IBM Security

IBM Security

Комплексное решение SOC

Олег Бакшинский
Ведущий советник по вопросам
информационной безопасности

Потенциальный заказчик SOC in a Box

- Планируется построение SOC
- В компании присутствуют различные СЗИ, которые хотелось бы объединить в единую систему мониторинга и реагирования на инциденты
- Средняя или крупная организация с разветвленной филиальной сетью
- Возможно создание внутреннего MSSP (сервис ИБ внутри организации/между юр.лицами)
- Нет желания тратить 2-3 года для создания уникального SOC, нужен быстрый результат (6-12 месяцев)

Комплексное решение - SOC in a Box

- Решение представляет собой интегрированный комплекс MSSP SOC с поддержкой множества организаций (multi-tenant) на базе продуктов IBM Security: QRadar, Resilient , X-Force с опциональным добавлением продукта IBM i2 для задач расследования угроз, а также возможностью интеграции с продуктами Guardium (защита данных), Secret Server (контроль привилегированных пользователей) и Verify (учетные записи)
- Решение включает в себя продукты и компоненты интеграции, позволяющие построить полнофункциональный SOC, включая панели управления, сценарии инцидентов, отчеты и процедуры реагирования на выявленные инциденты
- В процессе демонстрации SOC предоставляются 3 типичных модели экрана, интерактивные панели:
  1) Администратора SOC
  2) Аналитика SOC
  3) Администратора панели дочерней/обслуживаемой организации.

QRadar + Resilient = SIEM + SOAR

QRadar
Приоритезация информации из Logs, Flows, Vulns, User, Config Data и т.п.

Процесс реагирования SOC на инцидент ИБ для ответа на угрозы, дыры, уязвимости

Создание инцидента
- Присвоение типа (напр. уязвимость)
- Присвоение бизнес характеристики в зависимости от типа (напр. Риск)

Сбор контекста и назначение задач
- Сбор дополнительных доказательств
- Применение требований регуляторов
- Назначение задач ответственным

Восстановление и Закрытие
- Постановка задач восстановления команде
- Подтверждение восстановления
- Закрытие инцидента
- Отчет/Уведомление

База всех инцидентов ИБ

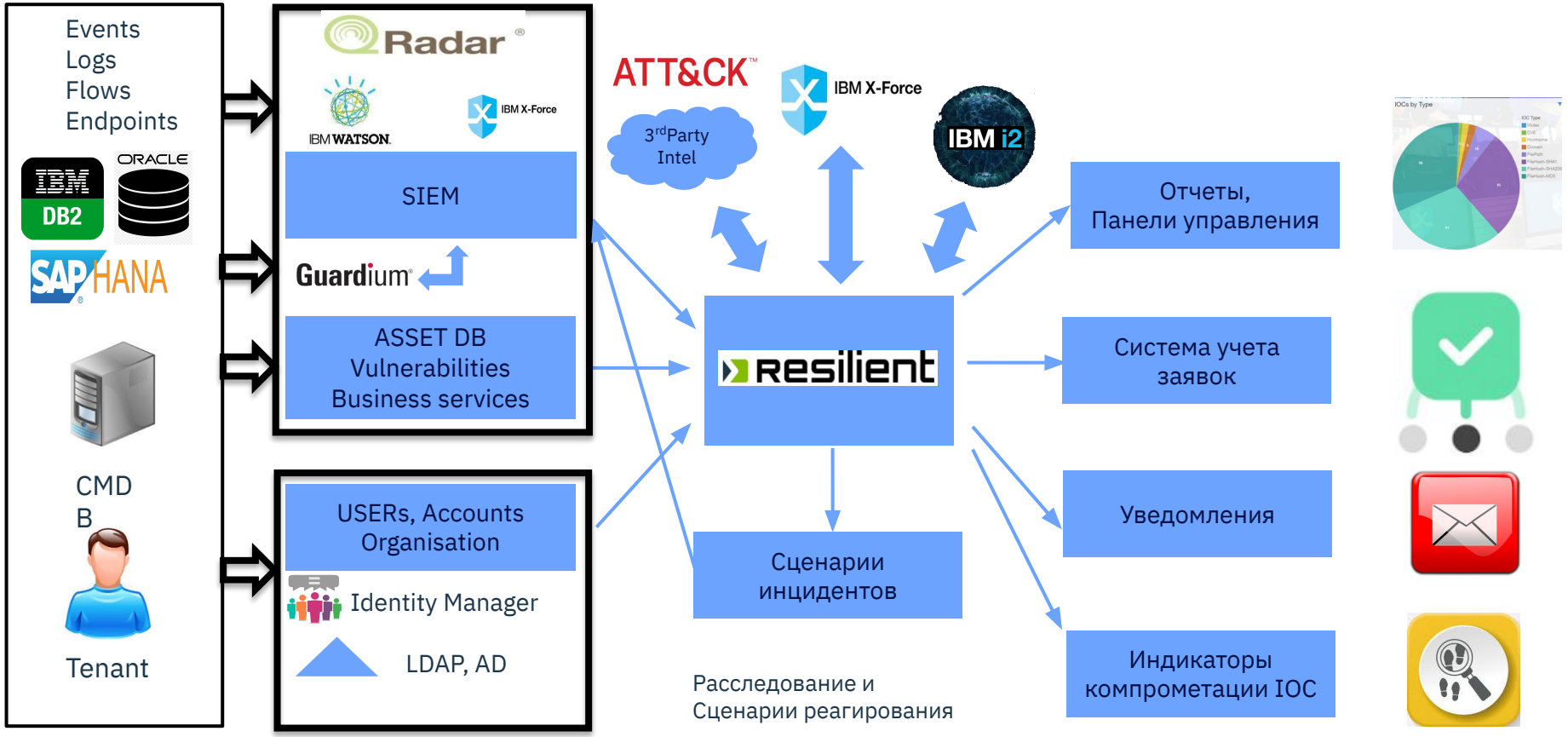
Постоянная аналитика ИБ

Три этапа инцидента ИБ

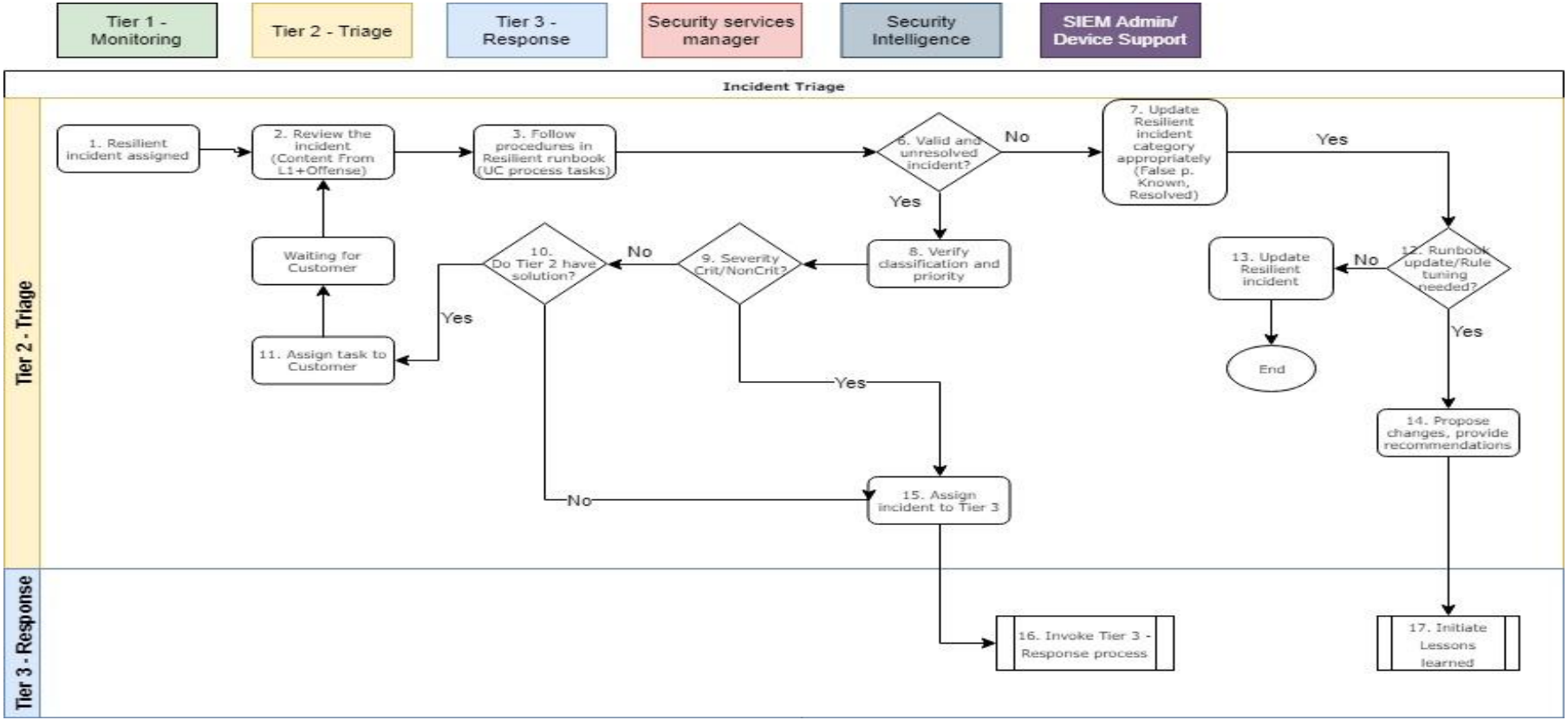
Отчет по инциденту и уведомление

Улучшение процесса выявления инцидентов

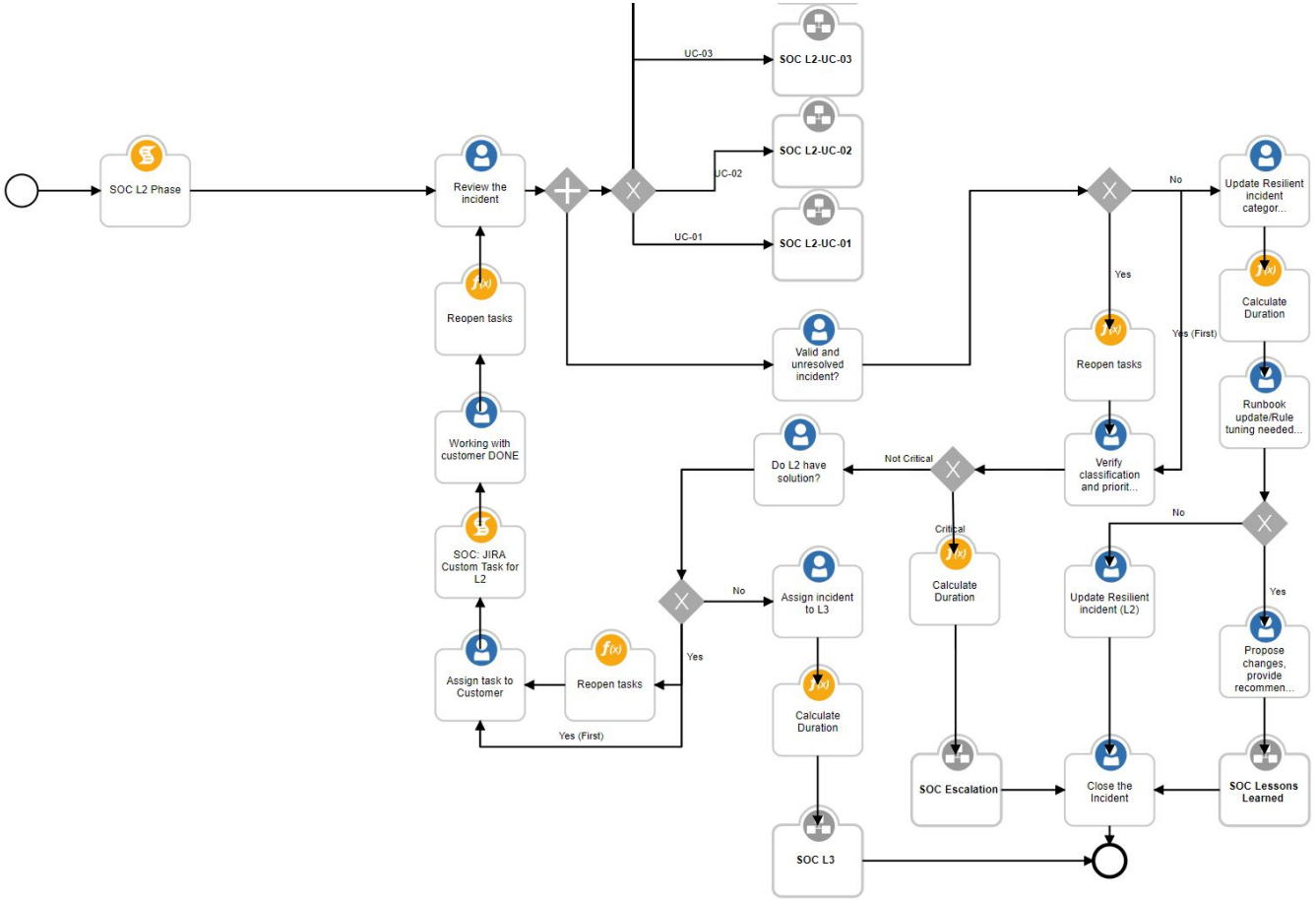
Верхнеуровневая архитектура SOCIB и его компоненты



