Мониторинг ИБ в организации

- Сложности внедрения мониторинга.
- Куплю SIEM. Это решит проблему?
- Чего вы достигните благодаря мониторингу?
- Какие есть варианты?

Мониторинг ИБ сегодня

Проблемы:

- Количество киберугроз неуклонно растет
- Объем информации циркулирующей на предприятиях постоянно увеличивается
- Большое количество рассредоточенных информационных ресурсов увеличивает время реагирования

Требуется:

- Механизм сбора/обработки информации, оповещения о важных событиях, а также хранения данных для их анализа
- Комплексный подход в сфере реагирования и расследования инцидентов
- Единое централизованное решение

Есть SIEM! Проблема мониторинга решена?

- Покупка экспертизы неизбежна
- Требуется настроить правила корреляции и заниматься их оптимизацией
- SIEM не расскажет о процедурах, которые необходимо провести в организации (инвентаризация, наведение порядка, четкие процедуры реагирования и др..)
- Знаем только о себе (отсутствует перекрестный обмен опытом об атаках)

Какие есть варианты?

Свой центр мониторинга

- Независимость
- Возможность в дальнейшем развивать как услугу
- Покупка дорогостоящего оборудования и инструментов
- Необходимость найма большого количества дорогих квалифицированных специалистов

Готовая услуга

- Ясные модели реагирования
- Опытные специалисты
- Информация об атаках из «чужого» и накопленного своего опыта
- Относительно небольшие операционные затраты
- Данное направление не развивается в организации заказчика (зависимость)
- Зачастую необходим

Частичный аутсорс

- Избавление от черновой работы
- Возможность использования чужих мощностей
- Необходимость найма квалифицированных специалистов 2-ой линии и аналитиков
- Ответственность за итоговое решение

Спасибо за внимание!