GSMK Система обнаружения и анализа несанкционированного доступа

GSMK Система обнаружения и анализа несанкционированного доступа

Высокоэффективная система обнаружения и анализа проникновений
Защитите «Ахиллесову пяту» вашей сети сигнализации

С момента технического основания протокола SS7 в 70-х годах прошлого века сложность современных сетей многократно выросла, а переход к новым технологиями сигнализации, например, Diameter, требует строгих полити безопасности и новых инструментов борьбы с мошенничеством, обрушением служб и шпионажем.

Oversight - это ключевая часть управления вашей сетью сигнализации, которая предусматривает эффективную аналитику и обнаружение угроз в трафике, проходящем через сигнальные точки, агенты Diameter, несущие и прочие каналы сигнализации.

Недавно были публично обнародованы уязвимости, присущие системам SS7 и Diameter, что открыло дверь для систематических нарушений в глобальном масштабе.

В современных реалиях, базовой фильтрации или межсетевого экранирования SS7, а также коммутационных сообщений Diameter для противодействия злоумышленникам, теперь, недостаточно ни для эффективной защиты оператора от финансовых потерь, ни для гарантии целостности сети с точки зрения безопасности данных или соответствия GDPR.

Без должных средств обнаружения и защиты от внешних атак ядро существующей инфраструктуры SS7 и Diamet не может быть безопасным:

Нарушение конфиденциальности пользователя услуг связи и хищение данных
Местонахождение пользователя может быть определено с точностью до улицы и его перемещение может отслеживаться постоянно.
Коды IMEI и IMSI могут быть считаны вместе со статусами вызовов и информацией об устройстве.
Незаконный перехват звонков и сообщений
Сообщения могут быть прочитаны, а звонки могут быть переадресованы неавторизованным третьим сторонам с использованием набора альтернативных методов, включая манипулирование данными абонента и извлечение ключа шифрования.
Мошенничество с платежами
Финансовые потери из мошенничества с платежами становятся все существенней.
Возможны манипуляции с данными абонента, включая несанкционированный перевод с предоплатной на пост-оплатную систему и USSD атаки на систему счетов.
Отказ в обслуживании (DoS)
В последнее время особую популярность получили направленные атаки через ISD/DSD или общая перегрузка сигнальных каналов, что наносит ущерб каналам передачи критических данных (критической инфраструктуре), а также голосовым службам.

Главные преимущества системы
Обнаружения проникновений операторского класса SS7 и Diameter

Масштабируемая архитектура системы
Совместимость с требованиями избыточности
Централизованное дистанционное управление
Графический интерфейс пользователя - интуитивно понятное управление системой
Узлы на основе Erlang/OTP
Профилирование элементов
Отказоустойчивость 99.999% рабочего времени
SLA, CARE и обязанности операторского класса
Полноценная поддержка SCTP/M3UA/M2PA
Поддержка M2PA
Анонимные отчеты для соответствия GDPR
Универсальная гибкость правил и действий
Полноценная поддержка OSS и облачных систем

Решение

Как признанный лидер отрасли в области надежного шифрования и сетевой безопасности, компания GSMK разработала систему Oversight для комплексного обнаружения аномалий сигнальной сети, непрерывного контрол и сигнализации.

AT Communication ©

Архитектура системы Oversight предусматривает прямую интеграцию в существующие сигнальные структуры и соответствует требованиям избыточности в пределах сбалансированной нагрузки на оборудование.

Дизайн системы

Система безопасности сети Oversight, основанная на модульном и масштабируемом подходе, состоит из модуля Oversight Manager, который осуществляет централизованную обработку данных, а также из нескольких узлов Oversight Detector в соответствии с количеством соединяемых и защищаемых узлов STP или DEA.

Программное обеспечение

Программное обеспечение на основе Erlang/OTP и операционная среда формируют высокопараллельную, отказоустойчивую безостановочную систему реального времени с максимальной доступностью и расширяемостью для надежного обнаружения атак и определения значения их параметров.

Визуализация и анализ

Основная задача любого инструмента анализа - это правильная графическая презентация поступающих данных. Только в этом случае данные станут информацией, а управление сложными системами не будет требовать длительного обучения.

Серверная часть системы формирует первоклассный пользовательский интерфейс на основе HTML5 (Клиентская часть Oversight) с интуитивно понятным централизованным управлением.
Визуализация предусматривает различные уровни эксплуатации, т.е. фильтр конфигурации, фильтр группировки, графики. журналы, отчеты, сигнализация и администрирование системы

Развертывание

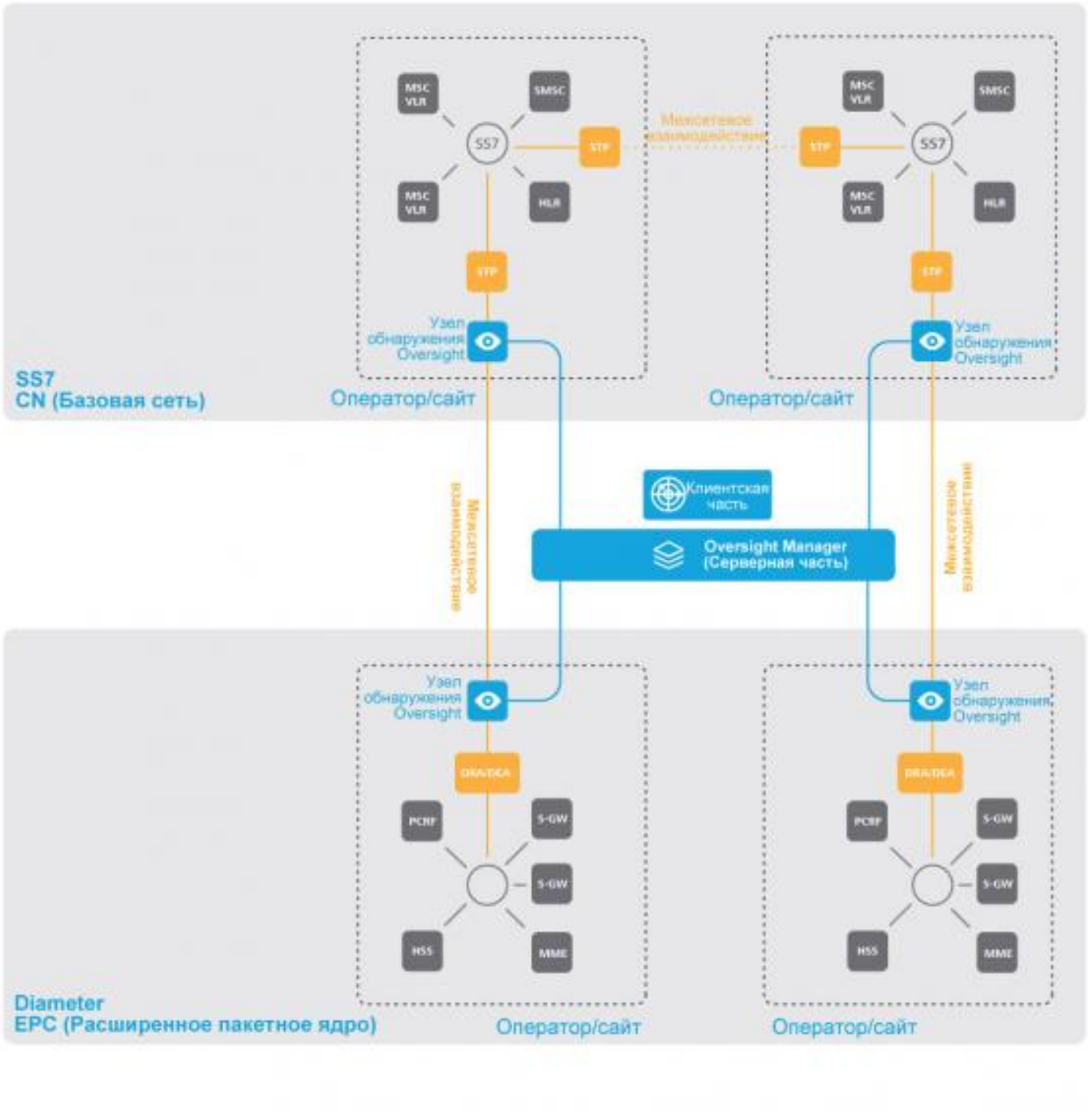
Компания GSMK осуществляет поддержку своих клиентов до, после и в процессе развертывания системы и осуществляет необходимый ее анализ, развертывание, обучение и калибровку в соответствии с индивидуальным SLA.

