RUSIEM
Всё под контролем

Усиление контроля безопасности с помощью SIEM в условиях изменения законодательных требований

Максим Степченков

Совладелец

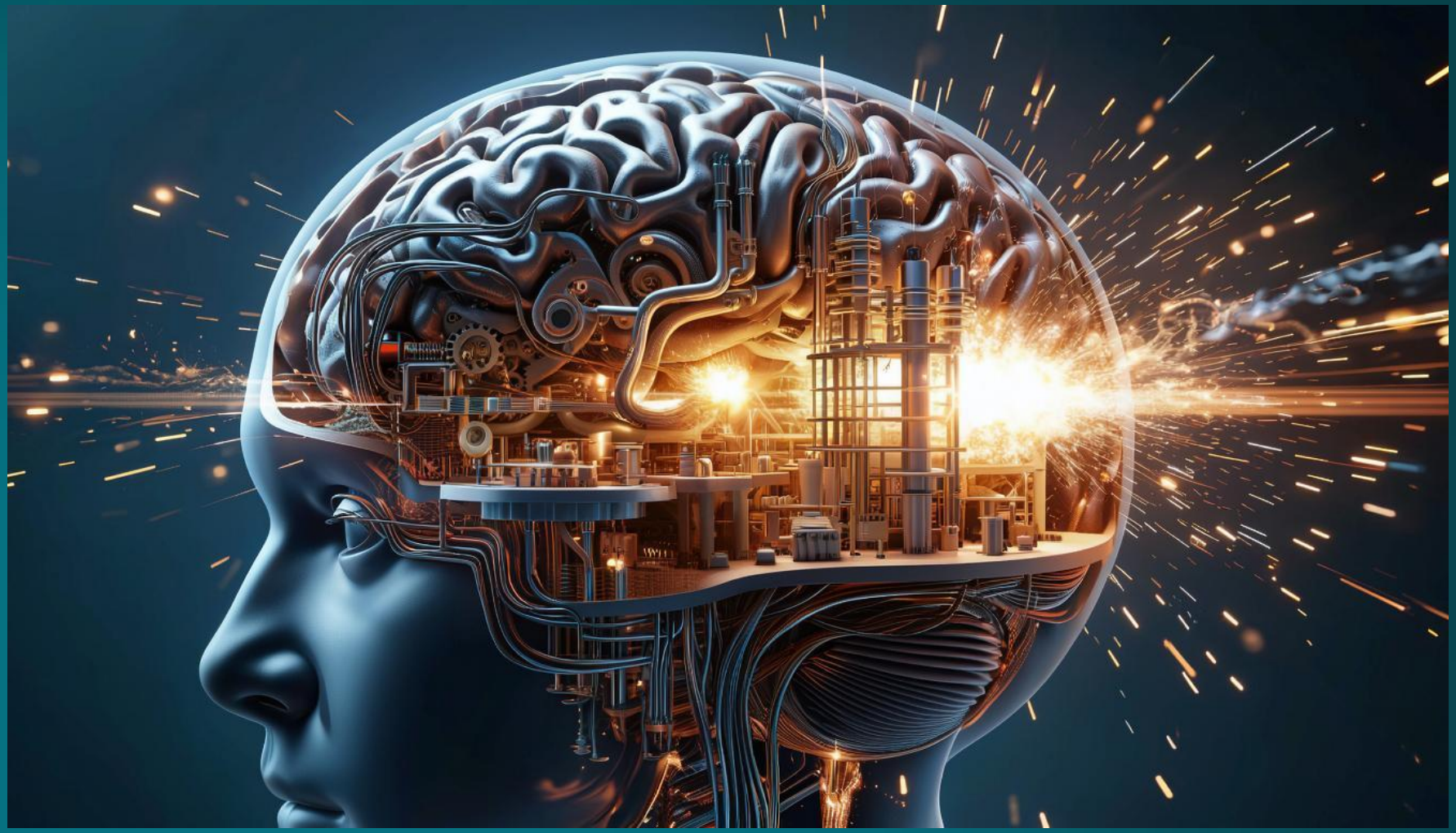
+7 903 164-31-31 m.stepchenkov@rusiem.com

+7 (495) 748-83-11

info@rusiem.com

rusiem.com

Что происходит с законами?



