RUSIEM

Всё под контролем

Обеспечение безопасности объектов критической информационной инфраструктуры. Практика внедрения RuSIEM на ОКИИ.

О компании RuSIEM

Программный код
Создан российскими программистами

> 300

Пилотных внедрений

Sk Сколково

Резидент Сколково

> 100

Партнеров в России и странах СНГ

2014

С этого года ведется активная разработка

10000

Установок free-версии в мире в 2017-18 годах

Отечественное ПО
Сертификат ФСТЭК

2020

ГК «Программный Продукт» вошла в состав учредителей

РЕШЕНИЕ

RUSIEM

Всё под контролем

система мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени, для крупных и средних компаний

Линейка продуктов

RvSIEM (free)
классическое решение класса LM

RuSIEM
коммерческая версия

RuSIEM Analytics

RuSIEM Agent
агент под Windows OS

RuSIEM Replicator
утилита для массовой установки и управления агентами

ЧТО 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 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

RUSIEM
Всё под контролем

КАК РАБОТАЕТ SIEM

Универсальный ответ – **взаимосвязь**

событий инфраструктуры. Некоторые собирают NetFlow. Используя эти данные, SIEM дает представление о событиях сети

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

Система собирает логи с источников

Имея все данные о каждом событии,

RUSIEM
Всё под контролем

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 (сетевых устройств, приложений, 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 атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

ДРАЙВЕРЫ РЫНКА

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»

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)

Проблематика объектов КИИ

- Формальный подход к ИБ
- Сложности обновления ПО в условиях производства
- Старое проприетарное оборудование
- Отсутствие ресурсов как финансовых, так и кадровых
- Отсутствие стандартизации и требуемой защиты систем в контуре предприятия
- Разветвленная филиальная структура
- Трудности защиты цифровой экосистемы компании в постоянно изменяющейся инфраструктуре
- Потребность мониторинга ИБ компании в реальном времени и ретроспективный анализ
- Обеспечение целостности инфраструктуры

RuSIEM как средство обеспечения эффективной кибербезопасности ОКИИ

Централизованное управление

Максимально предустановленный функционал

Подключение любых источников данных

Использование передовых технологий (ML, AI)

Обработка данных в центрах ИБ без нарушения целостности процессов в заказчике.

SIEM –как средство комплексной обработки ИБ

Оптимизация кадровых и финансовых ресурсов

Точность определения событий более 97%

Возможность проведения расследования по «горячим» следам. Обнаружение потенциальных угроз на ранних стадиях

ТЕХНОЛОГИИ

1. В основе решения заложена собственная технология, основанная на потребительском спросе, практическом опыте и техническом анализе конкурентов

2. Используются современные принципы разработки, позволяющие решению развиваться, заменять модули и пополнять решение новыми, подстраиваться под потребности клиентов

3. Практическое использование AI и DL технологии

Конкурентные преимущества

Полная поддержка русского языка

Приведенная к общему формату объектная нормализация

Встроенная управляемая и редактируемая корреляция

Высокая производительность (свыше 90000 событий на одну ноду)

Нет ограничений по количеству событий и источникам

Сохранение исходных RAW-событий

Нет ограничений по размеру архивного хранилища

Коннекторы от производителя

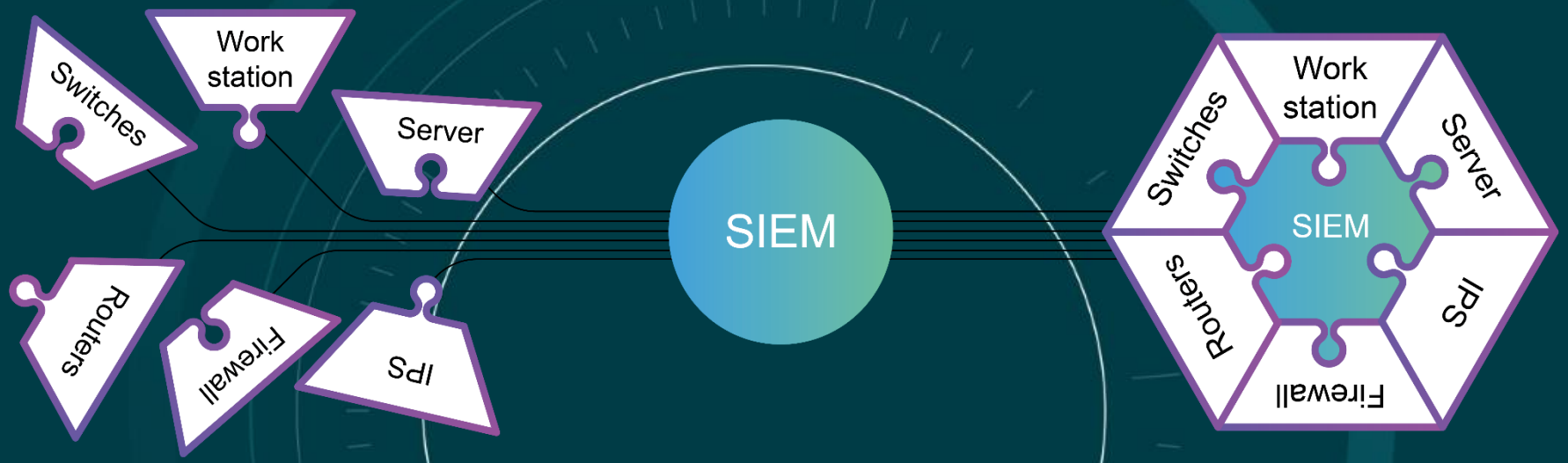
Real-time и историческая корреляция

Наличие собственных модульных агентов

Разделение нагрузки на несколько серверов или виртуальных машин

Легкая вертикальная масштабируемость

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

RUSIEM

Всё под контролем

Story Time

Заказчик выбрал наиболее производительное решение

Среди всех участников пилотов и конкурса только **RuSIEM** смог обеспечить поддержку более 80 000 тысяч событий, передаваемых со множества устройств заказчика

ГКУ СК КЦИТ

Создание центра мониторинга для объекта критической информационной инфраструктуры ГКУ СК КЦИТ

Результат:

- Сбор, обработка, отображение и долгосрочное хранение информации о событиях и подозрениях на инциденты ИБ, выявляемых в инфраструктуре организации;
- Предоставление инструментов для анализа событий и расследования инцидентов ИБ, в том числе, масштабных инцидентов ИБ;
- Предоставление исходной информации для определения влияния события или подозрений на инциденты ИБ.

Крупный ретейлер

СОБЫТИЕ 1
Проникновение, зашифровали пару серверов, потребовали выкуп

СОБЫТИЕ 2
Терминальный сервер скомпрометирован. 2 домена с Golden Ticket

СОБЫТИЕ 3
Брутфорс с получением доступа к серверу партнеров

9 МАРТА 2021
Выведены из строя более 10 серверов, потребовали выкуп. Пригрозили убить все

9 МАРТА 2021
Подключение специалистов к расследованию, развернули SIEM, выявили точки проникновения и зараженные узлы

10 МАРТА 2021
Ограничили распространение, изолировали сеть, сняли бэкапы критичных сервисов
Параллельно вели переговоры со злоумышленниками – затягивание времени

11 МАРТА – 25 МАРТА 2021
Защита сети

Заказчик самостоятельно стартовал пилот за 2 дня

- Инженер одной из ДЗО ГК Росатом самостоятельно скачал с сайта rusiem.com бесплатную версию RvSIEM.

Результат

После проведения пилота заказчик остался доволен и решил приобрести коммерческую версию RuSIEM на 10 000 EPS…

Заказчик на пилоте выявил «засланных казачков»

Заказчик на пилоте поставил цель выяснить: есть ли сотрудники, которые физически не прошли в банк (не прошли через СКУД), но авторизовались на рабочих станций. В итоге оказалось, что несколько человек незаконно имели доступ ко внутренним ресурсам…

Результат:

RuSIEM был закуплен, далее проведено внутреннее расследование и привлечены к ответственности виновные

Заказчик на пилоте выявил «Таргетированную атаку»

- Сценарий атаки был следующий
  1.В начале «неизвестный злоумышленник» провёл «разведку» в форме сканирования
  2.На следующем этапе при помощи рассылки письма с зараженным вложением, произошёл запуск вредоносного кода на рабочей станции локальной сети.
- 3. Завершающий этап таргетированной атаки это исходящие HTTP соединение с одного из хостов локальной сети на адрес «неизвестного злоумышленника»
  Данные действия, первоначально никак не связанные между собой, при корреляции событий с разных источников были идентифицированы RuSIEM как «таргетированная атака», которая была вовремя выявлена и остановлена.

Результат:

RuSIEM был закуплен, далее продукт был масштабирован на всю ГК.

RUSIEM
Всё под контролем

Перспективы развития.

- **Машинное обучение и нейросети**
- **Простота работы с системой**
- **Решение околоИБшных задач**
- **Гибкость использования при сохранении производительности**

RUSIEM
Всё под контролем

Обращайтесь!

Апанович Юлия
менеджер по работе с ключевыми заказчиками RuSIEM

www.rusiem.com
u.apanovich@rusiem.com
+7(903)785 01 78