

Анализ информационной безопасности с помощью RSA Security Analytics

Владимир Вакациенко
Технический консультант, RSA



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 изоциренны, 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



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

Источник: Verizon 2012 Data Breach Investigations Report

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			

Расследование 85% взломов занимало недели и более

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”



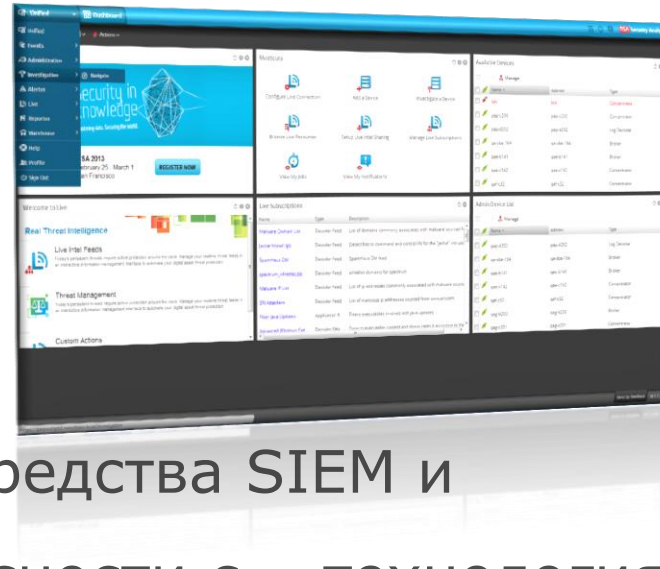
Масштабируемость

“Хранение и анализ как оперативных так и долговременных данных”

