Почему «не взлетают» SIEM-проекты?

Александр Кузнецов, CISM
Руководитель направления ИБ
НТЦ «Вулкан»

2016

Ещё раз о SIEM

Я это … пойдем SIEM внедрять …

Шо, опять!?

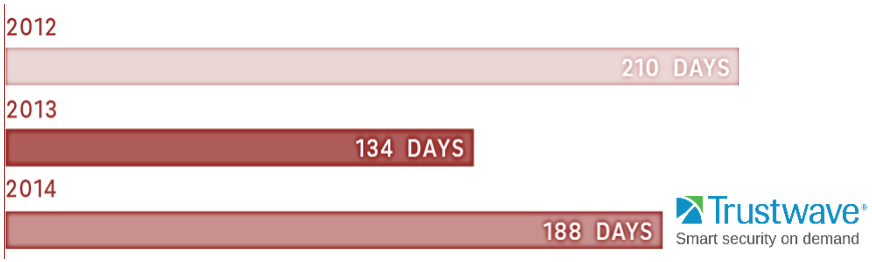
Кадры из м/а «Жил был пес»

Содержание

- Текущие тенденции: рост или спад?
- «Затык» SIEM-проекта: кто виноват?
- Меняется ли «сумма» от перемены SIEM местами?
- Готовность ИТ-инфраструктуры к внедрению SIEM
- SIEM-команда: работа за пределами технологии
- SIEM и аутсорсинг
- Управление событиями: шашечки или ехать?
- Вместо заключения

Текущие тенденции: рост или спад?

- Рост SIEM-рынка в мире (Gartner)
- Появление ряда отечественных SIEM-продуктов
- Развитие функционала SIEM-решений (*Packets Analysis, Endpoint Analytics, Threat Intelligence*)
- Увеличение количества зафиксированных инцидентов
- «Сохранение» среднего времени выявления вторжений

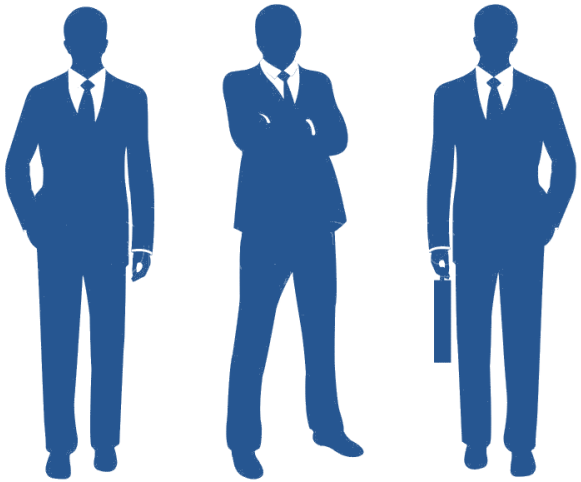


В 2015 году зафиксировано на 38% больше инцидентов, чем в 2014 году

pwc

- Открытая критика SIEM-проектов

«Затык» SIEM-проект: кто виноват?



Интегратор | **Заказчик** | **Вендор**

Получение $	Сохранение $	Получение $
Внедрение системы	Решение задач	Поставка системы
«Вход» в заказчика	*Достижимо только если они были чётко сформулированы*	Ежегодная техн. поддержка
Success Stories		Success Stories

Меняется ли «сумма» от перемены SIEM местами?

- Logs
- NetFlow
- Packets
- Data:
  - Scanners
  - Threat Intelligence Centers (feeds)
  - Endpoint Analytics

Готовность ИТ-инфраструктуры к внедрению SIEM

- Сегментирована сеть
- Категоризированы ИТ-активы (как минимум сегменты сети)
- Определены точки и параметры взаимодействия сегментов между собой и «внешним миром»
- Настроен аудит событий
- Получены baselines по событиям и пороговые значения
- Обеспечен доступ источников событий к SIEM-системе

подготовил ИТ-инфраструктуру к внедрению СИЕМа?

Внимание, вопрос! *Кто отвечает за эти активности?*

SIEM-команда: работа за пределами технологии

Администратор:

- обслуживание системы (патчинг, резервирование), подключение источников
- управление доступом

Оператор-аналитик:

- анализ поступающих данных, тюнинг правил, поиск актуальных feed-ов, отчётность
- обработка инцидентов

- классическое системное и сетевое администрирование (Linux/Unix), *пунктуальность*

- широкий ИБ-кругозор, знание актуальных ИБ-угроз, *коммуникабельность*

SIEM и аутсорсинг

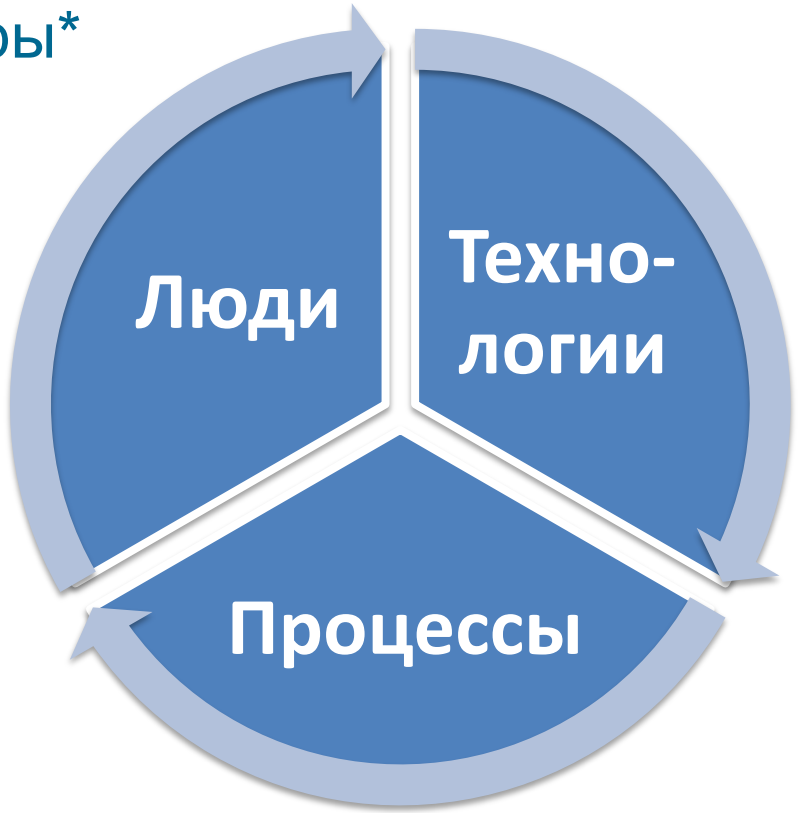
- Зоны для аутсорсинга:
  - администрирование SIEM-системы
  - модернизация SIEM-системы
  - подключение нестандартных источников событий
  - поставка feed-ов
  - интеграция SIEM-системы с системами управления инцидентами
  - участие в расследовании инцидентов

Управление событиями: шашечки или ехать?

Опять об этих процессах управления …

Управление событиями

- SIEM – это один из вариантов получения сведений о состоянии ИТ-инфраструктуры*
- Взаимосвязи с другими процессами управления:
  - Управление инцидентами
  - Управление проблемами
  - Управление изменениями
  - Управление уязвимостями
  - Управление активами



* - Второй известный вариант – это звонок «восторженного» пользователя

Вместо заключения

Успех SIEM-проекта лежит далеко за пределами технологии

Ваша SIEM-система много чего умеет. Позвольте ей доказать это!

Спасибо за внимание!

Александр Кузнецов, CISM
Руководитель направления ИБ
НТЦ «Вулкан»

105318, г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru