нетология

Best practices современной информационной безопасности

Алексей Федин

Алексей Федин

Ведущий инженер
по информационной безопасности

Алексей Федин

План занятия

1. Предисловие
2. SIEM
3. SOC
4. DMZ
5. Особенности компаний
6. DevSecOps
7. Итоги
8. Домашнее задание

Предисловие

Предисловие

На этом занятии мы:

- рассмотрим **современный взгляд на информационную безопасность**;
- узнаем, зачем нужны SIEM и SOC;
- поговорим об SDLC.

SIEM

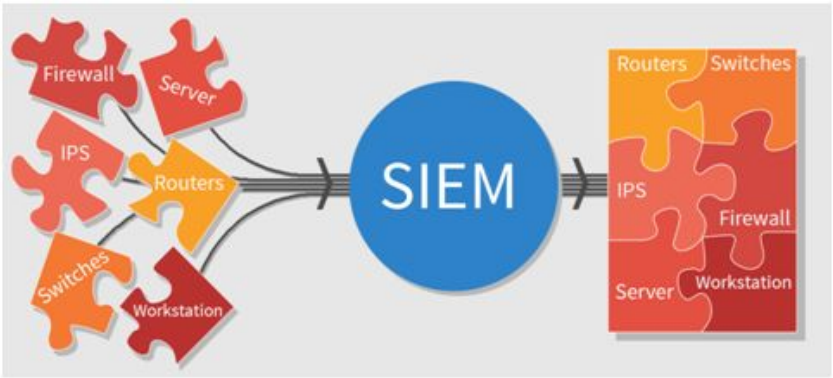
SIEM

SIEM (Security Information and Event Management, управление событиями и информацией о безопасности):

- технология, обеспечивающая анализ в реальном времени событий безопасности элементов информационной системы;
- процесс, объединяющий активность внутри информационной системы в единый набор данных.

SIEM: задачи

- сбор, обработка и анализ событий безопасности в режиме реального времени (логи, трафик);
- обнаружение атак (события, корреляции);
- оценка защищенности ресурсов (данные аудита);
- анализ и управление рисками безопасности (активы);
- проведение расследований инцидентов;
- принятие решений по защите информации;
- формирование отчетных документов.



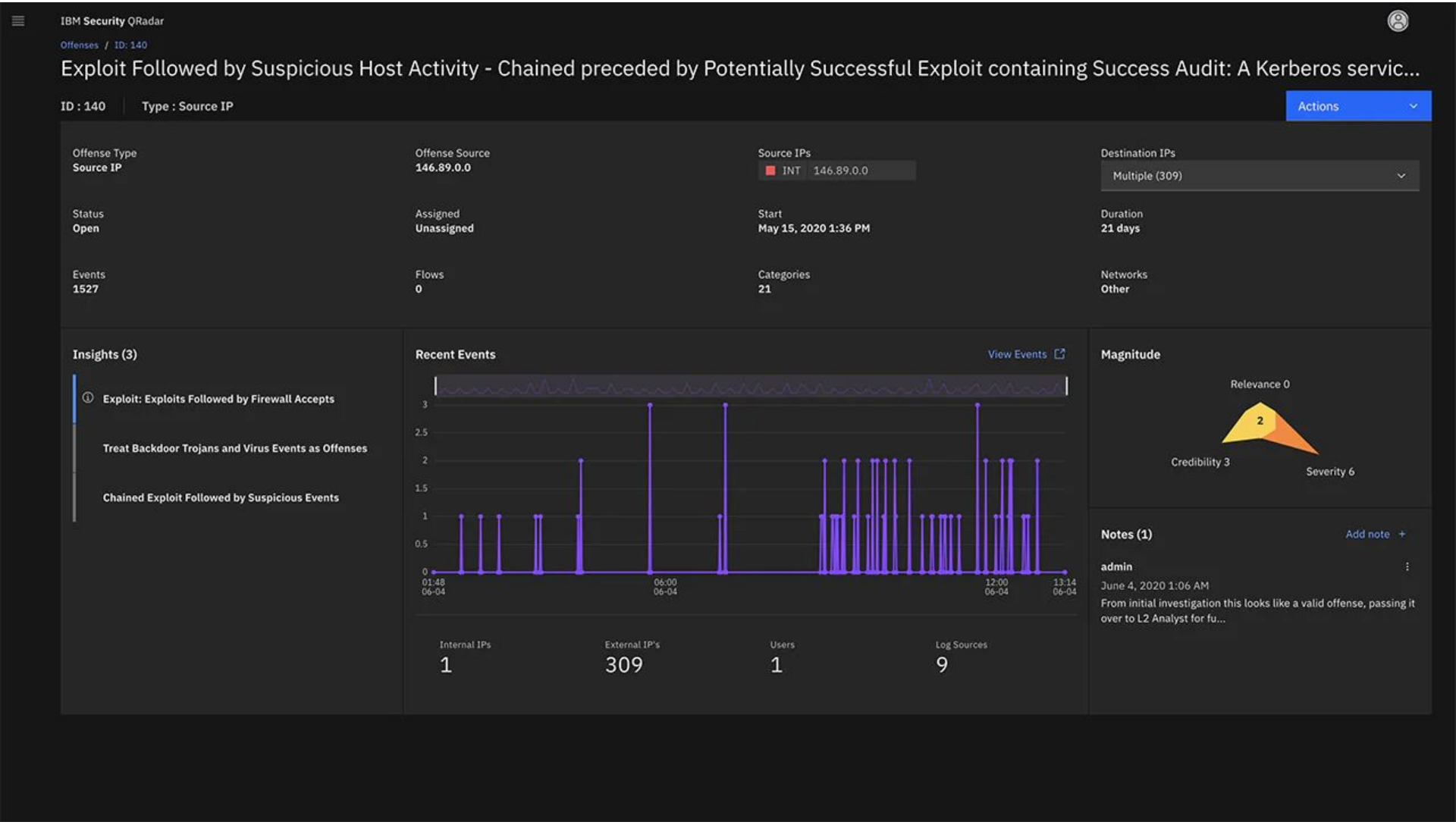
Источник

SIEM: источники данных

- данные аутентификации,
- DLP,
- IDS/IPS,
- антивирусы,
- журналы событий и логи,
- межсетевые экраны,
- активное сетевое оборудование,
- сканеры уязвимостей,
- системы инвентаризации.

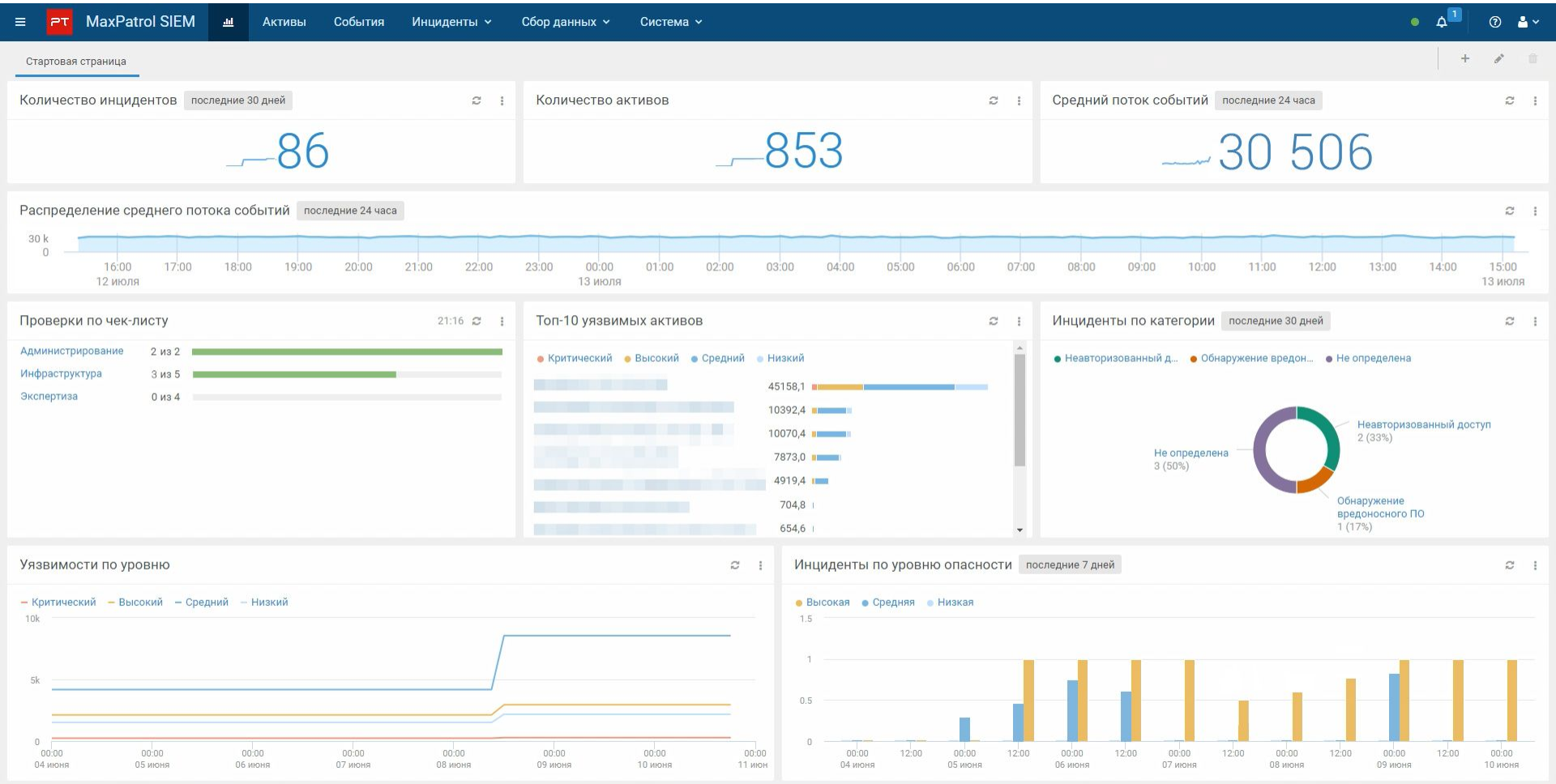
SIEM: примеры

Источник



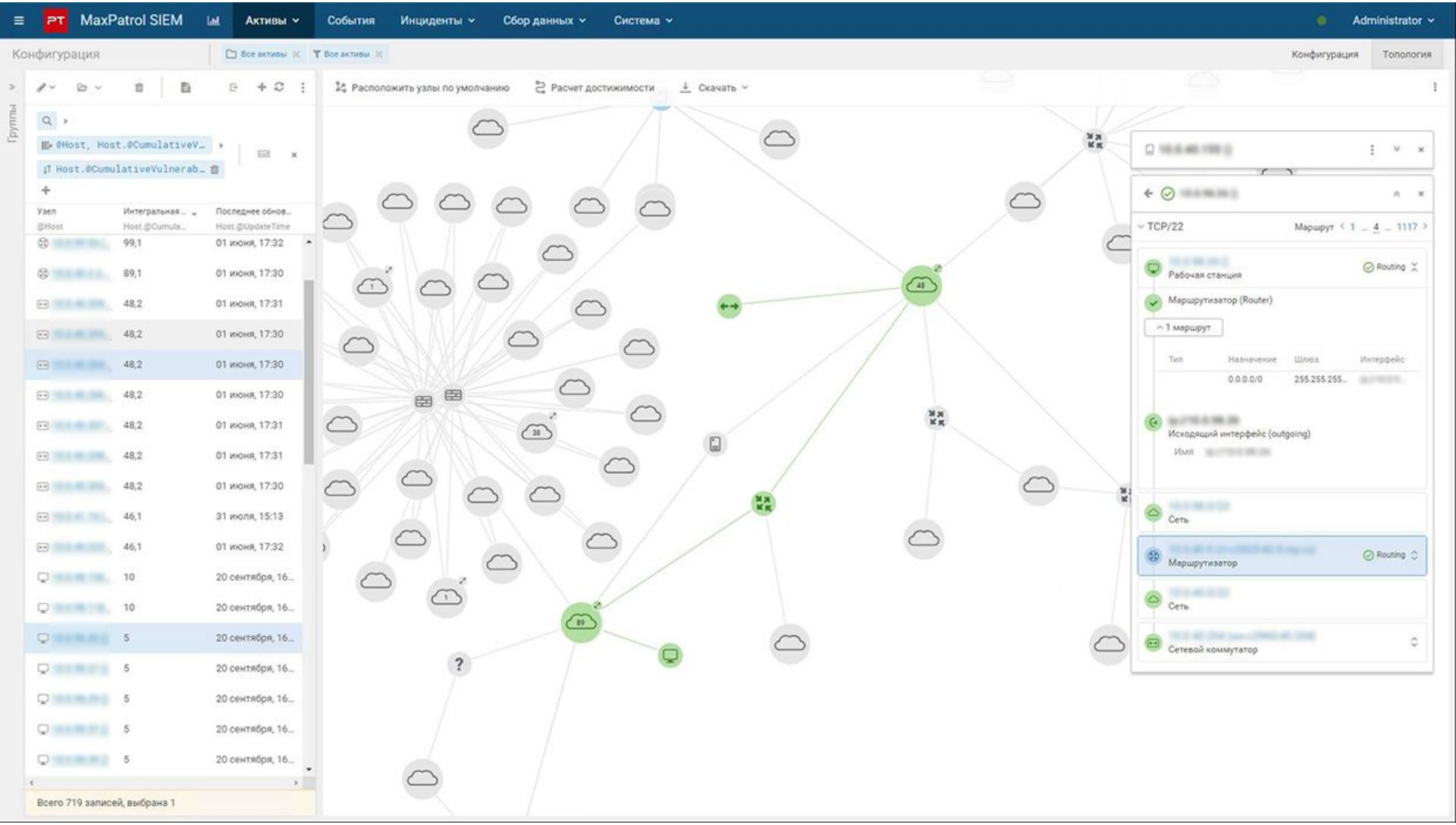
SIEM: примеры

Источник



SIEM: примеры

Источник



SIEM: минусы

- стоимость,
- пассивное средство мониторинга,
- необходим подготовленный персонал (минимум: аналитик + инженер).

SOC

SOC

SOC (Security Operation Center, центр мониторинга кибербезопасности) — это персонал, в задачи которого входит обнаружение, анализ и оперативное реагирование на инциденты кибербезопасности.

Источник

SOC: основные задачи

- мониторинг системы в режиме реального времени (SIEM);
- предотвращение актуальных угроз (сканеры безопасности, отчеты об уязвимостях);
- реагирование на произошедшие инциденты (forensic’a);
- формировать отчетов о состоянии ИТ-системы и системы безопасности.

SOC: возможности

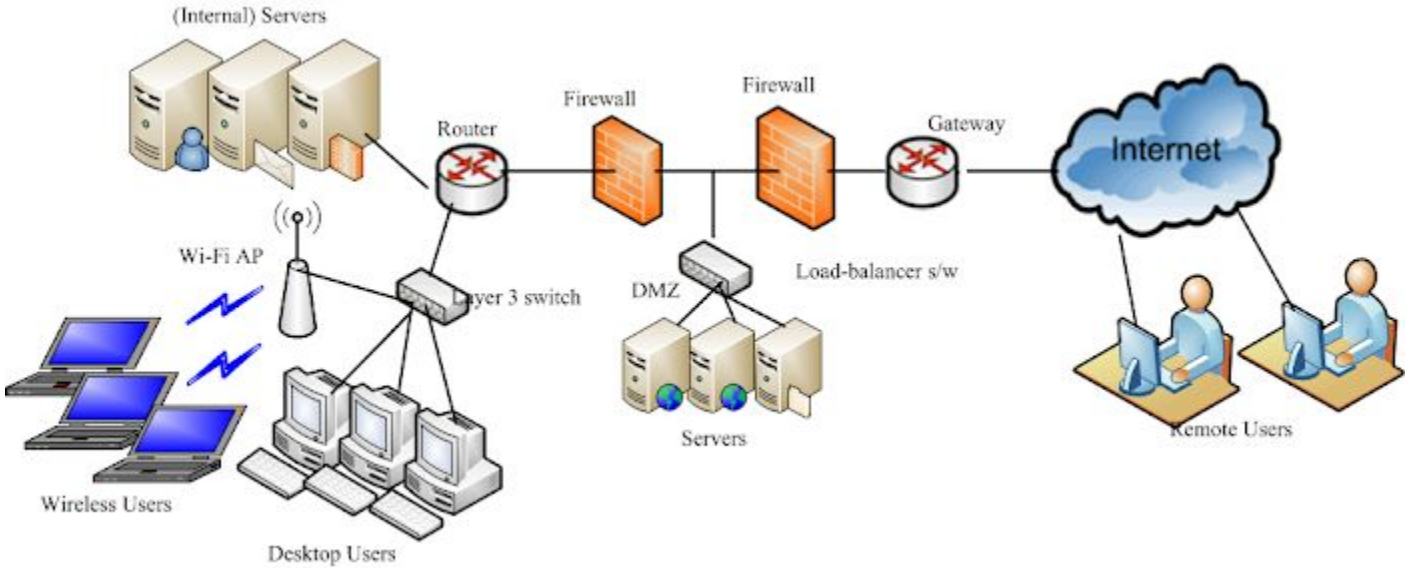
Источник

DMZ

DMZ

DMZ (демилитаризованная зона) — отдельный сетевой сегмент, в котором размещены сервисы, публикуемые в Интернет.

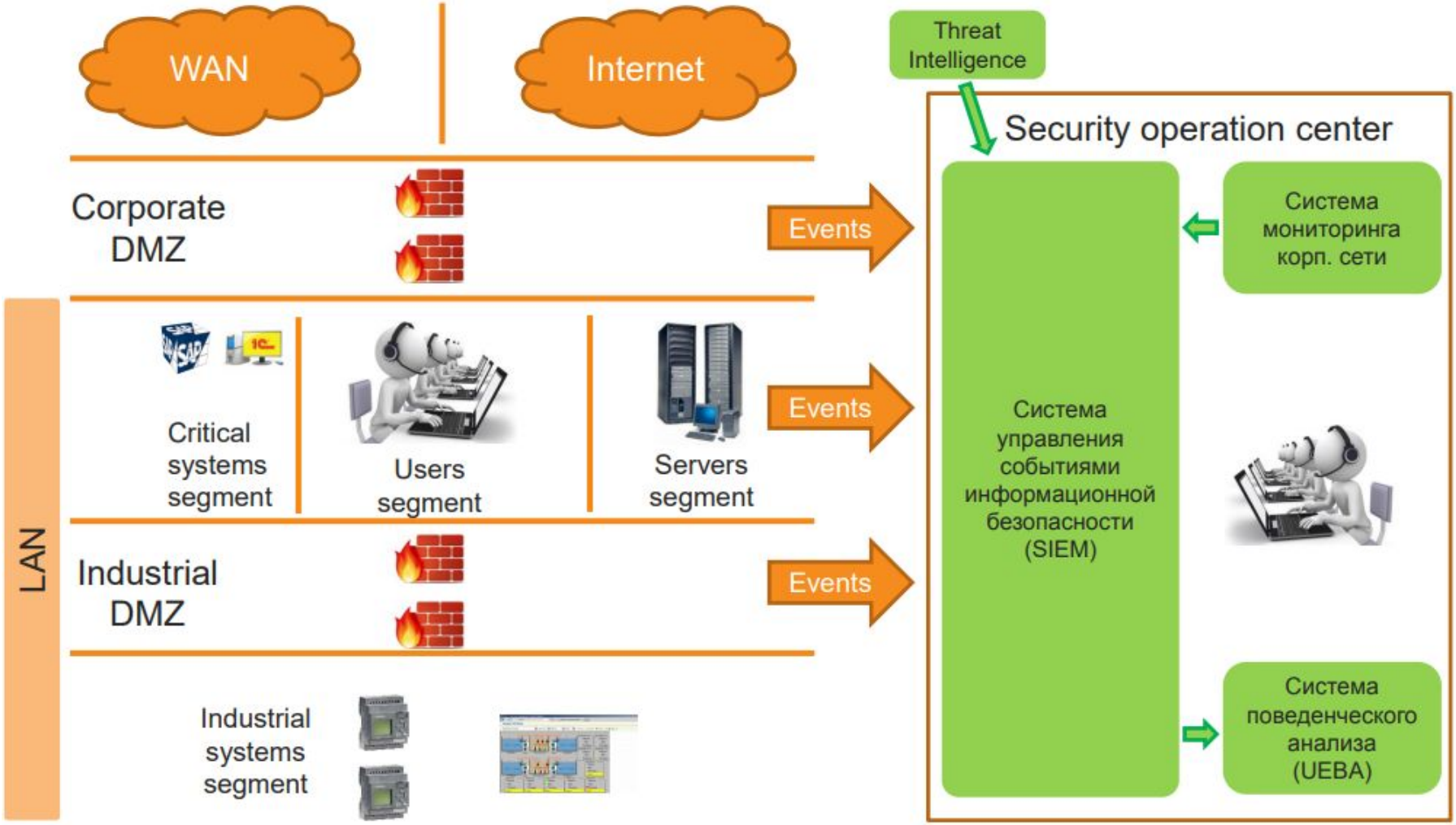
Имеет смысл на стыках Интернет-DMZ и DMZ-сеть компании устанавливать межсетевые экраны разных производителей.