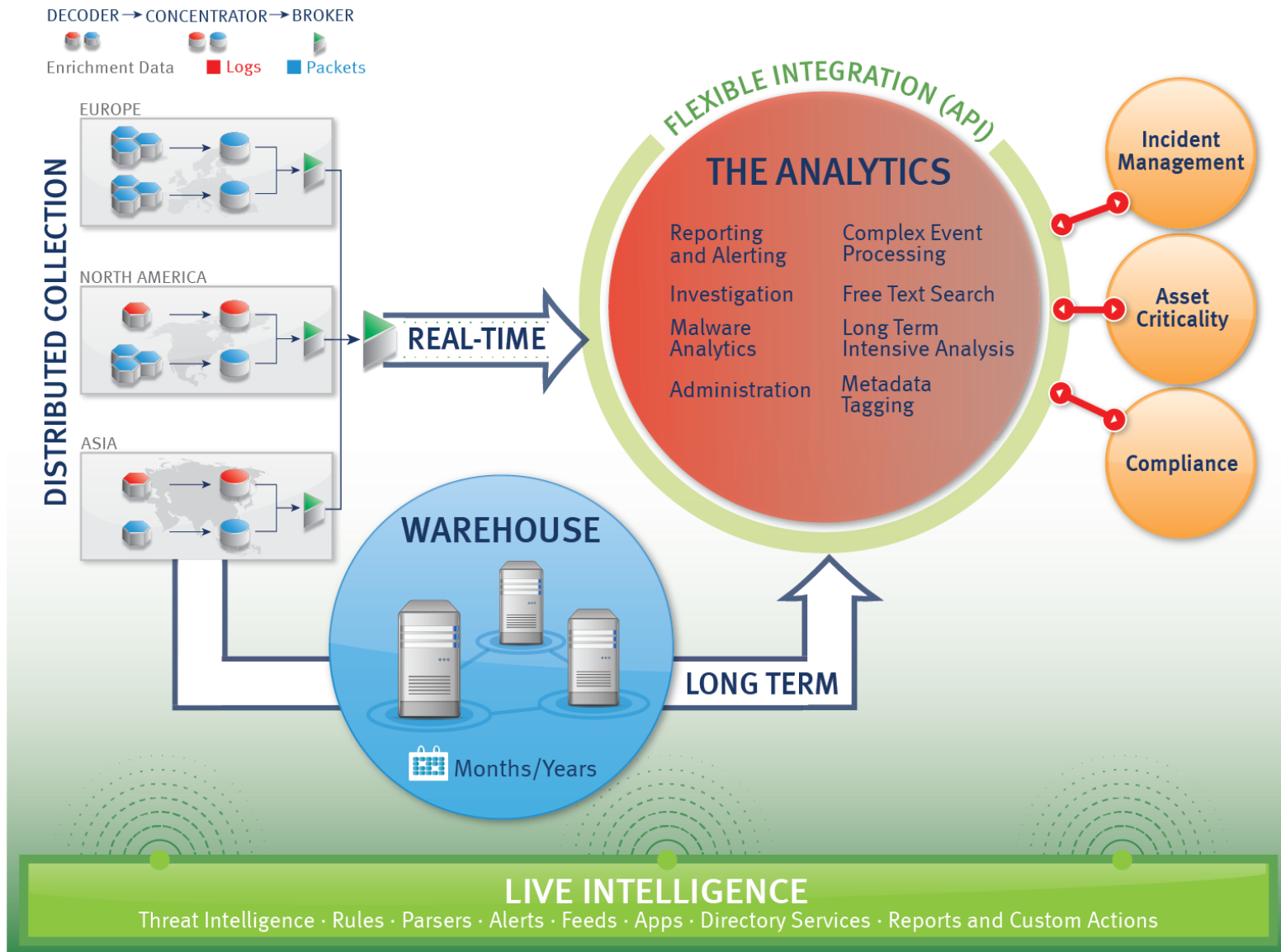


Что такое Security Analytics?

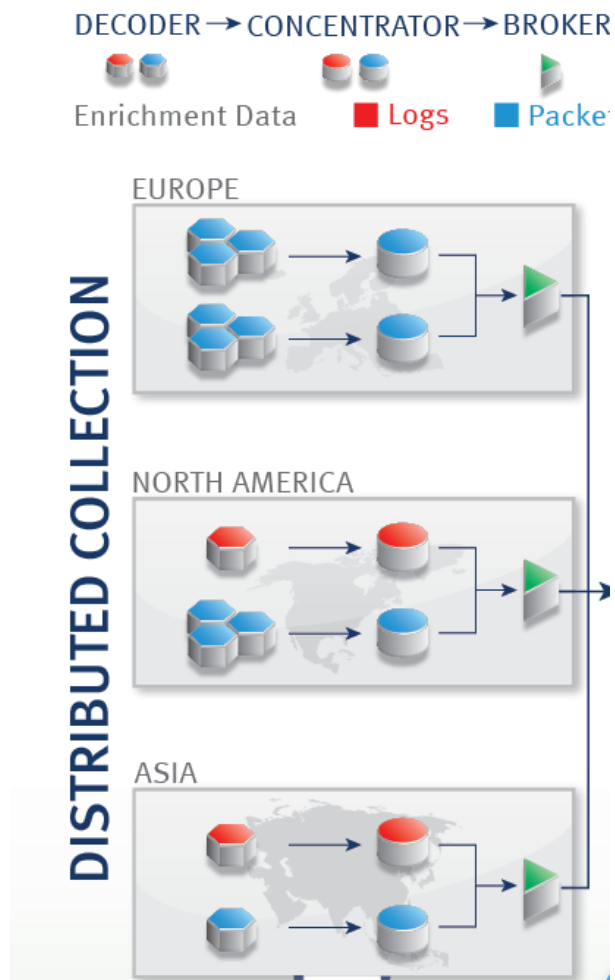
- Унифицированная платформа нового поколения для:
 - Мониторинга безопасности
 - Расследования инцидентов
 - Отчетности о соответствии требованиям
- Объединяет традиционные средства SIEM и мониторинга сетевой безопасности с технологиями обработки и анализа Больших Данных
- RSA Security Analytics новый 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



LIVE

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

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

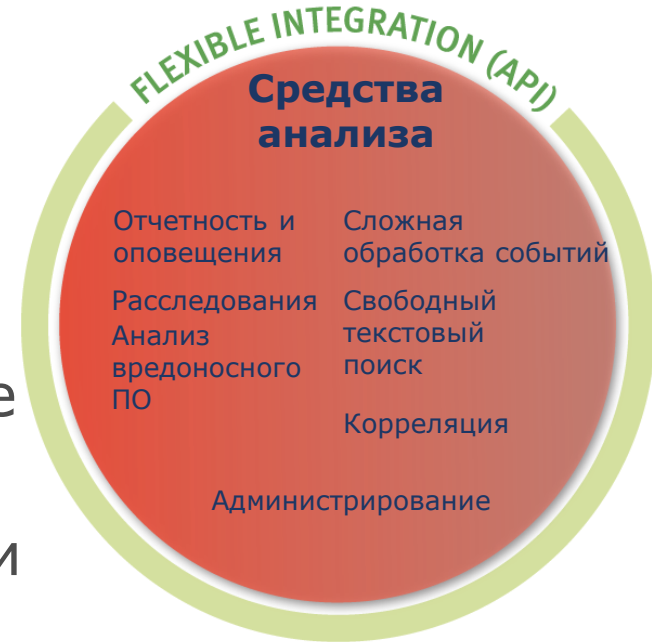
RSA Security Analytics Warehouse



- 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

The screenshot displays the RSA Security Analytics unified interface, which is a comprehensive dashboard for network security analysis. The interface is organized into several key sections:

- Navigation and Reporting:** The top navigation bar includes 'Investigation', 'Dashboard', and 'Navigate'. Below it, there are options for 'Reporter', 'Define', 'Schedule', and 'View'. A secondary bar contains 'Reports' and 'Charts'.
- Alerts and Top Alerts:** On the left side, there are sections for 'Alerts State', 'Top Alerts', and 'System', along with a 'Port Scan Activity' section.
- Key Stats and System Info:** The main dashboard area is divided into several panels. 'Key Stats' provides a summary of capture rates and dropped packets. 'Device System Info' and 'Appliance System Info' show resource usage like CPU, memory, and uptime. 'Physical Drives' indicates the status of storage hardware.
- Gauges and Charts:** A 'Gauges - Page 1 of 2' section features several circular gauges for 'Memory Process', 'CPU', 'Memory Process Max', 'Assembler Packet Bytes', 'Capture Packets Dropped', and 'Capture Packet Average Size'. Below this, 'Timeline Charts - Page 1 of 1' shows horizontal bar charts for the same metrics over time.
- Chart Stats Tray:** On the right side, a 'Chart Stats Tray' allows users to search for specific metrics (e.g., 'Packet') and view detailed statistics for various 'Assembler Packet' and 'Capture Packet' categories, including current and maximum values.
- Historical and Network Data:** At the bottom, there are 'Historical Timeline Charts' and a network traffic analysis section showing 'TCP Destination Port' with a list of active ports and their associated protocols.



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

- **Задаёт 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

Investigation | Navigate | Malware | RSA Security Analytics

<< Back to Summary | Actions | Page Options

Static	NextGen	Community	Sandbox	AV	Date Archived	Event Time	# File	Source Address	Identity	Destination Addr	Destination Country	Alias Host	Event Type
99.68	63.88	0.00	0.00		2013-03-20T02:54:07	2013-03-12T22:12:45	1	128.164.75.230		62.183.68.110	RU	uim.ru	NextG
99.68	59.88	0.00	0.00		2013-03-19T18:20:24	2013-03-12T21:22:20	1	128.164.79.187		60.28.196.84	CN	im.xiaonei.com	NextG
99.68	54.88	0.00	0.00		2013-03-19T21:44:29	2013-03-12T21:40:15	1	128.164.61.161		209.133.74.38	US		NextG
99.68	51.88	0.00	0.00		2013-03-19T18:38:54	2013-03-12T21:25:38	3	161.253.35.203		209.85.133.176	US		NextG
99.68	51.88	0.00	0.00		2013-03-20T02:56:58	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	42.88	0.00	0.00		2013-03-20T02:56:58	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	36.88	0.00	0.00		2013-03-20T02:56:58	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	36.88	0.00	0.00		2013-03-20T07:10:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T18:10:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T18:10:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T21:50:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T22:00:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T22:00:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-19T23:00:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG
99.67	34.88	0.00	0.00		2013-03-20T00:00:00	2013-03-12T22:13:13	1	128.164.102.79		209.85.133.176	US		NextG

Page 1 of 87 | 25

Analysis Results for Event 2412

Scanned device	File Count	NextGen Score	Static Score	Community Score	Sandbox Score
Concentrator 1	1	24.88	99.67	n/a	n/a

Archived at: Mon, 18 Mar 2013 10:51:48 GMT
Event Type: NextGen

Top Indicators of Compromise

- Static (PE) - DOS Header: DOS Bootloader Contains Garbled DOS Banner**
DOS Banner: Brought to you by EMX / ISTANBUL mode
- Static (PE) - Meta: Version Information has Abnormal Company Info (Based on Copyright)**
File: keygen.exe, type: IMAGE_FILE_MACHINE_I386, size: 53760, pe size: 53760, md5: e2fd4009fa1a6bf3e6cad86a0cc89ea3, sha1: e0b27fadb2a42efb598ef543863d371dff4d544d
- Static (PE) - Packers: Packed with UPX Packer**
Packer Name: UPX 2.90-2 (LZMA), Signature: 60 BE ?? ?? ?? 8D BE ?? ?? ?? ?? 57 83 CD FF EB 10 90 90 90 90 90 90 8A 06 46 88 07 47 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C0 01 DB
- Static (PE) - Packers: Packed with UPX Packer**
Section Name: UPX1, virtual size: d000, virtual address: 11000, raw size: c200, raw address: 400, reloc address: 0, line numbers: 0, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
- Static (PE) - File Size: Abnormally Small in Size (<100k)**
File: keygen.exe, type: IMAGE_FILE_MACHINE_I386, size: 53760, pe size: 53760, md5: e2fd4009fa1a6bf3e6cad86a0cc89ea3, sha1: e0b27fadb2a42efb598ef543863d371dff4d544d
- NextGen - Web Anomaly: Web Based Event with NULL Alias Host**
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands
- NextGen - Web Anomaly: Web Session with NULL User Agent**
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands
- Static (PE) - Checksum: No Checksum Value**
Checksum Value Set to: 0xd
- NextGen - Domain: alias.host does not Exist**
Destination IP: 85.17.52.47, Protocol: 2048, Port: 80, Service: 80, Alias: , TLD: com, Country: Netherlands

99.87 NextGen Results
Meta Highlights



Использование бизнес-контекста

The screenshot displays the RSA Security Analytics interface. It features a 'Unified Dashboard' with sections for 'Security Analytics News', 'Digital Dashboards', 'Basic Event Correlation', 'Online Help', and 'Featured Live Resources'. A 'Jobs' window is open, showing a list of tasks with columns for 'Progress', 'Job Name', 'Recurring', 'Component', and 'Status'. Below the dashboard, there are sections for 'Live Subscriptions' and 'New Live Resources'.

RSA Security Analytics

Данные об информационной безопасности

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

The diagram shows three user icons (a man in a suit, a woman, and another man) arranged in a circle with arrows indicating a flow between them. To the right is a hierarchical organizational chart with a diamond at the top, followed by a rectangle, and then two more diamonds at the bottom level.

AIMS: Advanced Incident Management for Security

RSA Archer

Данные об организации и пользователях

Обзор Asset Criticality Intelligence (ACI)



Demo - RSA Security Analytics 10 - v8.2c08 Server: Security Analytics Clients v8.2c03 Time Left: 6d 19h 57m Help

Investigation :: RSA Security

https://security_analytics/investigation/6/navigate/values

Tools and Status Unified View :: RSA S... Investigation :: RSA ... Administration :: RS...

Investigation Dashboard Navigate RSA Security Analytics

Select Device All Data Total Descending Event Count Custom Drill Export ACI Actions

nw_concentrator >

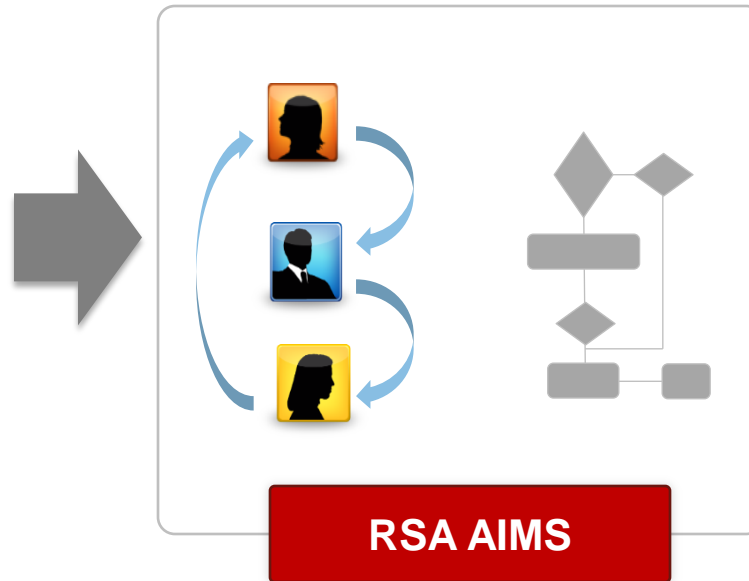
2013 01 03 22:32 All Data 2013 01 07 14:19 Show Chart

- Threat Category
Closed - Click to Open
- Threat Description
Closed - Click to Open
- Threat Source
Closed - Click to Open
- 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

admin Send Us Feedback 10.0.5.0



Advanced Incident Management for Security (AIMS)



Advanced Incident Management for Security

Navigation Menu

- Incident Management
- Incidents
- Investigations
- Ethics Violations
- Response Procedures
- Contacts
- Issue Management
- Findings
- Remediation Plans
- Exception Requests

Welcome, Atok Ojha

Incidents by Owner

Open Incidents by Incident Own *

Incident Close Rate

Days to Close (Last 30)

Incident Summary

Open Incidents by Priority

Incident Trends

Incidents Reported by Month and Pri *

Incidents by Facility

Active Incidents, Ethics Violation Reports & Investigations

Most Recently Reported Incidents

Incident ID	Date/Time Reported	Incident Summary	Priority	Status	Category	Affected Business Unit
INC-455	10/23/2012 2:17 PM	test incident 2	High	New		
INC-454	10/23/2012 2:17 PM	Test incident 1	High	New		
INC-453	10/23/2012 2:00 PM	summary	High	New	Fraud - Blackmail	

Investigations Summary

Investigations by Request Type *

Investigations by Owner

Open Investigations by Investigation *

Investigation Owner	Count of Investigation Owner
Analyst, Joe	1
Havlak, Scott	1

Beth's Sample Report

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 через Fiber Channel
 - Высокоемкостные и высокопроизводительные конфигурации
 - От 46TB до 1.5 PB (XXL) общей емкости



Варианты платформы Security Analytics

Data Center	Up to 5 DACs	3-node Warehouse	Branch	Single 1 DAC	SMB
<p>Usage: Enterprise Monitoring SOC Operations</p>  <p>Decoder Concentrator Broker</p> <p>Features: 1U Form Factor Distributed Visibility Modular Capacity Options DAC & SAN Capacity Available</p>	 <p>22TB 32TB 142TB</p>	 <p>Ultra Performance 30TB</p>  <p>High Capacity 120TB</p>	<p>Usage: Remote Office Small Security Team</p>  <p>Hybrid Security Analytics Server</p> <p>Features: 1U Form Factor 10TB Capacity DAC Capacity Available</p>	 <p>22TB 32TB</p>	<p>Usage: Small Enterprise Distributed MSSP</p>  <p>All-In-One</p> <p>Features: 1U Form Factor 10TB Capacity</p>
<p>Пакеты: 2 Gbps Логи: 30,000 eps</p>			<p>Пакеты: 622 Mbps Логи: 10,000 eps</p>		<p>Пакеты: 310 Mbps Логи: 7,500 eps</p>

