POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Современные системы мониторинга событий. Какие они?

Юдин Алексей

Директор по корпоративным продуктам

План доклада

— Проблемы и задачи решаемые системой мониторинга
— Вопросы сбора событий с различных источников
— Приоритезация событий – как понять что важно
— Инфраструктура системы в крупных и распределенных сетях
— Централизованное управление распределенной системой
— Хранение и работа с событиями
— Аналитическая поддержка системы
— Оперативное реагирование на инциденты
— Количество и качество персонала для работы с системой

Проблемы

— Получение, обработка и хранение событий от зоопарка источников
— Классификация, категоризация …. приоритезация событий
— Оперативные оповещения
— Отслеживание новых атак в системе
— Отсутствие ресурсов на управление и поддержку системы
— Отсутствие квалификации
— Масштабные инсталляции. Как поддерживать?
— Мощная аналитика или рутинная работа?
— Интеграция системы в общую структуру

SIEM = 

— Самостоятельно настраивается и собирает все события со всех источников

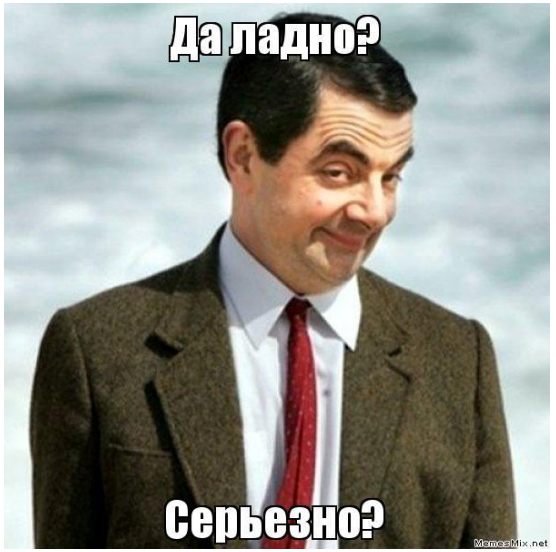
— Самостоятельно агрегирует, приоритезирует, коррелирует, формирует инциденты

— Самостоятельно отслеживает состояние своих компонентов

— Самостоятельно отслеживает новые угрозы

— Говорит кого сломали и бежит с радостной новостью к администратору

— Работает из коробки!



Сбор событий

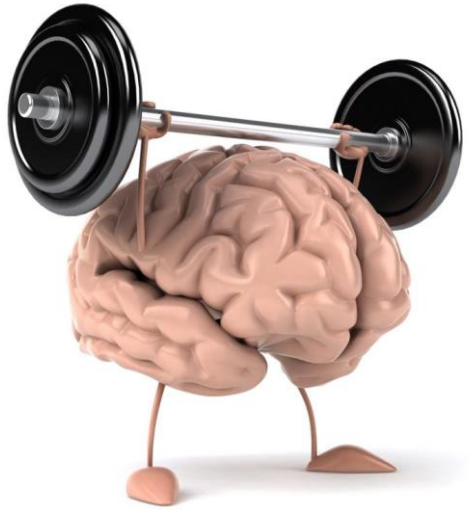
— Настройка источников = ИТ админы
— Получение учетных записей = ИТ админы
— Настройка коннекторов = оператор системы
— Отслеживание потока событий = оператор в режиме 24/7
— Нетиповые источники = ведущий аналитик
— Ограничения каналов связи = оптимизация потока данных
— Правила нормализации =партнер,аналитик ?
— Правила фильтрации и агрегации = ?

Сбор событий. Что нужно

— Готовые конфиги и скрипты для настройки источников
— Централизованная система управления доступом ко всем устройствам, серверам и рабочим станциям
— Система помощи по настройке коннекторов и отслеживанию их состояния
— Мониторинг потока событий с оповещением оператора о проблемах с доступом к источнику или аномалиях в потоке
— Легкое заведение нетиповых источников
— Автоматическая фильтрация и агрегация событий – только критичные события участвующие в запросах или корелляциях
— Автоматизированные механизмы типизации

