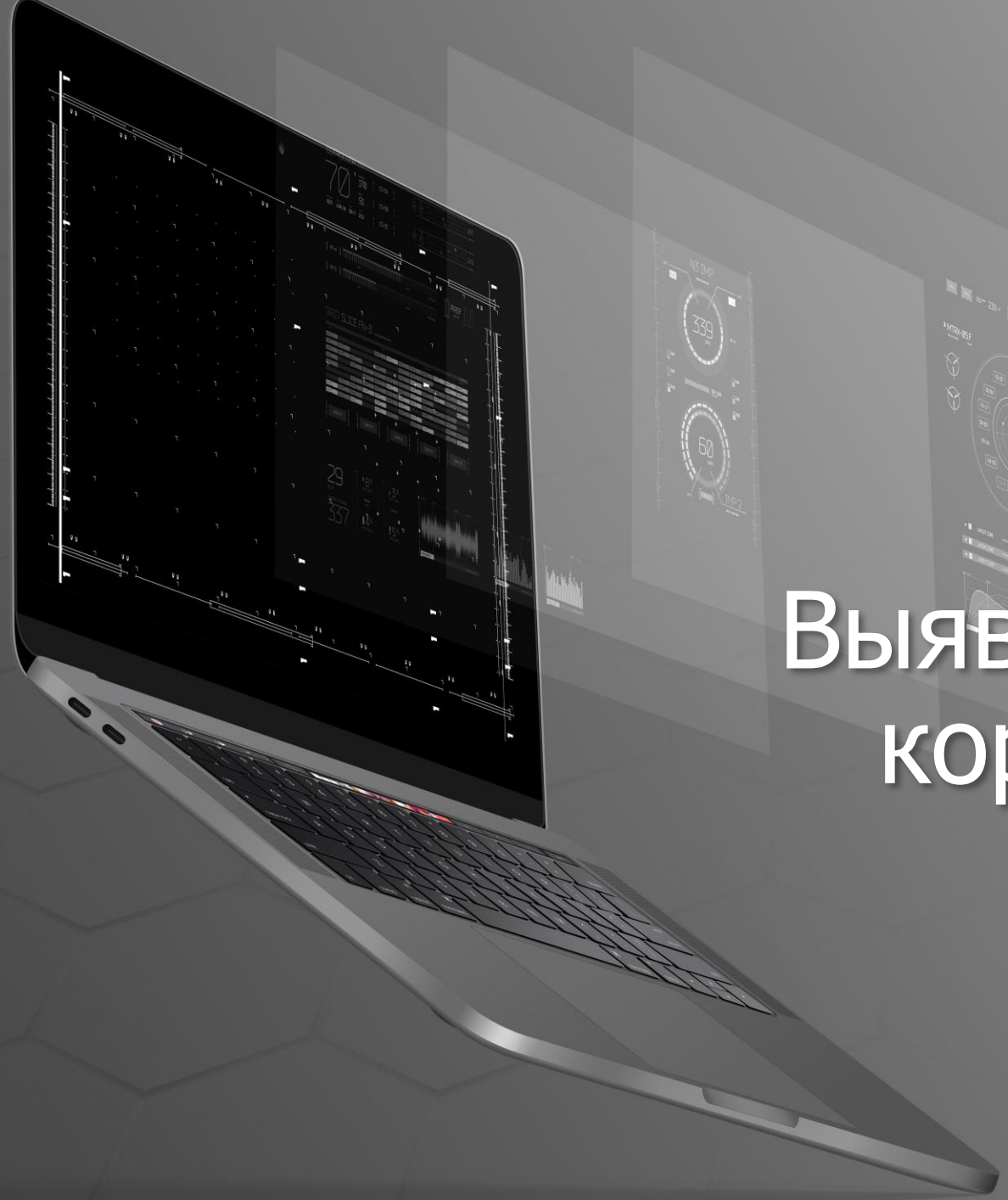


USSC

Серия #3

SecOps от УЦСБ

Выявляем инциденты в корпоративных сетях

Руслан Амиров

Директор USSC-SOC

О чем вебинар

- Что такое SIEM и чем SIEM отличается от Log Management
- Как определить, нужен ли SIEM в организации
- Как работать с инцидентами
- Как SOC может работать с SIEM организации
- Должен ли SOC взаимодействовать с ИТ-подразделением
- Как проводить реагирование на инциденты в корпоративных сетях

Происхождение SIEM

SEM (*Security Event Management, англ., управление событиями безопасности*) – системы, которые действуют в режиме, приближенном к реальному времени. Для этого им требуется: автоматический мониторинг событий, их сбор, корреляция, генерация предупреждающих сообщений

+

SIM (*Security Information Management, англ., управление информационной безопасностью*) – системы, которые, в свою очередь, анализируют накопленную информацию со стороны статистики, различных отклонений от нормального поведения и т.д.

=

SIEM (*Security Information and Event Management*) – системы, которые осуществляют мониторинг информационных систем, анализируют события безопасности в реальном времени, исходящие от сетевых устройств, средств защиты информации, ИТ-сервисов, инфраструктуры систем и приложений, и помогают обнаружить инциденты ИБ

Log Management vs. SIEM

USSC

Log Management:

- Централизованный сбор событий
- Фильтрация, нормализация, агрегация
- Хранение
- Поиск, визуализация

elastic graylog

SIEM:

- Функции Log Management System

+

- Корреляция + обогащение
- Оповещения
- Инструментарий для анализа инцидентов

splunk>

Radar MaxPatrol SIEM

RUSIEM FortiSIEM

Проблематика выявления инцидентов в корпоративных сетях

Средства защиты, серверы и сетевые устройства создают миллионы событий, терабайты логов

Реагировать на все инциденты ИБ неэффективно: 50–95% из них составляют ложные срабатывания на СЗИ

Данные с одного средства защиты не выявляют сложные и целенаправленные атаки

События разбросаны по разным системам и десяткам отчетов

Требования регуляторов в области информационной безопасности

Задачи, которые решает SIEM

- Консолидация событий
- Хранение событий
- Корреляция и обработка событий
- Предоставление инструментов для экспертного анализа
- Контекстное обогащение инцидентов
- Автоматическое оповещение Администратора ИБ
- Формирование отчетных документов

Консолидация событий

Консолидация – все события ИБ в одной консоли

1. Выбор источников
2. Подготовка источников

Консолидация событий: Выбор источников

USSC

Виды источников

- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения
- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Сетевое активное оборудование
- Сканеры уязвимостей
- Системы инвентаризации и asset-management
- Системы веб-фильтрации

И это еще не весь список

Консолидация событий: Подготовка источников

USSC

Служба ИБ vs Служба ИТ

ПРОТИВОСТОЯНИЕ
или
СИНЕРГИЯ?

USSC

Хранение событий

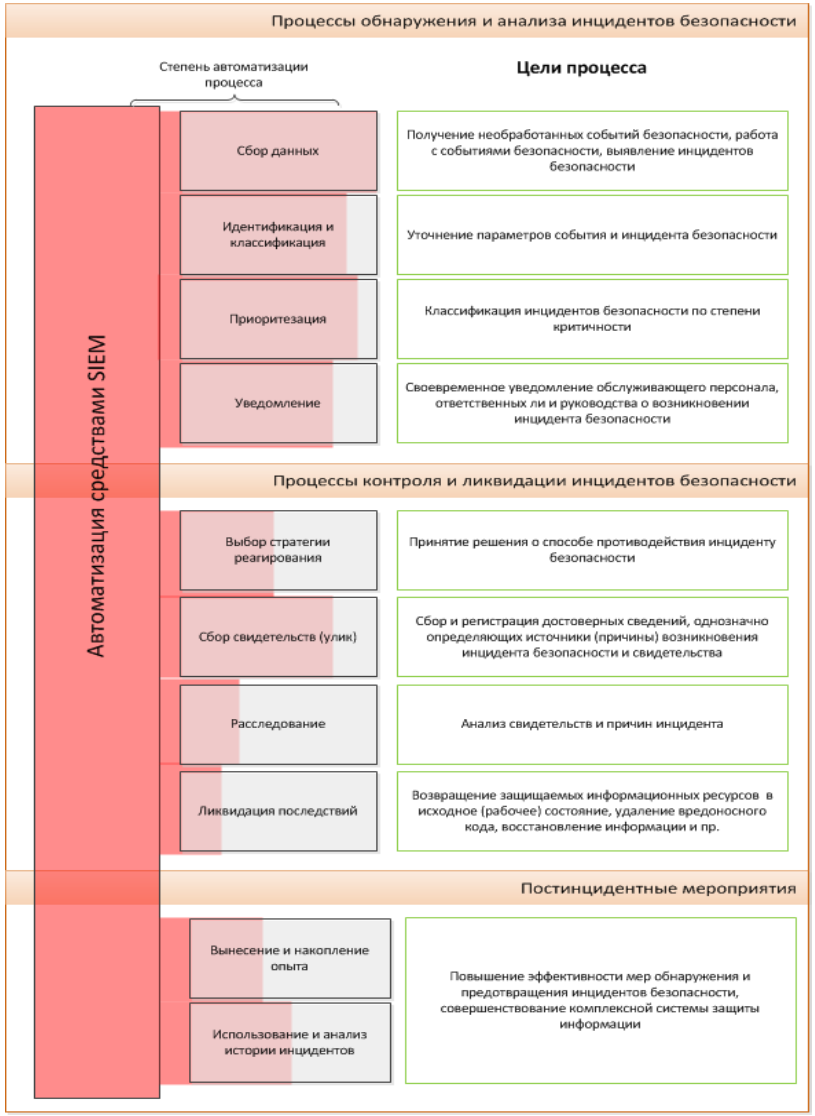
1. Нужно ***ОЧЕНЬ*** много дисков!
2. Оперативное и архивное хранение

