GIS DAYS

Экосистемный подход к построению системы ИБ: преимущества в обнаружении и расследовании инцидентов

Вяткин Олег Игоревич

Директор портфеля продуктов

СОЛАР

Что для нас экосистема ИБ-решений

- Глубоко интегрированные продукты
- Модульность, возможность сбора событий ИБ различными решениями при одинаковом формате работы в дальнейшем
- Оптимизация нагрузки на аналитические движки
- Единая логика управления, администрирования и общие подходы к интерфейсам

В чем плюсы для управления инцидентами?

- Повышение покрытия инфраструктуры сенсорами
- Быстрое получение данных по контексту события
- Меньше нагрузка – выше производительность
- Снижение когнитивной нагрузки на аналитиков

Общие сенсоры. Повышение покрытия

- Отсутствие конфликтов агентских модулей
- Экономия ресурсов хостов
- Возможность создания единой системы менеджмента
- Сбор данных с большей части инфраструктуры
- Упрощение развертывания более продвинутых сенсорных модулей

Кросс-обогащение и подтверждение инцидентов

- Кросс-обогащение данных - использование информации из разных источников для более точного анализа инцидентов
- Уменьшение нагрузки при обработке за счет снижения роли ресурсоемких кросс-корреляций
- Оптимизация процесса работы – меньше переключений между различными консолями

Оптимизация нагрузки при анализе

- Общие аналитические модули для решений разных классов
- Единая база информационных активов
- Возможность распределить нагрузку на аналитические модули, требующие больших ресурсов, в первую очередь, использующие ML

Видение экосистемного подхода

- Модульные универсальные агенты
- Максимальное использование общих сетевых сенсоров
- Единые форматы событий, инцидентов и иных сущностей
- Использование централизованных аналитических компонентов

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1

SOLAR