ИБ как продукт. Нестандартные подходы к формальной безопасности.

Черновский Александр
Технический директор «SoftMall»

softmall.ru

ИБ как продукт

- Программные и аппаратные средства ИБ
- Персонал, отвечающие за ИБ
- Последовательность действий персонала и используемых программных/аппаратных средств

Переход к «новой» безопасности

Текущая безопасность

- Средство антивирусной защиты
- Защита от несанкционированного доступа
- Межсетевой экран
- IDS/IPS (опционально)

Новая безопасность

- Endpoint Detection & Response
- Network Traffic Analysis
- Sandbox
- Threat Intelligence
- SIEM

Этапы разработки продукта

1. Определение продукта
2. **Создание MVP**
3. Аналитика
4. Проектирование, тестирование, разработка
5. Выпуск и дальнейшее развитие

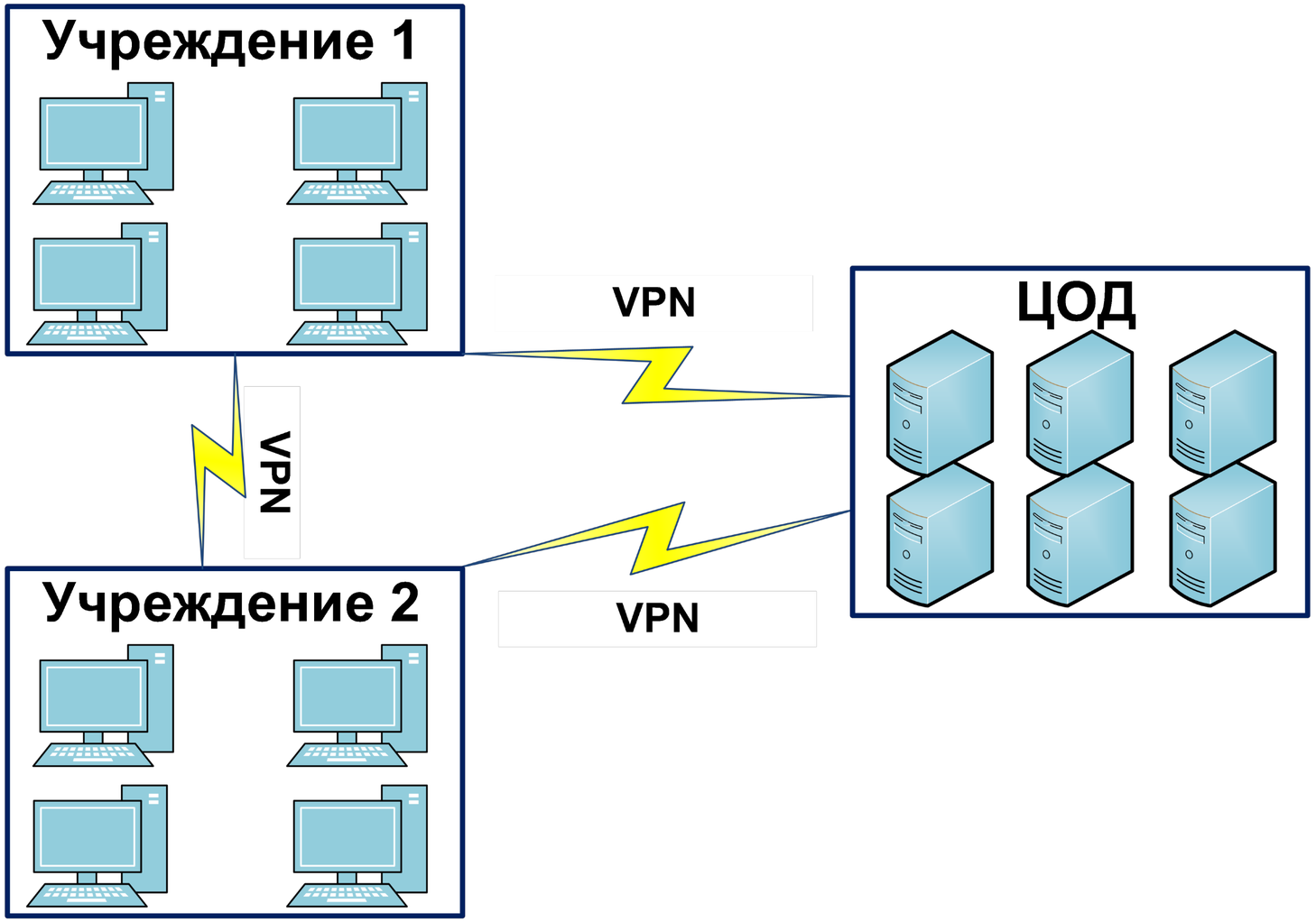
MVP (минимально жизнеспособный продукт) - продукт, обладающий минимальными, но достаточными для выполнения первичных требований функциями.