Особенности обработки событий безопасности

USSC

Типовые операции

- нормализация событий ИБ
- фильтрация событий ИБ
- обогащение событий ИБ
- агрегация событий ИБ
- корреляция событий ИБ
- приоритизация инцидентов и событий ИБ



Обработка событий: Нормализация

Нормализация – приведение события в понятный вид

1. Экспертная оценка события
2. Определение схемы взаимодействия
3. Определение категории события

Обработка событий: Нормализация. Пример

USSC

Источник события

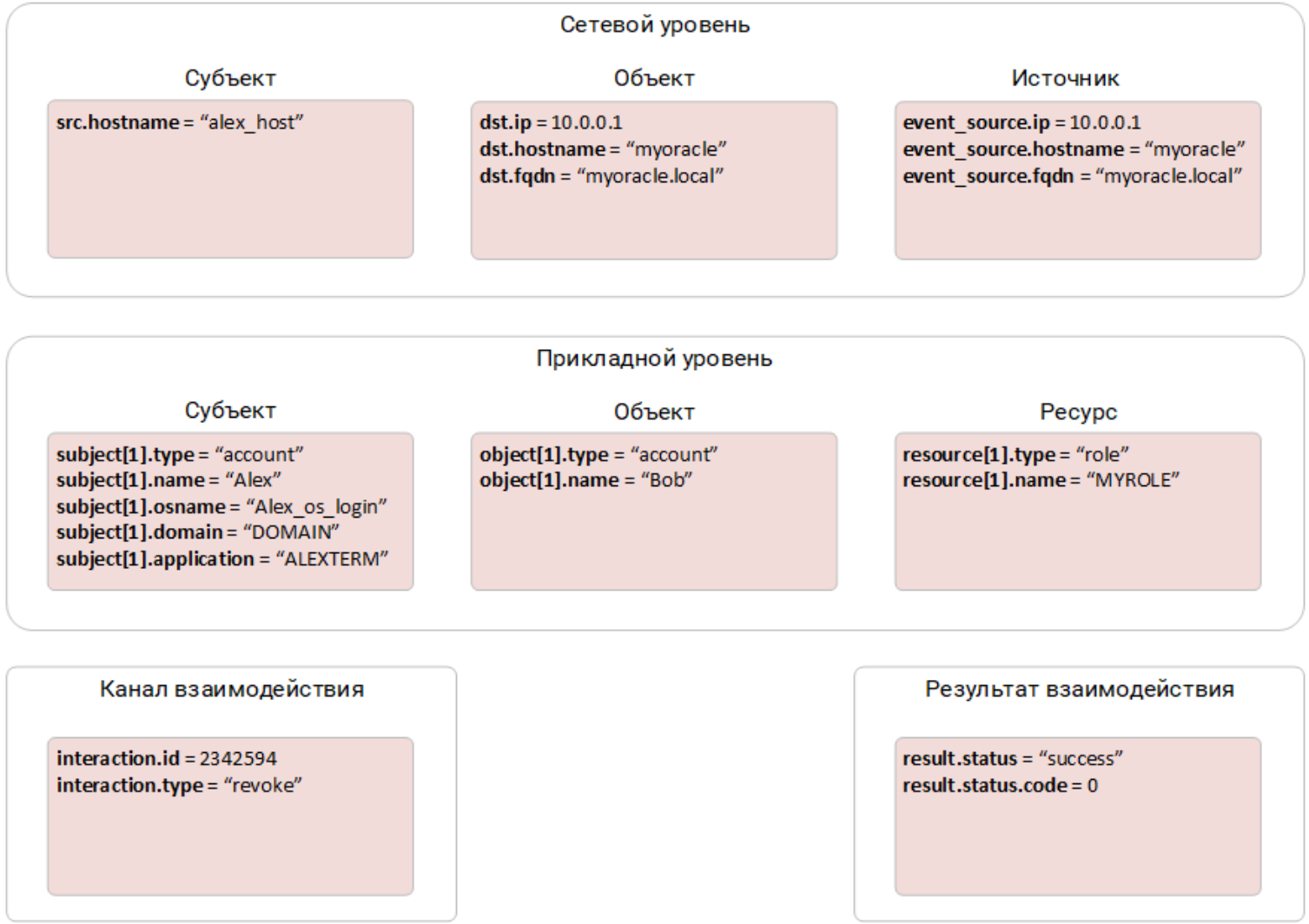
IP: 10.0.0.1
Hostname: myoracle
FQDN: myoracle.local

Исходное событие

{ "grantee": "BOB", "db_username": "ALEX", "obj_name": "MYROLE", "priv_used": "AUDIT SYSTEM", "obj_privilege": null, "os_username": "Alex_os_login", "userhost": "DOMAIN\\Alex_host", "new_owner": null, "return_code": 0, "session_id": 2342594, "action_name": "REVOKE ROLE", "terminal": "ALEXTERM", "scn": 2522342, "entry_id": 5, "owner": null, "event_date": "20.08.2018 12:44:11", "sys_privilege": null, "admin_option": null, "new_object_name": null, "audit_option": null }

Обработка событий: Нормализация. Результат

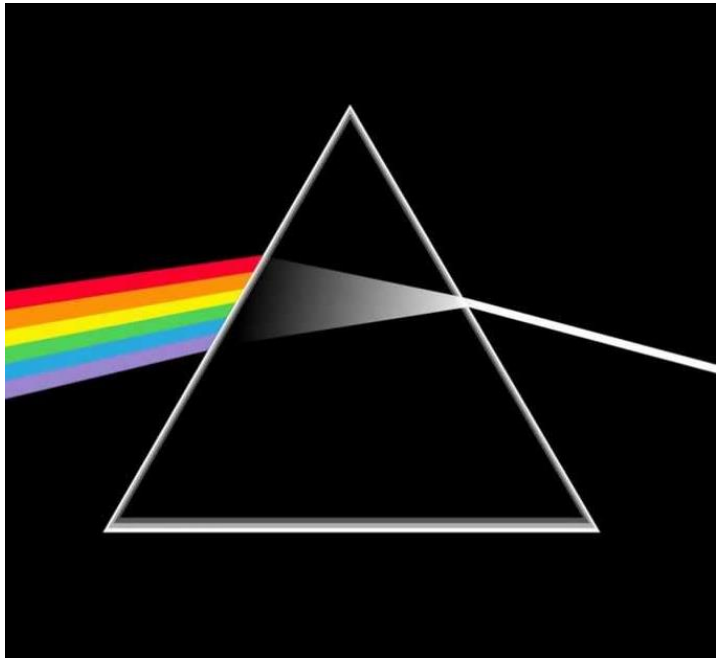
USSC



Обработка событий: Агрегация

Агрегация – объединение повторяющихся событий в одно

1. Выявляем повторяющиеся события
2. Определяем критерии объединения
3. Экономим ресурсы



Обработка событий: Обогащение

Обогащение – получение информации из внешних источников

1. Событие не всегда содержит полную информацию
2. Информацию можно извлекать из внешних источников
3. Экономия времени на расследование

Обработка событий: Приоритизация

Приоритизация – определение важности события

1. Определить область действия
2. Определить важность активов и пользователей
3. Определить повторяемость

Правила корреляции

Корреляция (в рамках SIEM) – сопоставление информации из разных событий с целью последующего реагирования

Способы реагирования

- Создать новое событие
- Отправить уведомление администратору
- Выполнить скрипт
- Открыть кейс внутри SIEM
- Записать информацию в список

