

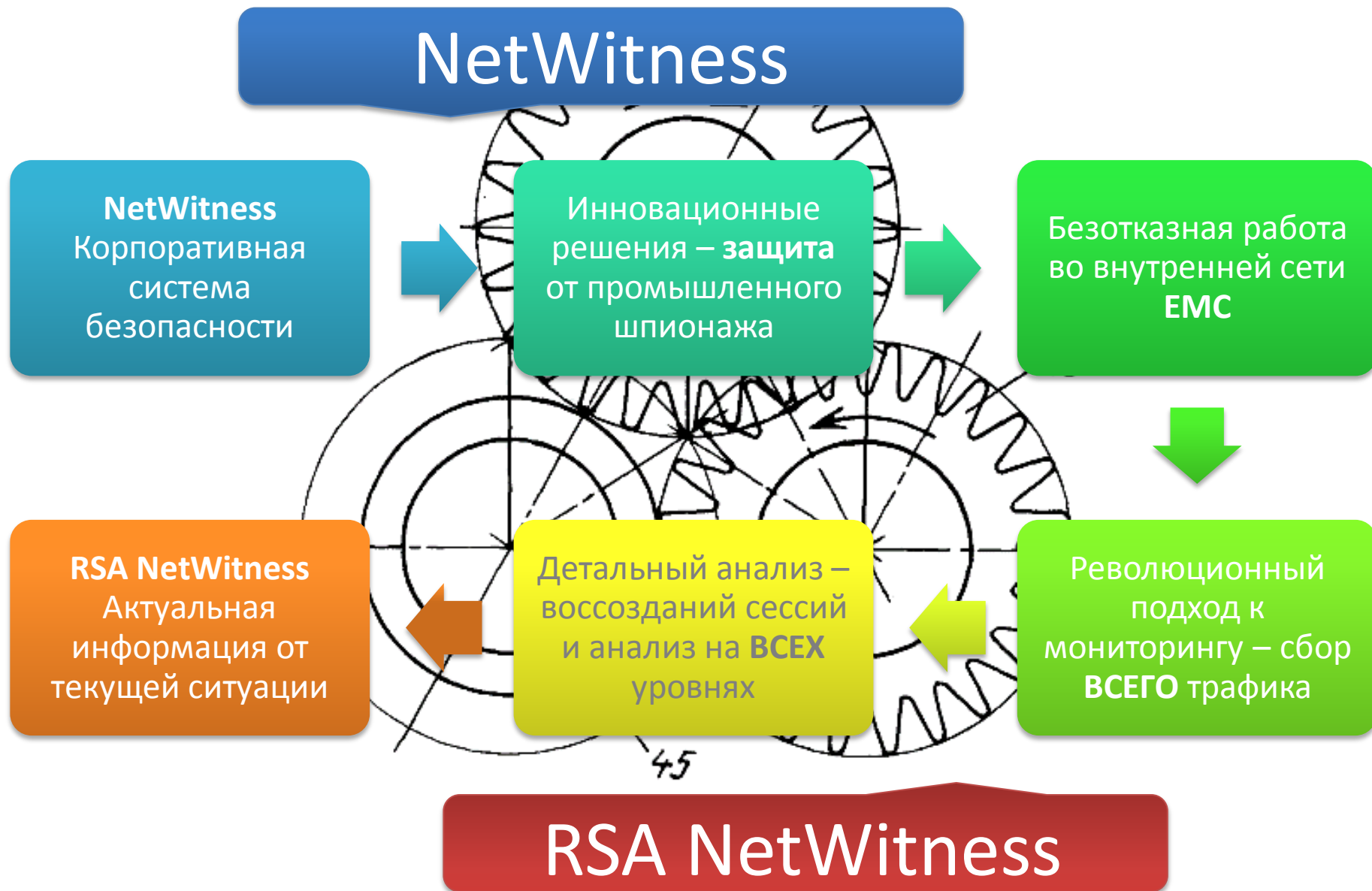
Обзор платформы RSA NetWitness

Автор: Pete Kuzeev, Security Expert, RRC Moscow



The Security Division of EMC

Ресурсы: www.emc.com www.rsa.com www.netwitness.com



» Decoder:



- ▶ Сбор, обработка и хранение сетевых пакетов

» Concentrator:

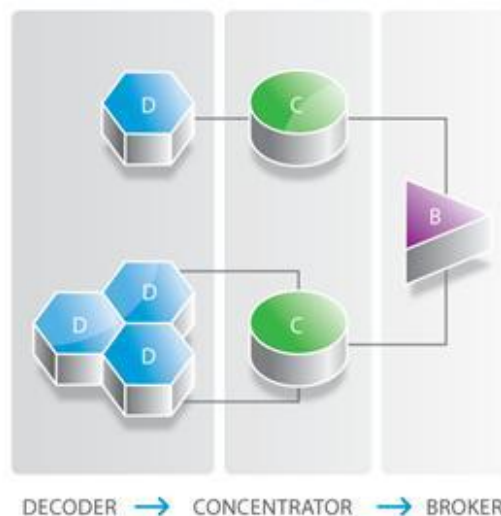


- ▶ Агрегация и индексация метаданных в режиме реального времени

» Broker:



- ▶ Распределение запросов



SDK



INFORMER
automated reporting
and alerting



INVESTIGATOR™
interactive
network forensics



SIEMLink™

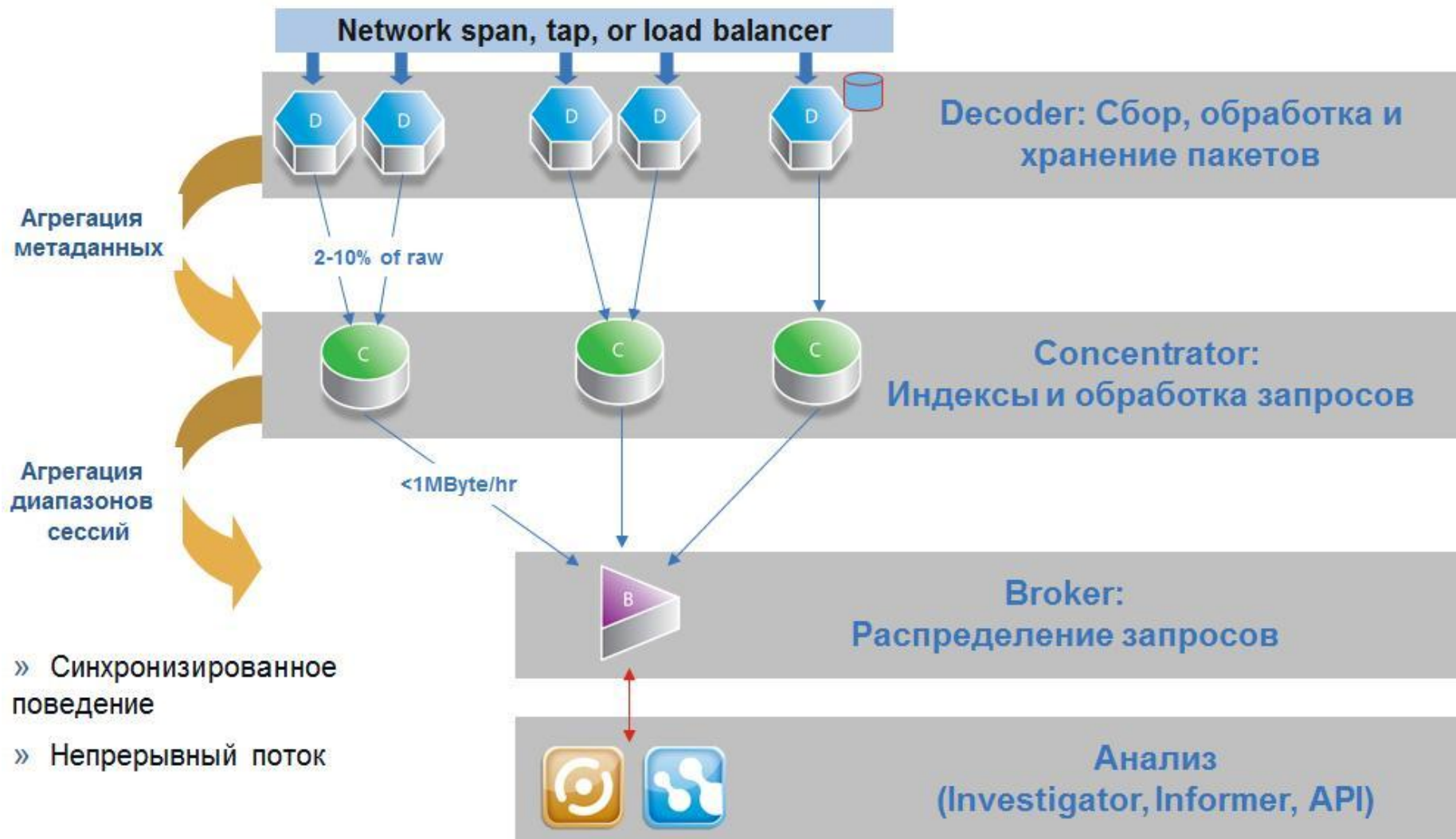
Decoder



Concentrator



Hybrid



LIVE

Visualise

Spectrum

Investigator

Informer

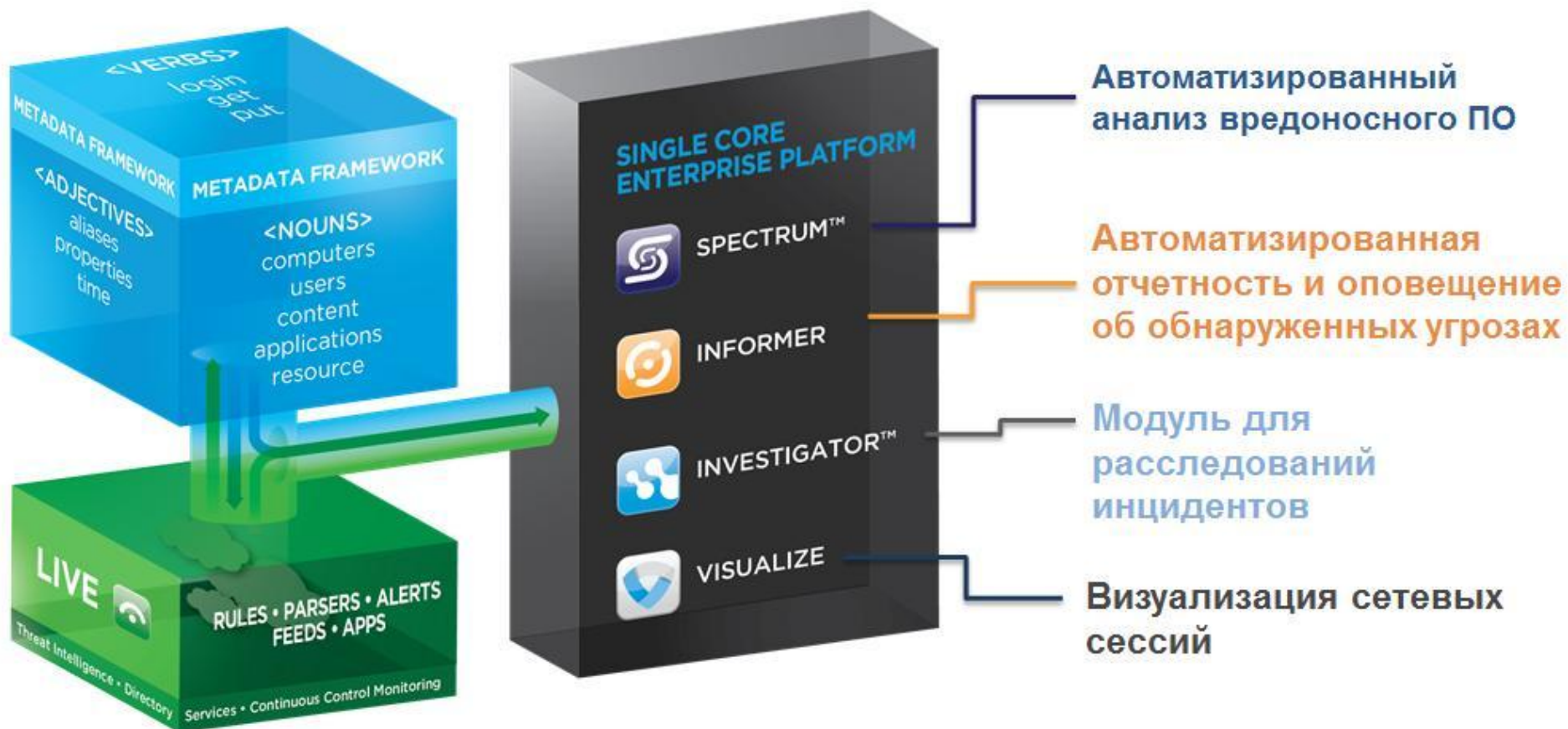
Правила

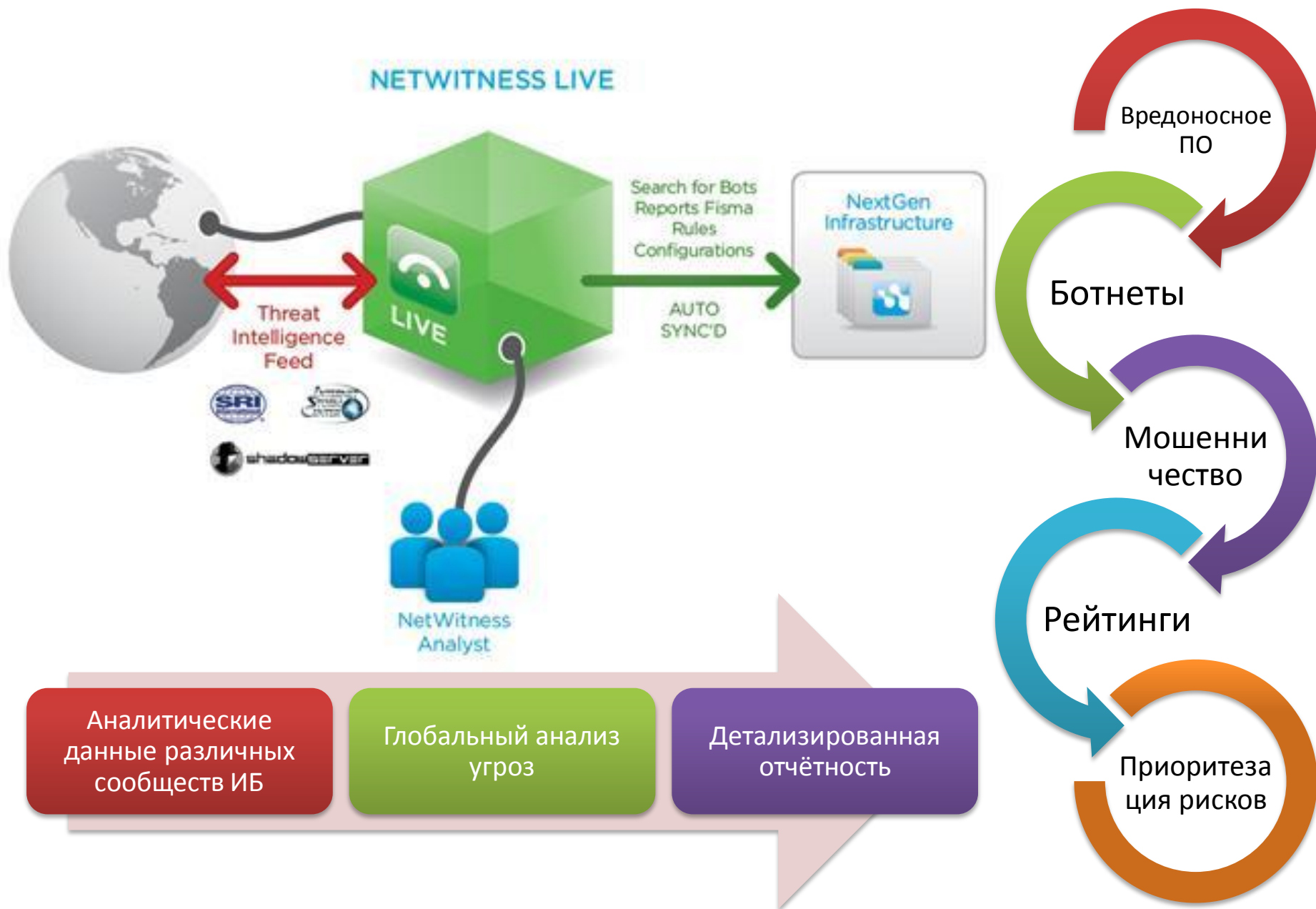
Обработчики

Оповещения

Фиды

Приложения





RRC Облачные сервисы – варианты подписок

BASIC (FREE)

Open Source Threat
Intelligence
Advanced Threat Content

- » Informer Threat/Security Reports
 - » BOT/C&C reports
- » Exploit Kit Identification
 - » Zero-Day Indicators
- » Compromise Indicators
- » Prioritized Risk Levels

INTELLIGENCE SOURCES



ENHANCED (Subscription)

User Identity
Spam/Phish/Threat
Intelligence

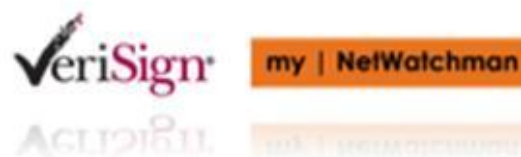
- » Trend Intelligence
- » Anonymous Proxies
- » Website Classification
- » Spam/Phish/Threat Intelligence
- » NetWitness Identity (AD Integration)

INTELLIGENCE SOURCES



PREMIUM (Subscription)

Fraud Intelligence
Financial Services Intelligence



Основная

Подписки для
уязвимостей уровня
critical бесплатны

Расширенная

Для крупных
компаний,
нуждающихся в
дополнительных
сервисах

Премиальная

Для предприятий
госсектора,
работающих с
материалами
высокой
секретности

RRC Investigator – Ответы на ваши вопросы

Интерактивный
анализ
содержимого
сетевых сессий

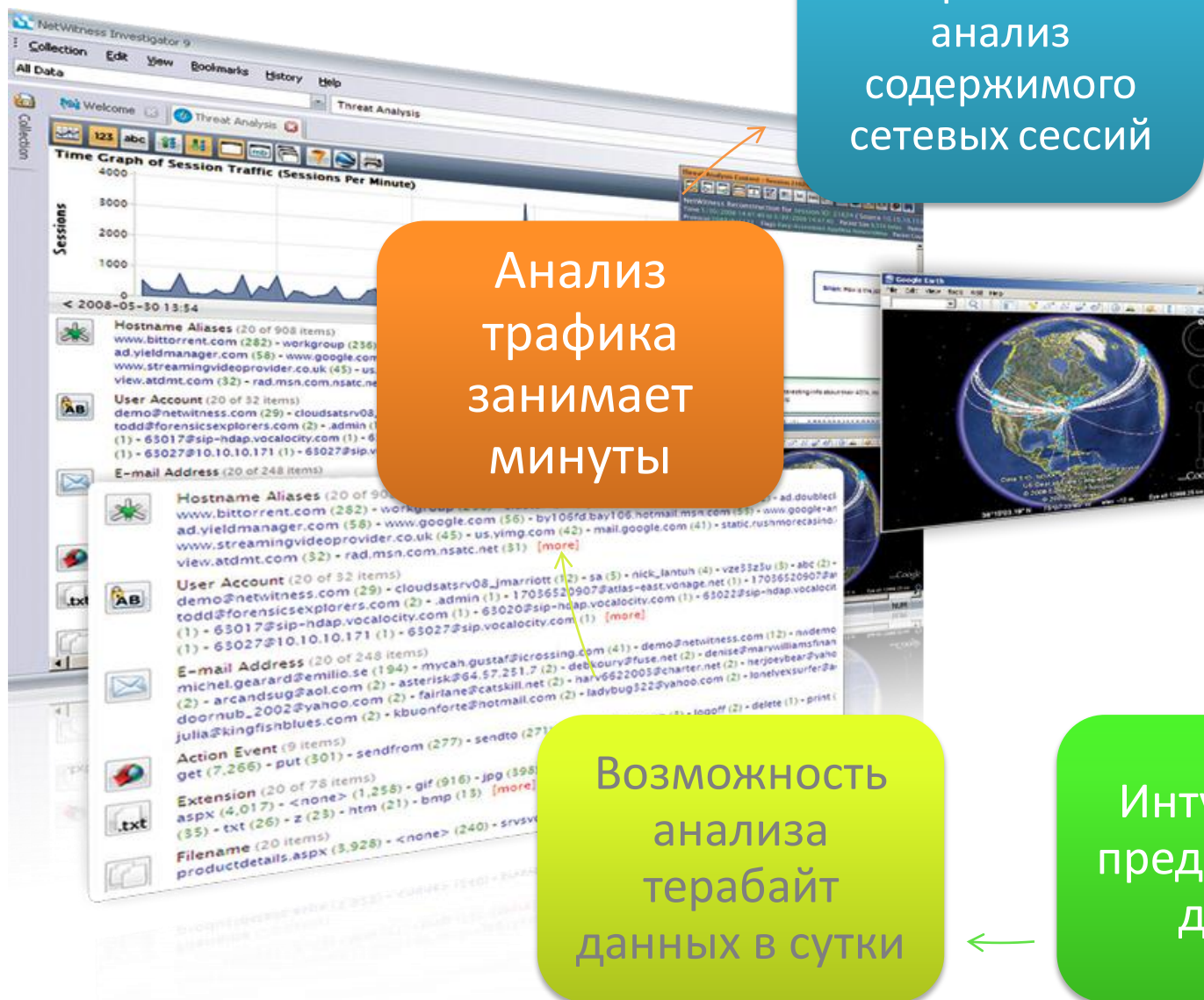


Анализ
трафика
занимает
минуты

Любые
направления
анализа –
гибкость в
расследованиях

Возможность
анализа
терабайт
данных в сутки

Интуитивное
представление
данных



The screenshot displays the NetWitness Investigator 9 interface. The main window is titled "Demo Collection Content - Session 1". It shows a "NetWitness Reconstruction for session ID: 1" with source IP 10.21.3.39 and target IP 65.54.228.55. The session occurred on 11/14/2008 from 17:50:37 to 17:50:39, with a packet size of 6,165 bytes and a payload size of 3,439 bytes. The protocol is 2048/6/1122, and flags include Keep Assembled, AppMeta, NetworkMeta, and Packet Count 49.

The left pane shows a list of events for the session, including a "View" button and a large blue icon representing a conversation. The right pane displays a reconstructed conversation between Todd and Chris W. The bottom status bar shows "Live Capture" and "Packets Captured: 0".

Time	Service	Size	Events	Displaying 1 - 1 of 1
2008-Nov-14 17:50:37	IP / TCP / MSN IM	6.02 KB	00:11:0A:A4:3C:98 -> 00:1A:70:8E:69:0D 10.21.3.39 -> 65.54.228.55 6141 -> 1863 (msn im) payload: 3439 medium: 1 tcp.flags: 26 streams: 2 packets: 49 lifetime: 2 action: sendto email: chris@investigator.demo action: login email: todd@invest.demo action: sendfrom email: chris@investigator.demo country.dst: United States latdec.dst: 38.000000 longdec.dst: -97.000000	

Todd: Hey! Just wanted to let you know that I am recording this conversation with NetWitness Investigator.

Chris W.: Okay thanks for the heads up. Whats going on?

Todd: I wanted to demonstrate how NetWitness extracts meta data from network packets.

Chris W.: When you say meta data, you mean all the useful stuff like usernames, e-mails, computers, and files right?

Todd: Exactly! We also reconstruct the content so it is very easy to read.

Chris W.: You mean the days of viewing packets as hex dumps are over?

Todd: Ha! That option is there if needed but I prefer quickly reading the conversation as

Collection Edit View Bookmarks History Help

Last 24 Hours of Collection Time Frenzy:50005 > HTTP > common document formats

Welcome Frenzy:50005

2011-01-11 13:05 2011-01-12 13:04 >

Threat Source (5 items)
netwitness (8,863) - malwaredomainlist-files (108) - sans (8) - malwaredomainlist-ip (5) - zeustracker-ip (1)

Threat Category (4 items)
informational (8,863) - suspicious (312) - malware (277) - botnet (1)

Threat Description (20 items)
rfi:209.33.220.8:stormpages.com (56) - rfi:111.221.42.24:lpkpm.com (16) - exploit kit:178.63.173.115:sdrfdajndgqw.lpq.co (11) - obfuscated iframe directs to exploit:58.64.186.92:www.momonala.com (7) - ie exploit:211.234.117.132 (6) - koobface (4) - trojan carberp calls home:213.5.71.51:teencantrityt.us (2) - trojan:216.97.231.190:forumz.zhaishen.com (2) - 2.usofrance.fr:16276 (1) - default account: edimax (1) - default account: osicom (1) - default account: vxworks (1) - directs to trojan:198.77.71.192:adgallery.whitehousedrugpolicy.gov (1) - exploit kit:83.69.226.221:www.topvorun.biz (1) - obfuscated script directs to exploits:119.6.39.38:www.vastsea.com (1) - obfuscated script downloads trojan using java:62.146.15.33:www.hacher-uhren.de (1) - redirects to exploits:67.202.87.234:www.realinnovation.com (1) - redirects to mebroot:212.92.23.189:www.thermotelvictoria.hu (1) - trojan:195.122.131.16:rapidshare.com (1) - zeus v1 config file:193.104.146.12 (1) [more]

Decoder Source (1 item)
frenzy (8,863)

Feed Description [open]

Service Type (1 item)
HTTP (8,863)

Hostname Aliases (20 items)
download.java.net (787) - fxfeeds.mozilla.com (353) - newssrs.bbc.co.uk (148) - maven.alfresco.com (342) - dist.wso2.com (286) - hpc.arc.georgetown.edu (284) - mirrors.netdna.com (251) - mirror.rackspace.com (251) - insignia.chumby.com (205) - api.facebook.com (172) - mirror.atlanticmetro.net (165) - ftp-ssl2.smesslingen.de (111) - mirror.cogentco.com (99) [more]

Source IP Address (20 items)
10.21.3.55 (1,159) - 10.21.3.76 (822) - 10.21.3.46 (377) - 10.21.2.33 (246) - 10.21.3.38 (221) - 10.21.2.116 (192) - 10.21.1.51 (191) - 10.21.4.2 (146) - 10.21.2.109 (137) - 10.21.4.40 (121) - 10.21.3.14 (120) - 10.21.2.81 (120) - 10.21.4.246 (118) - 10.21.2.80 (114) - 10.21.4.15 (114) - 10.21.2.109 (109) - 10.21.2.109 (109) - 10.21.2.109 (109) - 10.21.2.109 (109) - 10.21.2.109 (109) - 10.21.2.109 (109)

Выбор метаданных

Выбор действия правой кнопки

- Apply IEQUALS Drill
- Apply IEQUALS Drill in New Tab
- Apply as Root Drill in New Tab
- CentralOps Whois for IPs and Hostnames
- Google
- Google Keyword Search
- Google Malware Diagnostic for IPs and Hostnames
- McAfee SiteAdvisor for Hostnames
- MyNetWatchman IP Incidents
- NBTSTAT
- SANS IP History
- SamSpade
- Edit Custom Actions...

Capture

Line Rate: 0 / 0 Mbs Packets Captured: 0

The screenshot displays the NetWitness Investigator web interface. At the top, a menu bar includes 'Collection', 'Edit', 'View', 'Bookmarks', 'History', and 'Help'. Below this, a breadcrumb trail shows 'Demo Collection > Sessions for HTTP'. The main content area is divided into several sections:

- Session Details:** A list of metadata on the right side, including:
 - referer: <http://www.netwitness.com/samplepage/>
 - client: Mozilla/4.0
 - alias.ip: 64.78.4.164
 - alias.host: www.netwitness.com
 - content: text/html
 - content: image/jpeg
 - content: image/jpeg
 - content: image/jpeg
 - country.dst: United States
 - city.dst: Sunnyvale
 - latdec.dst: 37.369701
 - longdec.dst: -122.021400
- Session content preview:** A large central area showing a preview of the session content. It includes a timestamp '2008-Nov-14 17:58:47', a protocol indicator 'IP / TCP / HTTP', and a size '26.95 KB'. Below this, a 'View' button is visible next to a thumbnail of the session content.
- Session Details (Bottom Right):** A detailed view of the session data, including:
 - 00:11:0A:A4:3C:98 -> 00:1A:70:8E:69:0D
 - 10.21.3.39 -> 64.78.4.164
 - 8240 -> 80 (http)
 - payload: 25803
 - medium: 1
 - tcp.flags: 30
 - streams: 2
 - packets: 33
 - lifetime: 2
 - action: get
 - directory: /samplepage/
 - filename: nw-header.jpg
 - extension: jpg
 - referer: <http://www.netwitness.com/samplepage/>
 - client: Mozilla/4.0
 - alias.ip: 64.78.4.164
 - alias.host: www.netwitness.com
 - content: image/jpeg
 - country.dst: United States
 - city.dst: Sunnyvale

At the bottom, a 'Capture' section shows a 'Line Rate' of '0 / 0 Mbps' and 'Packets Captured: 0'. A large blue icon with a white stylized 'W' is also visible on the right side of the interface.

RRC Investigator – Анализ содержимого

The screenshot displays the RRC Investigator application interface. At the top, the menu bar includes Collection, Edit, View, Bookmarks, History, and Help. The main window shows a packet capture session titled "Demo Collection > Sessions for RTP". The packet list table has columns for Time, Service, Size, and Events. The selected packet (2008-Nov-14 17:52:57) is of service "IP / UDP / RTP" and size "271.47 KB". The Events column shows details like "00:1A:70:8E:69:0D -> 00:04:F2:05:6C:C0" and "64.57.248.132 -> 10.21.3.40".

