

ОСОБЕННОСТИ ПРИМЕНЕНИЯ SOC, SOAR, IRP В ТЕКУЩИХ УСЛОВИЯХ

КОНСТАНТИН САМАТОВ

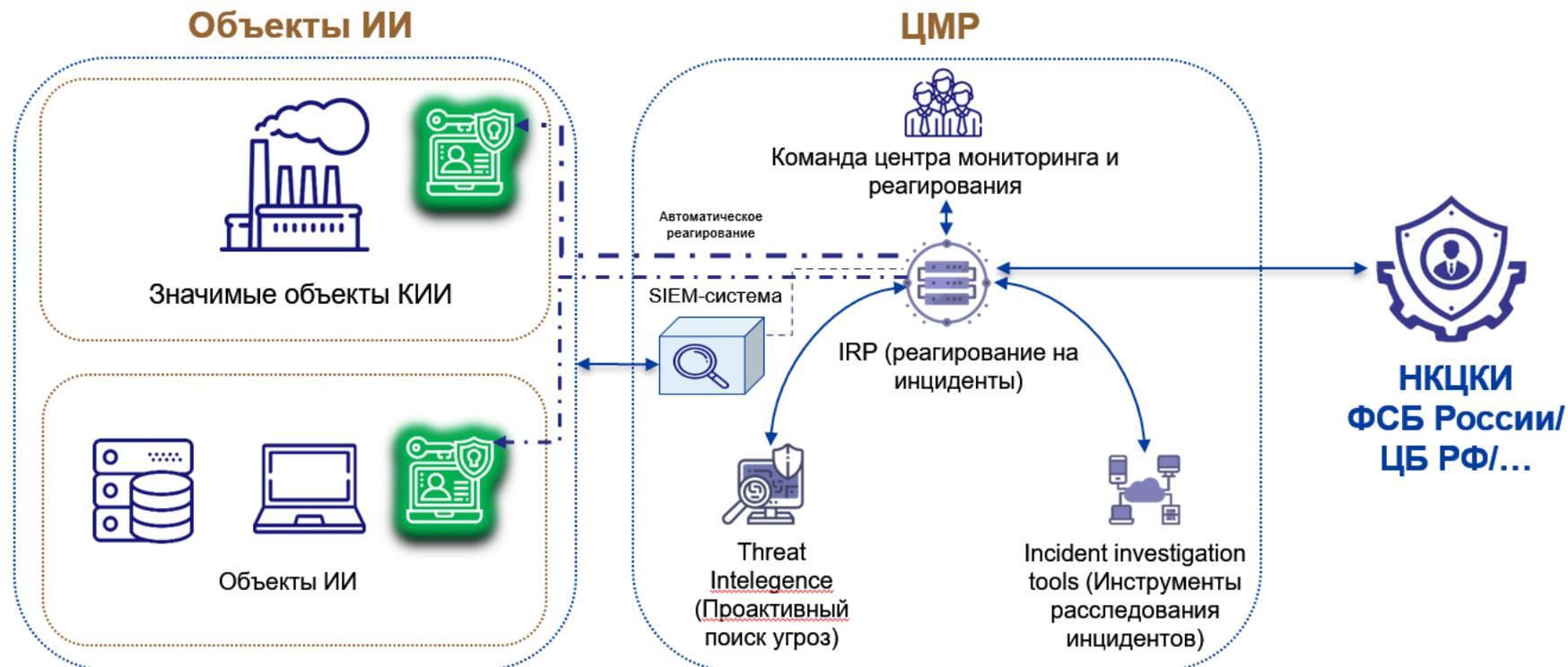
Член Правления Ассоциации руководителей служб информационной безопасности

ИМПОРТОЗАМЕЩЕНИЕ АББРЕВИАТУР

Security Operation Center (SOC) – Центр мониторинга и реагирования на инциденты информационной безопасности (ЦМРИИБ) или КЦ ГосСОПКА (подвид)

Security Orchestration, Automation and Response (SOAR) – система автоматизации реагирования на инциденты ИБ (САРИИБ)

Incident Response Platform (IRP) – платформа автоматизации реагирования (расследования) на инциденты ИБ (ПАРИИБ)



ОСОБЕННОСТИ ТЕКУЩИХ УСЛОВИЙ



Массовые атаки

(Бот) Сканирование внешнего периметра

Вредоносные спам рассылки

Роботизированный фишинг

Атаки направленные на отказ в обслуживании (D(D)OS)



Таргетированные атаки

Распространение вредоносных файлов (программ) через фишинговые рассылки

Проникновение в локальную сеть

Эксплуатация уязвимостей

Целенаправленные атаки АРТ-группировками (Advanced Persistent Threat)

Атаки через поставщиков

Сотрудник ГРИИБ



Счастливым
Довольным
Востребованным

Особенности применения ЦМР

КАК ВЫБРАТЬ СОК: ЧИТАЕМ УПАКОВКУ

Смотрим на функции

Взаимодействие с персоналом
и пользователями

Обнаружение КА и КИ

Обслуживание технических
средств ЦМР

Оценка (анализ)
защищенности

Расследование КИ

Яблочный сок
Восстановленный
Осветленный

Состав:

Пищевая цен

Углеводы — 11 г,
Энергетическая ценность
48 ккал (204 кДж).
** средние значения

1 литр

Годен до:
31.10.2016

Аналитика угроз

Техническая экспертиза

Правовое обеспечение

Менеджмент/руководство

Нет СОКа



Особенности применения САРИИБ (SOAR) и ПАРИИБ (IRP)



Жесткие настройки по рекомендациям регуляторов



Не решает организационные вопросы: реагирование на КА и КИ в нерабочее время

Стандартные алгоритмы реагирования (playbook) не работают

Нестандартные атаки для которых нет настроек



Спасибо за
внимание!