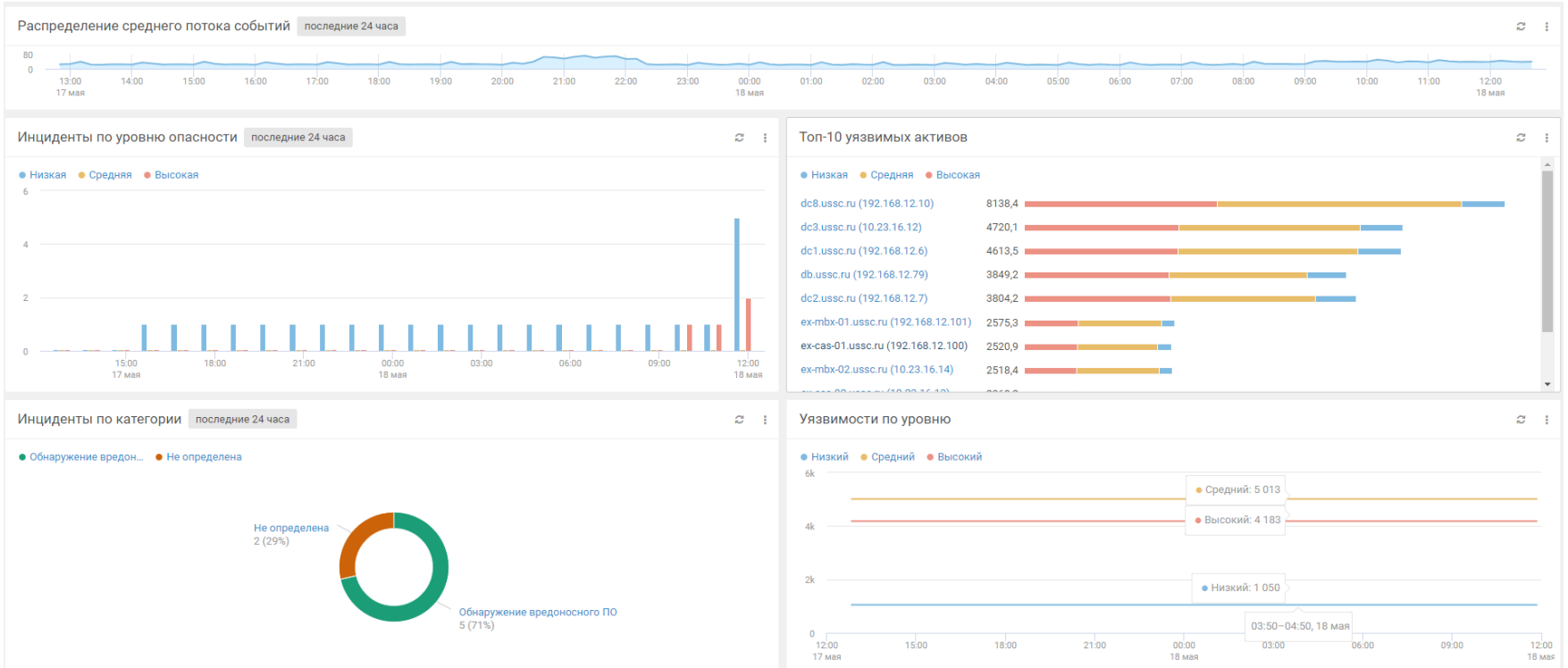
Правила корреляции: Методы

Сигнатурные методы (Rule based) — методы, в которых человек должен добавить некие правила определения инцидентов

Бессигнатурные — черный ящик, который сам отличает хорошее от плохого (на основе логики, заложенной вендором)

Визуализация

Визуализация – отображение информации из разных событий в виде графиков, диаграмм, списков в режиме реального времени или за определенный промежуток времени



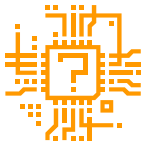
Нужна ли SIEM-система в организации?

SIEM-система может быть востребована в организации, если необходимо:

1. Выявлять инциденты на базе более, чем 1 события безопасности
2. Получать оповещения об инцидентах
3. Обрабатывать ложные срабатывания
4. Иметь возможность интеграции с внешними системами (ServiceDesk, IPR, e-mail, мессенджеры и др.)

Что мешает эффективной работе с SIEM?

SIEM не способны выявлять новые угрозы до наступления последствий атак



Нет полных знаний о защищаемой инфраструктуре: качеством работы технологий обнаружения активов и инвентаризации Заказчики удовлетворены меньше, чем другими используемыми технологиями

Не хватает специалистов и компетенций в области ИБ для оперативного выявления атак

SIEM не подстраиваются под изменения в инфра-структуре, поэтому правила корреляции событий ИБ не работают или работают неэффективно

Open-source SIEM

USSC

1. Они существуют

2. Нужно уметь их «готовить»

3. Придется принять определенные риски

Из чего состоит open-source SIEM

USSC

SIEMonster

Эволюция SIEM

USSC

Что было

- Агенты на узлах
- Log Management + Event Management
- Корреляция
- CMDB
- Поддержка TI feed

Сейчас

- Безагентная схема
- Big Data
- UEBA и пр. аналитика
- Ретроспективная корреляция
- Интеграция с SOAR, GRC

Что будет

- NG SOAR
- Мета продукт
- All-in-one решение по безопасности
- ?

Эволюция систем автоматизации ИБ

Сценарии использования

- Оптимизация SOC
- Мониторинг угроз и реагирование
- Расследование инцидентов
- Управление бизнес-процессами ИБ

SOAR = SIR + SOA + TVM

SOAR = SOA + SIR + TIP

2015 — **2017** — **2019**

VA – оценка уязвимостей
SIEM – сбор и выявление событий ИБ
TVM – управление уязвимостями и угрозами

SOA – платформа оркестрации СрЗИ и автоматизации
SIR – платформа реагирования на инциденты
TIP – платформа оценки и анализа угроз

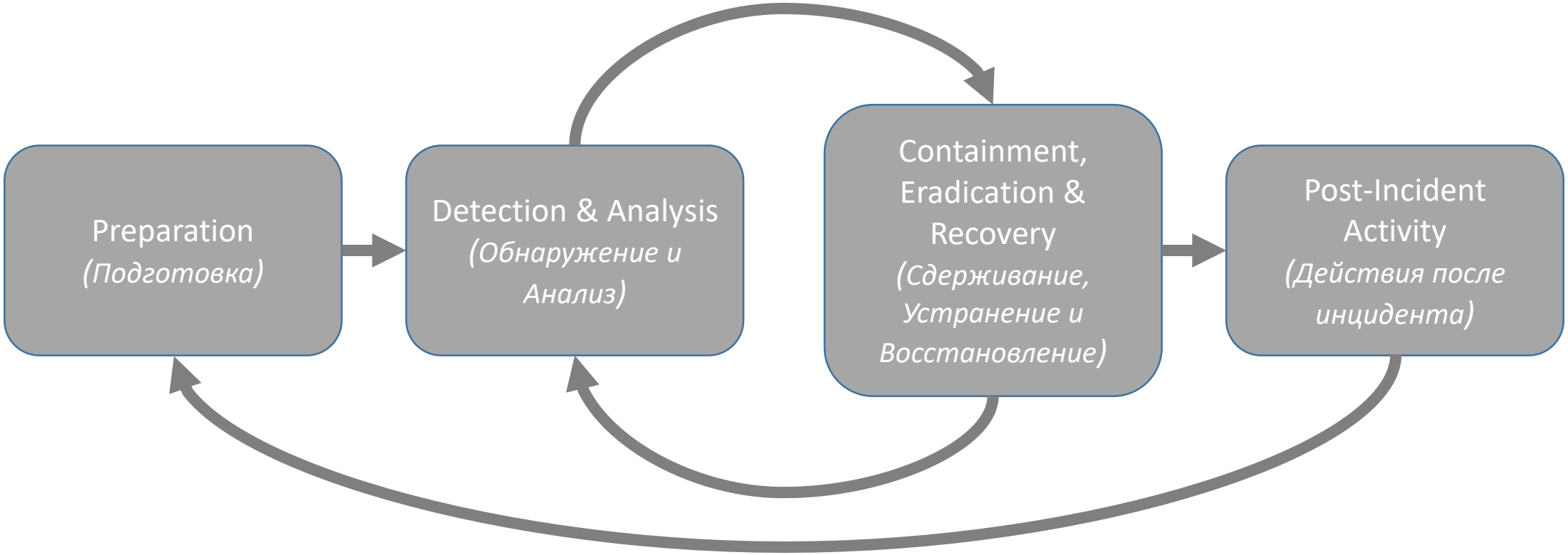
SOAR – действия по обеспечению безопасности, аналитика и отчетность
SOC – центр мониторинга ИБ и реагирования

Недостижимый идеал

SIEM мечты:

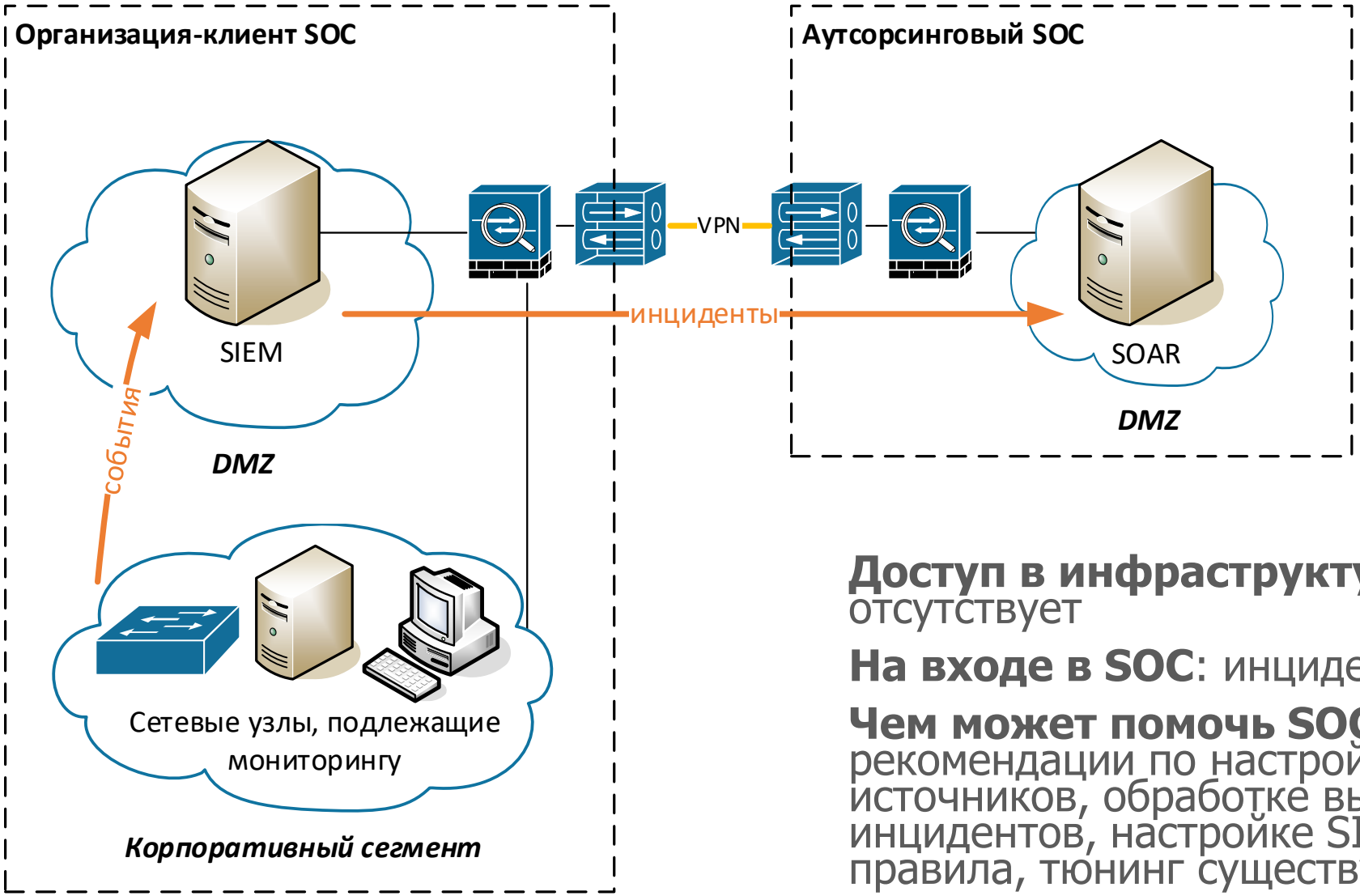
1. Способен обнаруживать актуальные на сегодня угрозы
2. Работоспособность SIEM минимально зависит от наличия экспертов в компании
3. Знает IT-инфраструктуру и подстраивается под ее изменения

Как проводить реагирование на инциденты?



