Система мониторинга безопасности сети RSA NetWitness

Усложнение угроз безопасности информации, высокий профессионализм нарушителей, появление угроз типа Advanced Persistance Treats заставляет организации искать новые решения для их нейтрализации или парирования.

Большинство нарушений безопасности связано с применением сетевых технологий и их выявление часто требует глубокого анализа сетевого трафика. Эта задача сложна как технологически, так и с точки зрения выделяемых ресурсов. Существующие средства либо имеют ограничения (IDS/IPS), либо предоставляют возможность детально исследовать сетевой трафик, но требуют высочайшей квалификации специалиста, больших трудозатрат и недостаточно автоматизированы в части поиска следов подозрительной активности (снифферы и средства анализа пакетов).

RSA NetWitness — это решение нового класса, сочетающее в себе целый букет инновационных технологий мониторинга безопасности сети за счет сбора и анализа сетевого трафика и реализующее самые современные подходы в этой области.

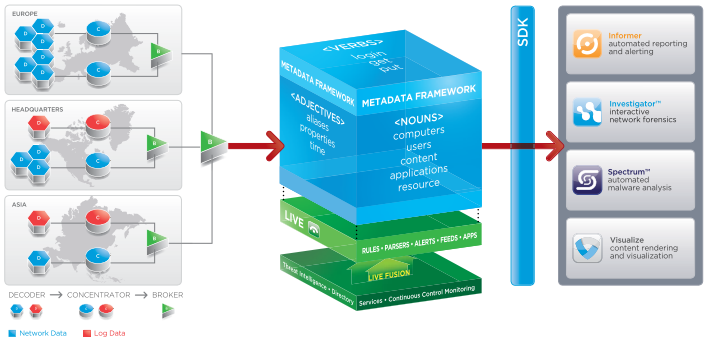
Возможности системы

Система RSA NetWitness — это масштабируемое решение для мониторинга безопасности сети, которое осуществляет:

- сбор, хранение и обработку всех проходящих по сети пакетов;
- быстрый анализ гигантских (терабайты) объемов данных;
- восстановление, визуализацию и интерактивный анализ сетевых сессий с интуитивно понятным представлением данных (голос, файлы, почтовые сообщения, диалоги IM, web-страницы);
- контекстный поиск по содержимому сессий;
- выделение и анализ метаданных сетевых сессий;
- автоматизированный безсигнатурный поиск вредоносного ПО в сетевом трафике с приоритезацией угроз;
- предоставление исчерпывающей информации для расследования инцидентов безопасности;
- автоматизированное оповещение об угрозах и формирование многоуровневой отчетности (в том числе экспорт во внешние системы в форматах HTML, CSV и PDF);
- интеграцию с SIEM-системами;
- оперативное ситуационное информирование с помощью интегрированных консолей (Dashboards).

Архитектура

NetWitness — модульное решение, состоящее из аппаратной платформы NetWitness NextGen и набора приложений NetWitness AppSuite.

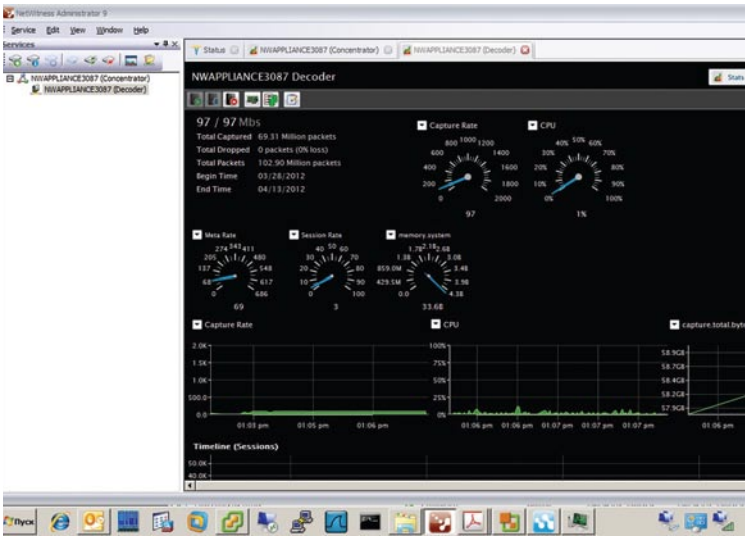


Платформа NetWitness NextGen — это три программно-аппаратных компонента: Decoder, Concentrator и Broker.

Decoder — устройство-сниффер, собирающие данные со SPAN-портов сетевого оборудования или TAP-устройств и передающие их концентраторам.

Concentrator — устройство, которое в режиме реального времени объединяют метаданные для анализа и в свою очередь передает их в брокер.

Broker — устройство, обрабатывающие запросы, касающиеся всей сети и данных с различных концентраторов (единая точка доступа ко всем метаданным).

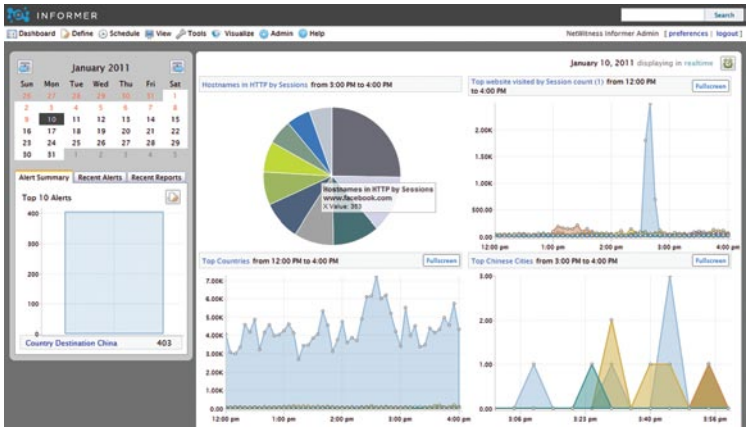


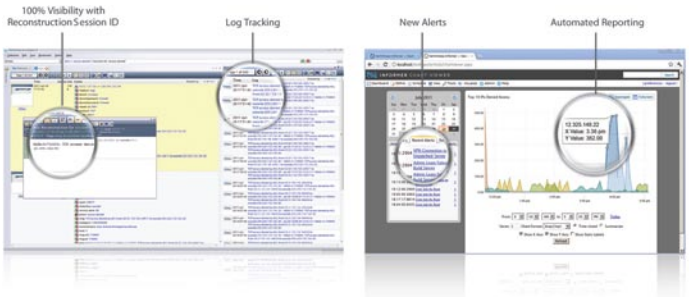
Модельный ряд устройств NextGen учитывает различные варианты реализации аппаратного комплекса:

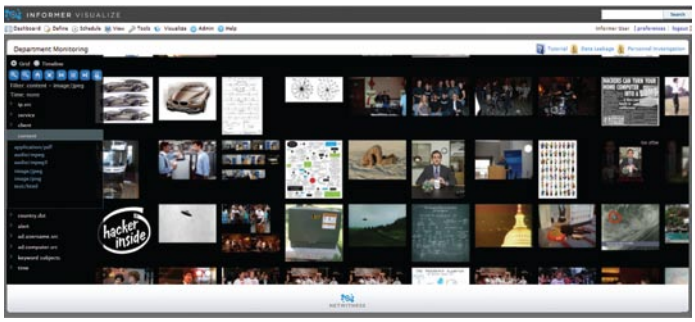
- Portable — портативная версия;
- Branch — версия для организаций с сетью филиалов;
- DataCenter — версия для центров обработки данных;
- Service Provider — комплекс для поставщиков услуг.

НТЦ ВУЛКАН

RSA
The Security Division of EMC







NetWitness AppSuite выполняет анализ информации, собранной NextGen. В его состав входят:

- **Informer** — приложение, предназначенное для формирования отчетности и оповещений об обнаруженных угрозах;
- **Investigator** — приложение, предназначенное для работы с метаданными и интерактивного анализа содержимого сетевых сессий, а также интуитивного представления результатов обработки;
- **Spectrum** — средство обнаружения вредоносного ПО, осуществляющий поиск в сетевом трафике на основе тысяч критериев и показателей;
- **NetWitness for Logs** — решение, осуществляющее корреляционный анализ данных из журналов событий и данных о сетевой активности (расширяет аналитические возможности SIEM-платформы RSA enVision, а также других SIEM-решений);
- **Vizualize** — приложение для интерактивной визуализации сессий (изображений, файлов, аудио и т.д.) с поддержкой multi-touch и drill-down;
- **SIEMLink** — средство для интеграции NetWitness с SIEM-системами;
- **Live** — сервис глобального анализа угроз, предоставляющий оповещения, отчеты и индикаторы.

Ценность для бизнеса и ИТ

Ключевой результат применения системы RSA NetWitness — повышение оперативности и полноты реакции службы ИБ на сетевые угрозы:

- понимание того, «чем дышит» сетевая инфраструктура;
- быстрая, полезная и достоверная аналитика сетевых сессий;
- уменьшение времени реакции на ИБ-инциденты и прерывания в оказании ИТ-услуг;
- качественная и интерактивная визуализация оперативной информации о сетевой активности;
- предоставление материалов (полномасштабной доказательной базы) для расследования ИБ-инцидентов;
- предоставление статистических данных для анализа рисков ИБ;
- помощь в противодействии целенаправленным атакам;
- повышение дисциплины и контроль соблюдения корпоративных правил безопасной работы в сети.

Профессиональный сервис

НТЦ «Вулкан», авторизованный партнер RSA, The Security Division of EMC, предлагает:

- демонстрацию возможностей RSA NetWitness и проведение пилотных проектов;
- разработку инженерно-технических решений по применению системы RSA NetWitness;
- разработку технической и эксплуатационной документации на русском языке;
- подбор (sizing), поставку и внедрение оборудования и приложений NetWitness;
- создание систем управления ИБ-инцидентами;
- интеграцию с другими системами (ServiceDesk, eGRC) и средствами управления событиями (SIEM);
- техническую поддержку на русском языке, в том числе выездную.

НТЦ «Вулкан»
105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
info@ntc-vulkan.ru
www.ntc-vulkan.ru