hef tech

Где будет наш инфобез через 5 лет?

Денис Андреевский

Генеральный директор
ООО Гефест Технолоджиз

Ключевые направления, в которые пойдем:

1. Интеграция
2. Автоматизация процессов
3. Экспертность систем
4. Расширение контекста ИБ
5. Интеллектуальность обработки ML & AI, XDR
6. Сертификация. Атаки на цепочки поставок

Главные сферы автоматизации:

1. Аналитика – связанные с инцидентом сущности (артефакты атаки)
2. Доуточнение типа и реальных границ атаки
3. Kill Chain – определение текущей стадии атаки
4. Категорирование инцидента
5. Киберразведка (IOC – м.б. малый срок жизни). Связка с TTP и Базовой моделью угроз (Не только ИСПДН)

Мало кто такой уровень зрелости в Заказчике может поддержать

Не считаем команды MSSP. Заказчика нужно развивать.

Система д.б. экспертной, с пресетами:

1. Правила корреляции
2. Планы реагирования (Playbooks)
3. Сценарии атак
4. Актуальная модель угроз (контроль изменения ландшафта). Отдельно, ИТ- процессы: управления активами, изменениями, уязвимостями
5. Прозрачные способы актуализации перечней: где взять, как сформировать, проверить работоспособность

Определенный уровень паранойи: чем не управляем, какие инциденты не способны предотвратить.

Кадровый вопрос

Обучение ИБ. Лет 5 обучения + 2 опыта – свежая кровь в инфобезе. Учиться просто ИБ, абстрактному?

Документы, сетевая безопасность, администрирование СЗИ

Программа обучения. Структура ИБ – Специализации:

1. Методология (Регламенты, процессы угрозы, риски)
2. Аудиты, пентесты.
3. Администрирование СЗИ
4. SOC (Мониторинг, реагирование, L1, L2, L3)
5. Архитектор ИБ
6. Аналитика и киберразведка (гипотезы, поведенческие инструменты)

Как помочь регуляторам в ИБ:

1. Выпущено большое количество законов и подзаконных актов в области ИБ
2. Обязательность исполнения требований (не через пару лет, а сейчас)

Нужно идти дальше!

В качестве подсказки Уважаемым Регуляторам:

Протоколы проверок пора усовершенствовать. Два примера из КИИ 187 ФЗ. Успешное прохождение аудита, в первом случае не было функции как таковой, во втором нет SOC, взаимодействия с ГОССОПКА

Отраслевые центры ГОССОПКА: Базовые модели угроз, сценарии атак, сценарии реагирования.

Конкурировать с лучшими зарубежными образцами. За рамками локального рынка.

ML & AI – не подорожник для всего, а Система принятия решений автоматизации аналитики, реагирования, киберразведки .

Спасибо за внимание!

Вопросы?