Источник

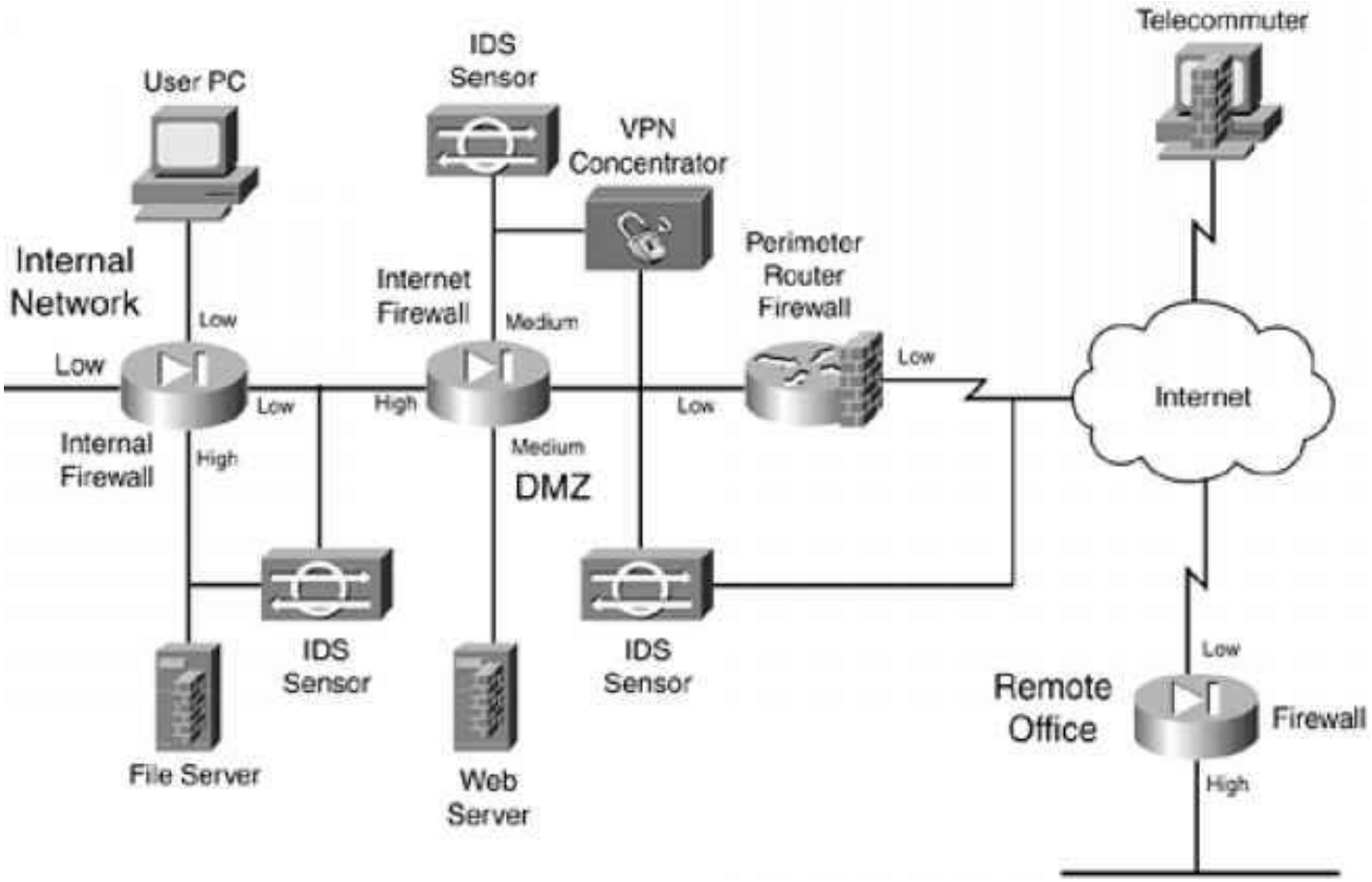
Best practices

Best practices: сегментация сети



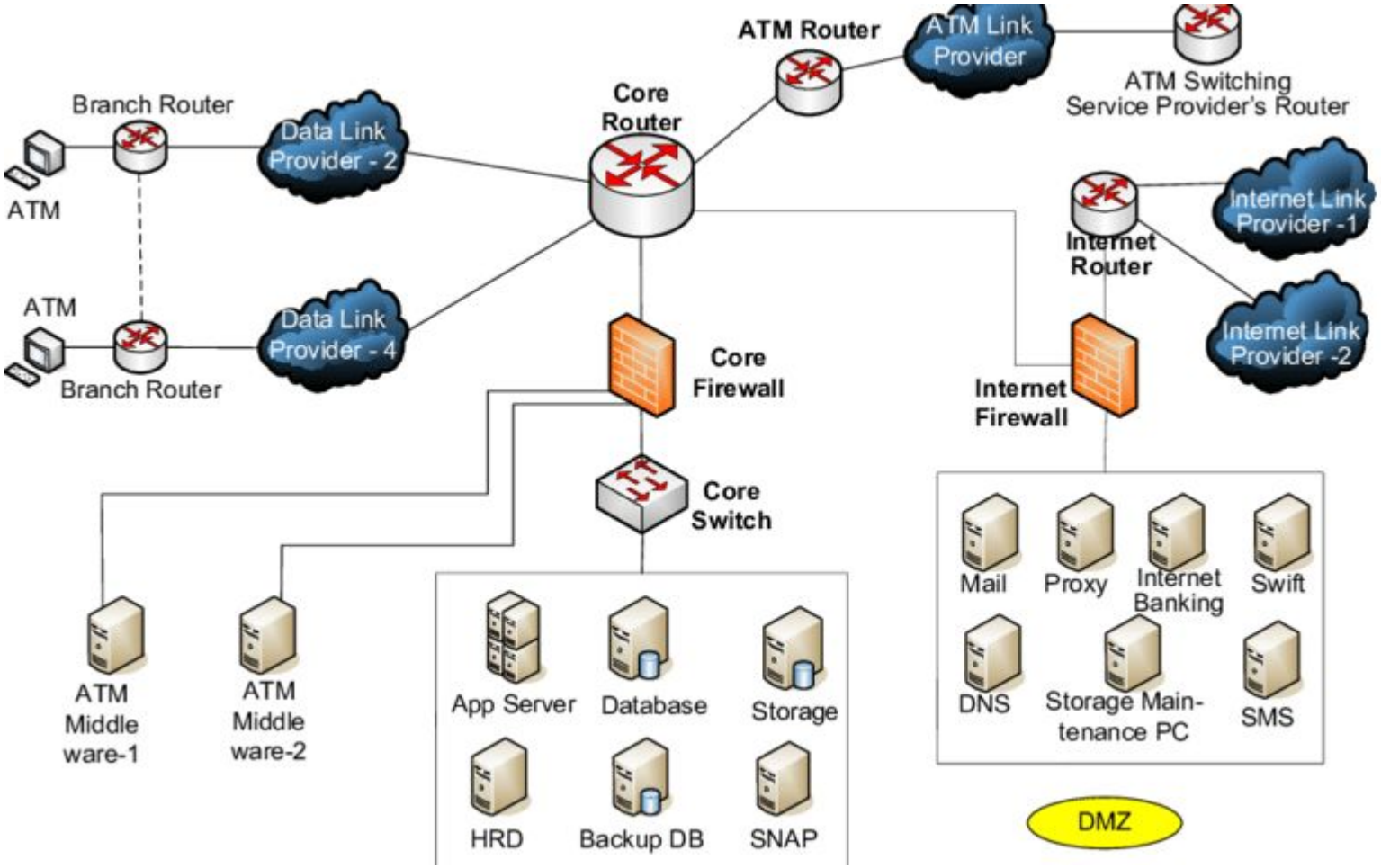
Источник

Best practices: улучшенная защита сети



Источник

Best practices: сеть банка



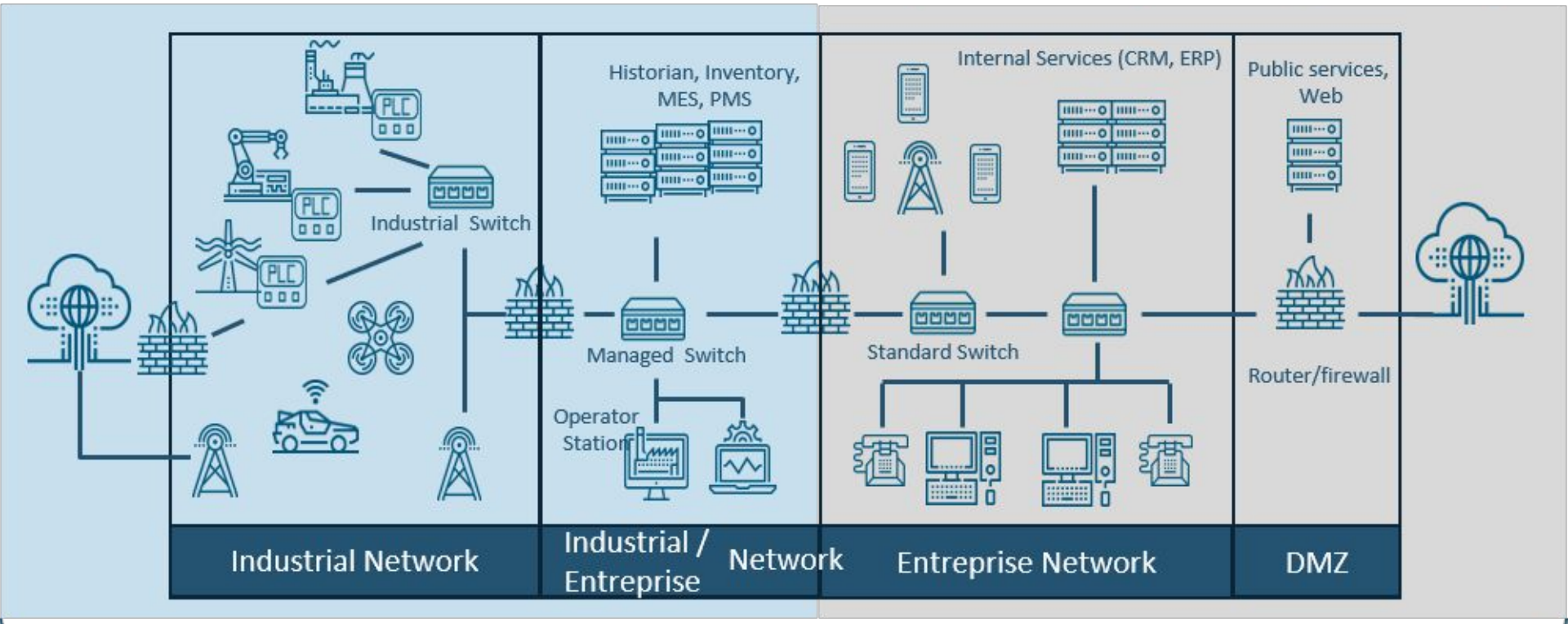
Источник

Best practices: ИБ для АСУ ТП

Operational (OT) Security
(IEC62443, ISO21434, NIST800-82…)

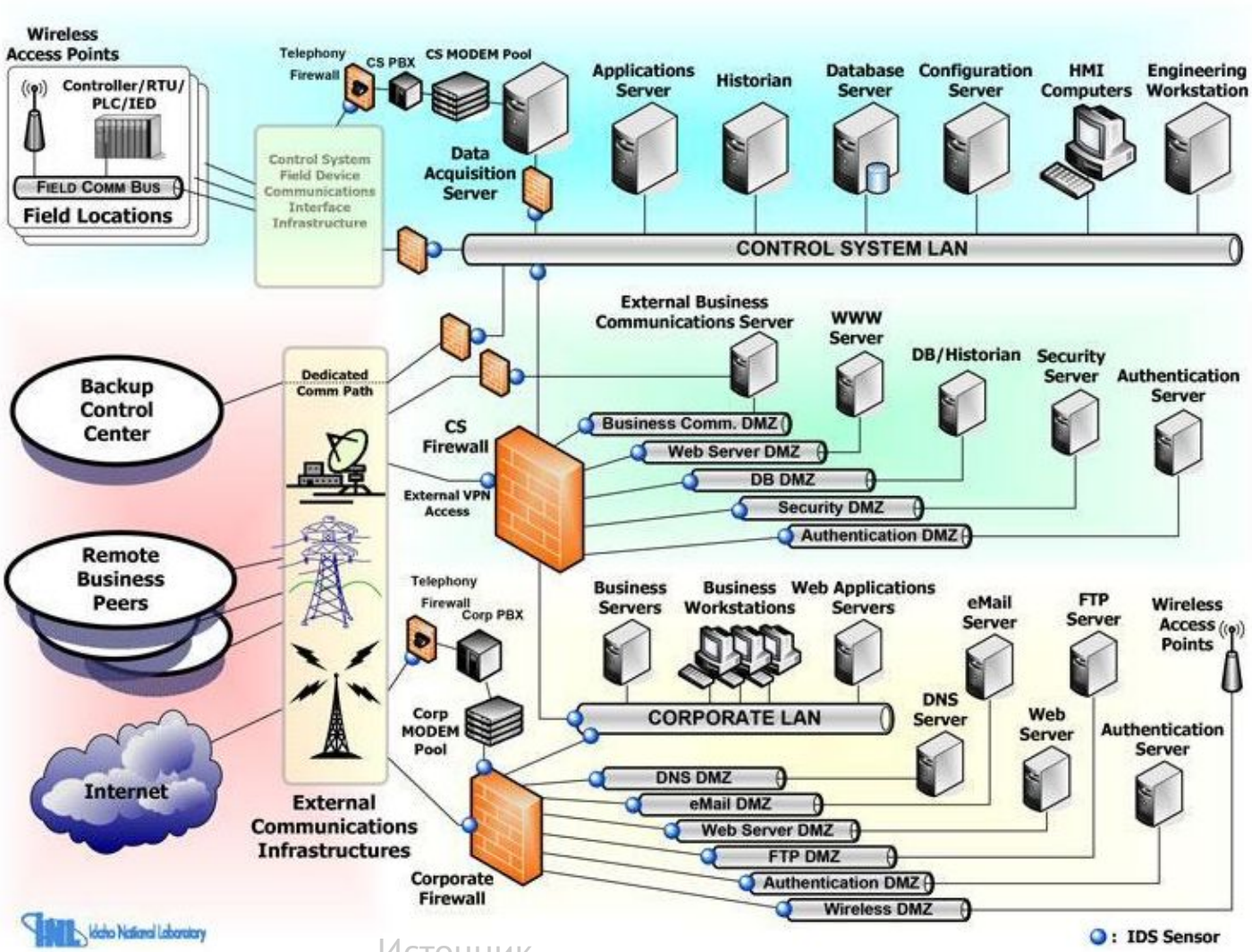
IT Security
(ISO27k series, OSSTMM, NIST CSF…)

Источник



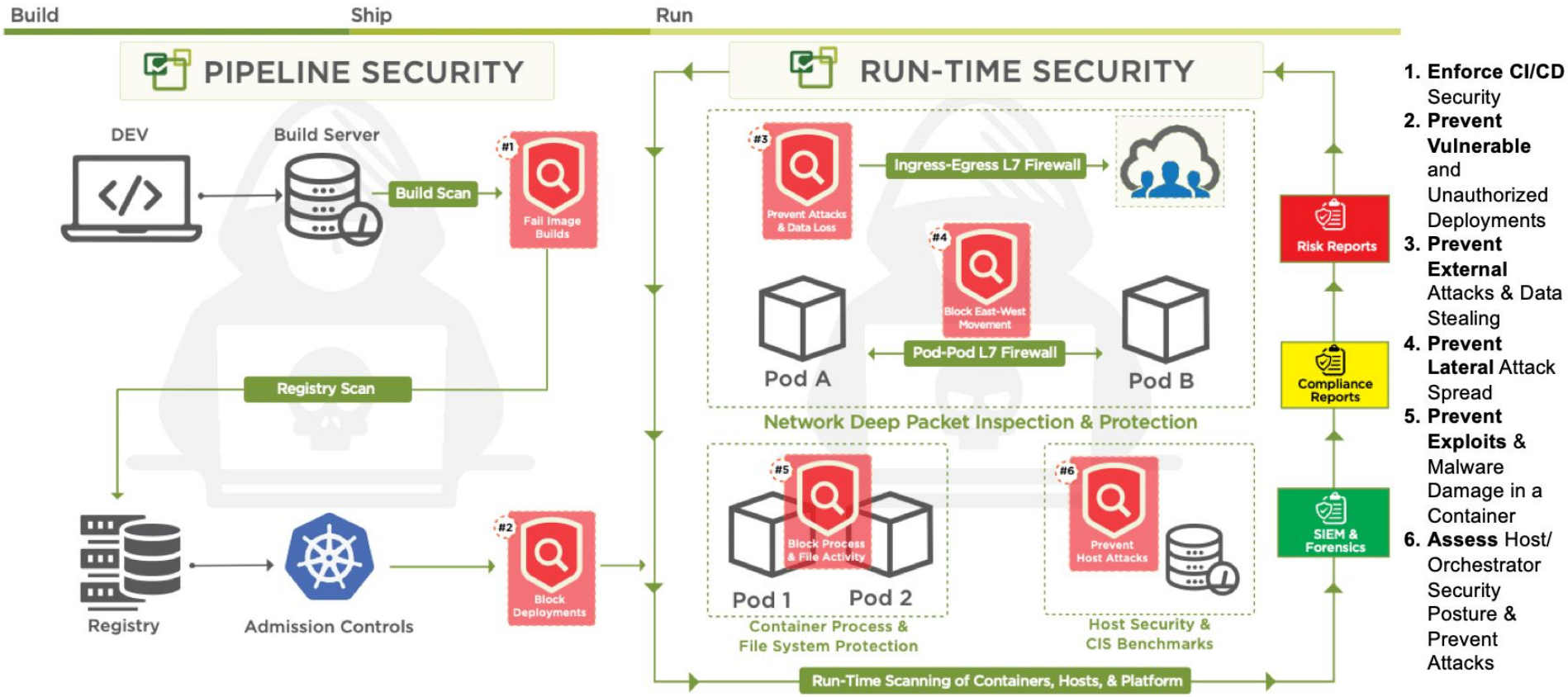
Data Privacy *(GDPR)*

Best practices: сеть объекта КИИ



Источник

Best practices: виртуализация



Источник

DevSecOps

DevSecOps: основные задачи

DevSecOps (Development, Security, Operations) — интеграция проверки безопасности на всех этапах жизненного цикла разработки программного обеспечения.

SDLC (Software Development Life Cycle, жизненный цикл разработки ПО) — замкнутый жизненный цикл ПО, разбитый на определенные этапы.

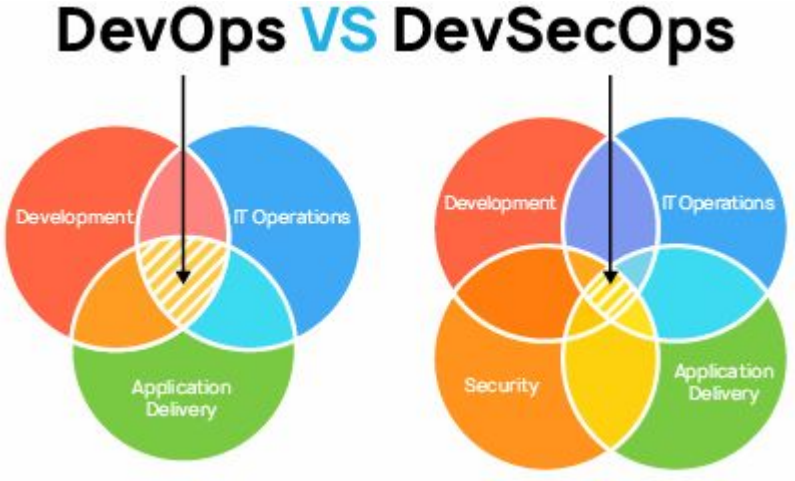
DevSecOps: SDLC

1. Анализ требований (выбор проблемы для решения).
2. Планирование (выбор стратегии решения).
3. Проектирование и дизайн (каким именно будет решение).
4. Разработка ПО (этап создания продукта).
5. Тестирование (проверка качества продукта).
6. Развертывание (установка и использование продукта).

DevSecOps: DevOps и DevSecOps

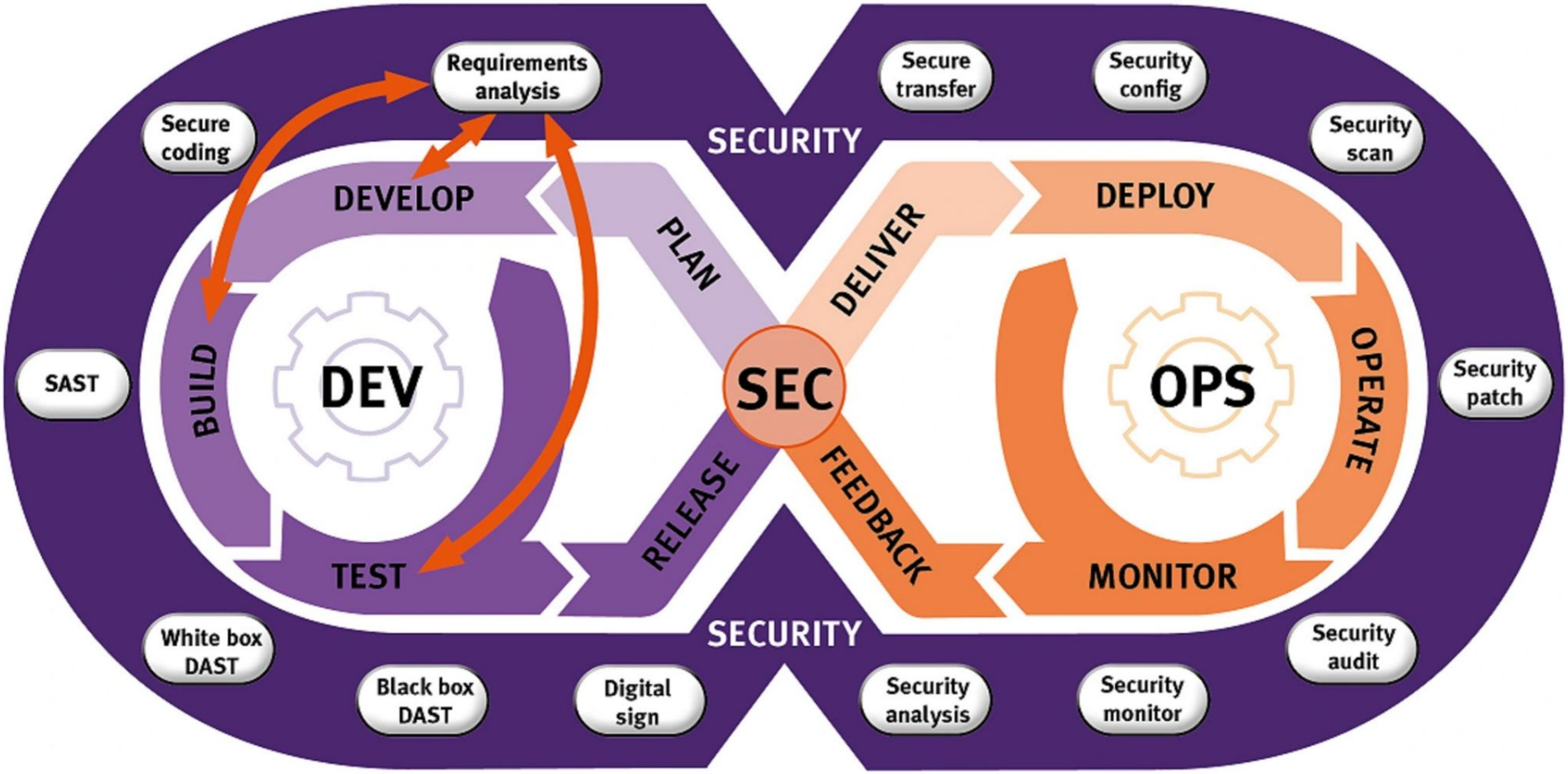
DevOps – методология, обеспечивающая взаимодействие разработчиков и системных администраторов на всех этапах SDLC.

DevSecOps – развитие методологии DevOps путём добавления в процесс обязательного обеспечения безопасности продукта.



