



конференция
РусКрипто'2013


<http://www.ruscrypto.ru/conference/>

Learn. Connect.
Collaborate. *together.*

Международный опыт построения глобальных систем обнаружения и предупреждения компьютерных атак

Лукацкий Алексей, консультант по безопасности

Основные задачи по Указу Президента №31с

1. Прогнозирование ситуации в области обеспечения информационной безопасности
 2. Обеспечение взаимодействия владельцев информационных ресурсов РФ, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак
 3. Осуществление контроля степени защищенности критической информационной инфраструктуры РФ от компьютерных атак
 4. Установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ
 5. Обмен информацией между ФОИВ и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах
- 

3 уровня реализации системы

Мониторинг атак и уязвимостей

```
graph TD; A[Мониторинг атак и уязвимостей] --> B[Рекомендации по отражению атак]; A --> C[Прогнозирование инцидентов]; B --> D[Автоматическое реагирование]; C --> E[Предвосхищение инцидентов];
```

Рекомендации по
отражению атак

Прогнозирование
инцидентов

Автоматическое
реагирование

Предвосхищение
инцидентов

Ключевые задачи при реализации системы

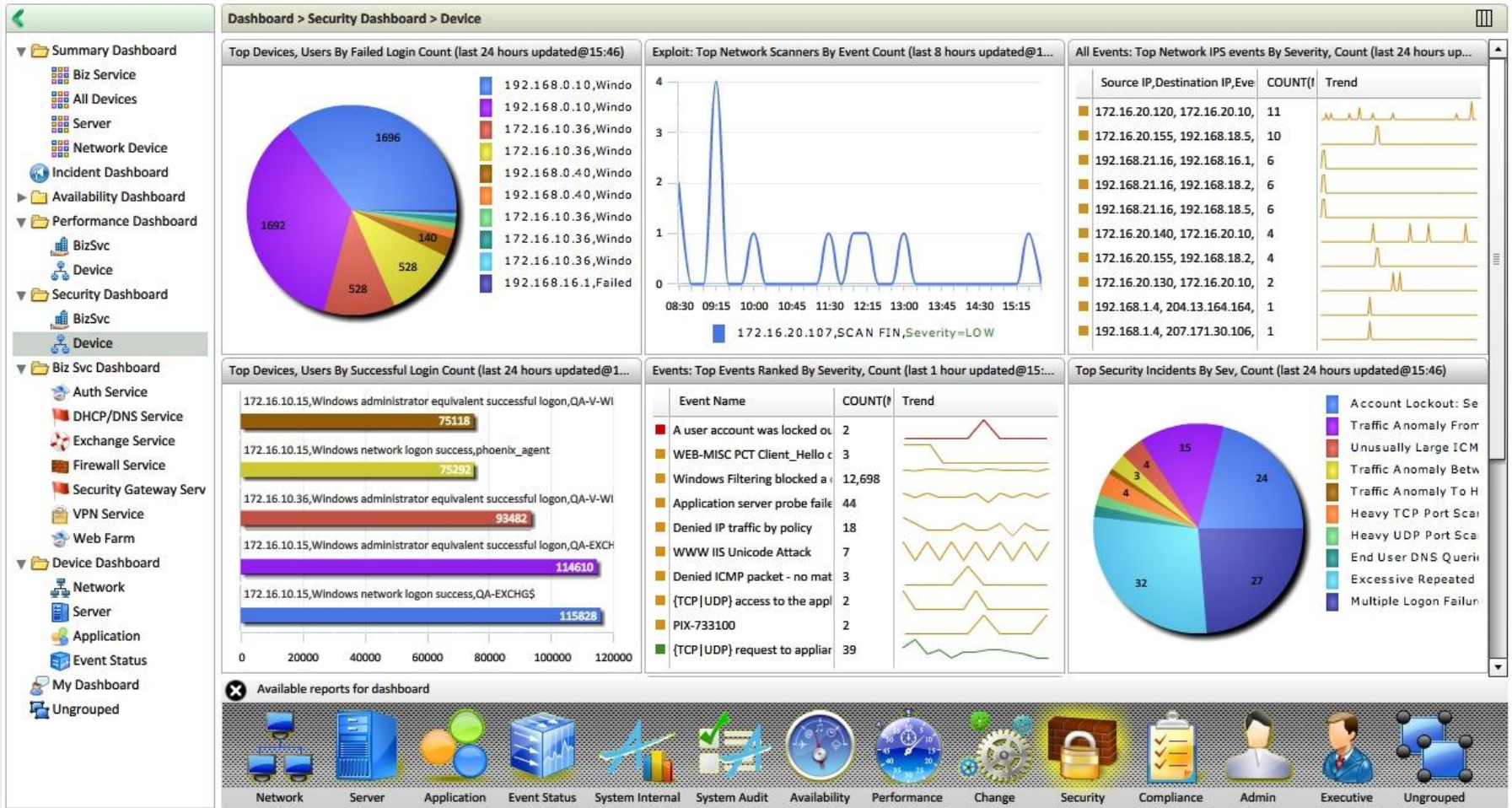
- Визуализировать атаки, инциденты и уровень защищенности
 - По различным срезам (география, ФОИВ, время, критичность...)
- Анализировать и коррелировать данные
 - Извлекать уроки
 - Прогнозировать инциденты и изменение уровня защищенности
- Собирать данные
 - Из своих источников
 - Из разрозненных security-источников
 - Big Data
- Реагировать
 - Подготовить рекомендации по реагированию
 - Автоматически отражать атаки и устранять уязвимости
- Обмениваться информацией



ВИЗУАЛІЗАЦІЯ



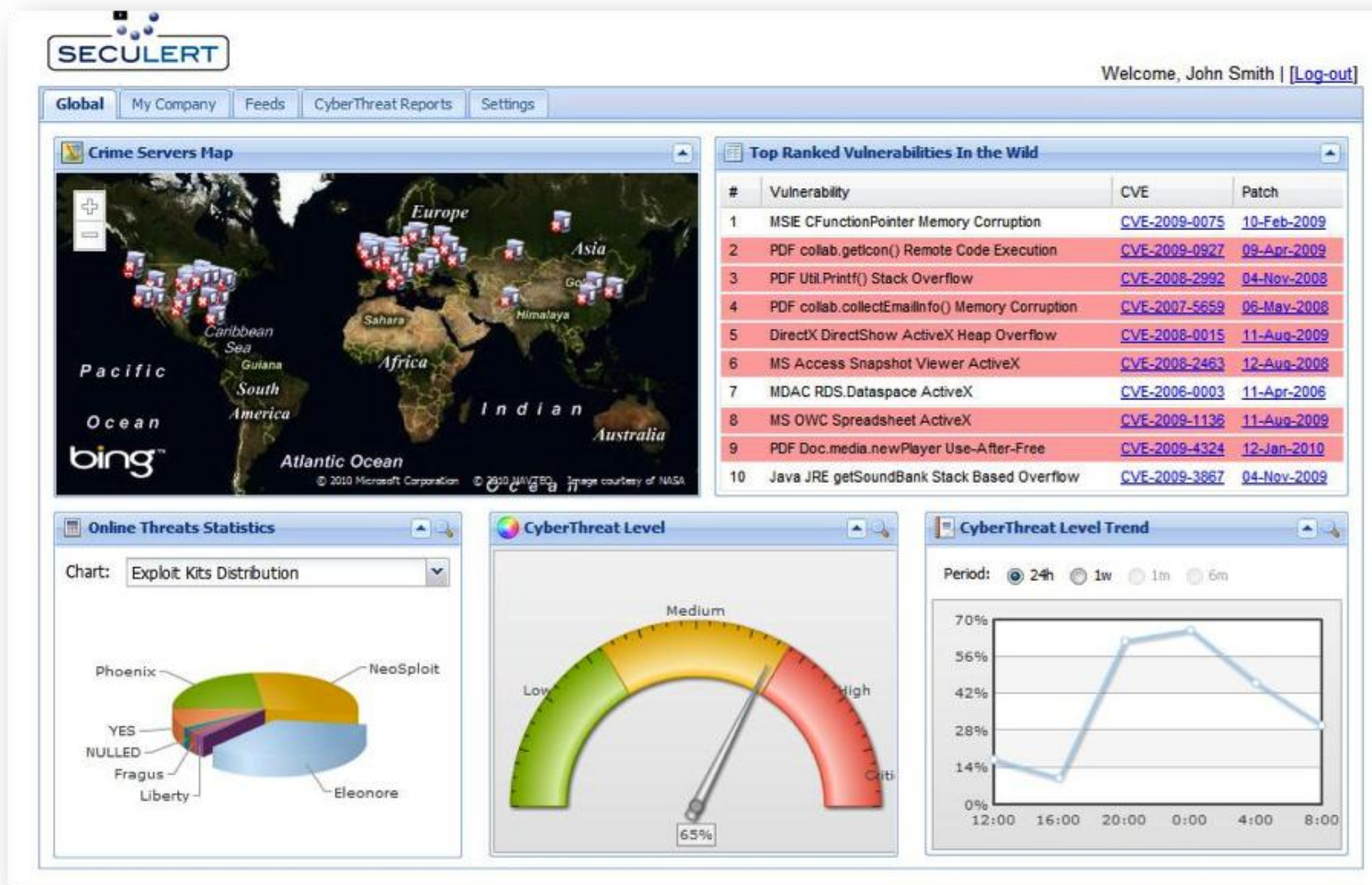
Облачный SIEM Curois: глубокая детализация



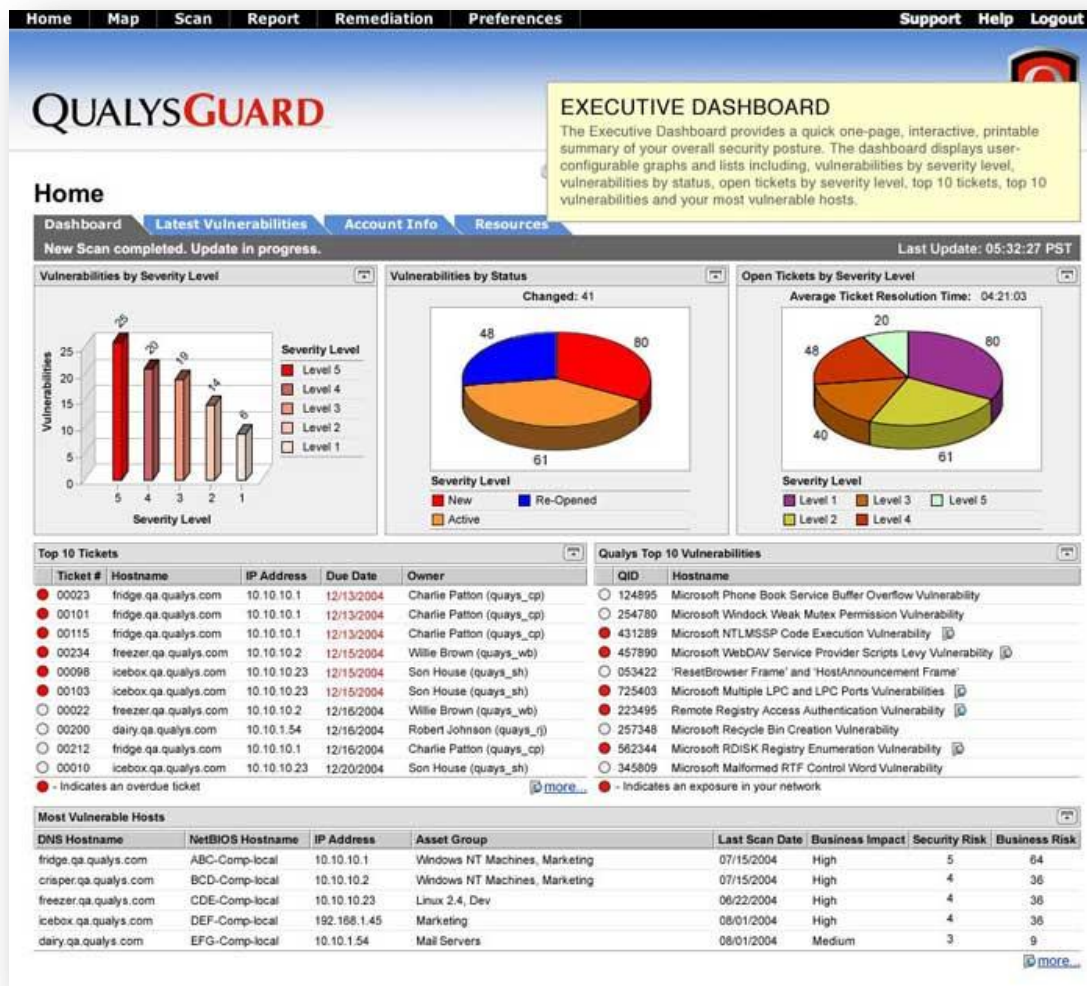
ScienceLogic Dashboard: взгляд с высоты птичьего полета

The screenshot displays the ScienceLogic dashboard interface. At the top, the ScienceLogic logo is visible on the left, and a user login area on the right shows 'Logged in as admin' with a 'Logout' button. Below the logo is a navigation menu with tabs for 'Home', 'Dashboards', 'Views', 'Events', 'Tickets', 'Knowledge', 'Reports', 'Registry', 'System', and 'Preferences'. The 'Dashboards' section is active, showing a 'Global NOC View' and a 'New' button. Below this are two filters: 'Connections Selected' (No Organizations Selected) and 'Device Groups Selected' (No Device Groups Selected). A 'Management Map' section shows a world map with several location markers. To the right of the map is a 'Customer Status' sidebar listing various customers with status indicators. The main area on the right is a 'Tickets' table with columns for 'Description', 'Description', 'Severity', 'Status', and 'Status'. Below the tickets table is a 'Custom device table' with columns for 'Device Name', 'Description', 'Current Sub', 'CPU', 'Mem', 'Disk', 'Avail', and 'Latency'. The bottom of the dashboard shows a copyright notice: 'Copyright © 2001 - 2012 ScienceLogic, Inc. All rights reserved.'

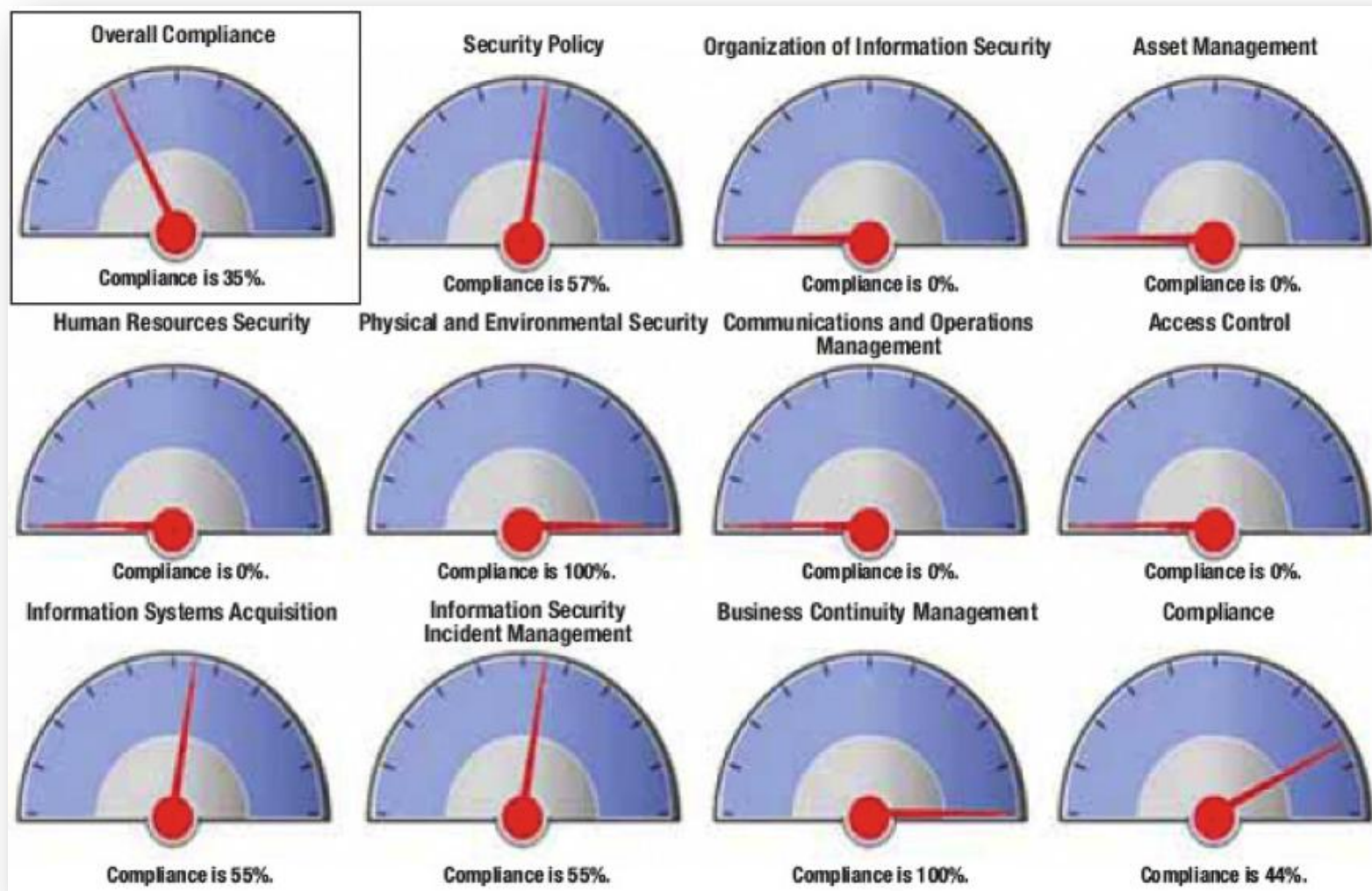
Seculert Dashboard: взгляд с разных точек зрения



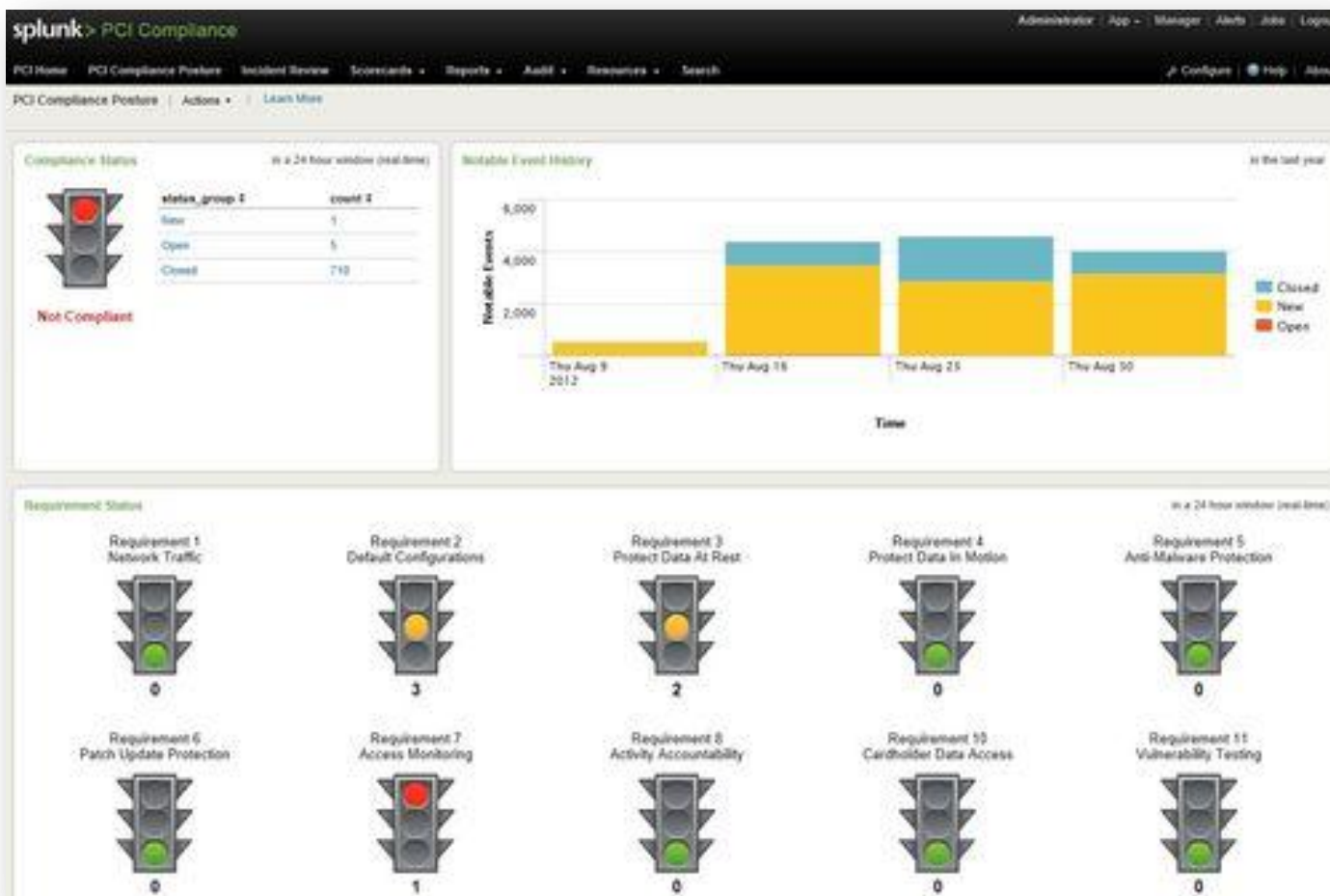
QualysGuard Executive Dashboard: анализ уровня защищенности



ISACA Compliance Dashboard: уровень соответствия НПА

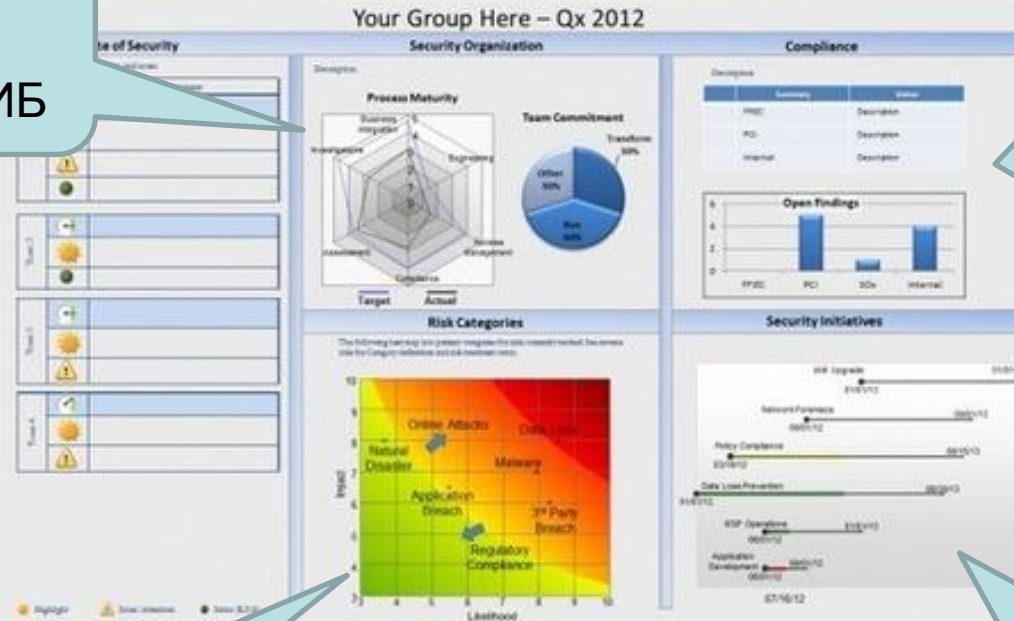


Оценка уровня соответствия PCI DSS с помощью Splunk



Визуализация слабых мест в глобальном обеспечении ИБ

Уровень зрелости процессов ИБ

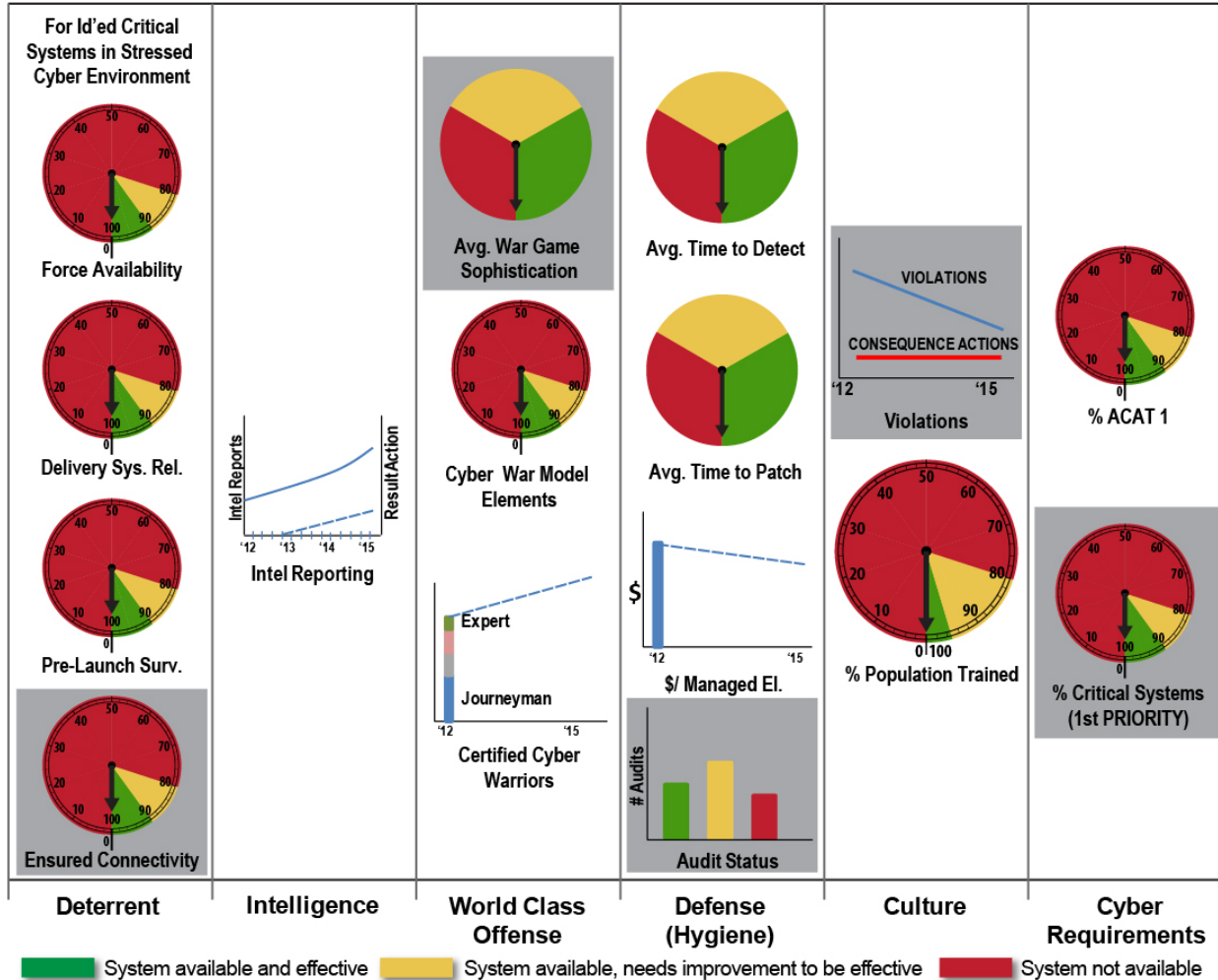


Уровень соответствия требованиям ИБ

Актуальные риски ИБ

Инициативы по ИБ

Проект системы визуализации уровня ИБ в Министерстве Обороны США



Проблемы

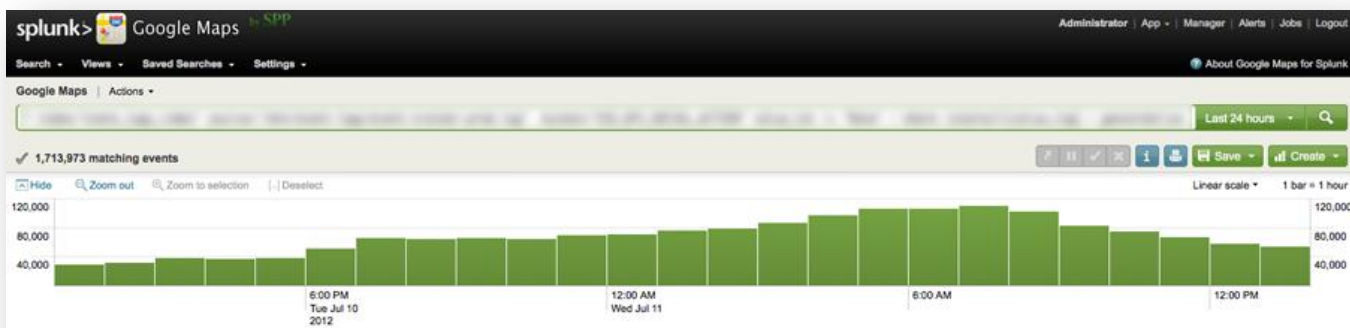
- Огромное количество данных – терабайты ежедневно
- Необходимость написания правил корреляции
- Определение пороговых значений
- Отсутствие четких критериев оценки
- Принятие решений на основе визуализированных данных
- Кто управляет всей системой?



ВИЗУАЛИЗАЦИЯ С ГЕОГРАФИЧЕСКОЙ ПРИВЯЗКОЙ



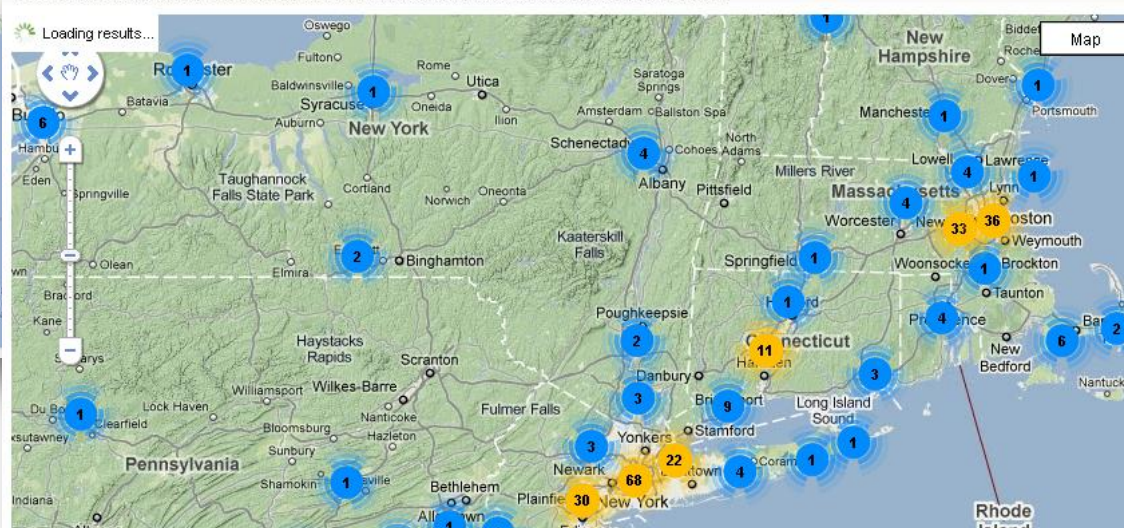
Анализ инцидентов с помощью Splunk с привязкой к местоположению