MVP

Продукт

Основная задача — получение обратной связи для формирования представления для дальнейшего развития продукта.

Примерная инфраструктура



- Удаленные подразделения
- Центральный сегмент, в котором размещаются системы и сервисы
- Взаимодействие подразделений друг с другом и с центральным сегментом построено с использованием VPN

История одного вечера

Реакция на увиденное

Содержимое увиденного

1. Source IP:1234 -> Destination IP:3389
2. Source IP:4321 -> Destination IP:3389
3. Source IP:5678 -> Destination IP:3389
.
.
100. Source IP:8765-> Destination IP:3389

BlueKeep

1. Source IP:1357 -> Destination IP:445
2. Source IP:7531 -> Destination IP:445
3. Source IP:3579 -> Destination IP:445
.
.
100. Source IP:9753 -> Destination IP:445

EternalBlue

Что было сделано

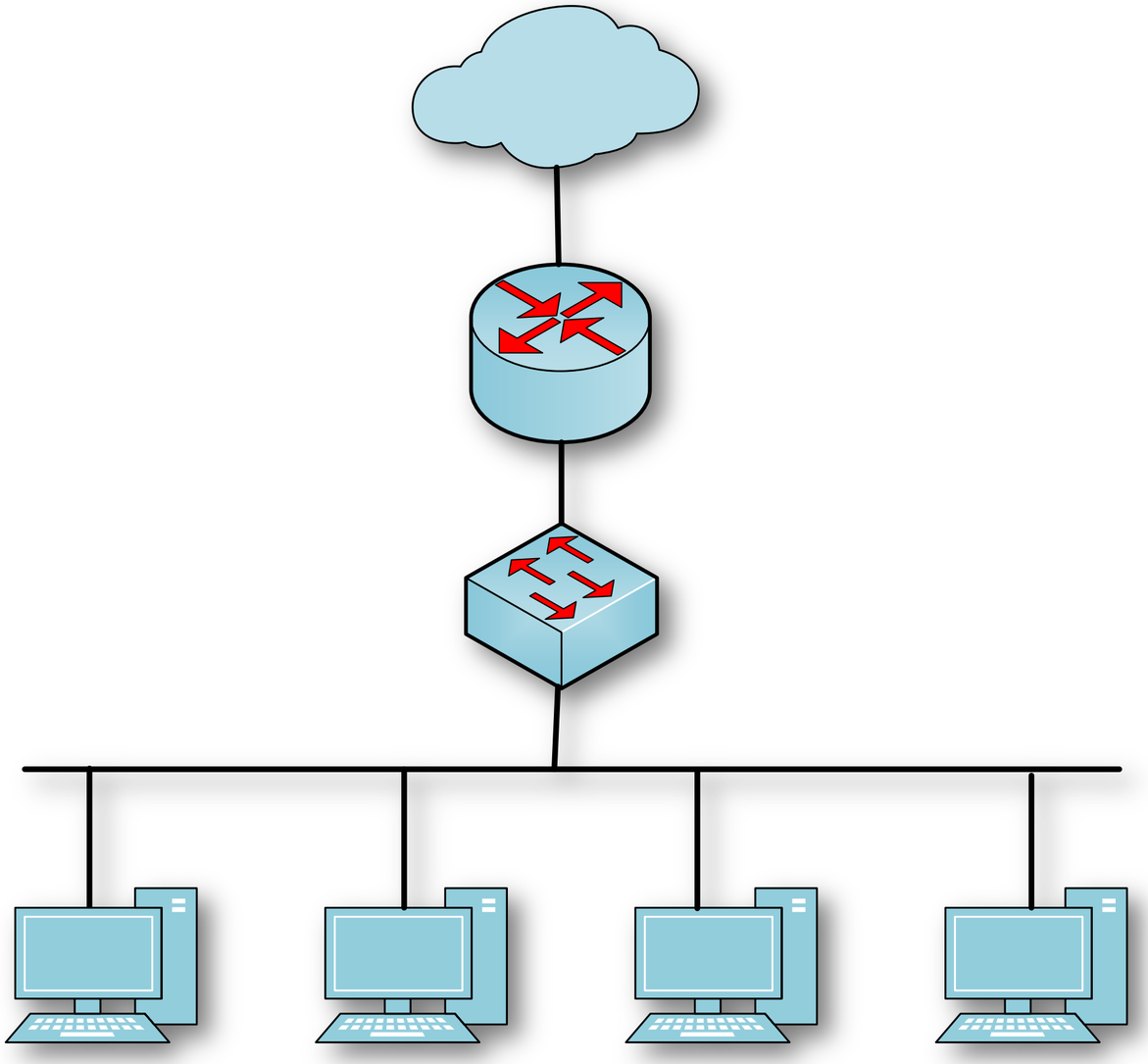
В процессе реагирования

- Анализ сетевого трафика и выявление зараженных хостов
- Блокирование доступа зараженных хостов к системам и сервисам центрального сегмента
- Настройка межсетевого экрана, как на уровне сети, так и на уровне зараженных хостов

В дальнейшем

- Автоматическое обновление правил имеющихся сенсоров (IDS)
- Централизация потоков событий с сенсоров (IDS) для мониторинга происходящего
- Постоянное оповещение ответственных специалистов о выявленных зараженных хостах
- Блокирование доступа к системам и

О текущей безопасности



- На компьютерах установлены средства антивирусной защиты.
- На границы сети межсетевой экран
- Проводится сканирование антивирусным ПО
- Пройдена оценка соответствия требованиям регуляторов