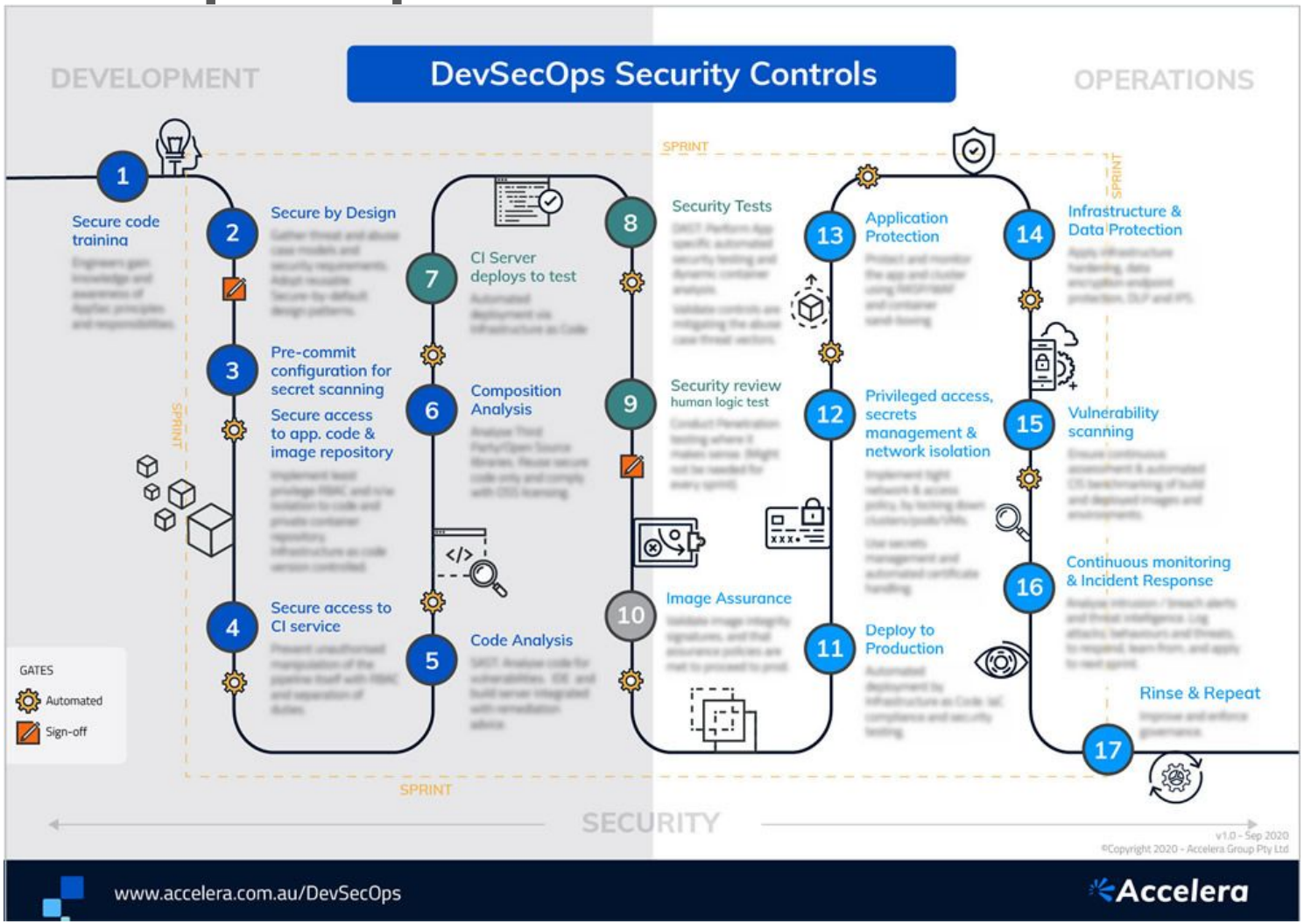
Источник

DevSecOps: SDLC и DevSecOps



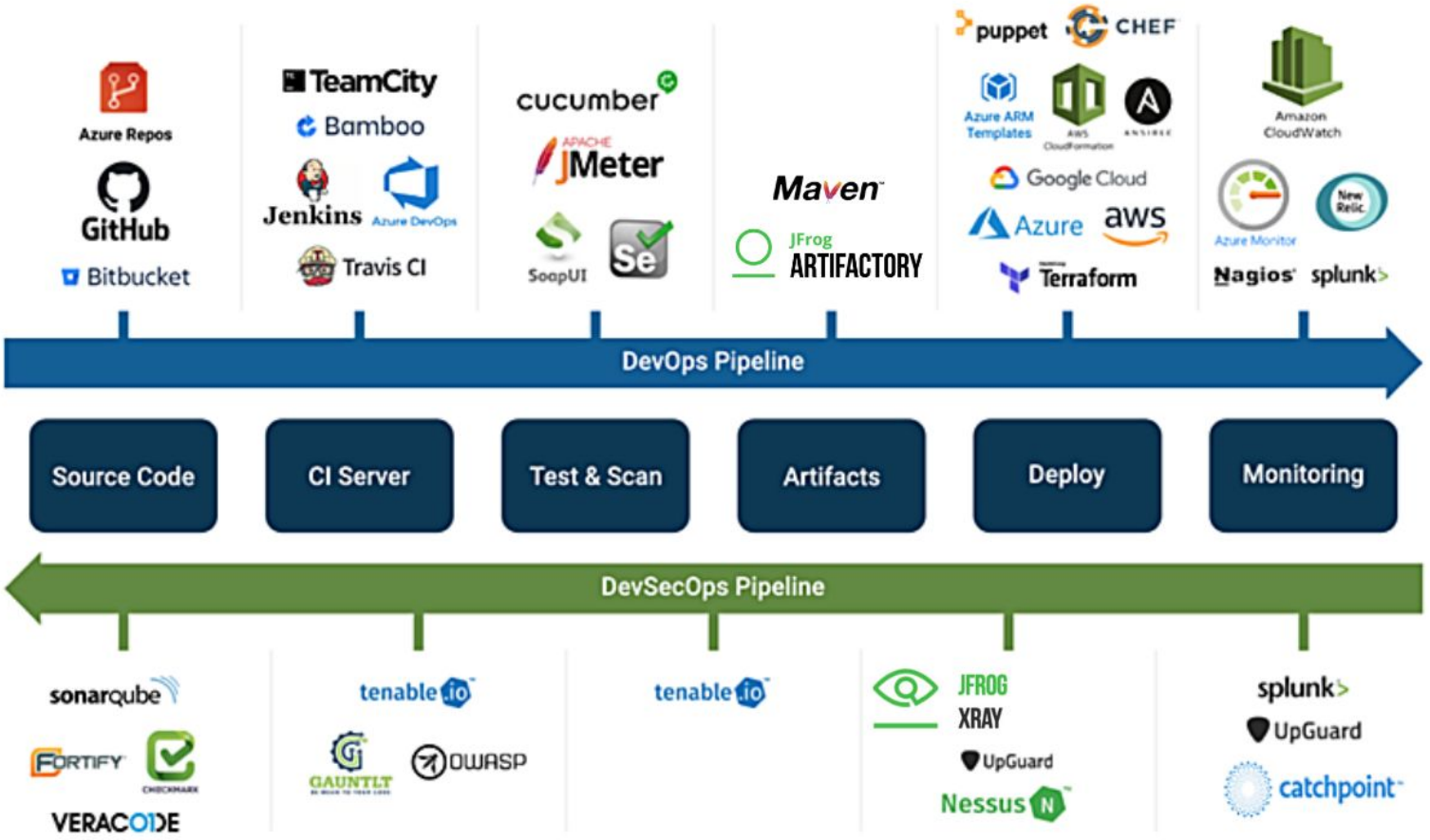
Источник

DevSecOps: меры безопасности



Источник

DevSecOps: инструменты



Источник

Итоги

Итоги

Сегодня мы познакомились с Best practices современной информационной безопасности:

- SOC,
- DevSecOps,
- решениями ИБ для различных компаний.

Домашнее задание

Домашнее задание будет у вас в личном кабинете в виде теста.

Вопросы по домашней работе задавайте **в чате** мессенджера Slack.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Алексей Федин

Алексей Федин