Рабочие процессы и роли SOCIB

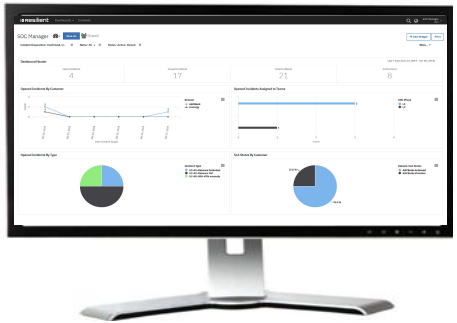


Рабочие процессы и роли SOCIB



Интерактивные панели сотрудников SOCIB

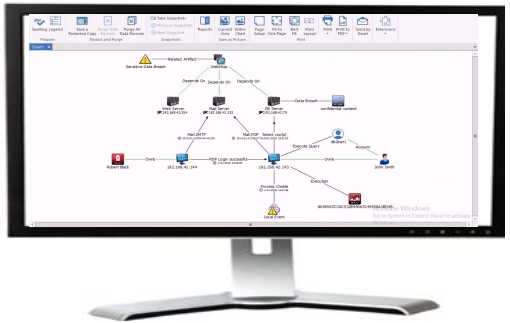
Администратор SOC



Оперативная деятельность SOC и KPI

Список инцидентов и Активностей по каждой организации

Аналитик SOC

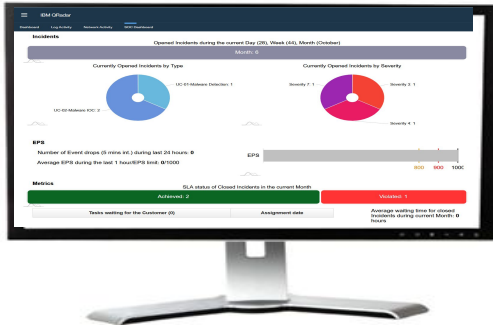


Реагирование на инциденты по сценариям в QRadar, Resilient, X-Force

Работа аналитиков L1, L2, L3

Расследования инцидентов с помощью i2

Дочерняя организация



Актуальный статус ИБ в дочерней организации

Задачи поставленные командой SOC

Коммуникации по заявкам

Отчеты, KPIs , SLAs

Основные преимущества комплексного решения

Комплексная модель SOC в рамках организации

Оптимизация функций различных решений и отсутствие дублирования

Внедрение под контролем вендора

Оптимизация расходов на услуги по установке и поддержке

Оптимизация закупочных процедур и стоимости решений

Больший объем работ в составе комплекса

Дополнительные преимущества комплексного решения

Консалтинг в рамках построения SOC

Методология разработки сценариев инцидентов

Методология разработки регламентов реагирования

Multy Tenant дизайн SIEM и операционной модели SOC

Разработка HA/DR моделей и тестирование выхода из строя

Проверенные на практике интеграции в рамках сценариев инцидентов

IBM Security

СПАСИБО

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM