

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.

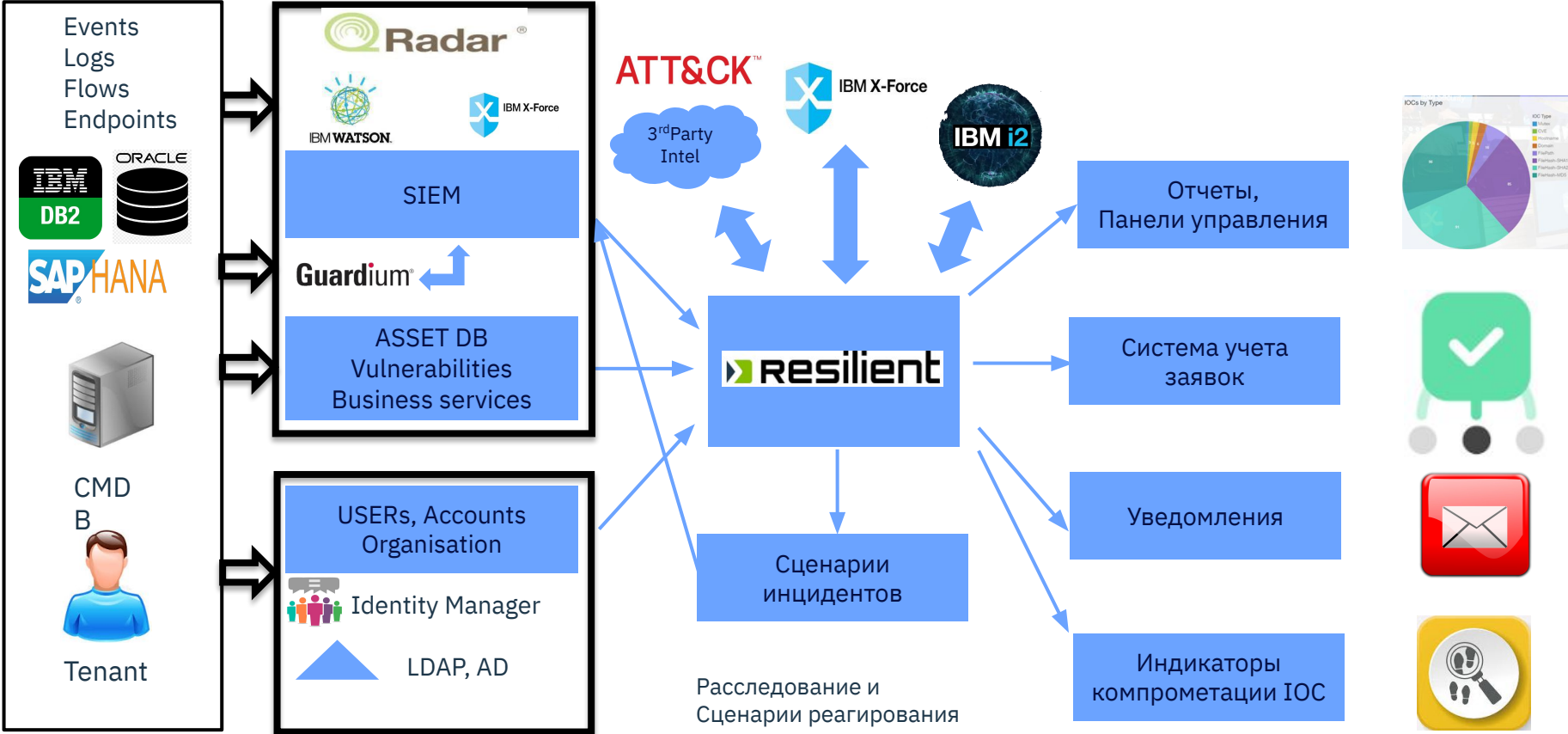
QRadar + Resilient = SIEM + SOAR

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



Верхнеуровневая архитектура SOClB и его компоненты



Рабочие процессы и роли SOCIB

Tier 1 - Monitoring

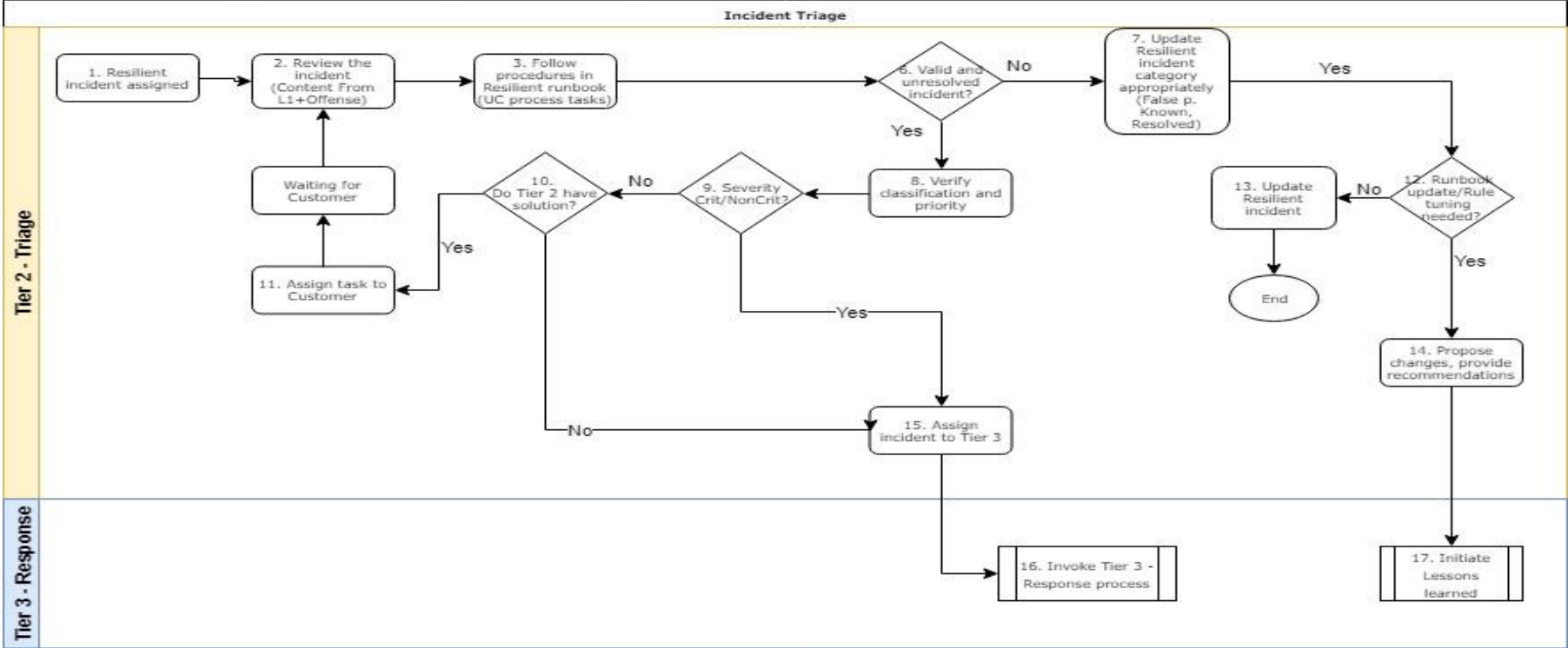
Tier 2 - Triage

Tier 3 - Response

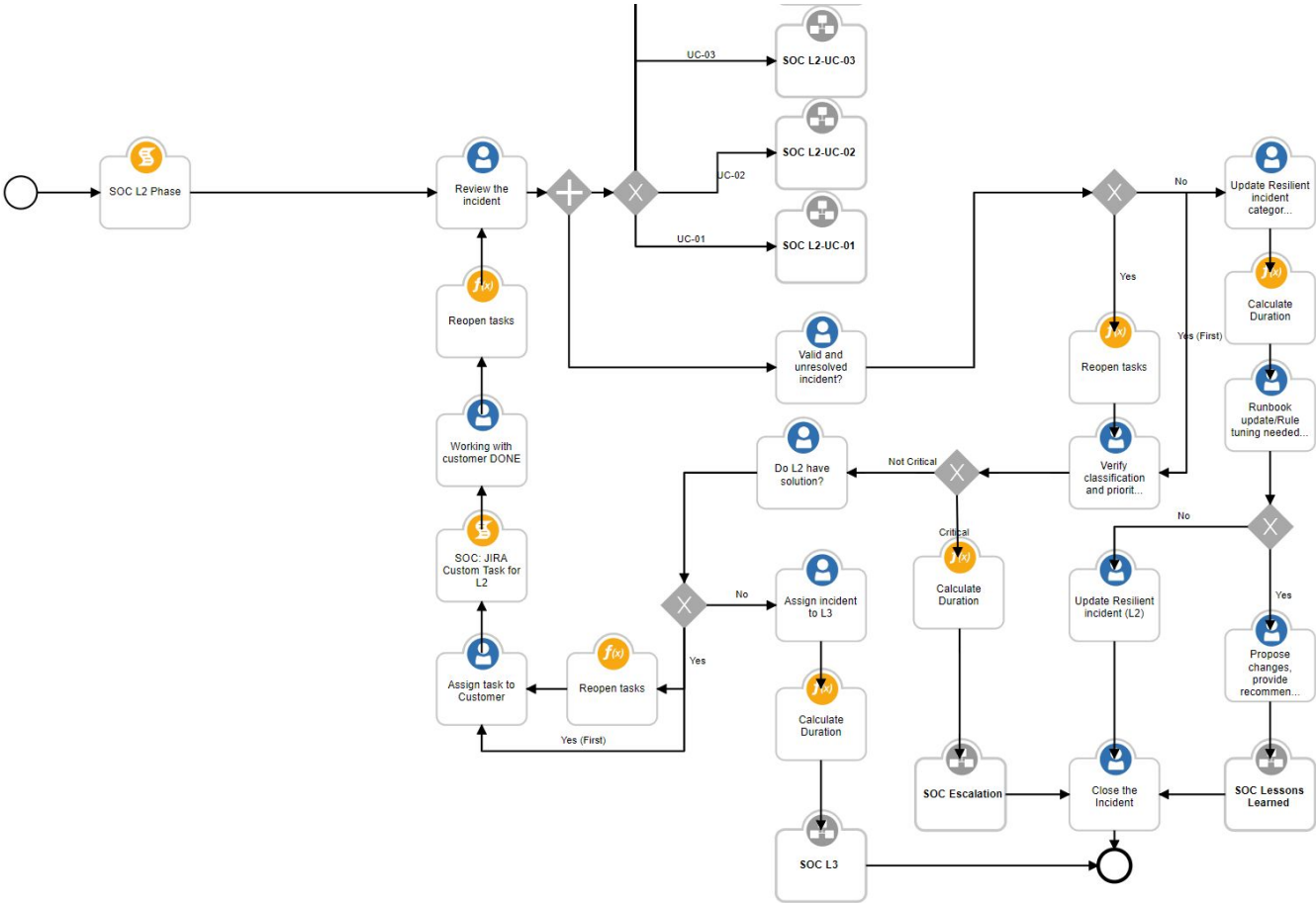
Security services manager

Security Intelligence

SIEM Admin/ Device Support



Рабочие процессы и роли SOCIB



Интерактивные панели сотрудников SOCIB

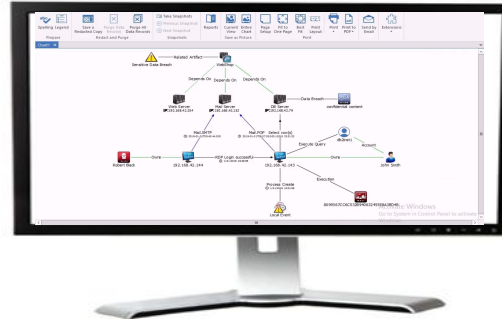
Администратор SOC



Оперативная деятельность SOC и KPI

Список инцидентов и Активностей по каждой организации

Аналитик SOC

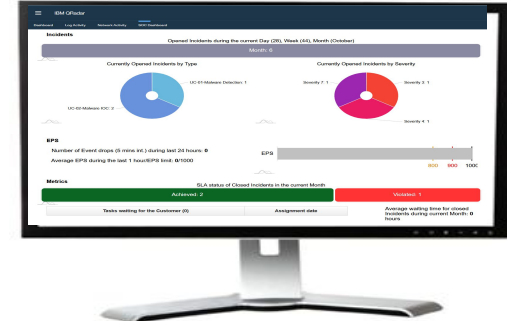


Реагирование на инциденты по сценариям в QRadar, Resilient, X-Force

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

Большой 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

СПАСИБО

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  ibm.com/security/community
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions



© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.