Приказ ФСТЭК России № 239: суть требований для ЗОКИИ в части управления событиями информационной безопасности

Приказ № 239 определяет набор требований по обеспечению безопасности значимых объектов КИИ: организация мер защиты, создание систем безопасности и обеспечение устойчивого функционирования объектов. Для практического выполнения важно перейти от разрозненных действий к упорядоченному процессу: идентификация источников событий, журналирование, защита журналов и регламенты реагирования

Ключевые моменты

- Требования распространяются на все значимые объекты КИИ. Также по решению субъекта КИИ настоящие Требования могут применяться для обеспечения безопасности объектов КИИ, не отнесенных к значимым объектам
- Обязательна регистрация и хранение событий безопасности
- Необходимо обеспечить защиту журналов и контроль доступа
- Важна документированная организация реагирования на инциденты

Источники событий: практическая база для выполнения требований

Приказ требует обеспечения регистрации событий и контроля за состоянием систем. На практике это выполняется подключением ключевых типов источников событий, которые дают полноту картины инцидентов и соответствуют требованиям по журналированию

Корректный набор источников обеспечивает соответствие пунктам Приказа о регистрации и хранении событий и даёт основу для адекватного реагирования

Источники

- Сетевые устройства и межсетевые экраны
- Серверные ОС и журналы приложений
- СУБД и сервисы бизнес-приложений
- Средства защиты (антивирусы, IDS/IPS, СКЗИ, DLP)
- Логи доступа пользователей и системных администраторов

Источники событий: практическая база для выполнения требований

Приказ ФСТЭК России № 239 требует регистрации и возможности анализа событий, а также мер реагирования — это достигается набором корреляционных правил и процедур реагирования (инцидент-менеджмент). Правила должны закрывать сценарии, представляющие наибольшую опасность для ЗОКИИ

Корректная корреляция превращает сырые логи в управляемые инциденты и обеспечивает исполнение требований по своевременному реагированию и отчётности

Примеры правил

- Множественные неуспешные аутентификации → блок/уведомление
- Привилегированная активность в нерабочее время → проверка

Формулировка правил — практический выбор оператора; Приказ устанавливает обязанность регистрации, анализа и реагирования, а не конкретный набор корреляций

Как выполнить требования Приказа № 239

Определить категории значимости и список объектов КИИ, а также критичные процессы

→

Определить список ПО и программно-аппаратных средств защиты

→

Настроить регистрацию и защиту журналов событий

↓

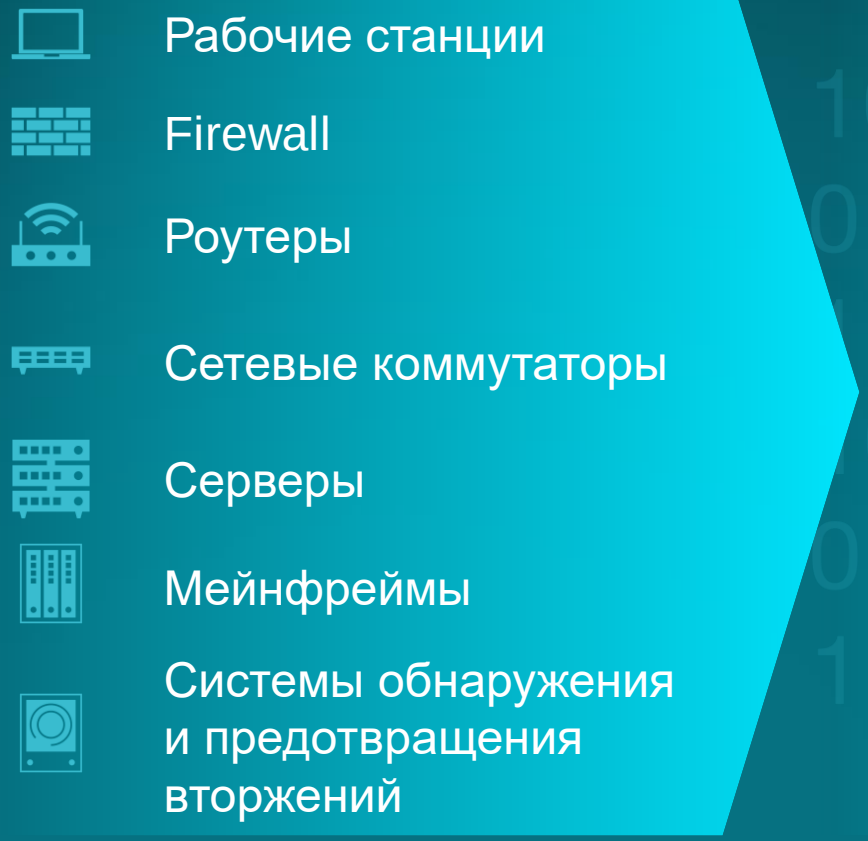
Внедрить корреляцию и выстроить процедуру реагирования

←

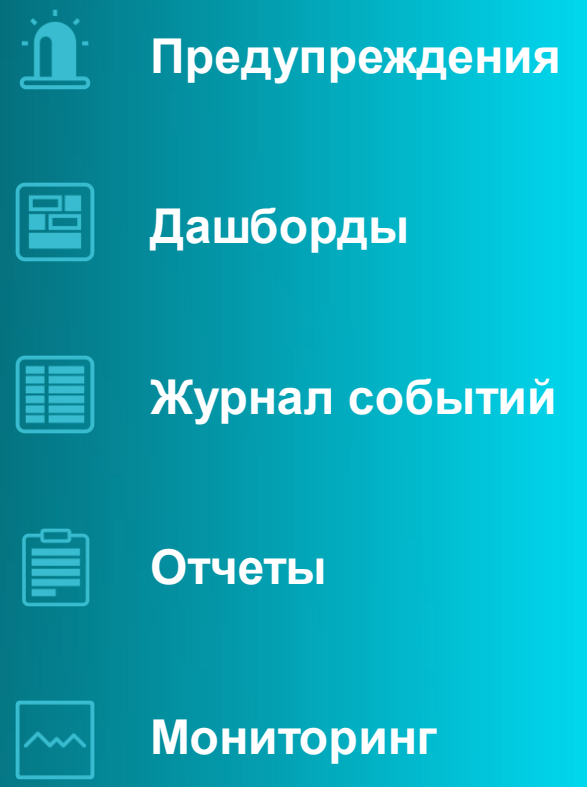
Вести отчётность и совершенствовать

Важно не только реализовать технические средства, но и закрепить регламенты, роли и процессы — только так требования Приказа будут выполняться устойчиво и документируемо

Схема работы SIEM



SIEM



Типы источников

ЛЮБЫЕ

- Межсетевые экраны
- IPS
- DNS logs
- АСУТП
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения
- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы

Где может применяться SIEM

Сценарии выявления угроз

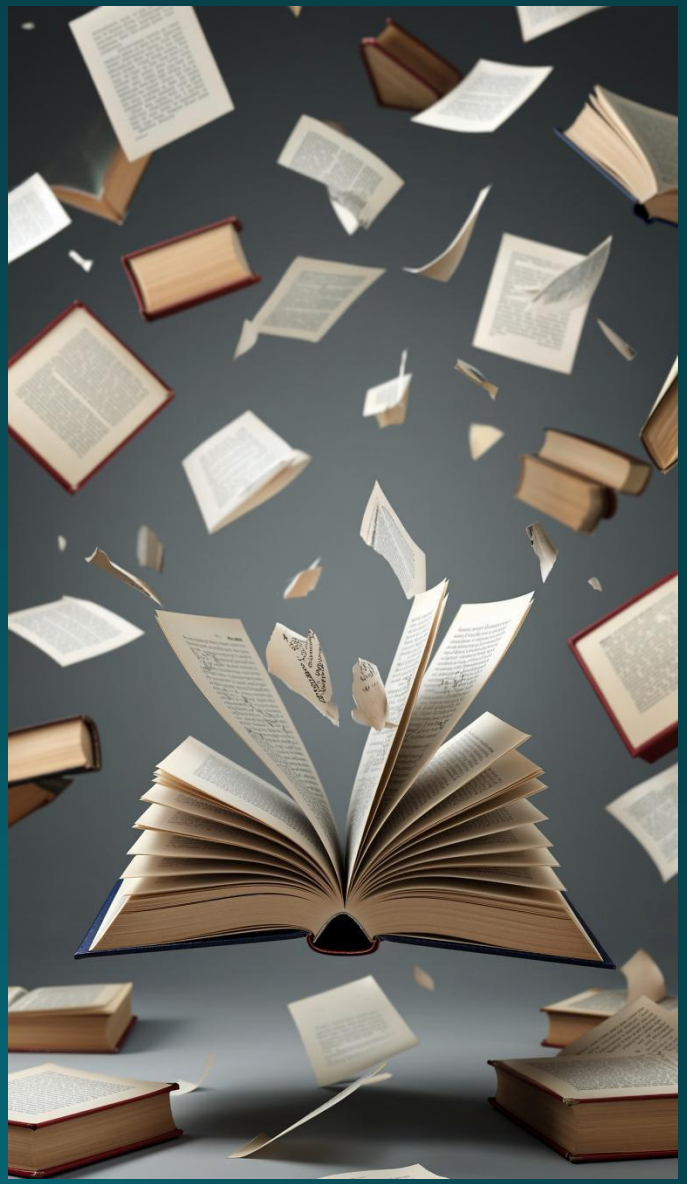
- Сетевые атаки
- Фрод и мошенничество
- Обнаружение несанкционированного доступа
- Повышение привилегий
- Обнаружение распределённых по времени атаках
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке ПО
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- и прочее…

Типы выявляемых инцидентов

- Информационная безопасность
- Инциденты ИТ
- Физическая безопасность
- Экономическая безопасность
- Инциденты на производстве
- Инциденты, связанные с персоналом
- Инциденты, возникающие при разработке
- и другие типы инцидентов….

Коротко о том, что происходит

Законодательные изменения всегда обширны – изменения в одном законе неизбежно влекут за собой другие



Подписывайтесь в Telegram

RuSIEM @rusiem

последние новости, важные события

https://t.me/rusiem

RuSIEM Support @rusiemsupport

возможность быстро связаться с технической поддержкой

https://t.me/rusiemsupport