



EMC FORUM 2013

LEAD YOUR TRANSFORMATION

15 октября | Москва, Центр международной торговли

ОПЕРАТИВНЫЙ АНАЛИЗ
БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ
НА БАЗЕ RSA SECURITY ANALYTICS

Александр Иржавский, НТЦ «Вулкан»

ПОТРЕБНОСТИ В ОПЕРАТИВНОМ АНАЛИЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТ-инфраструктура и корпоративные сети становятся больше и сложнее

Атаки нарушителей становятся множественнее, динамичнее, изощреннее (APT)

Проблемы с безопасностью дорожают:

- Простои ИТ, производства, менеджмента
- Мошенничество и злоупотребления
- Утечка клиентской информации, персональных данных, ноу-хау
- Репутационные потери и отток клиентов

При этом: эффективность традиционных средств защиты мала

60% компаний из FORTUNE500
получали на свои внутренние email
адреса специально созданный
вредоносный код

В 88% компаний из FORTUNE500
была зарегистрирована активность
ботнетов в локальных сетях

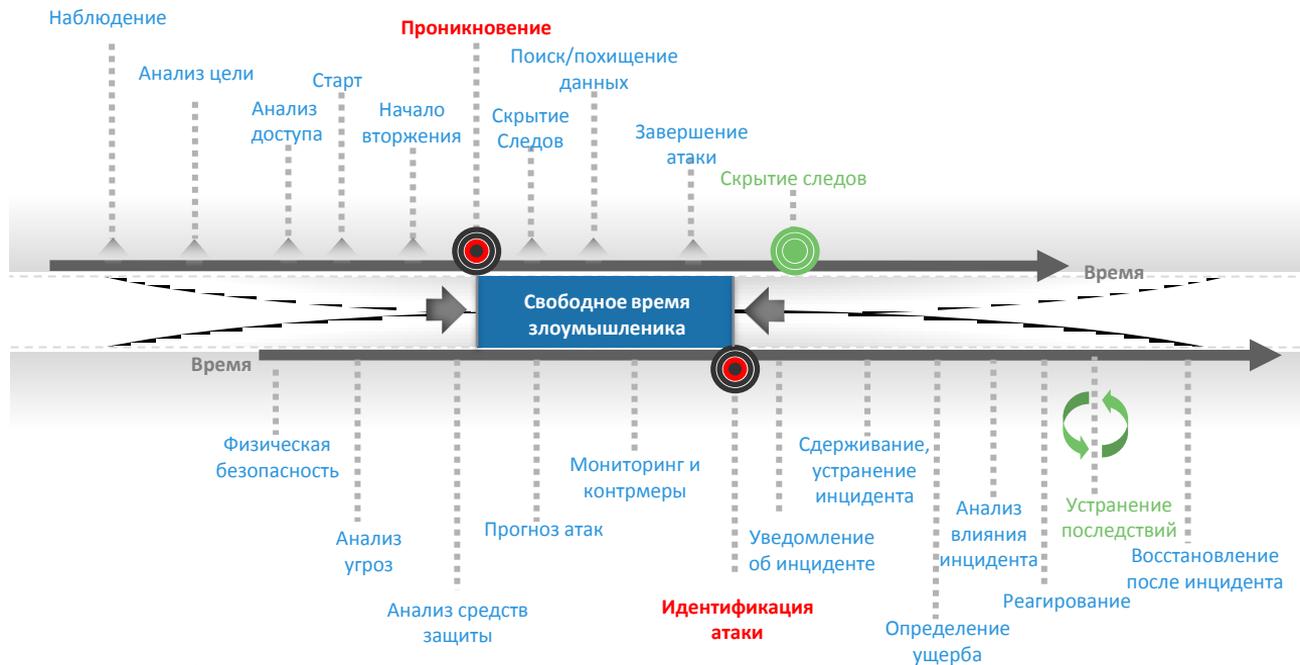
79% успешных кибератак
требуют на расследование
несколько недель

30% из 60 миллионов
известных вариантов
вредоносного кода было создано
в прошлом году



Источники: RSA Security Brief, Ponemon Institute Survey Conducted «Growing Risk of Advanced Threats», Verizon 2011 Data Breach Investigations Report

УМЕНЬШЕНИЕ СВОБОДНОГО ВРЕМЕНИ ДЛЯ ЗЛОУМЫШЛЕННИКОВ



Источник: NERC HILF Report

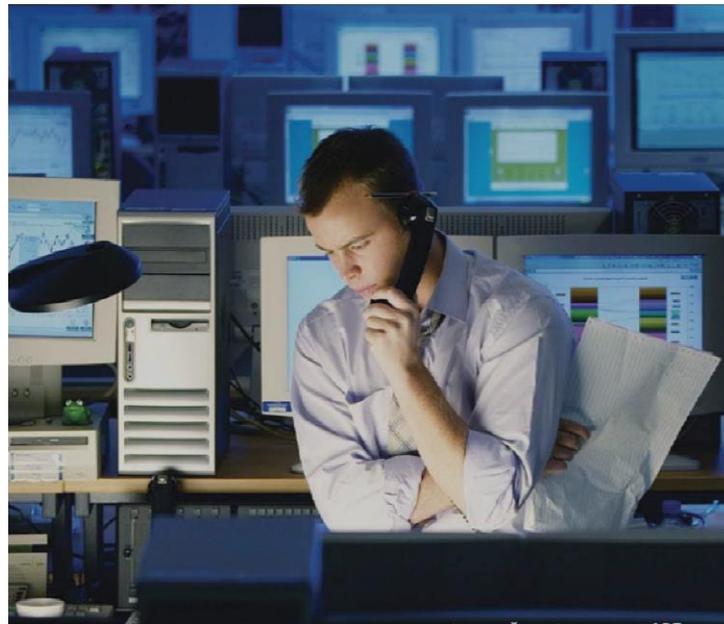
БЕЗОПАСНОСТЬ СТАНОВИТСЯ ПРОБЛЕМОЙ БОЛЬШИХ ДАННЫХ

Высокий уровень подготовки злоумышленников означает необходимость анализа большего количества данных для идентификации атаки

Усложнение ИТ-инфраструктуры означает, что даже простые атаки можно замаскировать

Современные трудности, с которыми сталкиваются специалисты по ИБ:

- 40% опрошенных утверждают, что перегружены собираемыми данными об ИБ
- 35% опрошенных утверждают, что не имеют времени и компетенции для анализа всей собираемой информации



EMA, The Rise of Data-Driven Security, Crawford, Aug 2012

НОВЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ МОНИТОРИНГА ИБ

Визуализация без ограничений

“Анализ всего, что происходит в
ИТ-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 данных”



ЧТО ТАКОЕ SECURITY ANALYTICS?

RSA Security Analytics – новый подход к борьбе с угрозами повышенной сложности (APT)

Унифицированная платформа нового поколения для:

- Мониторинга безопасности
- Расследования инцидентов
- Отчетности о соответствии требованиям

RSA Security Analytics объединяет три технологии:

- традиционные средства SIEM
- средства мониторинга сетевой безопасности
- технологии обработки и анализа Больших Данных

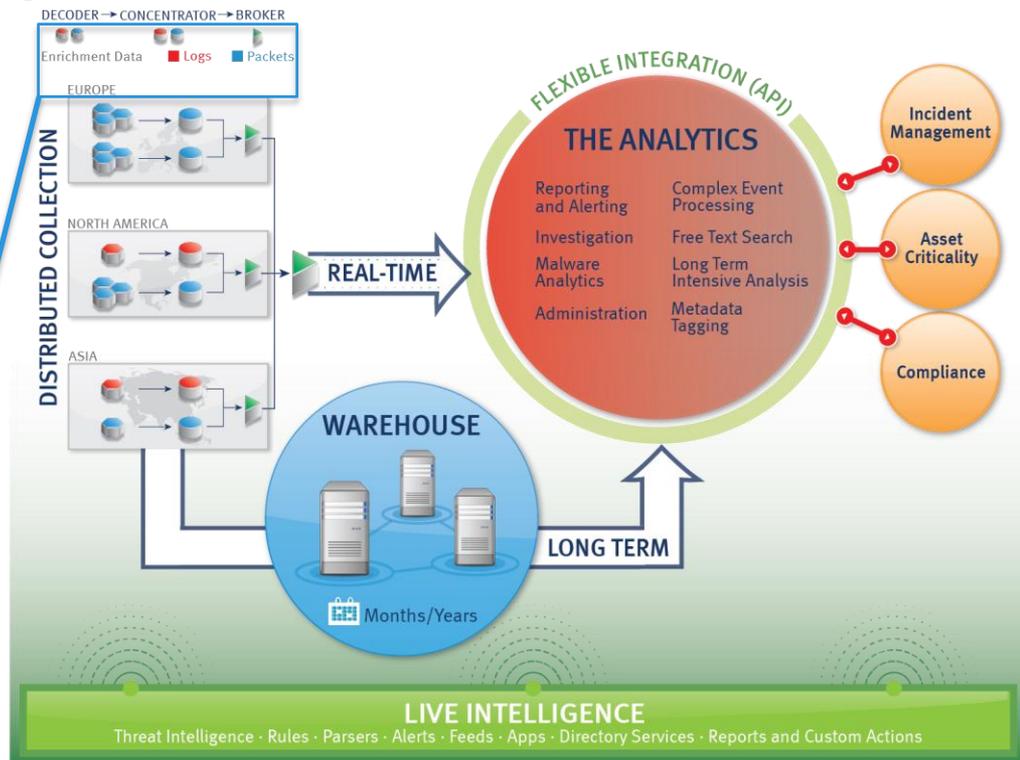


← Главное отличие
Security Analytics
от других систем мониторинга ИБ

АРХИТЕКТУРА RSA SECURITY ANALYTICS

Инфраструктура сбора данных
RSA NetWitness NextGen:

- Единая платформа для сбора и анализа:
 - информации о сетевом трафике
 - журналов событий
- Распределенная масштабируемая архитектура



КОНСОЛИДАЦИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ДАННЫХ ОБ УГРОЗАХ

LIVE INTELLIGENCE

Threat Intelligence · Rules · Parsers · Alerts · Feeds · Apps · Directory Services · Reports and Custom Actions

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

Возможность 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

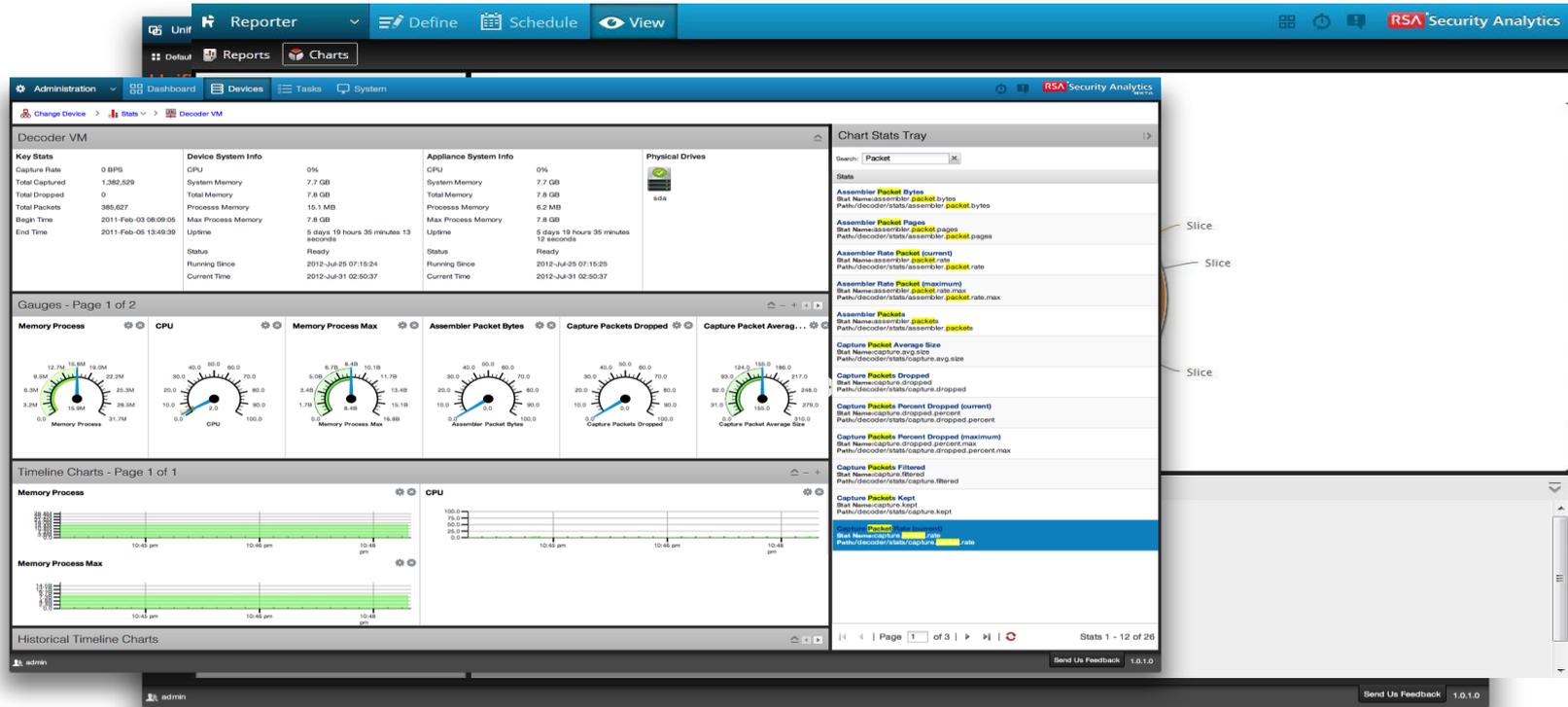
Соответствие требованиям регуляторов по долгосрочному хранению

МОЩНАЯ АНАЛИТИКА RSA SECURITY ANALYTICS

- Всесторонний анализ ИБ 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



Slice
Slice
Slice

АНАЛИЗ ВРЕДОНОСНОГО КОДА БЕЗ ИСПОЛЬЗОВАНИЯ СИГНАТУР

SA анализирует ВСЕ что происходит в сети по ВСЕМ протоколам, включая ВСЕ «исполняемое» содержимое.

NextGen

- Анализирует появление файла в сети и соответствующие сетевые сессии
Например: страна происхождения, 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 локально или как SaaS-подписка

ИСПОЛЬЗОВАНИЕ БИЗНЕС-КОНТЕКСТА

Security Analy
бизнес-конте

The screenshot displays the RSA Security Analytics 10 interface. The browser address bar shows the URL `https://security_analytics/investigation/6/navigate/values`. The main content area is titled "nw_concentrator" and shows data for 2013-01-03 at 22:32. The "All Data" section lists several threat-related items, each with a "Closed - Click to Open" link:

- Threat Category
- Threat Description
- Threat Source
- Asset Business Unit (5 values): payroll (5,534) - corporate (2,945) - finance (2,150) - research (968) - globalit (738)
- Asset Criticality (2 values): medium (6,467) - high (2,772)
- Asset Facility (2 values): bedford (6,041) - reston (5,670)
- Source IP Address (20 of 20+ values): 192.168.254.114 (10,288) - 192.168.254.111 (9,666) - 192.168.5.10 (5,150) - 192.168.254.115 (4,741) - 192.168.254.113 (4,739) - 10.10.36.30 (1,097) - 192.168.5.169 (516) - 10.10.36.100 (305) - 192.168.5.132 (248) - 46.56.3.101 (160) - 192.168.5.172 (128) - 192.168.5.145 (126) - 192.168.5.178 (114) - 192.168.5.189 (110) - 127.0.0.1 (48) - 80.80.208.193 (36) - 10.10.36.7 (26) - 10.10.36.6 (26) - 10.10.36.5 (26) - 10.10.36.4 (26) ... show more

A red rectangular box highlights the "Asset Business Unit" section. On the left, a sidebar menu includes options like "Unified", "Dashboard", "Security Analysis News", "Introducing Security Analytics", "Digital Dashboards", "Basic Event Correlation", "Custom Drill", "Export", "ACI", and "Address". The bottom of the interface shows a user profile for "admin" and a "Send Us Feedback" button.

Данни

security

СЛЯХ

РЕЗУЛЬТАТ

Уменьшение риска интеллектуальных целевых атак

Уменьшение времени анализа с нескольких дней до нескольких минут

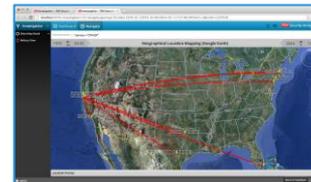
Уменьшение свободного времени злоумышленников

Повышение эффективности процессов обеспечения ИБ

Навыки подразделений ИБ улучшаются за счет использования интеллектуальных данных

Информация хранится централизованно, и расследования проводятся значительно быстрее

Применяется более гибкая модель управления безопасностью на основе анализа рисков



ЧТО ПОСТАВЛЯЕТСЯ?

Единая аппаратная платформа

- Для всех компонентов (Decoder, Concentrator, Broker)
- Decoder и Concentrator используют либо SAN либо Direct Attached Capacity (DAC)

Хранение данных:

- Direct Attached Capacity (DAC)
 - Подключение через SAS
 - Высокая емкость 32TB (для Decoder)
 - Высокая производительность 17.4 TB (для Concentrator)
- SAN
 - Подключение через Fiber Channel
 - Высокоемкостные и высокопроизводительные конфигурации
 - От 46TB до 1.5 PB (XXL) общей емкости



ВАРИАНТЫ КОМПЛЕКТАЦИИ

Data Center	Up to 5 DACs	3-node Warehouse	Branch	Single DAC	SMB
Usage: Enterprise Monitoring SOC Operations	 22TB	 Ultra Performance 30TB	Usage: Remote Office Small Security Team	 22TB	Usage: Small Enterprise Distributed MSSP
 Decoder	 32TB	 High Capacity 120TB	 Hybrid	 All-In-One	
 Concentrator			 Security Analytics Server	 32TB	
 Broker	 142TB		Features: 1U Form Factor 10TB Capacity DAC Capacity Available		Features: 1U Form Factor 10TB Capacity
Features: 1U Form Factor Distributed Visibility Modular Capacity Options DAC & SAN Capacity Available			Пакеты: 622 Mbps Логи: 10,000 eps		Пакеты: 310 Mbps Логи: 7,500 eps

ГДЕ ПОДРОБНЕЕ ОЗНАКОМИТЬСЯ И ПРОТЕСТИРОВАТЬ РЕШЕНИЕ?



Александр Иржавский

НТЦ «Вулкан», официальный партнер RSA

A.Irzhavsky@ntc-vulkan.ru

+7 (495) 663-95-16



The Security Division of EMC

Владимир Вакациенко

RSA, The Security Division of EMC - Россия

Vladimir.Vakatsienko@emc.com

+7 (495) 785-66-22



СПАСИБО ЗА ВНИМАНИЕ!

КОНТАКТЫ

Александр Иржавский

a.irzhavsky@ntc-vulkan.ru

EMC²®