A callout box with the text "Разные представления содержимого: txt, hex, pkt, native..." points to the "Demo Collection Content - Session 3" pane. This pane shows "NetWitness Reconstruction for session ID: 3 (Source 64.57.248.132 : 29108, Target 10.21.3.40 : 2236)". Below this, it indicates "Time 11/14/2008 17:52:57 to 11/14/2008 17:56:45", "Calculated Packet Size 978,622 bytes", "Calculated Payload Size 786,556 bytes", "Protocol 2048/17/1720", "Flags Incomplete", "Keep Assembled AppMeta NetworkMeta", and "Packet Count 4,573".

Below the reconstruction pane, there are two audio playback sections. The first is labeled "CCITT u-Law, 8.000 kHz, 8 Bit, Mono Side 1 Discussion" and features a black audio waveform. A callout box with the text "Воспроизведение содержимого" points to this waveform. The second section is labeled "CCITT u-Law, 8.000 kHz, 8 Bit, Mono Side 2 Discussion".

At the bottom, the "Capture" pane shows the "Line Rate" as "0 / 0 Mbps" and "Packets Captured: 0".

The screenshot displays the NetWitness Investigator web interface. At the top, the navigation bar includes 'Collection', 'Edit', 'View', 'Bookmarks', 'History', and 'Help'. Below this, a status bar shows 'Last 24 Hours of Collection Time' and the current search path 'Frenzy:50005 > china > Content Search'. The main search area features the NetWitness logo and a search bar containing 'passport.maxthon.cn'. A 'Pause' button is located to the right of the search bar. Below the search bar, a progress indicator shows '[Sessions 25386752 to 25882341, 99%] Searching session 25582985...'. The search results are listed in a table with columns for IP, TCP/HTTP details, and Found Date. The first result shows a connection from 10.21.4.21 to 60.28.210.17 on port 80, with a found date of Tue, 11 Jan 2011 02:59:49 GMT. A black arrow points from the search bar to the first result. A grey callout box with a blue border contains the text 'Поиск содержимого. Поддерживаются также регулярные выражения'. In the bottom right corner, there is a blue square icon with a white stylized 'W' logo. The bottom status bar shows 'Capture' mode, 'Line Rate: 0 / 0 Mbs', and 'Packets Captured: 0'.

Collection Edit View Bookmarks History Help

Last 24 Hours of Collection Time Frenzy:50005 > china > Content Search

Searching

NETWITNESS TOTAL NETWORK KNOWLEDGE

Searching For passport.maxthon.cn Pause

Search Options: Case sensitive

[Sessions 25386752 to 25882341, 99%] Searching session 25582985...

IP / TCP / HTTP [10.21.4.21 -> 60.28.210.17]
OpenSSL/0.9.8e-fips-rhel5 PHP/5.2.11 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.8.8 Server at passport.maxthon.cn Port 80</address> </body></html> HTTP/1.1 302 Found Date: Tue, 11 Jan 2011 02:59:49 GMT Server: Ap 2011-Jan-10 21:59:33 -- 11.97 KB

IP / TCP / HTTP [10.21.4.104 -> 60.28.210.17]
OpenSSL/0.9.8e-fips-rhel5 PHP/5.2.11 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.8.8 Server at passport.maxthon.cn Port 80</address> </body></html> HTTP/1.1 302 Found Date: Tue, 11 Jan 2011 03:00:44 GMT Server: Ap 2011-Jan-10 22:00:41 -- 11.69 KB

IP / TCP / HTTP [10.21.4.21 -> 60.28.210.14]
> <hr> <address>Apache/2.2.14 (Unix) mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.8.8 Server at passport.maxthon.cn Port 80</address> </body></html> HTTP/1.1 302 Found Date: Tue, 11 Jan 2011 04:09:14 GMT Server: Ap 2011-Jan-10 23:09:12 -- 10.72 KB

IP / TCP / HTTP [10.21.4.104 -> 60.28.210.14]
> <hr> <address>Apache/2.2.14 (Unix) mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.8.8 Server at passport.maxthon.cn Port 80</address> </body></html> HTTP/1.1 302 Found Date: Tue, 11 Jan 2011 04:09:57 GMT Server: Ap 2011-Jan-10 23:09:55 -- 10.10 KB

IP / TCP / HTTP [10.21.4.21 -> 60.28.210.7]
OpenSSL/0.9.8e-fips-rhel5 PHP/5.2.11 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.8.8 Server at passport.maxthon.cn Port 80</address> </body></html> HTTP/1.1 302 Found Date: Tue, 11 Jan 2011 04:24:07 GMT Server: Ap 2011-Jan-10 23:24:04 -- 11.97 KB

Capture

Line Rate: 0 / 0 Mbs Packets Captured: 0

NUM

Поиск содержимого.
Поддерживаются также
регулярные выражения

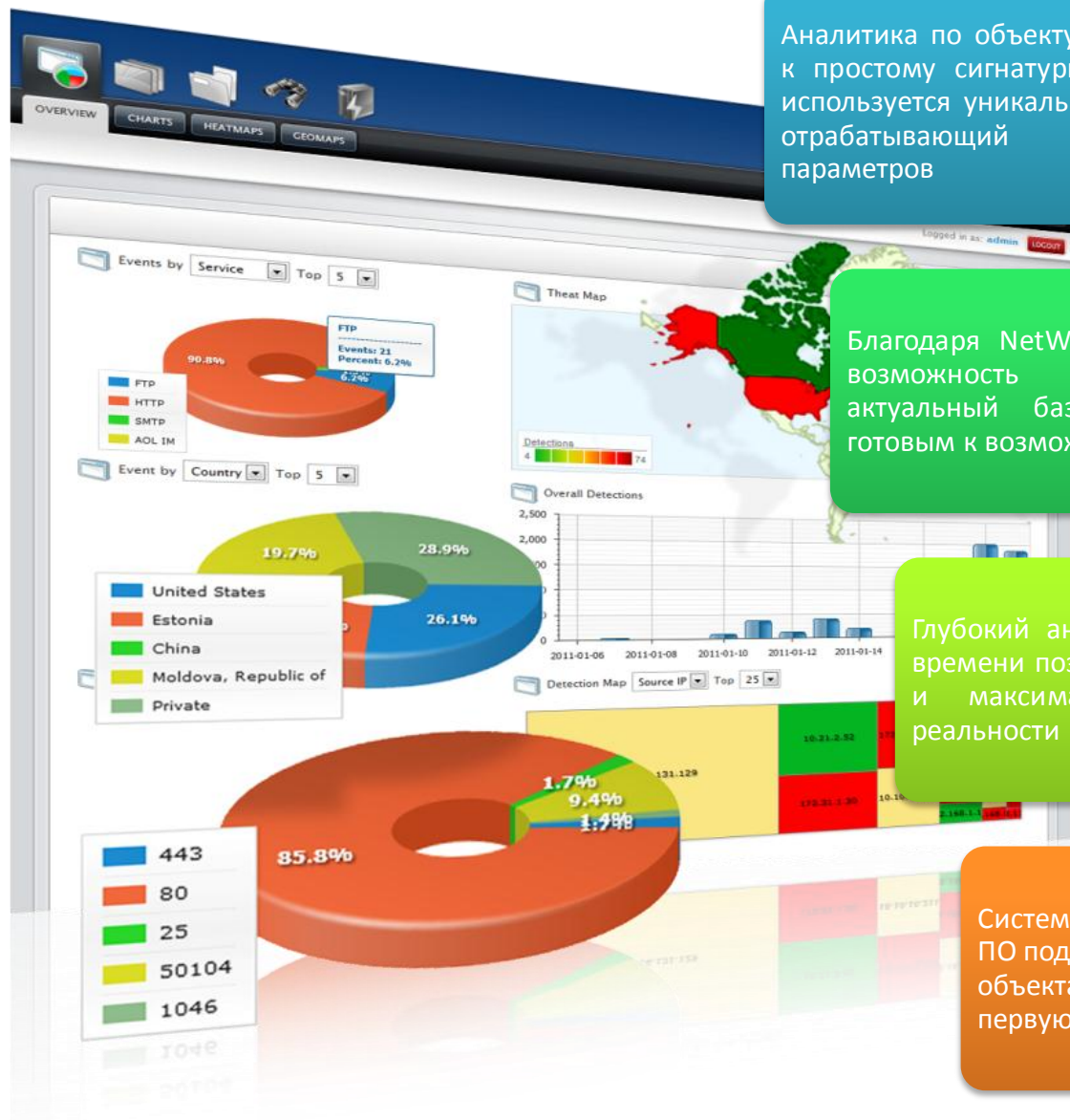


Аналитика по объекту не сводится к простому сигнатурному анализу, используется уникальный алгоритм, обрабатывающий тысячи параметров

Благодаря NetWitness Live появляется возможность использования актуальной базы знаний и быть готовым к возможным угрозам

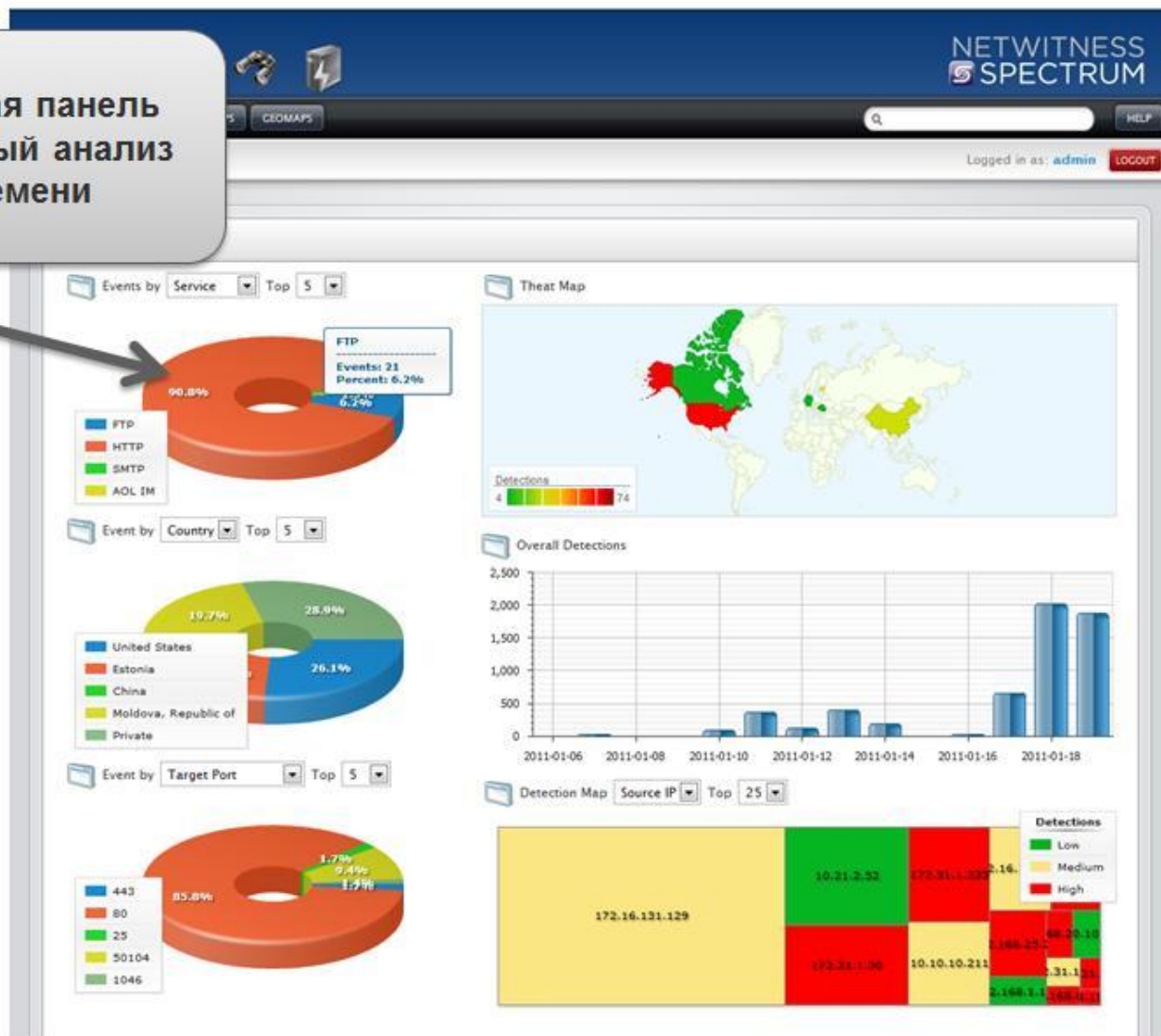
Глубокий анализ в режиме реального времени позволяет получать детальную и максимально приближенную к реальности картину сетевой активности

Система приоритезации вредоносного ПО подсказывает каким областям и объектам следует уделить внимание в первую очередь



RRC Spectrum – Инструментальная панель

Настраиваемая приборная панель обеспечивает непрерывный анализ угроз в реальном времени



Многосторонний анализ риска обеспечивает самую полную оценку и приоритетизацию подозрительных файлов



The screenshot displays the NetWitness Spectrum web interface. At the top, the header shows 'NETWITNESS SPECTRUM' and a search bar. Below the header, a table lists files with columns: File, NextGen, Community, Sandbox, Source Address, Alias Host, Destination Address, Destination Country, and Date. A 'File Details' pop-up window is open, showing information for 'ook.exe'. The details include a score of 100, size of 20,741, MIME type of application/exe, and a hash. It also lists several indicators: 'PE Country of Origin is China', 'PE is Abnormally Small in Size (<30K)', 'PE contains no Executable Sections (Characteristics)', 'PE has been Stripped of Informational Meta Strings', and 'PE Entry Point (AddressOfEntryPoint) was not found'. At the bottom of the pop-up, it states 'Total number of files found in this event: 1'. The main table shows multiple entries with scores of 100, originating from '192.168.25.251' and '192.168.221.129', and destined for various IP addresses in China and Private networks.

File	NextGen	Community	Sandbox	Source Address	Alias Host	Destination Address	Destination Country	Date
ook.exe	100	100	100	192.168.25.251	wow02.w125.west263.cn	125.65.76.2	China	2011-0
	100					61.188.38.158	China	2011-0
	100					125.65.76.2	China	2011-0
	100					59.38.111.11	China	2011-0
	100					192.168.221.129	Private	2011-0
	100					61.188.38.158	China	2011-0
	100					59.38.111.11	China	2011-0
	100					125.65.76.2	China	2011-0
	100					125.65.76.2	China	2011-0
	100					59.38.111.11	China	2011-0
	100					61.188.38.158	China	2011-0
	100					59.38.111.11	China	2011-0
	100					59.38.111.11	China	2011-0
	100					61.188.38.158	China	2011-0
	100					59.34.197.165	China	2011-0
	100					59.34.197.165	China	2011-0
	100					59.34.197.165	China	2011-0

File Details

ook.exe
was the most important file found in this event.

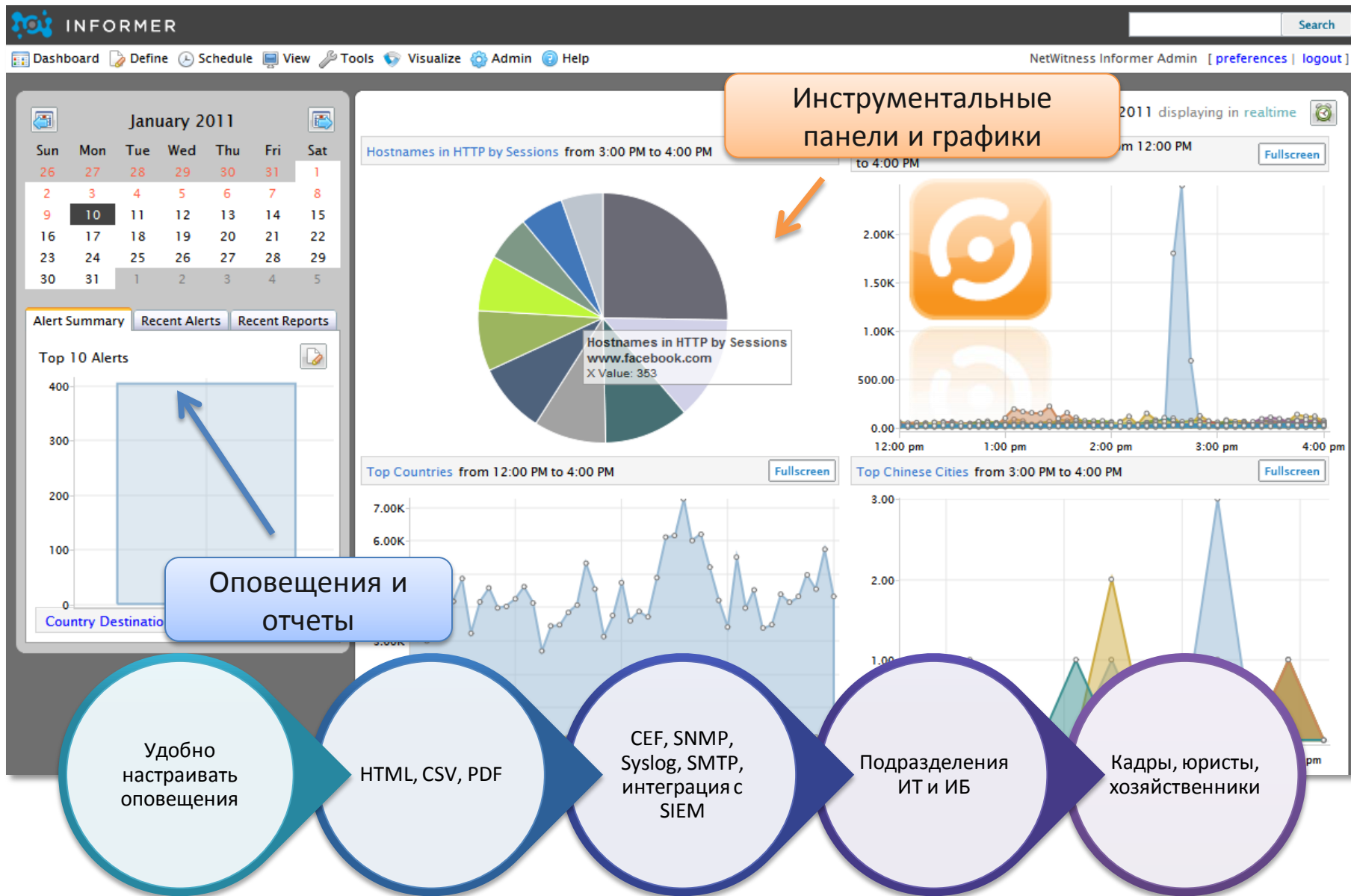
Score 100
Size 20,741
MIME Type application/exe
Hash fa000ca99692ccee784069742865b69

PE Country of Origin is China
PE is Abnormally Small in Size (<30K)
PE contains no Executable Sections (Characteristics)
PE has been Stripped of Informational Meta Strings
PE Entry Point (AddressOfEntryPoint) was not found
... click score to see more details

Total number of files found in this event: 1

Лучший анализ вредоносного ПО
вместе с возможностями анализа
NetWitness

RRC Informer – Автоматизация и оповещение



RRC Visualize – потрясающая наглядность

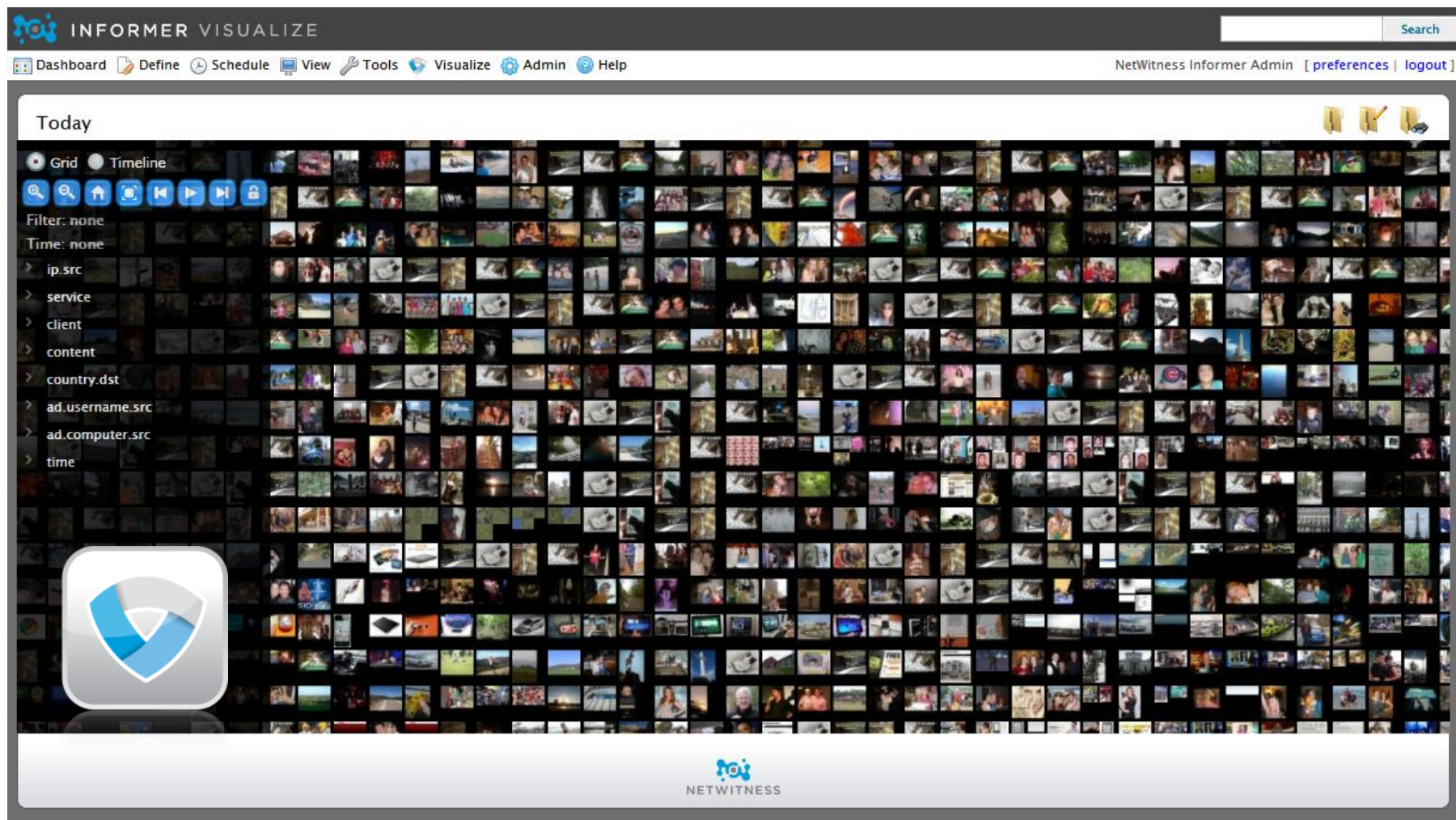


Революционный интерфейс
для анализа содержимого
сетевого трафика,
установленных сессий и
других сетевых действий

Извлекает в
интерактивном режиме
и представляет для
анализа изображения,
объекты, аудио, видео

Поддерживает
возможности задания
временных интервалов
для воспроизведения
содержимого

Доступны функции
быстрого обзора и
сортировки, навигация
по содержимому,
создание линков



Адрес источника

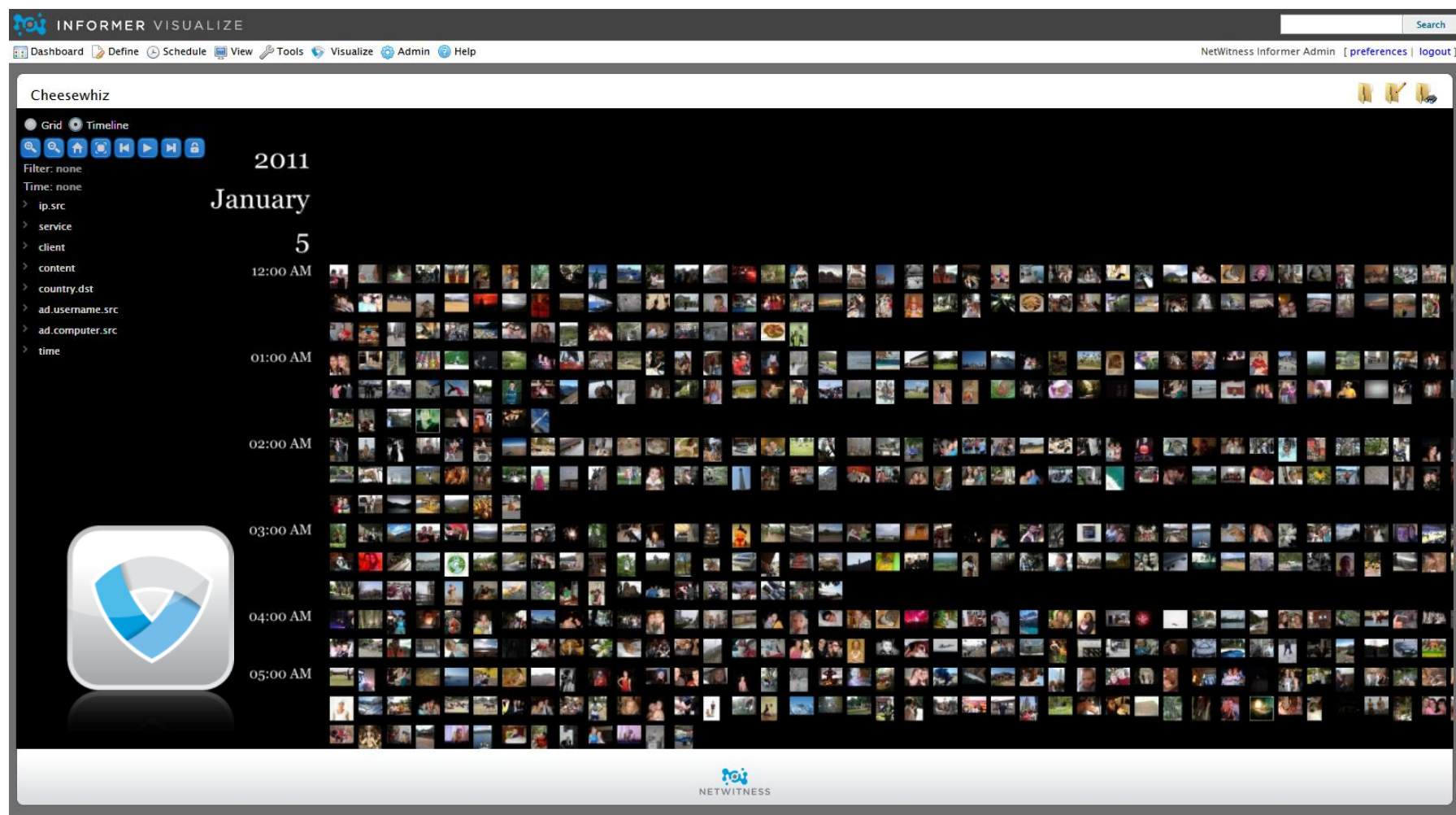
Служба

Клиент

Содержимое

Страна
назначения

Время



Адрес источника

Служба

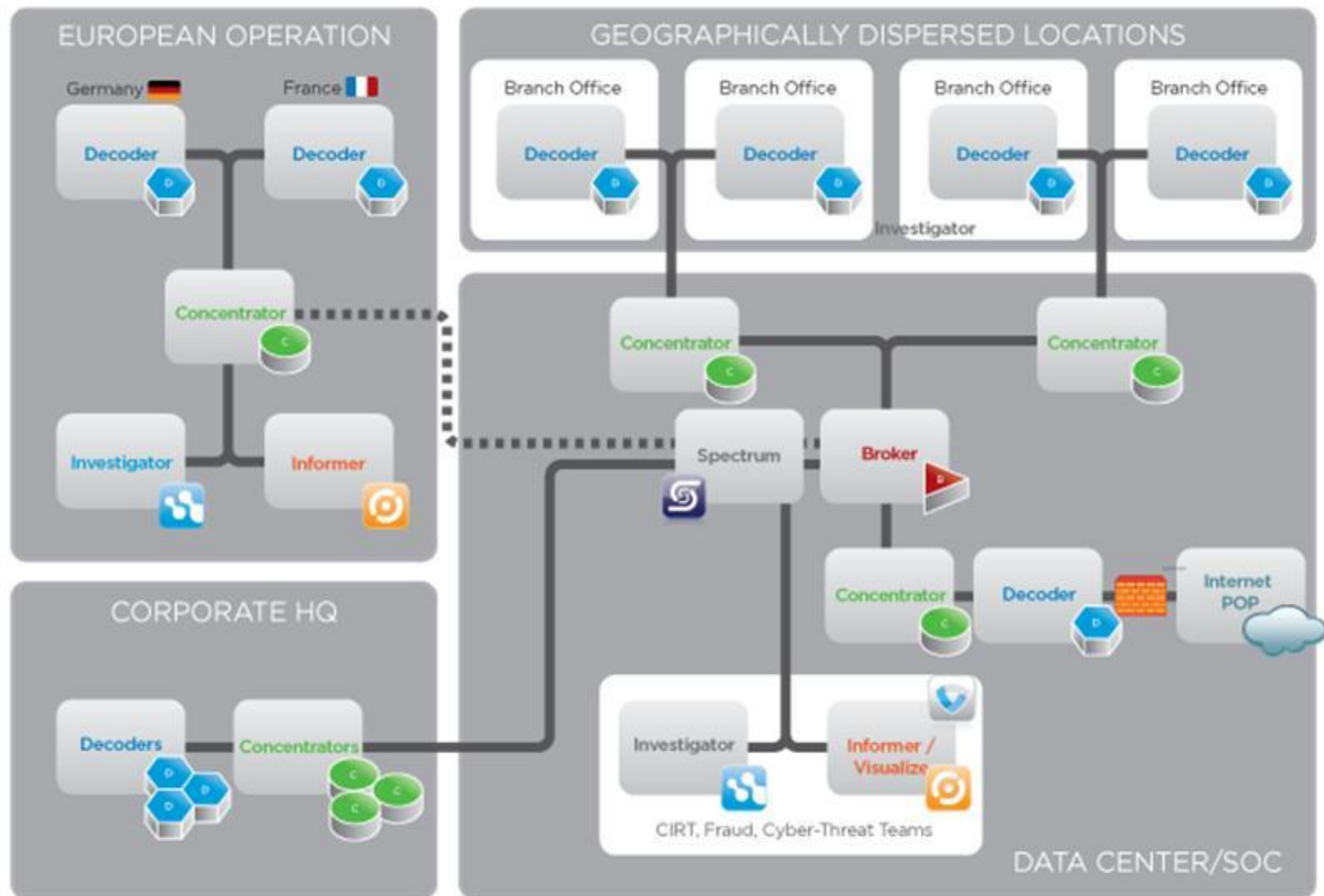
Клиент

Содержимое

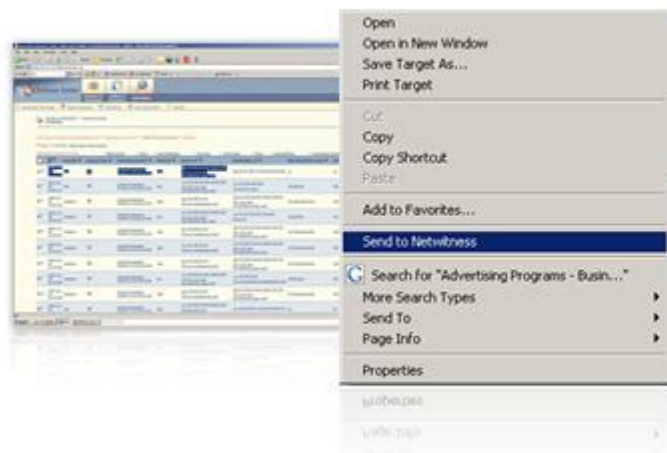
Страна
назначения

Время

[illegible]



Диспетчер событий



Event: Buffer Overflow
IP: 212.2.3.2 @ 11:32PM

Получения требуемых данных от приложения Investigator



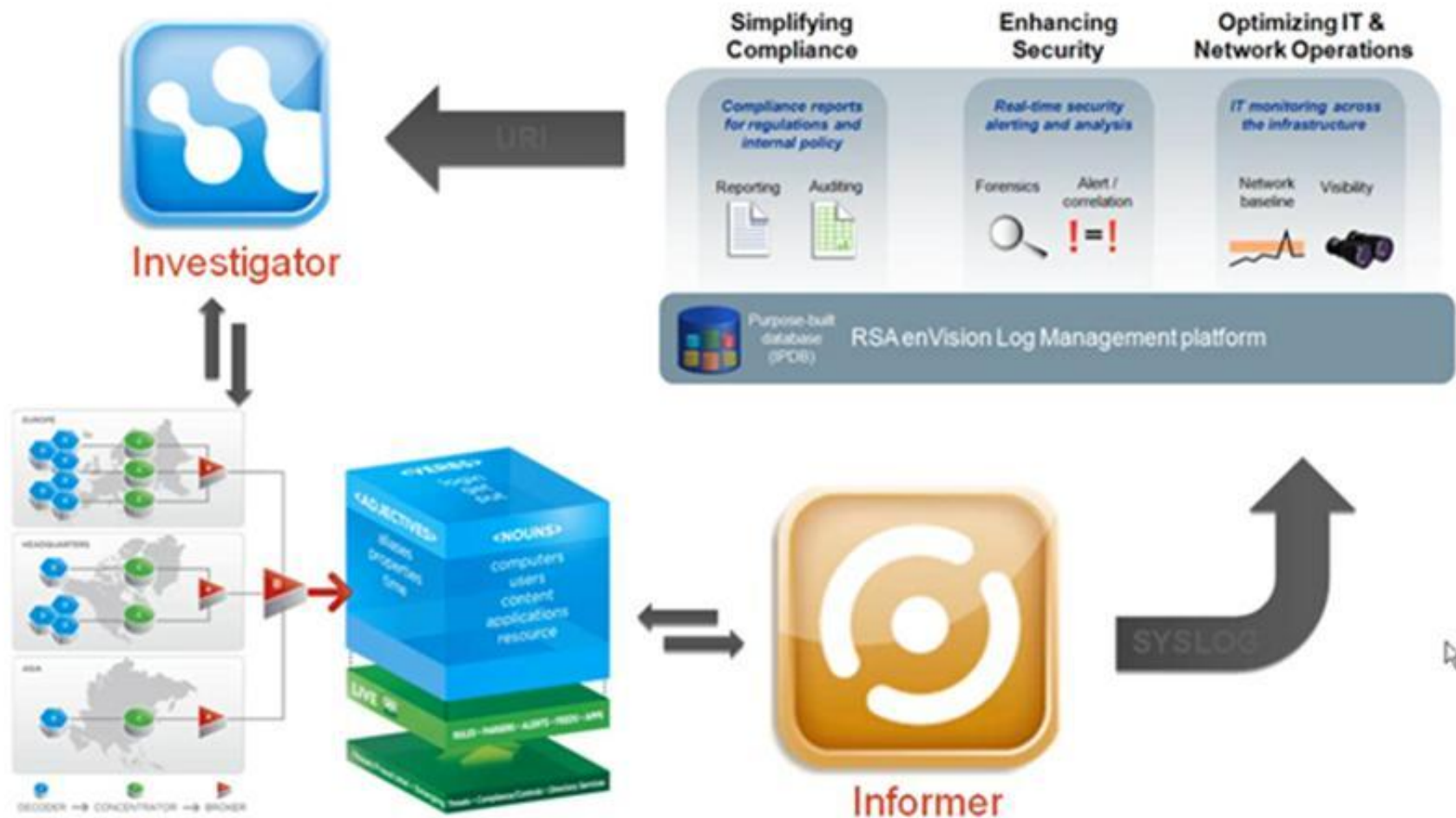
Иконка в tree

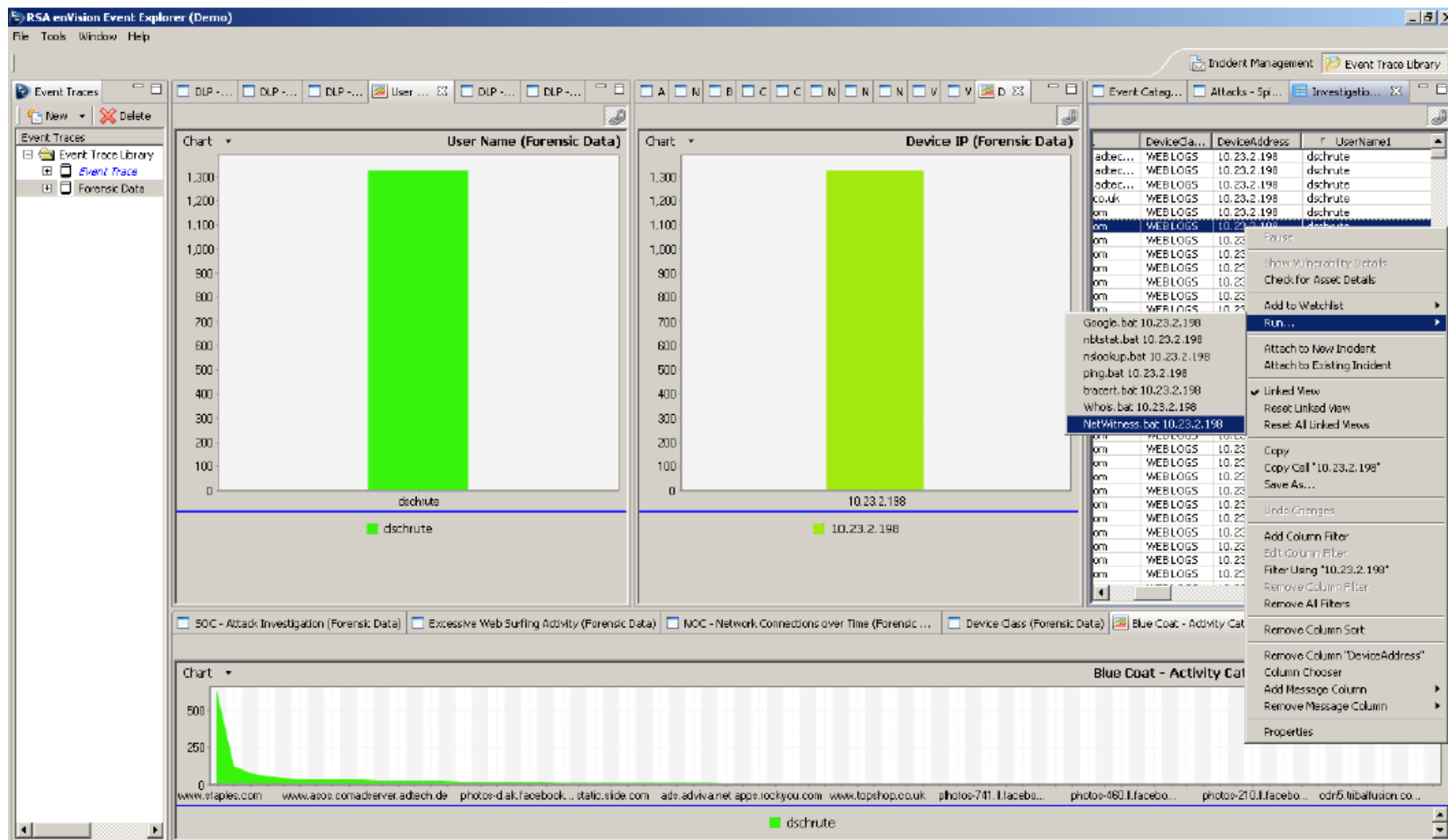
Windows приложение, обеспечивающее обмен данными NetWitness и произвольными сторонними приложениями

Совместим со всеми распространёнными SIEM, IDS/IPS и системами сетевого мониторинга

Поддерживает возможность контекстного вызова из произвольных Web консолей

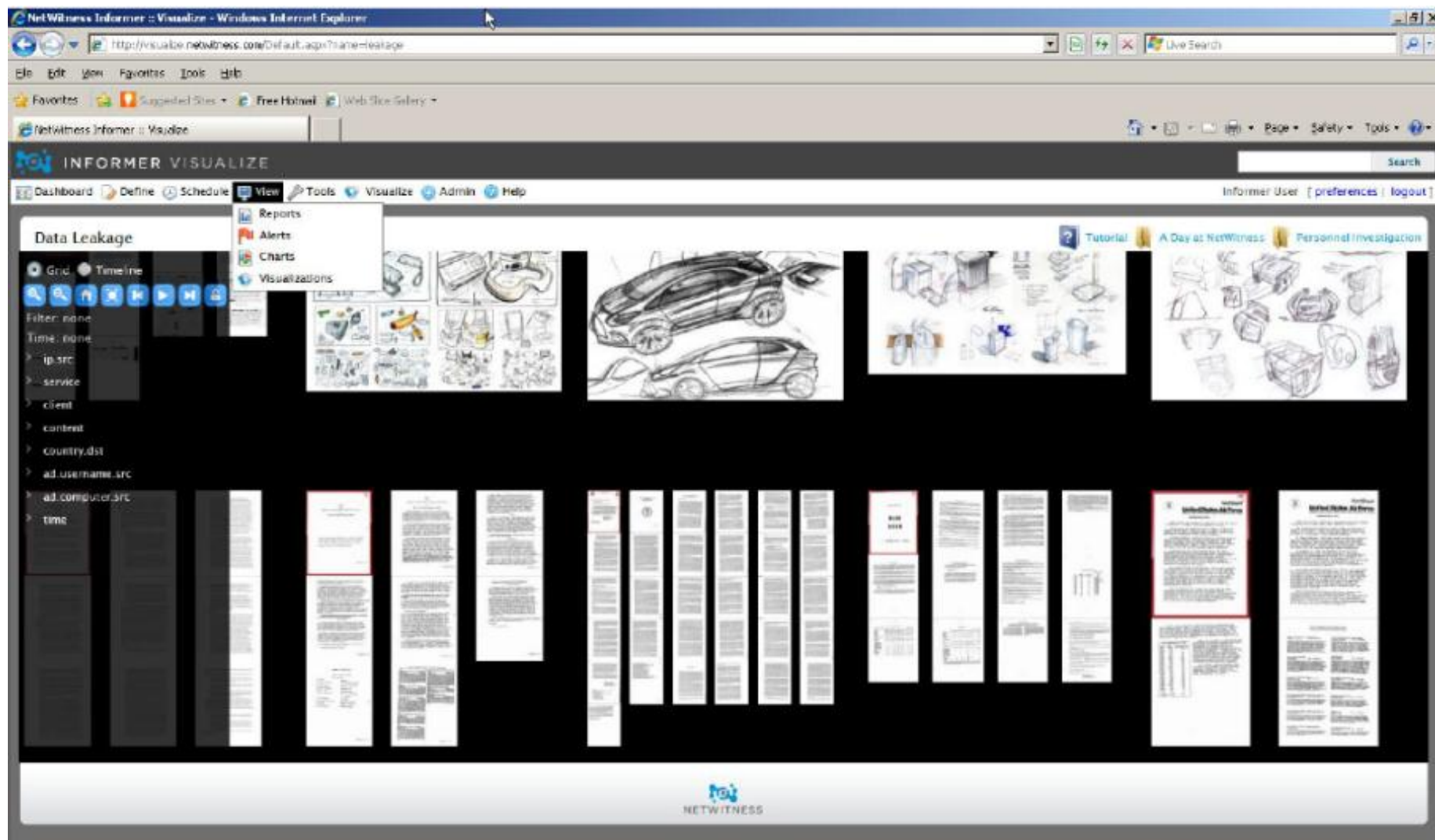
Reduce time for investigation / Gain actionable intelligence



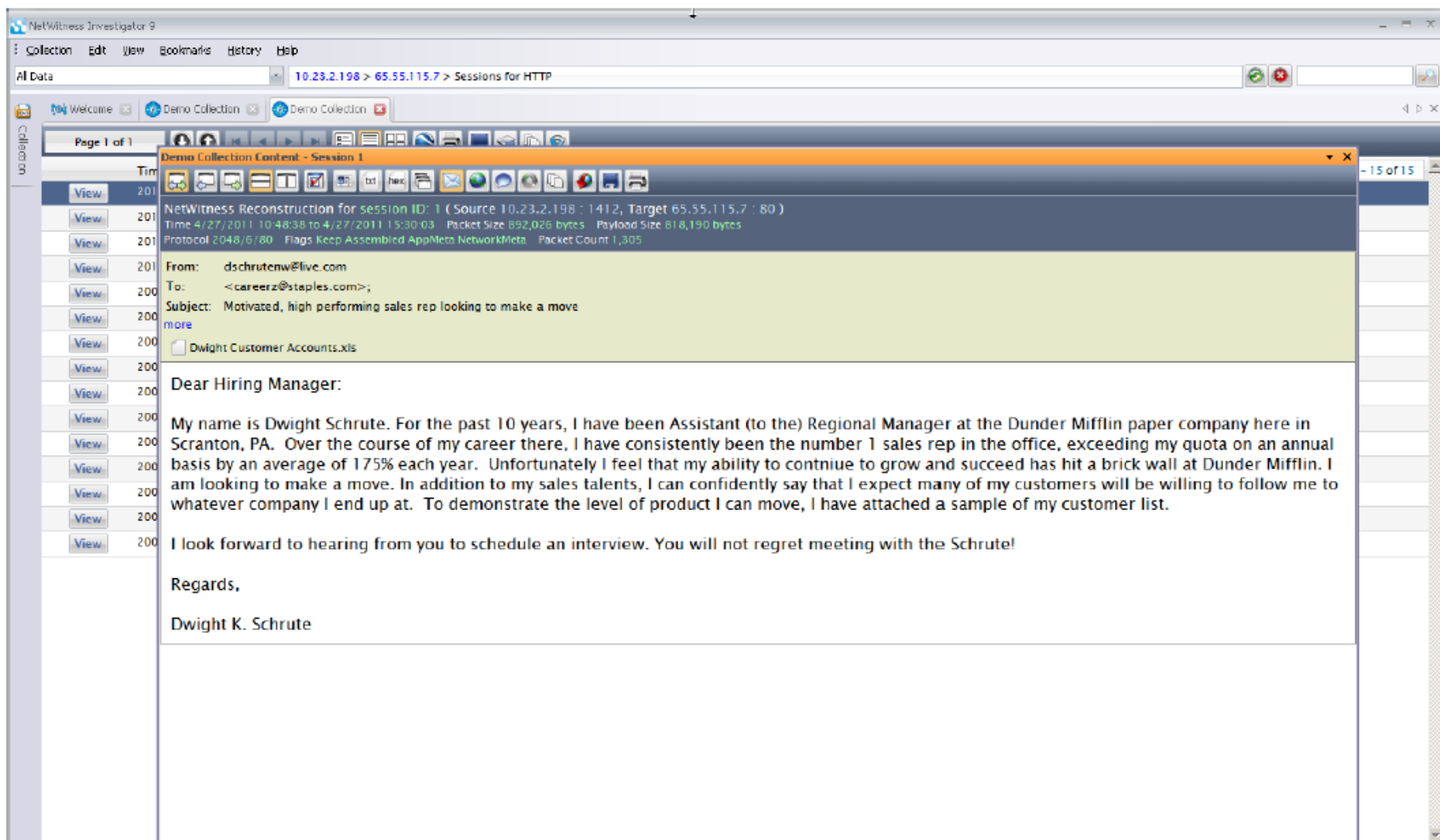


Открываем интерфейс NetWitness из RSA enVision и смотрим, какие данные передавал пользователь, вплоть до real time видео/аудио сессий

RRC RSA enVision – пример инсайда



Возросший трафик пользователя связан с тем, что он пытается предавать конкурентам коммерчески значимую информацию



После этого в его планы входит занять у конкурента удобную вакансию

Portable Tactical	Branch Fixed Capacity	Data Center High Performance	Service Provider Unlimited Scalability		
Usage: Incident Response Tactical Operations NWA50 "Eagle"  Features: •Briefcase form-factor •Encrypted/Removable Drives •2TB Retention	Usage: Remote Office Managed Services Small Security teams NWA200 Hybrid  NWA100 Broker  Features: •1U form-factor •Fixed capacity •Distributed visibility •8TB Retention	Usage: Enterprise Monitoring SOC Operations NWA1200/2400 Decoder  NWA1200/2400  NWA100 Broker  Features: •1U & 2U form-factors •Bandwidth Scalable •Distributed visibility •12 or 24TB Retention •DAS & SAN Storage Available EMC² where information lives[®] NetApp[®]	Usage: National Monitoring Large SOC Operations Indefinite retention  Features: •1U & 2U form-factors •Bandwidth Scalable •Distributed visibility •12 or 24TB Retention •DAS & SAN Storage Available		
Throughput	100Mbps	250Mbps	1Gbps	10Gbps	40Gbps
Saturated Storage	1TB/day	2.5TB/day	10TB/day	100TB/day	400TB/day



www.netwitness.com

www.rrc.ru

Спасибо за внимание!

pkuzeev@rrc.ru

Skype – zerottl

+7 985 9994824



The Security Division of EMC

