RUSIEM

Всё под контролем

SIEM

почему это важно

а не просто обязательно

О КОМПАНИИ RUSIEM

программный код создан российскими экспертами

>300

пилотных внедрений

резидент Сколково

>50

партнеров в странах СНГ

2014

с этого года ведется активная разработка

продукт включен в реестр отечественного ПО

10000

установок free-версии в мире в 2017-18 годах

ЧТО ТАКОЕ SIEM

SIEM (Security Information and Event Management) — решение для мониторинга и анализа любой активности, происходящей в организации

SIEM — это сложная комплексная система, позволяющая получать своевременную и всеобъемлющую информацию о состоянии ИТ-инфраструктуры предприятия

SEM

(Security Event Management) — управление событиями безопасности

- ✓ процесс централизации данных журнала компьютера из нескольких источников для улучшения обнаружения инцидентов безопасности и управления этими событиями посредством формализованного процесса реагирования

SIM

(Security Information Management) — управление информационной безопасностью

- ✓ процесс сбора, мониторинга и анализа данных из автоматически генерируемых компьютерных журналов

SIEM

SIEM – система мониторинга, которая позволит вам отслеживать состояние собственной инфраструктуры в реальном времени. Система анализа событий безопасности, исходящих от сетевых устройств и приложений, которая позволяет реагировать на инциденты безопасности до наступления существенного ущерба

ЗАЧЕМ НУЖНА SIEM

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по-отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них

Отдельные устройства, операционные системы только предоставляют события без детального анализа

Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств

Для этого и нужна SIEM-система

SIEM – система, которая собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем

Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями

КАК РАБОТАЕТ SIEM

- Универсальный ответ – **взаимосвязь**
- Система собирает логи с источников событий инфраструктуры. Некоторые собирают NetFlow. Используя эти данные, SIEM дает представление о событиях сети
- Имея все данные о каждом событии, мы можем настраивать свою систему на обнаружение конкретного инцидента. Правилами корреляции обусловлена настройка системы. Чем детальнее прорабатываются правила корреляции, тем полезнее будет для вас SIEM

ГДЕ МОЖЕТ ПРИМЕНЯТЬСЯ SIEM?

Везде, где из журналов событий можно извлечь полезную информацию

ПРИМЕРЫ СОБЫТИЙ

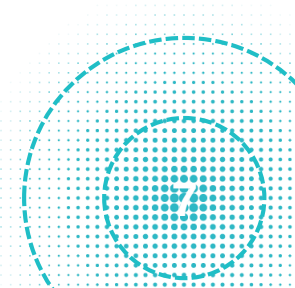
- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN-подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевые устройства, приложения, ОС)
- Выполнение требований законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атак
- Влияние отказа в инфраструктуре на бизнес-процессы

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

- Приказы ФСТЭК России №№ 17, 21, 31, 239
- 152-ФЗ, 161-ФЗ, 187-ФЗ
- ГОСТ 57580
- Приказ ФСБ России № 282
- СТО БР ИББС и РС БР ИББС-2.5-2014
- Международные стандарты PCI DSS, ISO 27001

Влияние регуляторов на рынок крайне ценно, так как многие СЗИ начинают использовать в приказном порядке, и лишь потом осознают их пользу

ФЗ и другие нормативные документы создают благоприятную среду для массового изучения и применения более сложных ИБ-продуктов, таких, как SIEM (EDR, PAM, XDR, наконец)



ДРАЙВЕРЫ РЫНКА

RUSIEM
Всё под контролем

ФЗ РФ
от 27 июля 2006 г.
№ 152-ФЗ
«О персональных данных»

ГОСТ Р 57580.1-2017
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

ФЗ РФ от 26 июля 2017 г.
№ 187-ФЗ
«О безопасности критической информационной инфраструктуры РФ»

ISO/IEC 27001
«Системы менеджмента информационной безопасности. Требования»

ГОСТ Р 57580.2-2018
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

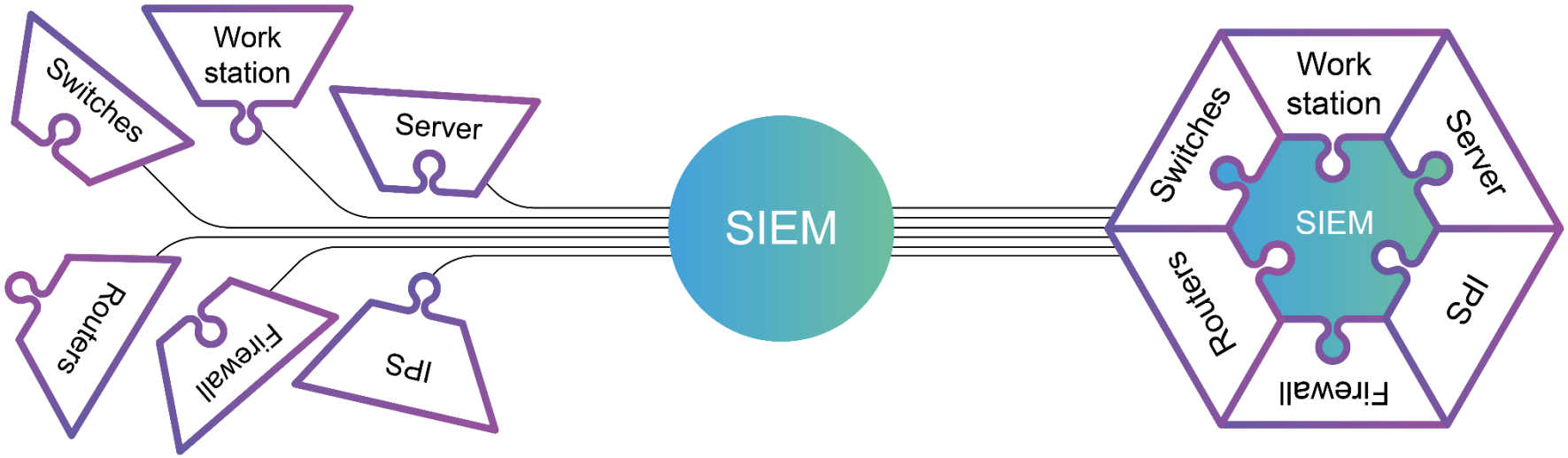
SIEM НА ПОЛКЕ

SIEM – дорогая и сложная система, которая способна приносить массу пользы, если начать ею пользоваться

SIEM ДЛЯ ПРОИЗВОДСТВА

Конвейер работает, не работает коммутатор, через который мы ведем управление. Как много времени уйдет на устранение причины простоя? А если есть SIEM?

ПРИМЕР ИСПОЛЬЗОВАНИЯ SIEM



- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения
- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Сетевое активное оборудование
- Сканеры уязвимостей
- Система инвентаризации и asset-management (а у некоторых СИЕМ есть даже свой внутренний функционал работы с активами)
- Система веб-фильтрации

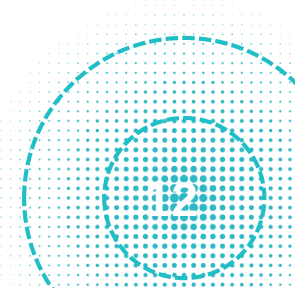
ВМЕСТО ИТОГА

Не отказывайтесь от того, что у вас и так есть

А если нет?

Не отказывайтесь поразмышлять на тему

«А чем SIEM может быть полезен мне?»



Спасибо за внимание!

Валерий Купрюшин, менеджер по техническому сопровождению продаж RuSIEM

www.rusiem.com

info@rusiem.com

+7(495)748-83-11