Приоритезация событий и инцидентов

— Много входных данных
— Отслеживание современных тенденции атак
— Отсутствие времени на разработку и тестирование правил корреляции
— Отсутствие проверенных баз знаний с правилами корреляциями
— Наличие экспертизы по особенностям работы всех типов информационных систем
— Высокие требования к знаниям в области ИБ
— Оперативное отслеживание изменений в инфраструктуре
— Понимание критичности своих активов
— Поддержка справочников для корреляций



Приоритезация. Что нужно

— Понимание своей инфраструктуры
— Поддержка базы правил корреляции из внешних баз знаний / обмен знаниями с коммьюнити
— Автоматические правила корреляции
— Выявление аномалий по статистическим признакам
— Группировка похожих событий и инцидентов
— Оценка критичности события по метрикам объектов
— Историческая корреляция с учетом уязвимостей, векторов атак , состояния активов на тот момент времени

Реагирование на проблемы

— Оповещение всеми доступными способами
— Временное блокирование подозрительных активов
— Правильный процесс реагирования на инциденты
— KnowledgeBase проведенных мероприятий и лучших практик
— Лучшее реагирование – предотвращение !
— Создание команд оперативного реагирования

Инфраструктура. Хранение. Поддержка

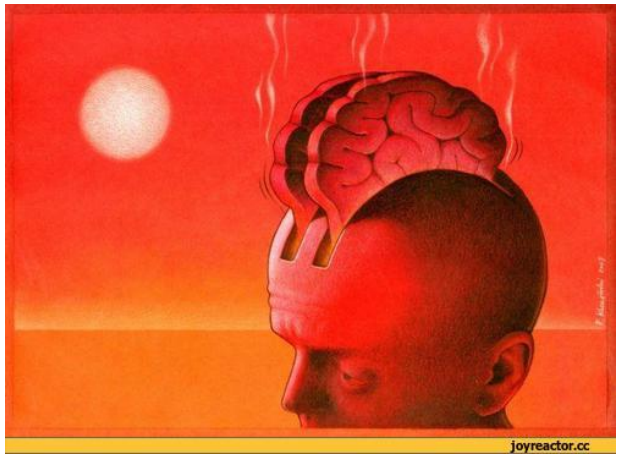
— Где развернуть компоненты системы?
— Виртуальные сервера или физические?
— Закладывать ли в систему масштабирование или докупить необходимое потом?
— Как понять какие особенности есть при хранении событий?
— Будет ли меня поддерживать производитель с моим функционалом?
— Система не работает, куда бежать?
— Невозможность заранее просчитать поток событий
— А может проще положить систему на полку?

Инфраструктура. Хранение. Поддержка

— Виртуализация – наше все
— Прозрачное масштабирование системы
— Возможность увеличения производительности и объема хранилища без докупки лицензий
— Оптимизация передачи данных по слабым каналам связи
— Возможность доработки продукта производителем
— Использование новых технологий в анализе и обработке событий
— Возможность удобного разворачивания и настройки системы
— Программы обучения персонала и обмена опытом
— Оперативная поддержка

Централизованное управление

— Представим что оператор один
  - Хорошо когда у оператора одна система на 500 пользователей с парой коннекторов
  - Плохо когда это гроздья серверов с парой сотен сборщиков
— Нужно обновить правила корреляции и нормализации на всех компонентах
— Один из наших офисов на 1000 человек переезжает
— У нас реструктуризация сети!
— Что-то происходит с удаленным филиалом в Новом- Уренгое…но я не могу подключиться по удаленке!
— Нужно быстро развернуть 10000 агентов…



Централизованное управление

— Централизованное управление всеми компонентами системы (один человек управляет инфраструктурой на 10000 источников)

— Централизованный мониторинг всех показателей работы компонентов

— Централизованное распределение баз знаний и настроек по всем компонентам

— Управление не только сборщиками, но и серверами

— Мониторинг и управление интеграционной обвязкой

Требования к персоналу

— Кого проще найти - 20 аналитиков или 5 мега гуру ?

— Сколько может сидеть среднестатистический человек перед монитором, не отрываясь каждый день ?

— Нужен ли четкий процесс и регламент расследования и что делать в экстренных случаях ?

— Как посчитать сколько нужно человек на эффективную работу системы?

— Как померить эффективность работы персонала?

— Как снизить человеческий фактор?

POSITIVE TECHNOLOGIES