NIST SP 800-61 «Computer Security Incident Handling Guide» Rev.2

Как SOC может работать с SIEM

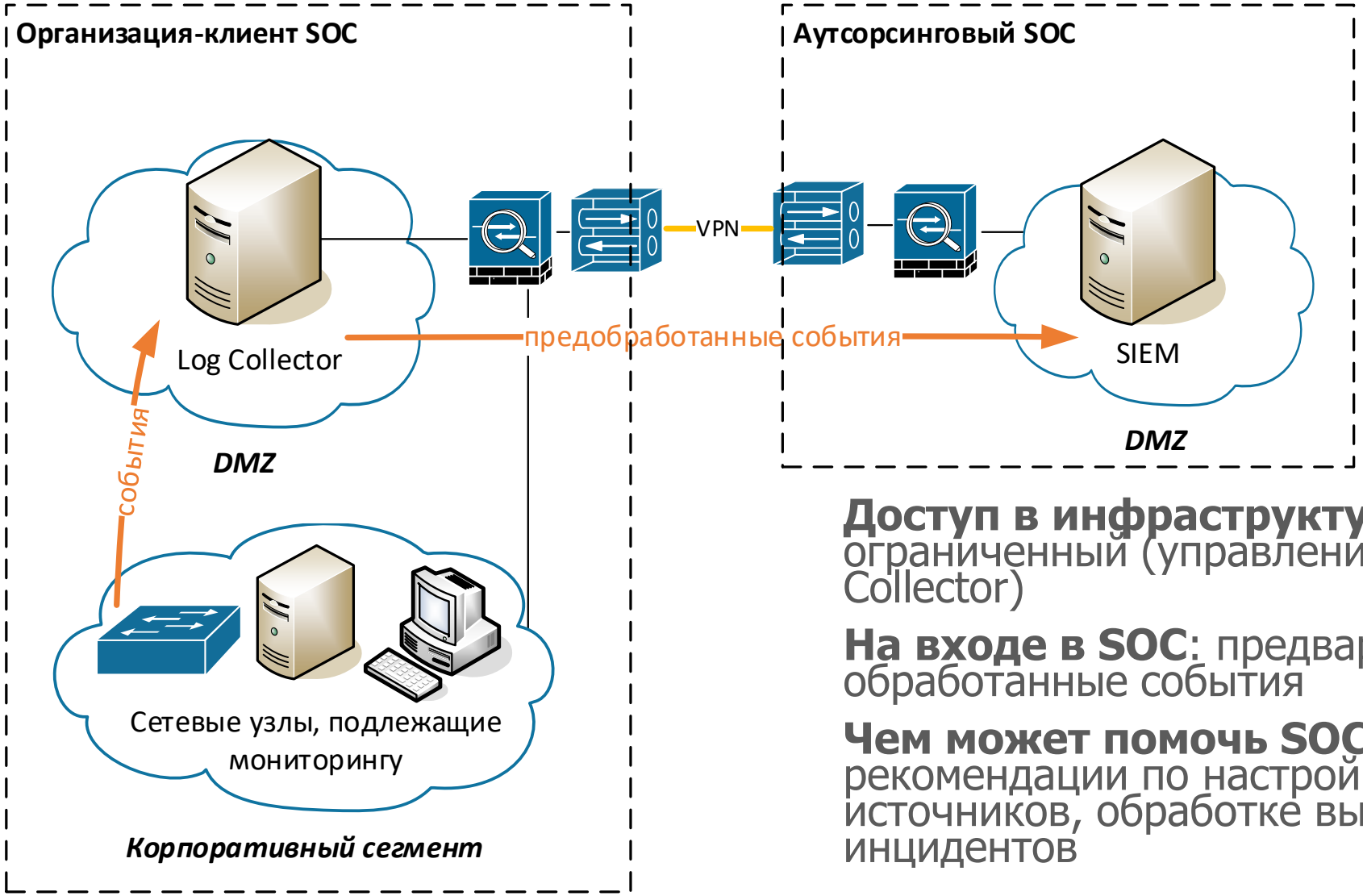


Доступ в инфраструктуру: отсутствует

На входе в SOC: инциденты

Чем может помочь SOC: рекомендации по настройке аудита источников, обработке выявленных инцидентов, настройке SIEM (новые правила, тюнинг существующих)

Как SOC может работать с SIEM

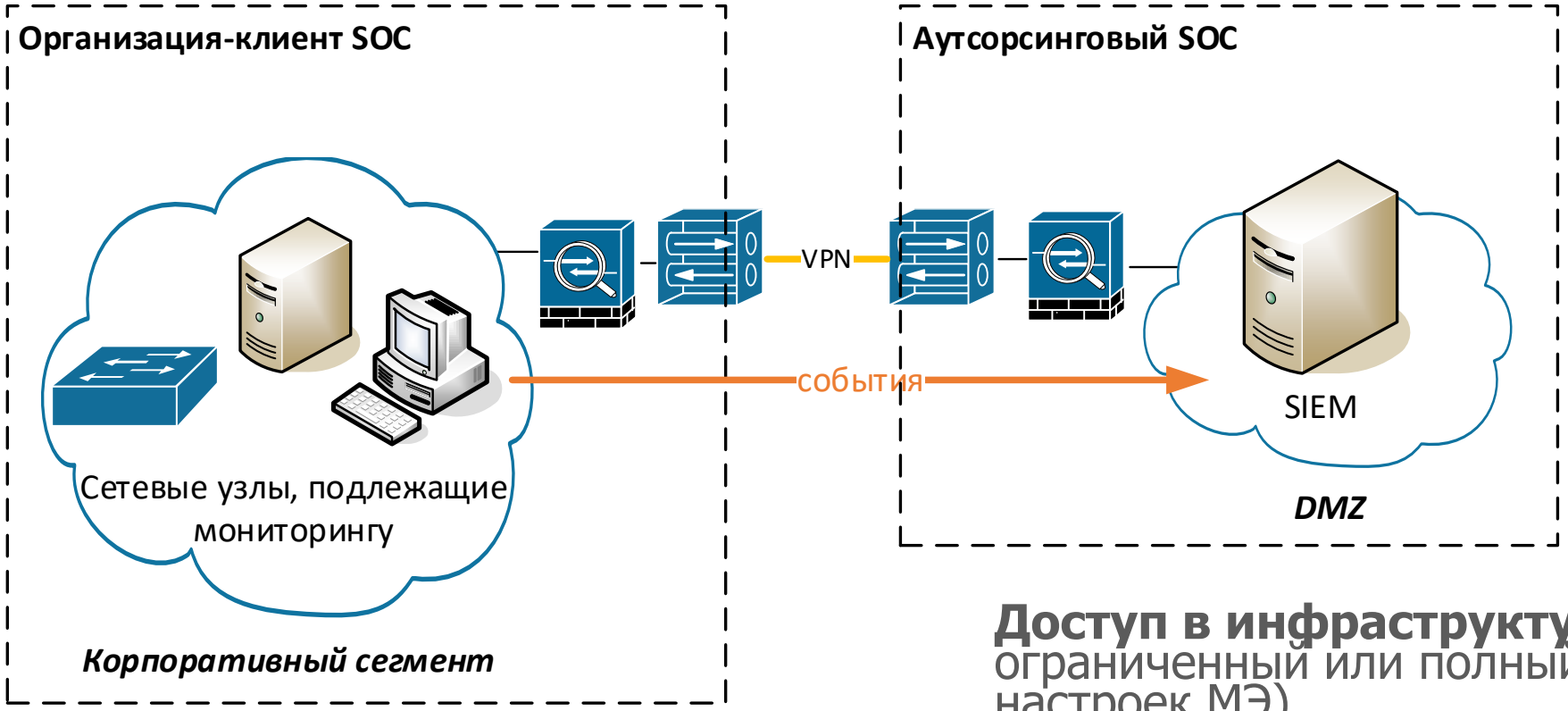


Доступ в инфраструктуру: ограниченный (управление Log Collector)

На входе в SOC: предварительно обработанные события

Чем может помочь SOC: рекомендации по настройке аудита источников, обработке выявленных инцидентов

Как SOC может работать с SIEM



Доступ в инфраструктуру: ограниченный или полный (зависит от настроек МЭ)

На входе в SOC: события

Чем может помочь SOC: рекомендации по настройке аудита источников, обработке выявленных инцидентов

Как SOC может работать с SIEM

Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389 «Рекомендации по обеспечению безопасности ОКИИ при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов КИИ»:

- Инструктаж работников
- Выдача доверенных СВТ для удаленного доступа
- Идентификация ресурсов удаленного доступа
- Комплексная безопасность удаленных СВТ (2FA, АВЗ)
- Применение VPN для удаленного доступа
- Мониторинг ОКИИ

Информационное сообщение ФСТЭК России от 23 июня 2021 г. N240/24/3057 «Об утверждении Требований по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах»

Требования недоступны в открытых источниках, выпущены под грифом ДСП

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Руслан Амиров

Директор Центра мониторинга ИБ

USSC-SOC

+7 (343) 379-98-34 (доб. 1203)

ramirov@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU