23.11.2017

Практика SOC.

Маленькие аспекты большой сети

мтс

Ты знаешь, что можешь!

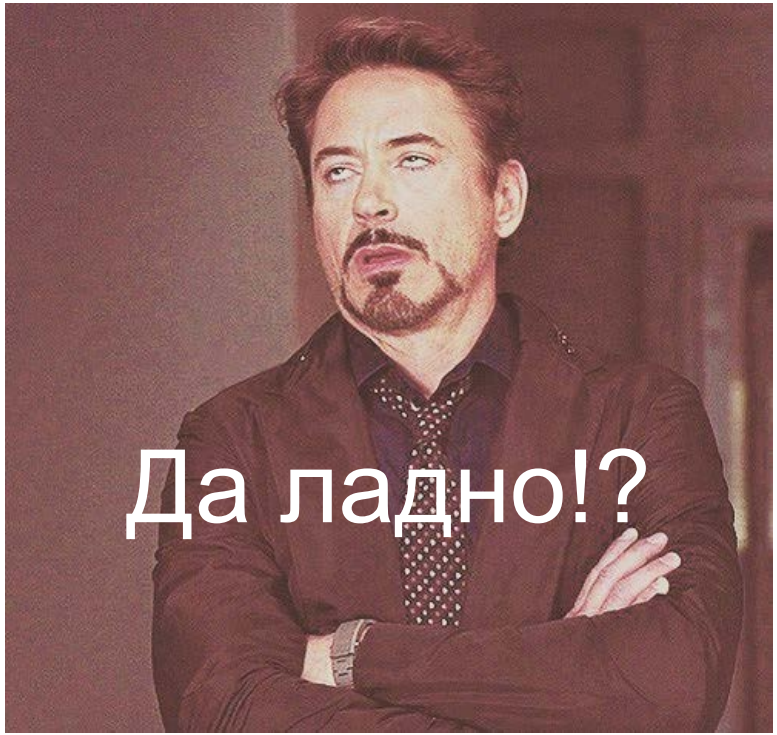
whoami

Андрей Дугин

Начальник отдела обеспечения информационной безопасности

МТС Ты знаешь, что можешь!

SOC – это люди, процессы и технологии



Зона покрытия

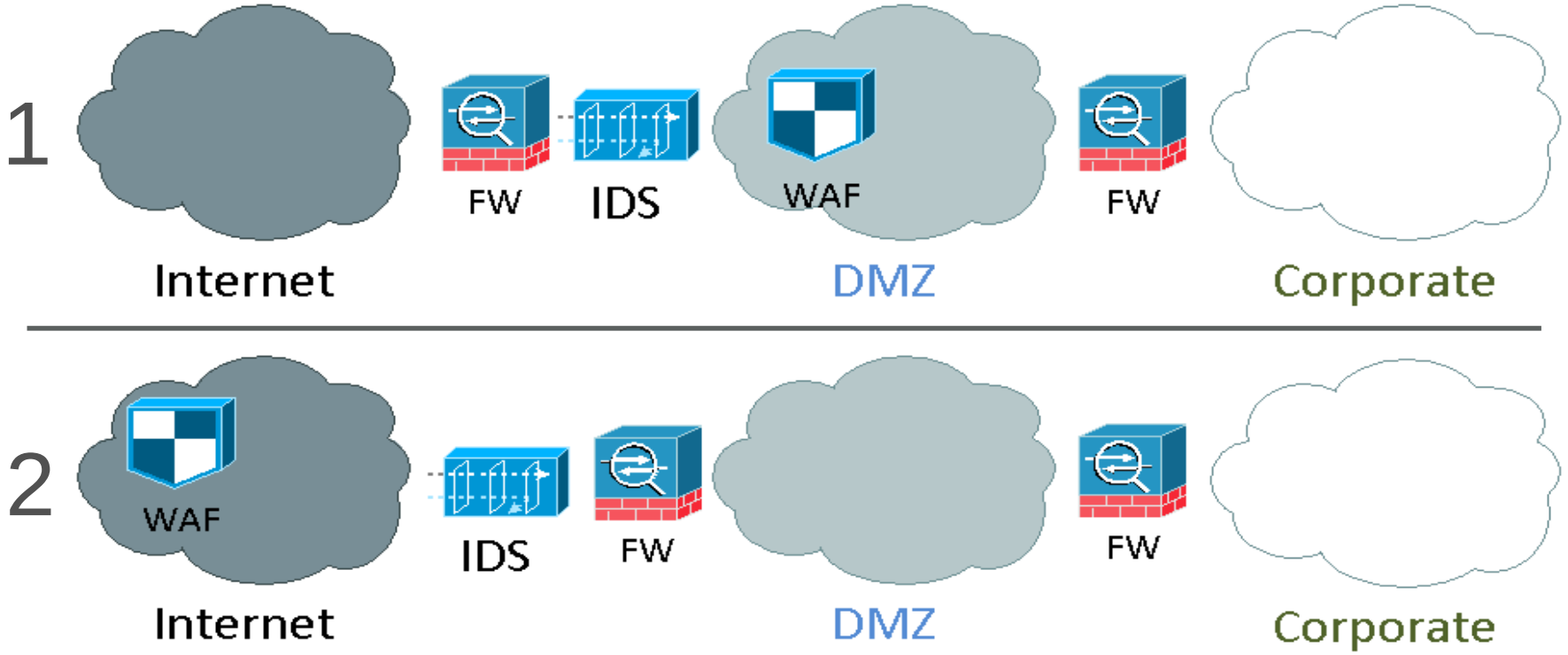
- 11 часовых поясов
- Десятки тысяч сотрудников
- Десятки тысяч ПК/ноутбуков
- Десятки тысяч серверов
- Тысячи единиц активного сетевого оборудования
- >1000 диапазонов внешних IP

SANS Top20 CSC

Архитектура сети

- Пропускная способность
- Надежность
- Управляемость
- Масштабируемость
- Безопасность
- Контролируемость

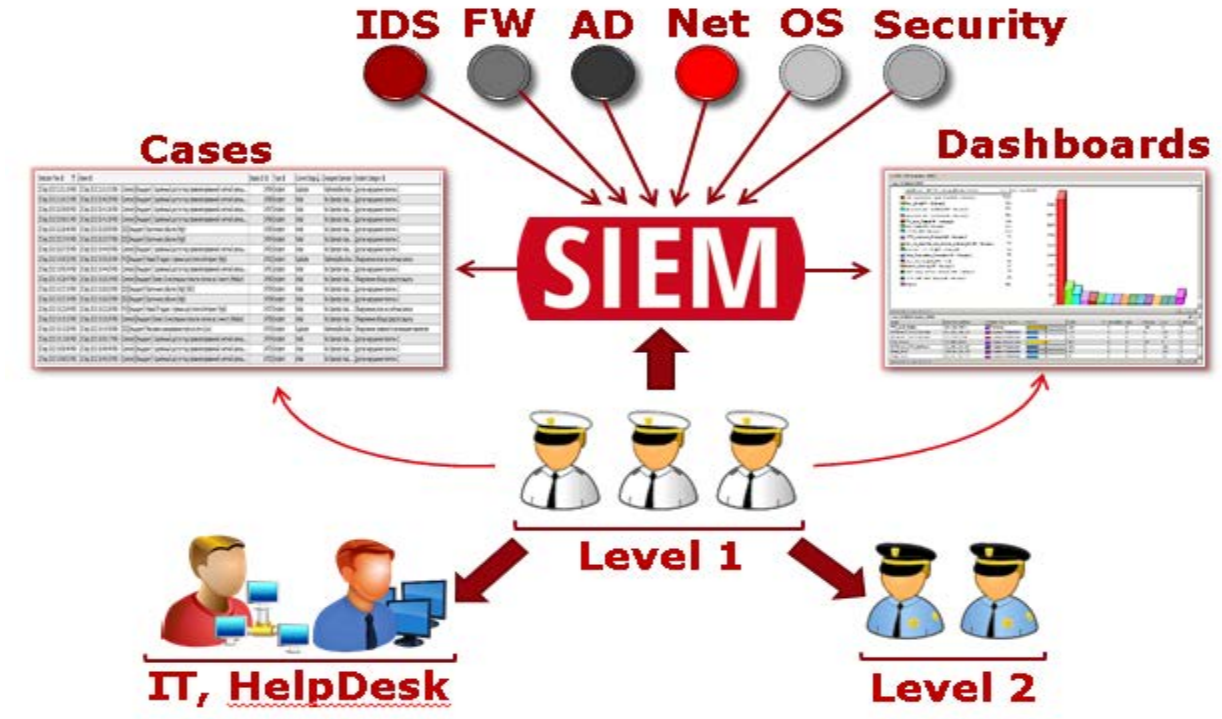
Варианты архитектуры



Централизация

- Инвентаризация
- IP-планирование
- CM / IM / PM / VM
- Консоль мониторинга
- Инфраструктурные сервисы

Централизация сбора событий ИБ



Дополнительная интеграция SIEM

- IP-планирование
- FCMDB
- IM / CM / VM
- SOC BI/GRC
- TI

Факторы процессов

- Политика ИБ
- Зрелость процессов компании
- Формализация SOC
- Нормативные документы
- Шаблоны и инструкции

Пример инструкции

1) Определить владельца ПК/системы, воспользовавшись данными из оповещения либо, при их отсутствии, инструкцией

2) Написать владельцу учётной записи/ПК/системы уведомительное письмо, воспользовавшись соответствующим e-mail шаблоном

3) В случае определения вирусной активности на хосте, создать заявки:

3.1) Если активность проявляет пользовательский ПК - создать заявку в группу поддержки пользователей на антивирусную проверку ПК и установку обновлений ОС Windows.

3.2) Если активность проявляет сервер - создать заявку в группе поддержки Windows или группе поддержки Unix на антивирусную проверку сервера и установку обновлений ОС.