Первый шаг к новой безопасности

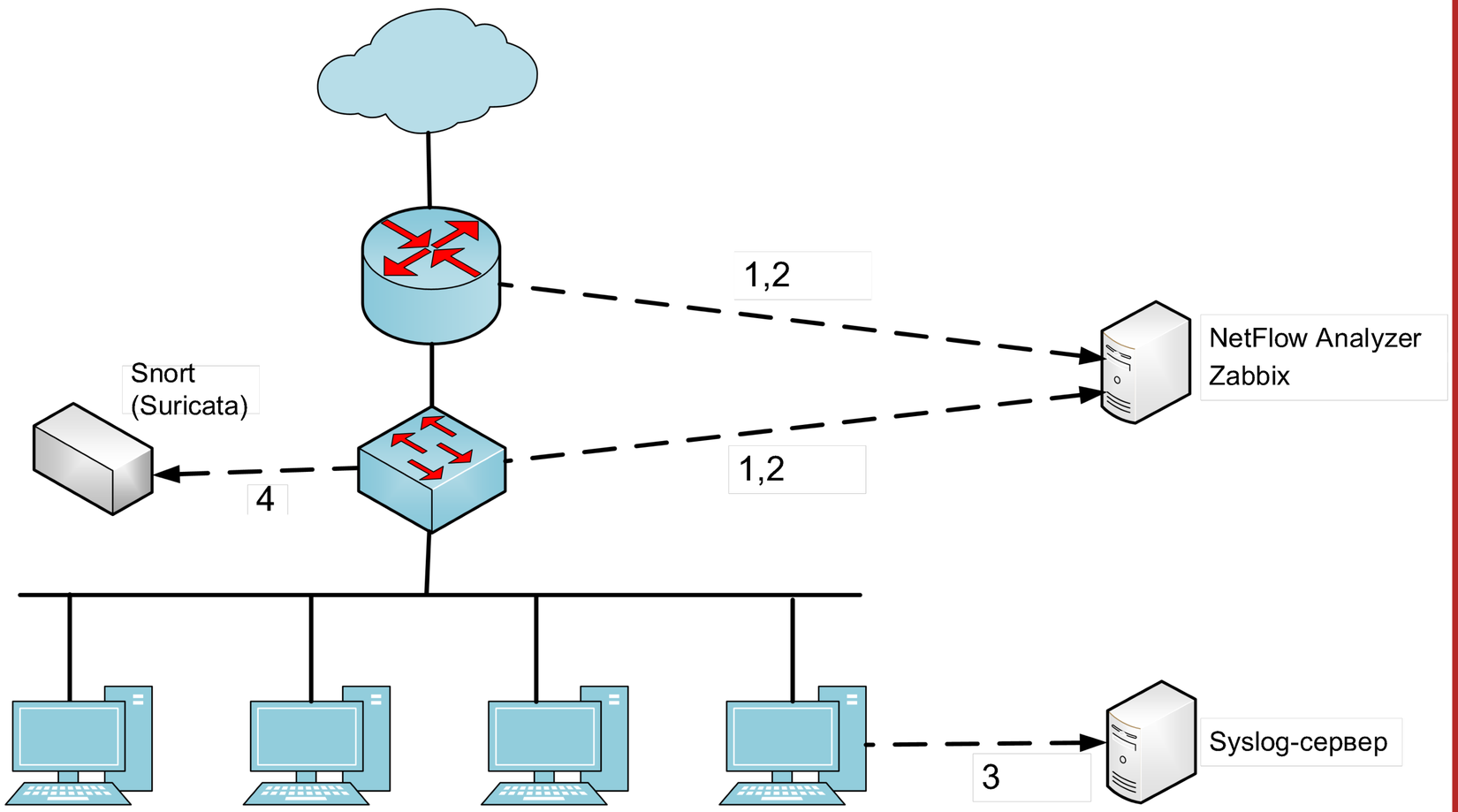
Уровень хоста

- Сбор журнала событий ОС
- Сбор журналов событий, журналов действий, журналов трафика СЗИ
- Использование всего доступного функционала СЗИ

Уровень сети

- Использование инструментов сбора и анализа сетевого трафика
- Использование инструментов мониторинга сетевого оборудования
- Использование свободно распространяемых инструментов (например, IDS/IPS)

Первый шаг к новой безопасности



1 – flow с сетевого оборудования

2 – передача данных об объеме сетевого трафика

3 – логи со средств защиты информации и операционных систем

4 – зеркало проходящего трафика

Результат

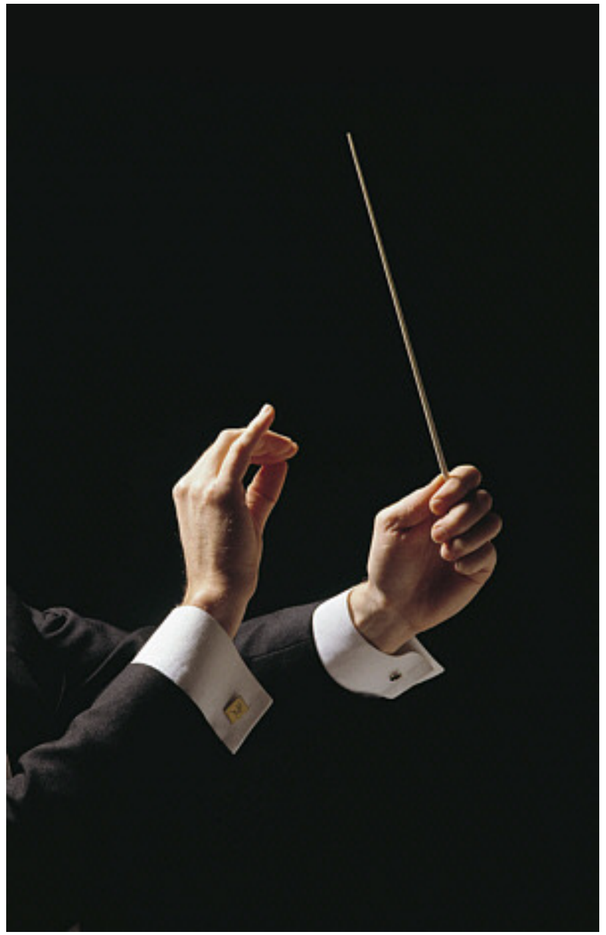
1. Обозначен перечень источников событий и активов требующих защиты
2. Сформирован требуемый набор средств защиты и их функциональные характеристики
3. Понятна «дорожная карта» по построению/модернизации системы ИБ

О чем поговорим

Проблемы в текущих реалиях

Чемпион безопасности
Дирижер на стык ИТ и ИБ

Кого есть смысл вовлекать



Проблемы в текущих условиях

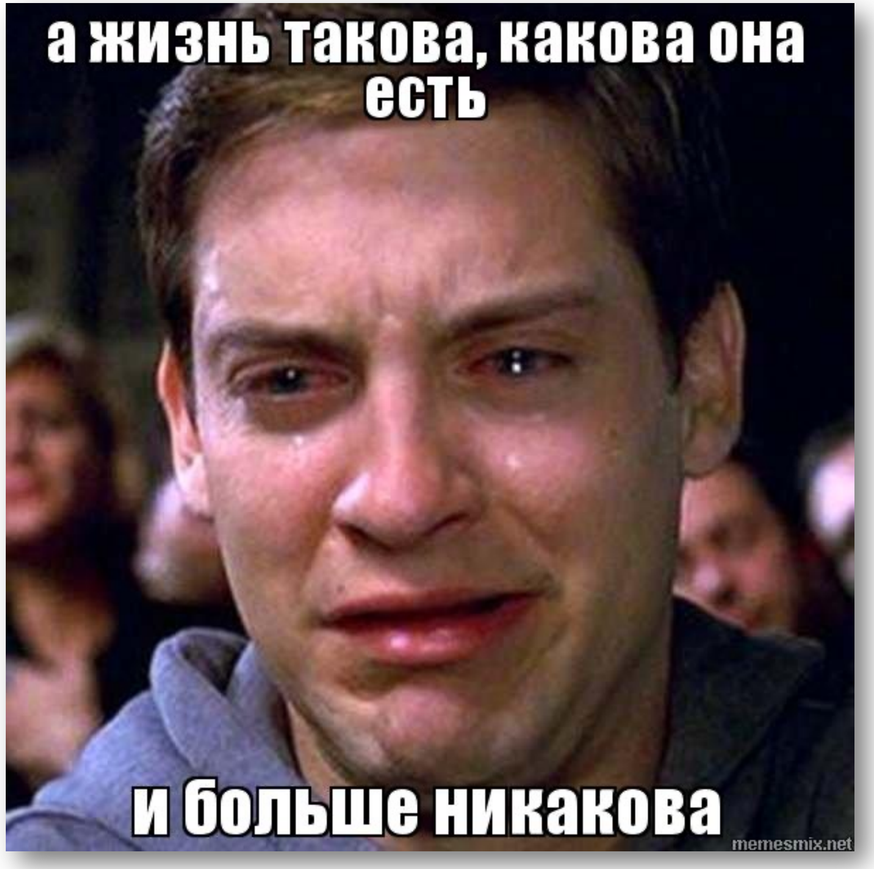
Ломают всех и больно

Хактивизм на уровне стран

Поддержка хактивизма

Все, про кого вспомнили/осветили в новостях

Заказали



История конфликта

Удобно использовать VS Безопасно использовать

Доступность VS Распространение

Стек TCP/IP?

Типовое распределение

- Сетевая безопасность
- Compliance
- Интеграция хостовых СЗИ
- Импортозамещение
- Техническая поддержка
- SoC

- Сетевые коммуникации
- Разработка
- Системное администрирование
- Импортозамещение
- Техническая поддержка

Кто спасёт ситуацию?

Security Champion! Кто такой чемпион безопасности?

- Нет best practice
- Нет выверенного манифеста
- Пишет OWASP
- Пишет TOP CISO
- Упоминает на профильных митапах и конференциях

Преимущества подхода

Команда

+ Упрощение и ускорение взаимодействия с ИБ
+ Компетенции ИБ в своей команде и продукте
+ Экономия времени и отсутствие лишних задач

Чемпион

+ Повышение заработной платы
+ Кураторство со стороны ИБ
+ Повышение своих компетенций в части ИБ
+ Повышение собственной значимости и стоимости

ИБ / Компания

+ Экономия человеческих ресурсов
+ Распределенная коллективная ответственность
+ Отсутствие необходимости изучать специфический продукт
+ Минимизация рассинхронизация ИТ и ИБ подразделений

Кого вовлекать в процесс

IF	(Лояльность & Добровольно)
THEN	(Одна штатная единица в направлении & Отсутствие санкций)
RETURN	Нет управления Есть влияние

Модернизация MVP

MVP

- Требования законодательства
- Необходимые инструменты
- Желаемый функционал
- Дополнительные ресурсы
- Внутренние регламенты, процессы и т.д.

Первая версия продукта

SoftMall

Спасибо за внимание!

Черновский Александр
Технический директор «SoftMall»