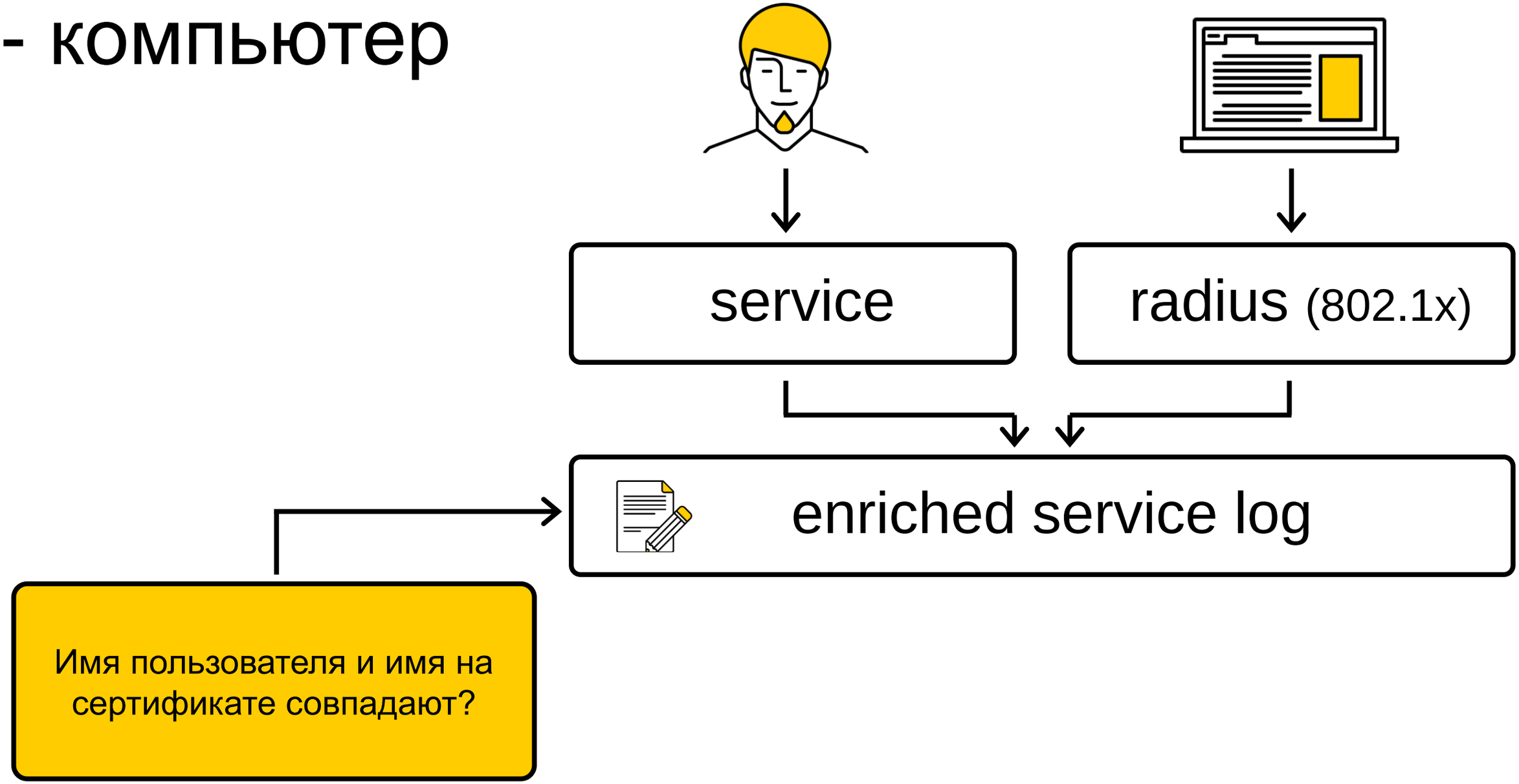
Принципы применения политик

Здравствуйте, [redacted]
Кто-то вошел в ваш аккаунт на устройстве Windows 8.1 через приложение Yandex Browser.
Список недавно использованных устройств приведен ниже.
Возможно, вы впервые вошли в систему на новом компьютере, телефоне или в новом браузере.
Кроме того, вы могли работать с ресурсами, находясь в режиме инкогнито, сменив настройки браузера или из виртуальной машины.
Если изменение имело место быть, просим вас закрыть тикет с соответствующим комментарием.
Если ничего подобного вы не делали, есть вероятность, что ваш аккаунт был взломан.
В этом случае просим отметить в тикете, что изменение вам не кажется легитимным.
▼ :
Смотрим какие браузеры использовались (показывается смена):
splunk
Смотрим куда ходили новым браузером:
splunk

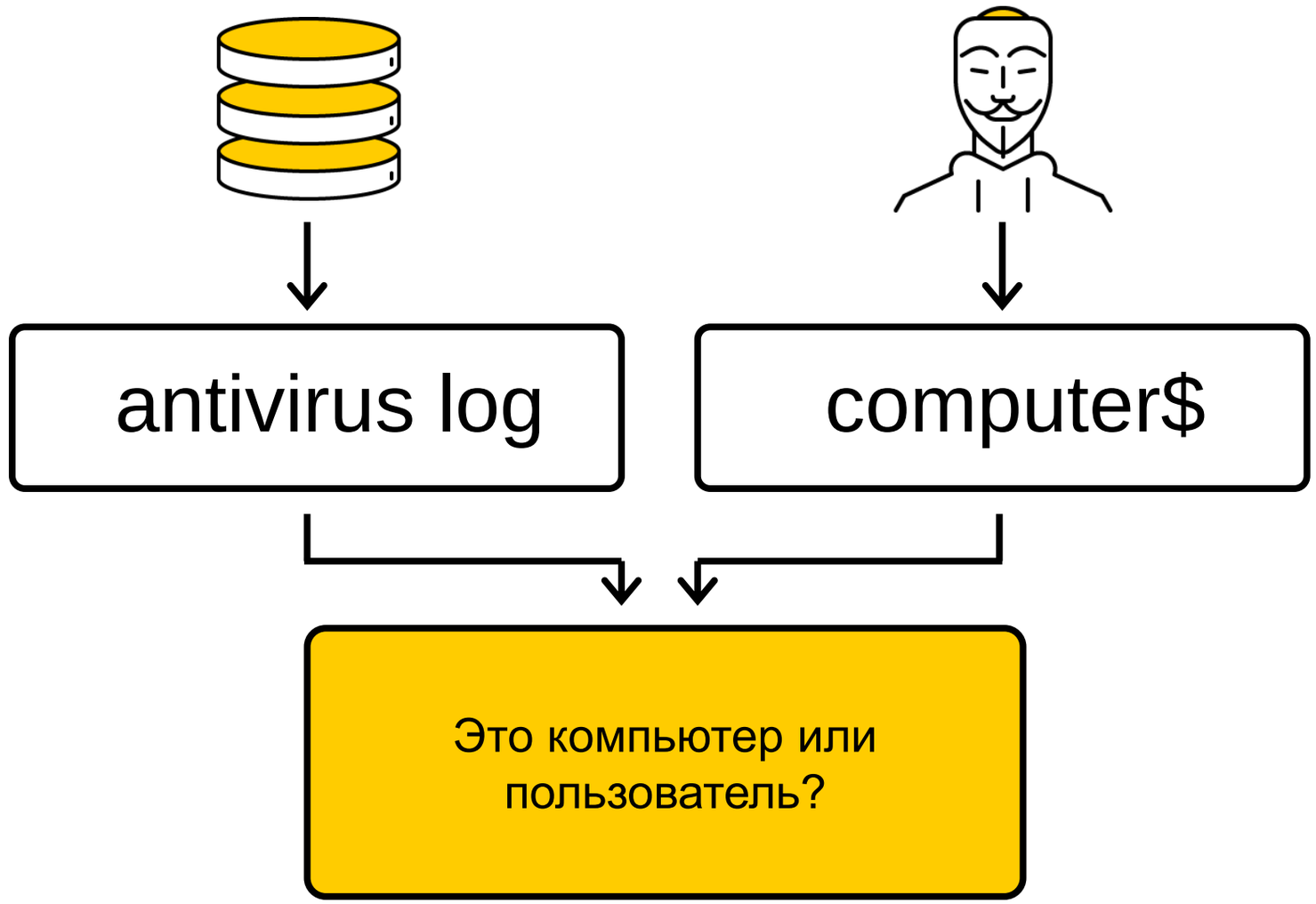
Содержимое алерта:

Ключ	Значение
epoch_time	[redacted]
new_OS	Windows 8.1
new_http_user_agent	Mozilla/5.0 (Windows NT 6.3; WOW64) [redacted] (KHTML, like Gecko) [redacted]
new_ua_family	Yandex Browser
new_yandexuid	-
old_OS	Mac OS X
old_http_user_agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_[redacted]) [redacted] (KHTML, like Gecko) [redacted]
old_yandexuid	[redacted]
user	[redacted]
time	[redacted]

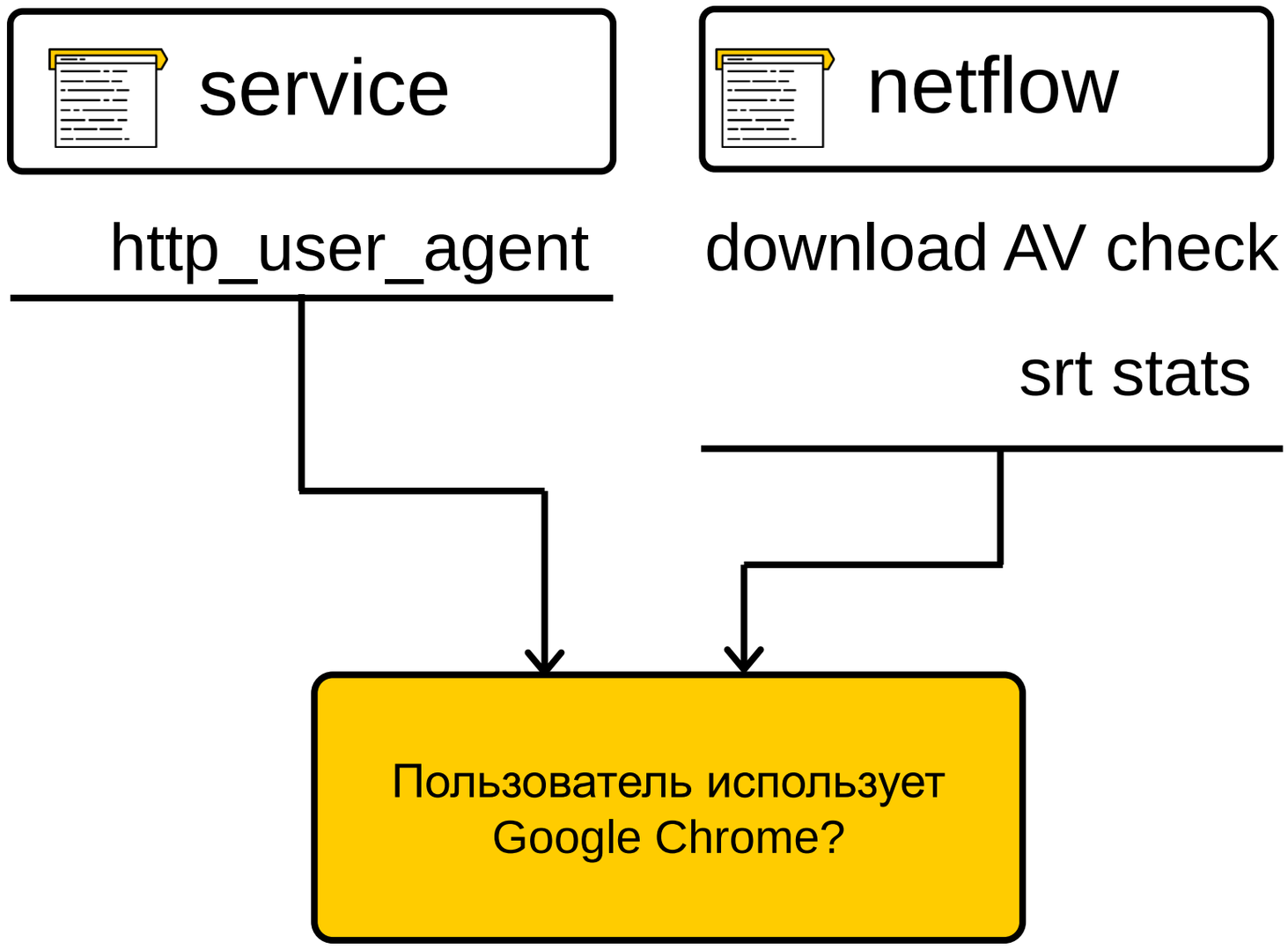
Пользователь - компьютер



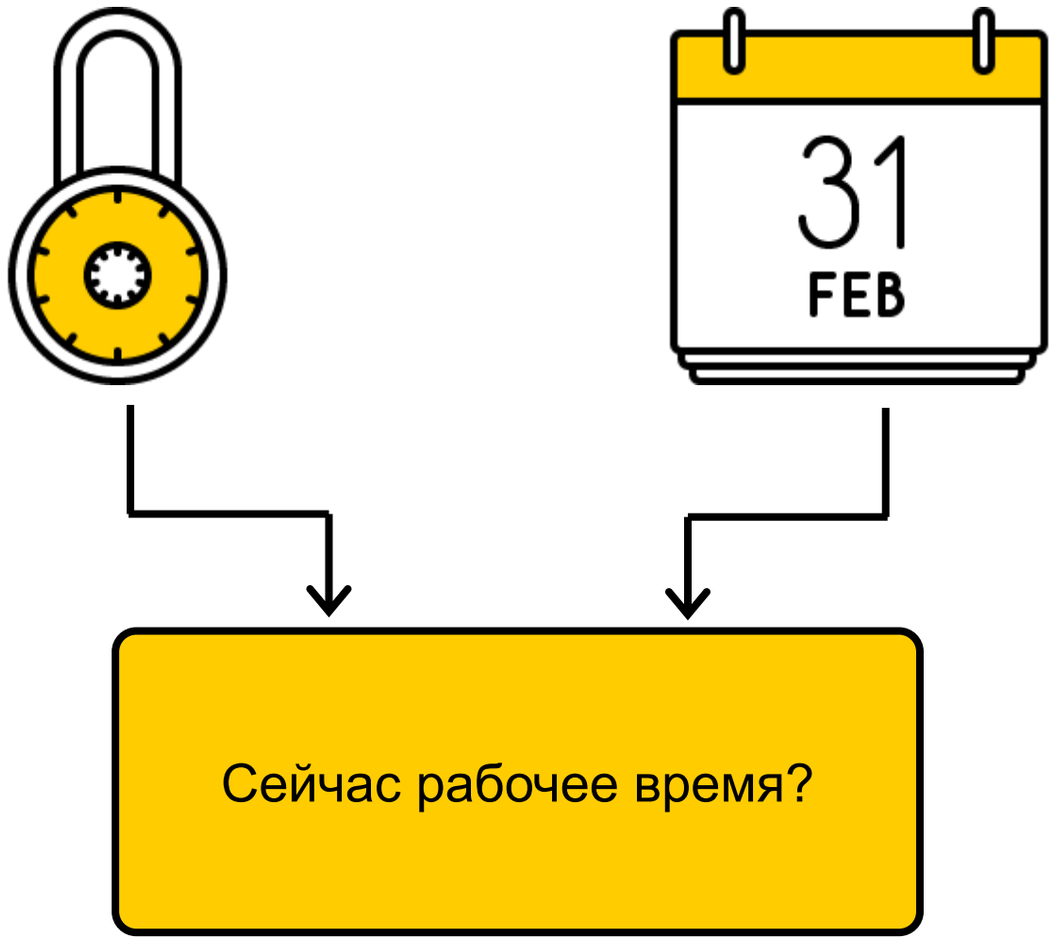
Пользователь или компьютер ?



To google or not to google?



Счастливые часов не наблюдают



Спасибо за внимание.

Контакты

Гоц Игорь

gots@yandex-team.ru