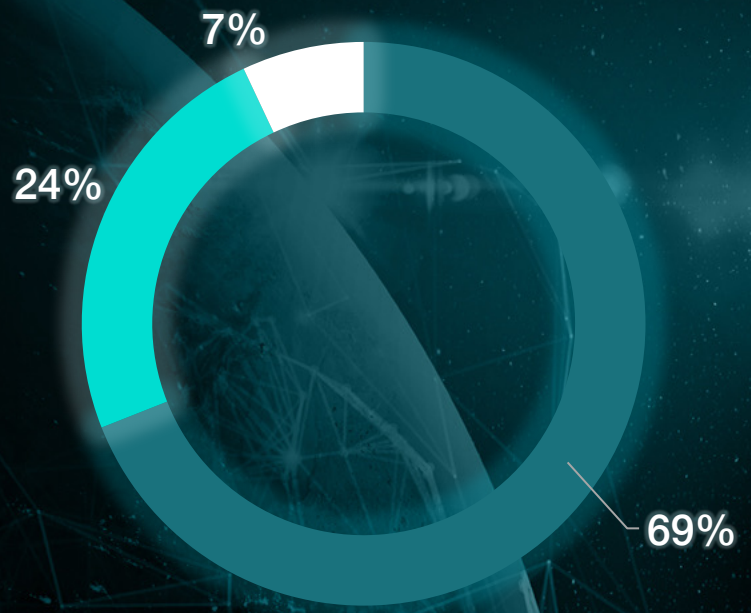
RUSIEM
Всё под контролем

Решение для контроля Вашего Бизнеса

Цели злоумышленника



Объекты атак

- Компьютеры, сервисы и сетевое оборудование
- Веб-ресурсы
- Люди

Чаще всего похищают

- Данные платежных карт
- Персональные данные
- Учетные данные
- Коммерческую тайну, ноу-хау
- Личную переписку

RUSIEM
Всё под контролем

Последствия

23%

организаций подверглись атакам, которые завершились прямыми финансовыми потерями

Возможные риски

- Фрод и мошенничество
- Нарушение непрерывности
- Несанкционированный доступ к данным
- Кибершпионаж и конкурентная разведка

Последствия

- Прямые финансовые потери
- Репутационные потери компании и ключевых лиц
- Компрометация данных
- Санкции со стороны регуляторов

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 сопоставлении 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

Что такое SIEM

Где может применяться SIEM?

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 ПО
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атак
- Влияние отказа в инфраструктуре на бизнес-процессы

Принцип работы SIEM

Сбор событий

Контроль инфраструктуры компании

Корреляция событий

Анализ всех поступающих событий

Управление и анализ

Выявление уязвимостей и аномалий

Выявление инцидентов

Составление цепочек событий и оценка риска

Принятие решения

Уведомление администратора об инциденте

События на вход

- 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

Линейка продуктов

RvSIEM (free)
классическое решение класса LM

RuSIEM
коммерческая версия

RuSIEM Analytics
модуль коммерческой версии

RuSIEM Agent
агент под Windows OS

RuSIEM Replicator
утилита для массовой установки и управления агентами

Первый отечественный SIEM

Программный код создан российскими программистами

> 300

Пилотных внедрений

Sk Сколково

Резидент Сколково

> 50

Партнеров в странах СНГ

2014

С этого года ведется активная разработка

Продукт включен в Единый реестр отечественного ПО

> 10000

Установок free-версии в мире

RUSIEM
Всё под контролем

Конкурентные преимущества

- Интеграция с ГосСОПКА и сертификация ФСТЭК России
- 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
- Вертикальная масштабируемость
- Горизонтальная масштабируемость
- Разделение нагрузки на несколько серверов или виртуальных машин
- Наличие собственных модульных агентов
- Real-time и историческая корреляция
- Коннекторы от производителя
- Нет ограничений по размеру архивного хранилища
- Сохранение исходных RAW-событий

КЛИЕНТЫ

Т2 ТИТАН2 ХОЛДИНГ

РСХБ страхование

ЦОДД

АКСОН

ФОРАБАНК

ГЕМОТЕСТ
МЕДИЦИНСКАЯ ЛАБОРАТОРИЯ

ПРИМ ТЕПЛО ЭНЕРГО

Пойдём!
Банк, который вам по душе