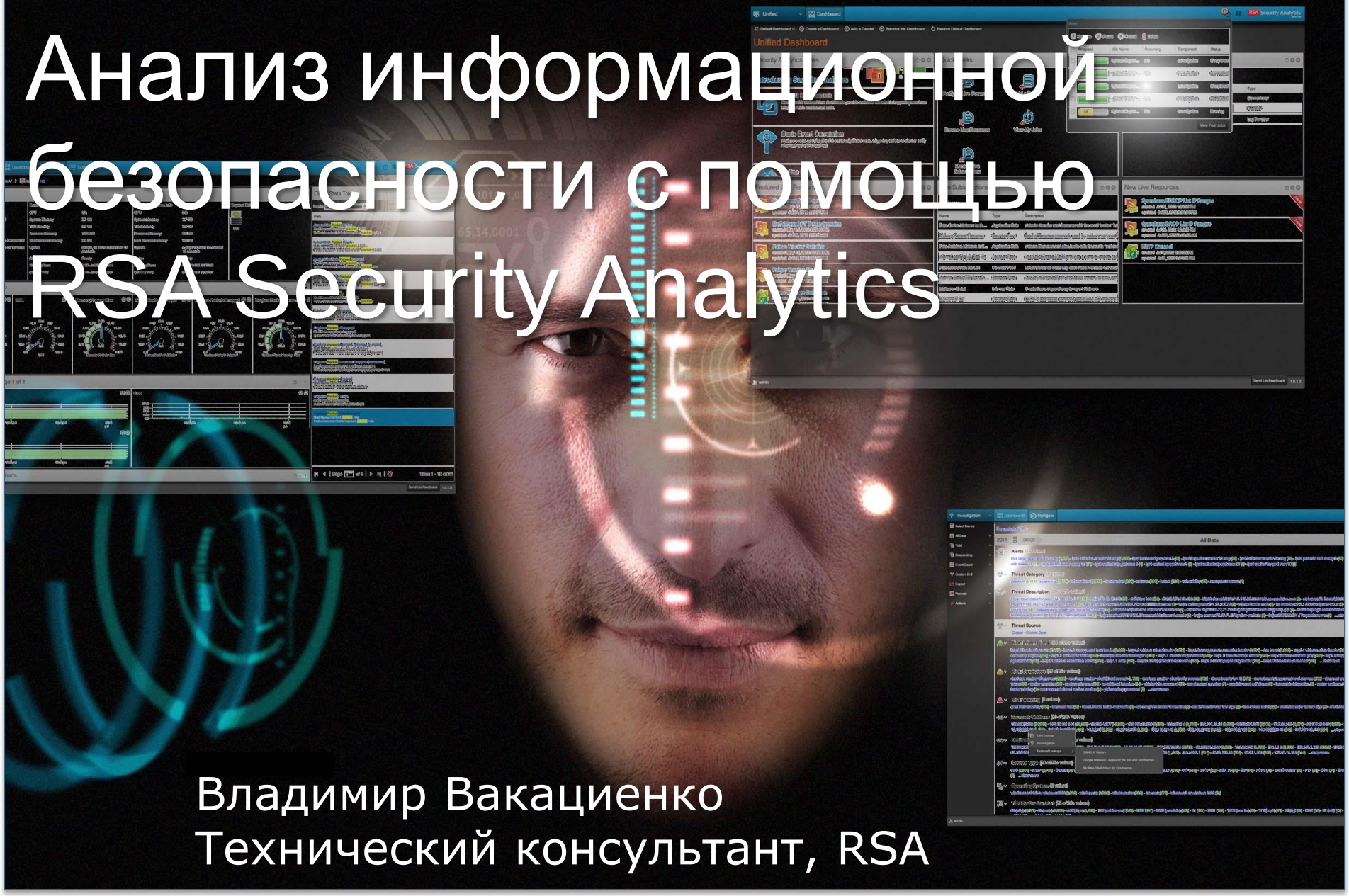
Анализ информационной безопасности с помощью RSA Security Analytics



Владимир Вакациенко
Технический консультант, RSA

RSA

EMC²

Классические SIEM системы

- Классические SIEM системы обеспечивают:
  - Отчеты по активности, связанной с устройствами и приложениями
  - Корреляцию, т.е. уведомления об уже известных последовательностях событий
  - Доказательства соответствия требованиям для внешних и внутренних аудиторов
  - Централизованное представление для различных источников событий

Однако, сегодня…

Угрозы изощренны, малозаметны и динамичны

Наиболее опасные атаки не были известны ранее, т.е. уникальны

Злоумышленники чаще всего не оставляют следов в логах

Традиционные средства защиты малоэффективны

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

99% взломов приводили к компроментации данных в течение “дней” или меньше и 85% приводили к похищению данных

Расследование 85% взломов занимало недели и более

Источник: Verizon 2012 Data Breach Investigations Report

Новые требования к системам мониторинга ИБ

Визуализация без ограничений

"Анализ всего, что происходит в инфраструктуре"

Оперативная аналитика

"Анализ и расследование потенциальных угроз в режиме близком к реальному времени"

"Интеллектуальные данные об угрозах"

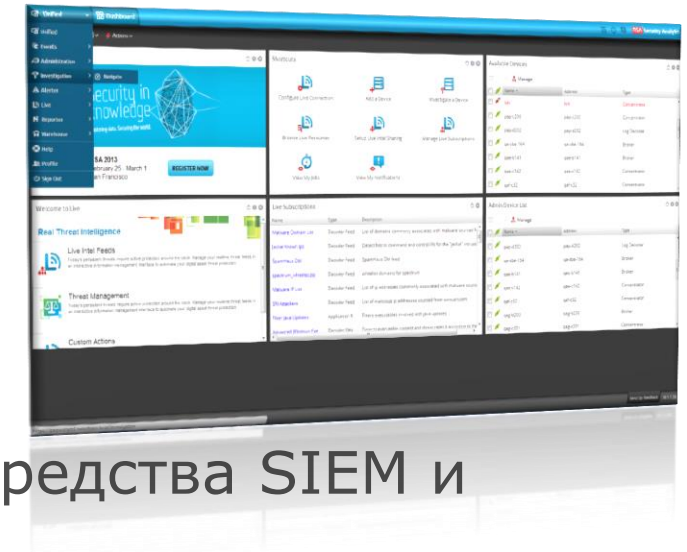
"Идентификация целей, угроз и инцидентов "

Масштабируемость

"Хранение и анализ как оперативных так и долговременных даннных"

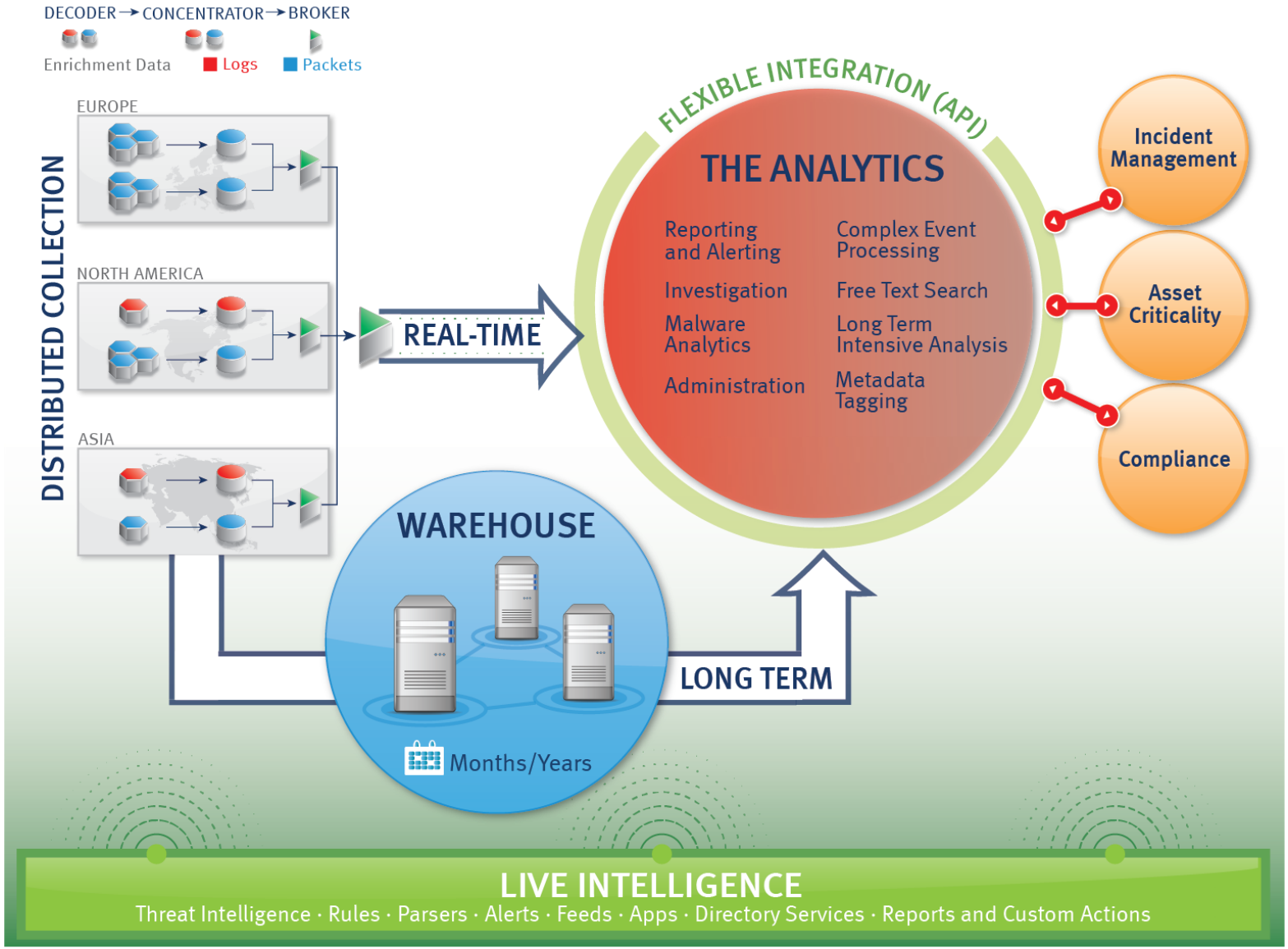
Что такое Security Analytics?

- Унифицированная платформа нового поколения для:
  - Мониторинга безопасности
  - Расследования инцидентов
  - Отчетности о соответствии требованиям

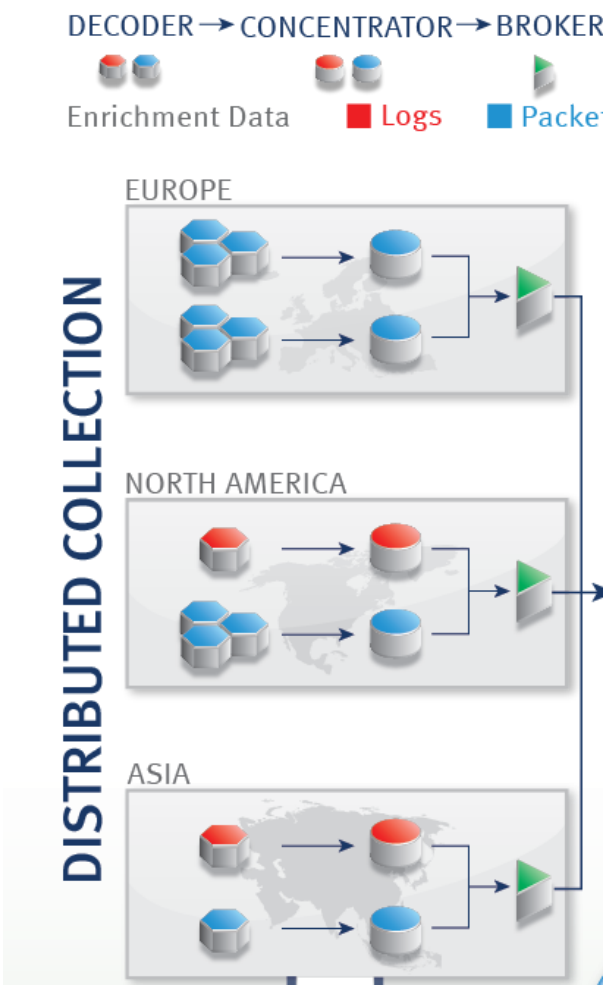


- Объединяет традиционные средства SIEM и мониторинга сетевой безопасности с технологиями обработки и анализа Больших Данных
- RSA Security Analytics новый подход к борьбе с угрозами повышенной сложности

Архитектура RSA Security Analytics



Инфраструктура сбора данных



- Единая платформа для сбора и анализа огромного количества информации о сетевом трафике и журналов событий
- Отлично зарекомендовавшая себя инфраструктура RSA NetWitness NextGen
- Распределенная масштабируемая архитектура
- “Коллективный разум” для анализа угроз

Интегрированные интеллектуальные данные об угрозах

Как узнать на что следует обращать внимание?

Сбор информации об интеллектуальных угрозах от сообщества ИБ & RSA FirstWatch

➔

Агрегация и консолидация наиболее значимой информации об угрозах и ее объединение с данными организации

➔

Автоматические обновления корреляционных правил, парсеров, отчетов, feed-ов, черные списки

Позволяет воспользоваться сторонними данными об обнаруженных угрозах и применять их для анализа текущих и исторических данных

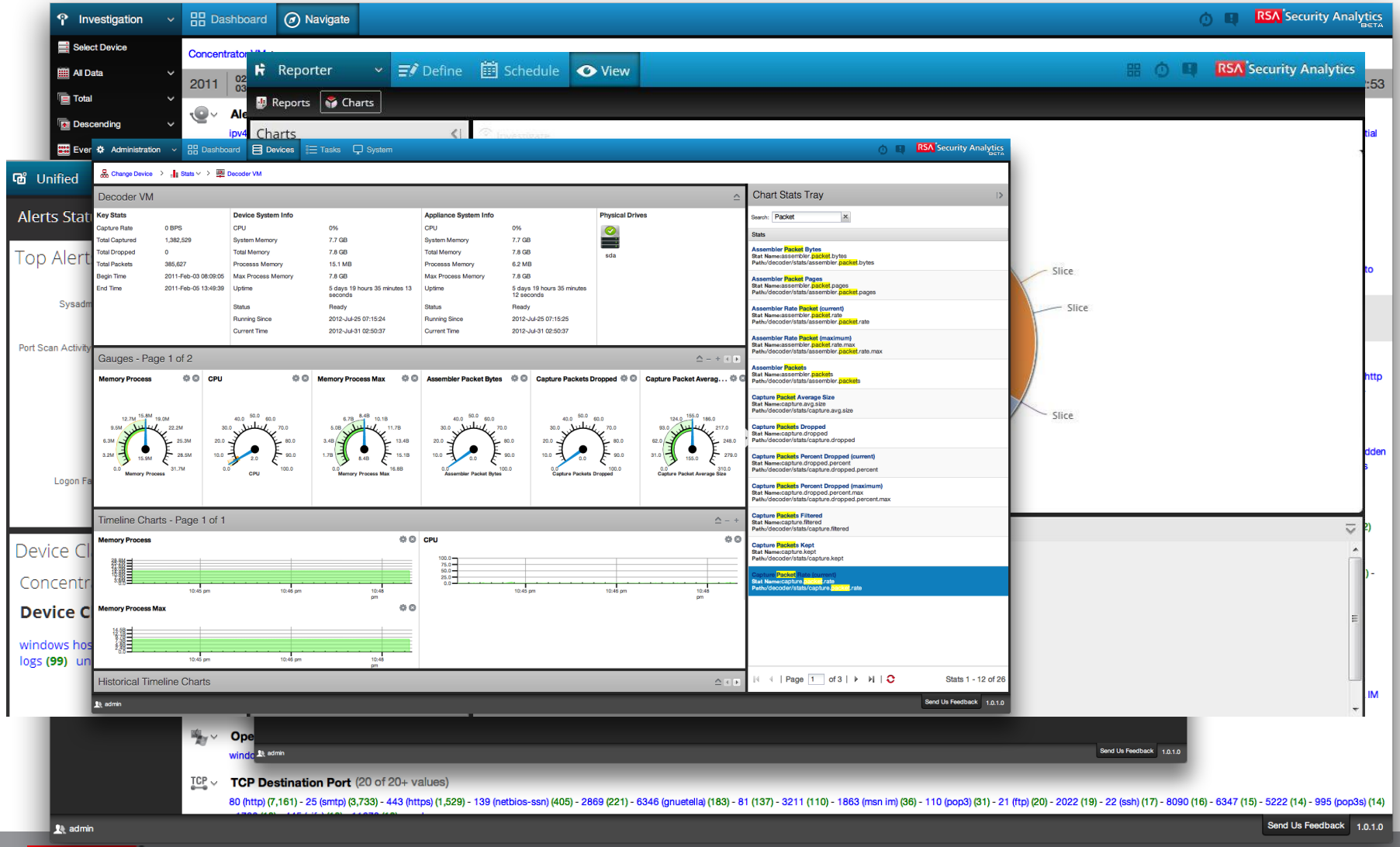
RSA Security Analytics Warehouse

- Долгосрочное хранение и анализ
  - Warehouse, оптимизированный для хранения данных ИБ
  - Хранение метаданных сетевых пакетов и журналов событий, “сырых” журналов
- Архитектура Hadoop для максимальной гибкости и масштабирования
- Сложная обработка событий
- “Google-подобный” текстовый поиск
- Соответствие требованиям регуляторов по долгосрочному хранению

Мощная аналитика Security Analytics

- Всесторонний анализ информационной безопасности организации
- Мониторинг в реальном времени и развитые средства расследований
- Интуитивно понятные аналитические средства
- Использование бизнес-контекста при расследованиях
- Автоматическая генерация разнообразных отчетов, включая отчеты за большие промежутки времени

Унифицированный интерфейс RSA Security Analytics

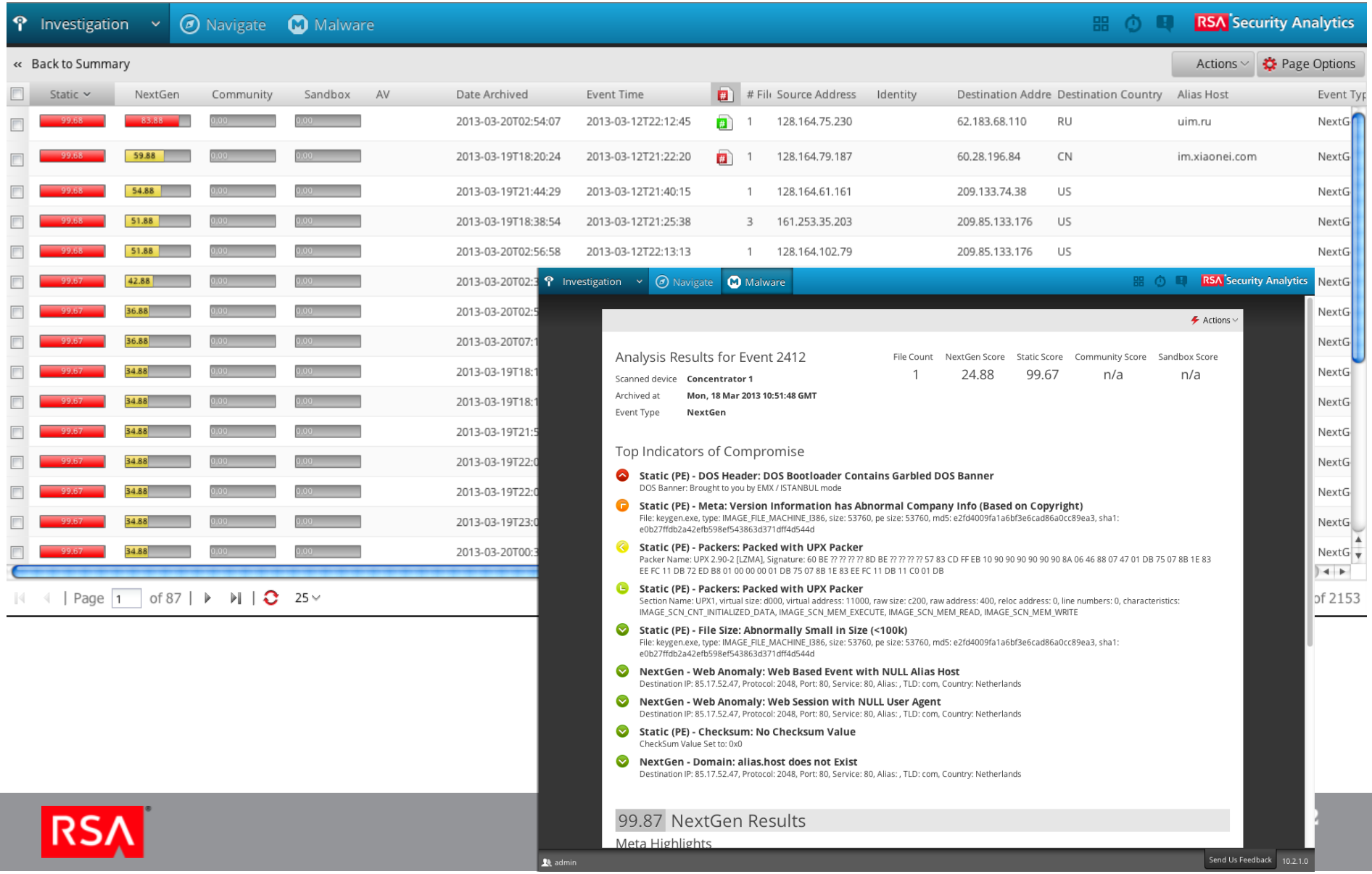


Анализ вредоносного ПО в RSA Security Analytics без использования сигнатур

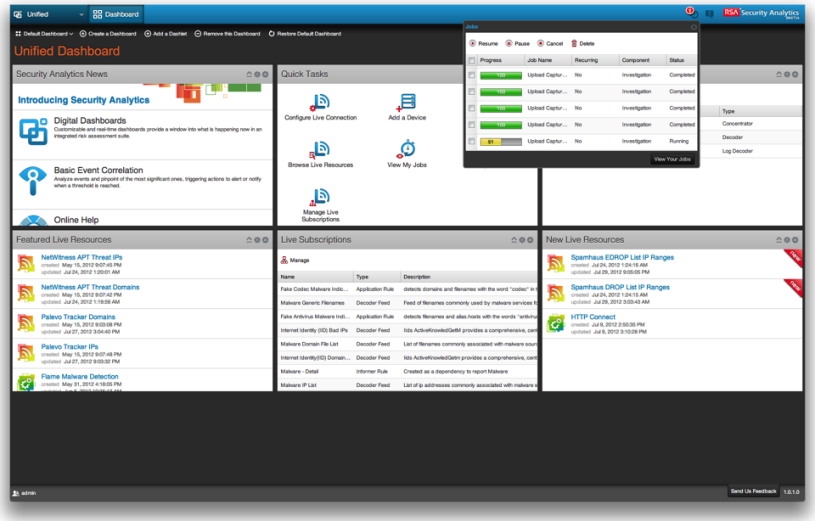
SA анализирует ВСЕ что происходит в сети по ВСЕМ протоколам, включая ВСЕ “исполняемое” содержимое.

NextGen	•**Задает сотни вопросов о появлении файла в сети и соответствующих сетевых сессиях** •**Например: Страна создания, Время создания, размер содержимого**
Статический анализ файла	•**JavaScript / Obfuscation, PDF Executable, Alerts present,** •**Size, Meta Tags, Cleaned, Packed, Obfuscated, и т.д.**
Community	•**Анализ информации из внешних источников - информационных и репутационных партнеров.**
Sandbox	•**Анализ поведения файлов в защищенной виртуальной среде** •**Может использоваться как локально, так и как SaaS подписка**

Автоматический скоринг вредоносного ПО

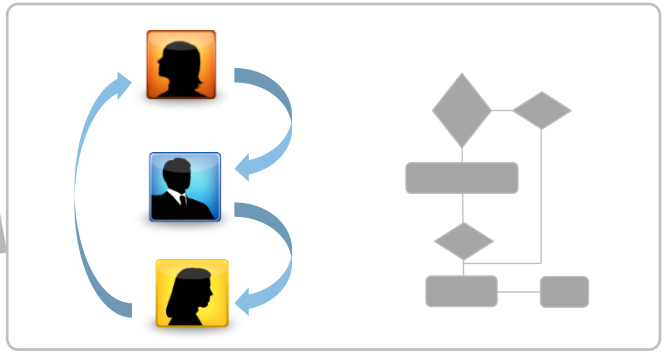


Использование бизнес-контекста



IP Add	Group	Rating	BU
198.100.1.0	Finance	High	Health Serv
198.51.100	HR	High	Health Serv
198.10.1.0	Purchase	Medium	Health Serv
192.10.0.0	Food & Bev	Low	Hospitality

ACI: Asset Criticality Intelligence



AIMS: Advanced Incident Management for Security

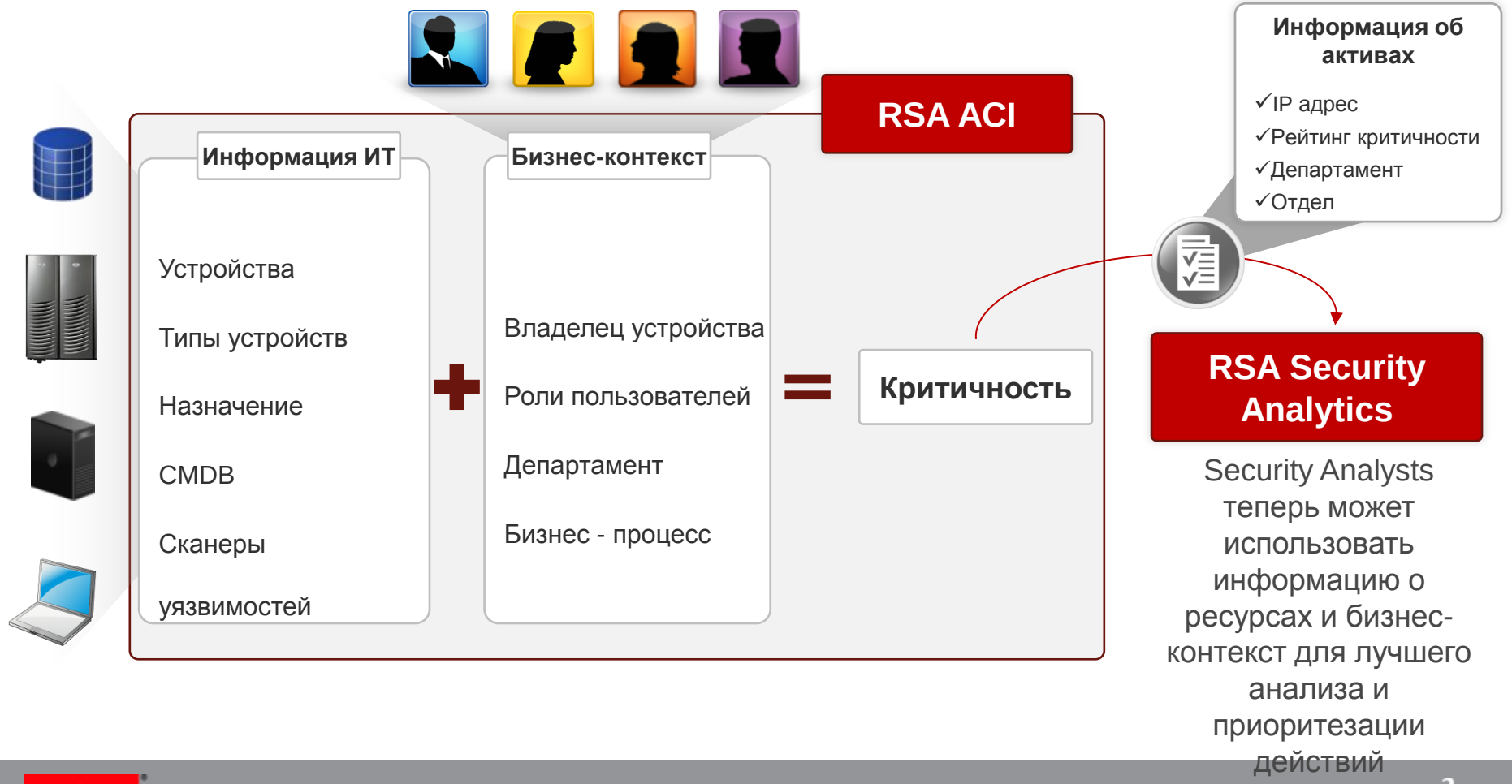
RSA Security Analytics

RSA Archer

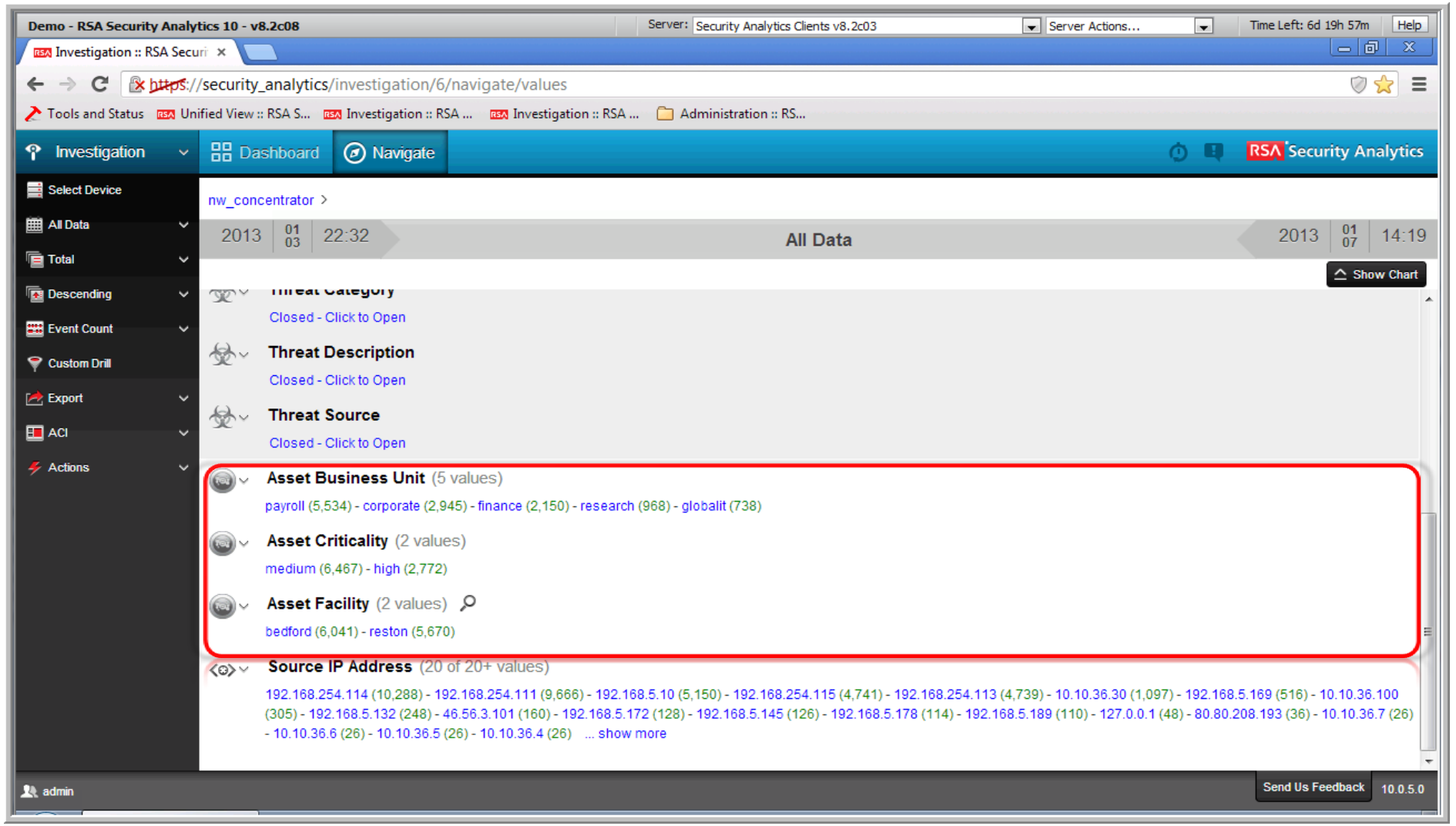
Данные об информационной безопасности

Данные об организации и пользователях

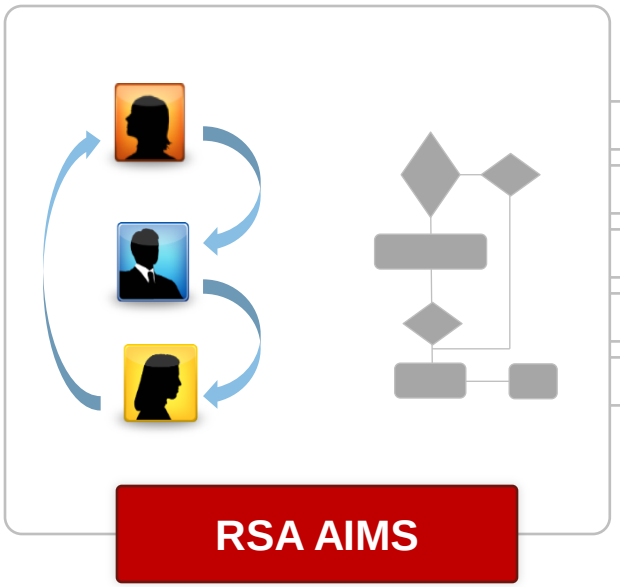
Обзор Asset Criticality Intelligence (ACI)



Security Analysts теперь может использовать информацию о ресурсах и бизнес-контекст для лучшего анализа и приоритезации действий

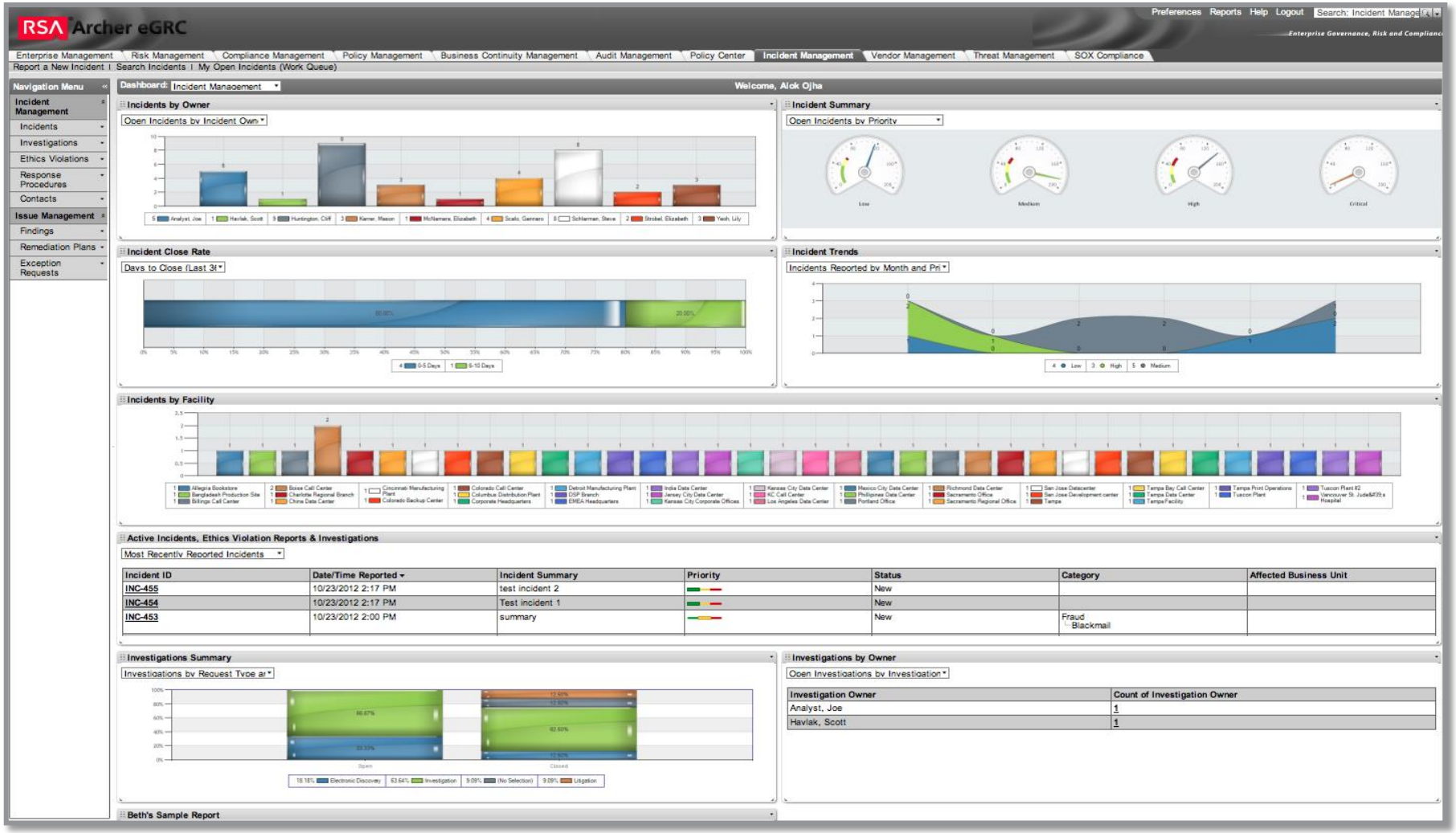


Advanced Incident Management for Security (AIMS)



- Обогащение данных
- Развитые Workflow
- Уведомления
- Отчетность
- Аудит

Advanced Incident Management for Security



Результат

- Уменьшение риска интеллектуальных целевых атак
  - Уменьшает время анализа с дней до нескольких минут
  - Уменьшает свободное время атакующих
- Поднимает эффективность информационной безопасности на новый уровень
  - Навыки подразделений ИБ увеличиваются за счет использования интеллектуальных данных
  - Информация хранится централизованно и расследования проводятся значительно быстрее.
- Применяет более гибкую модель управления безопасностью на основе анализа рисков


RSA


EMC²

Доп. слайды

Что мы поставляем

- Единая аппаратная платформа для всех компонент: Decoder, Concentrator, Broker
- Decoder и Concentrator используют либо SAN либо Direct Attached Capacity (DAC)
- Технические характеристики:
  - 96GB DDR3 RAM
  - Dual Hex Core Processors
  - Supports FC and SAS Storage
  - 3 x 1Gbps Input (1 management)
  - optional 10G interface

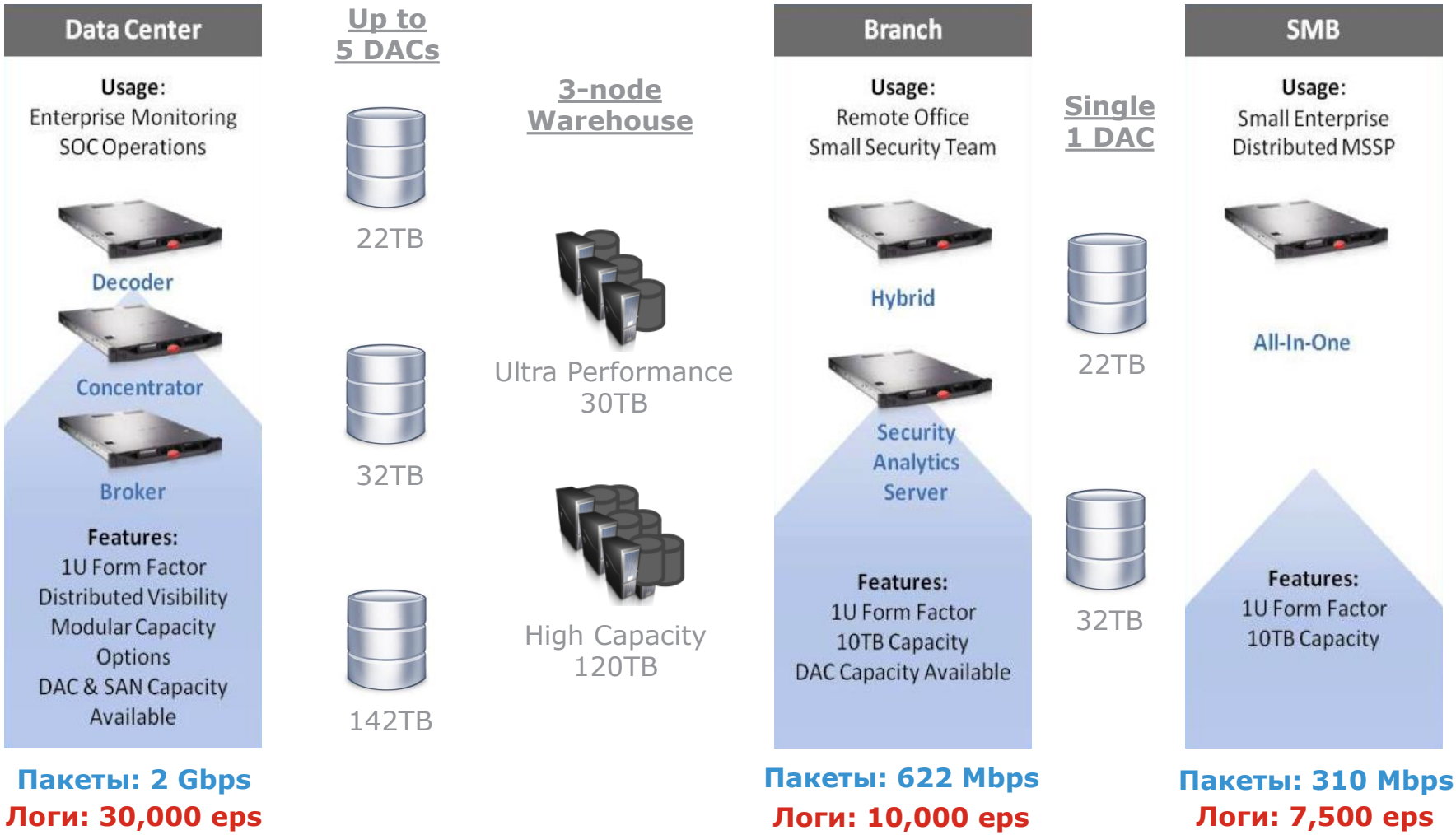
Хранение данных в RSA Security Analytics

- **Direct Attached Capacity (DAC)**
  - Подключение через SAS
  - Высокая емкость 32TB

    (для Decoder)
  - Высокая производительность 17.4 TB (для Concentrator)

- **SAN**
  - Подключение чераз Fiber Channel
  - Высокоемкостные и высокопроизводительные конфигурации
  - От 46TB до 1.5 PB (XXL) общей емкости

Варианты платформы Security Analytics



Пакеты: 2 Gbps
Логи: 30,000 eps

Пакеты: 622 Mbps
Логи: 10,000 eps

Пакеты: 310 Mbps
Логи: 7,500 eps