Лабораторная версия

Лабораторная версия системы доступна для проверки и обслуживания.

Архитектура системы Oversight

Множество технологий, множество сайтов, множество операторов, готовность к 5G

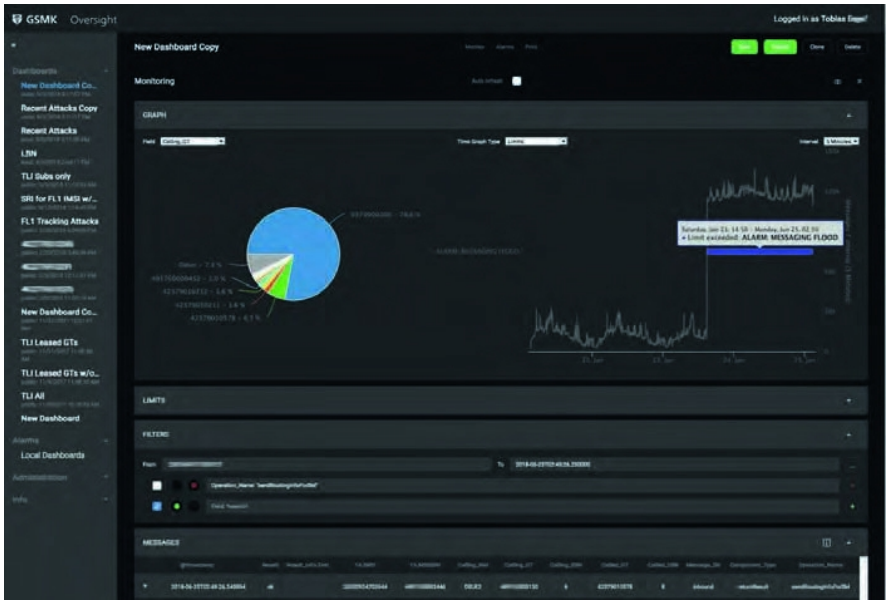


Пользовательский интерфейс Oversight

Визуализации данных и управление системой

Клиентская часть Oversight
Представление информации в виде приборной панели

Клиентская часть Oversight
Фильтры, пороги срабатывания и сигнализация



Клиентская часть Oversight
Тщательная проверка данных

Аппаратная часть Oversight

Визуализации данных и управление системой

Узел обнаружения Oversight
Высококачественное устройство
HP ProLiant, Поколение 10

Мониторинг системы

Серверная часть GSMK поддерживает контроль работоспособности через интерфейс клиентской части и SNMP (RFC 1157, RFC 3410) для задач централизованного мониторинга.

Мнеджер Oversight

Масштабируемый сервер высшего класса для критически важных приложений

Мониторинг системы

Серверная часть GSMK поддерживает контроль работоспособности через интерфейс клиентской части и SNMP (RFC 1157, RFC 3410) для задач централизованного мониторинга.

GSMK Oversight - Система обнаружения и анализа несанкционированного доступа