4) Зарегистрировать инцидент в реестре инцидентов.

Пример шаблона запроса информации

%Name%, добрый день!

Наши системы мониторинга регистрируют большое количество неудачных попыток аутентификации под учётной записью/с IP-адреса, принадлежащей/его Вам (**%username% or %IP% or %hostname%**).

Наиболее распространённые причины, которые могут вызывать данную активность:

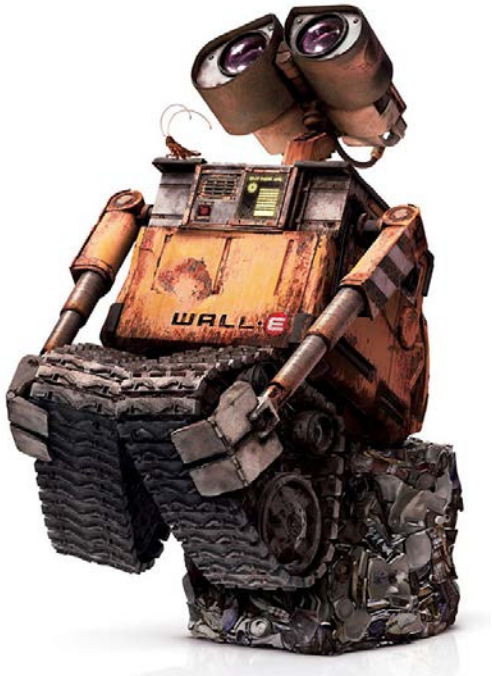
- Заражение ПК вредоносным программным обеспечением;
- Использование не валидных учётных данных в программном обеспечении (обычно после смены пароля).

В связи с этим просим Вас:

1) Провести полную проверку ПК/сервера на вирусы (см. приложенную инструкцию).
2) Проверить ПК на наличие приложений, использующих устаревший пароль от вашей учетной записи.
3) В ответном письме сообщить причины данной аномальной активности.

В случае повторения инцидента Ваша учетная запись может быть заблокирована до выяснения причин.

Человеческий фактор



- Контроль нагрузки:
  - Количество инцидентов
  - False Positive
- База знаний, инструкции
- Мотивация
- Работа в команде

МТС Ты знаешь, что можешь!