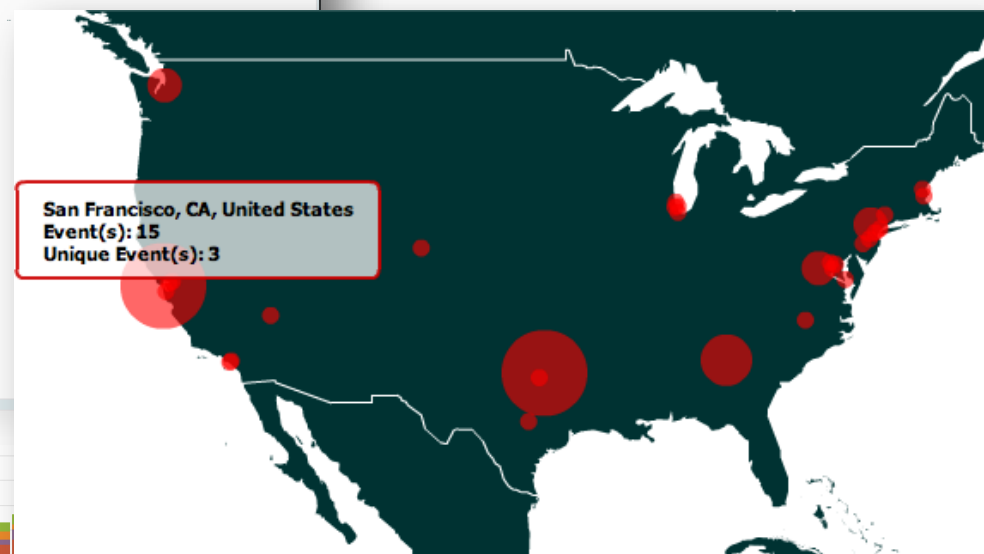
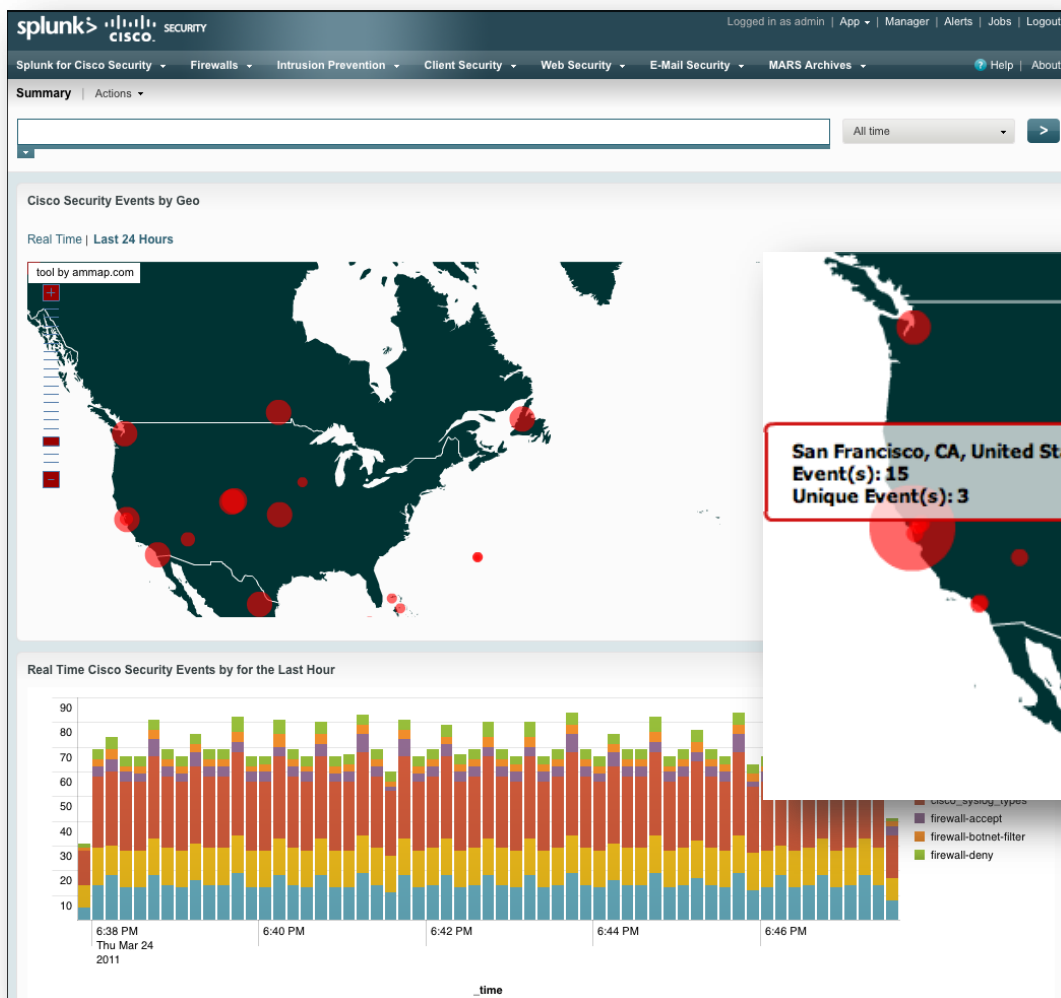
Views:
Map | Geo Results | Events
10000 results with location information (2259 distinct locations) in the last 24 hours



8,117 results in the last 30 seconds (from 10:48:14 AM to 10:48:44 AM on Friday, August 27, 2010)



Географическая привязка инцидентов с помощью Splunk в реальном времени



Проблемы

- Отсутствие привязки к российским геоинформационным системам
- Как идентифицировать реального заказчика атаки?



СБОР ДАННЫХ – СОБСТВЕННЫЕ ИСТОЧНИКИ



Центр мониторинга T-Mobile



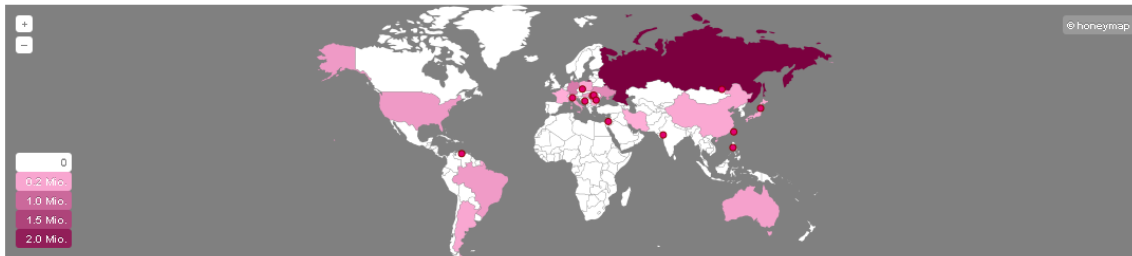
LIFE IS FOR SHARING.

OVERVIEW INFO IMPRINT



English German

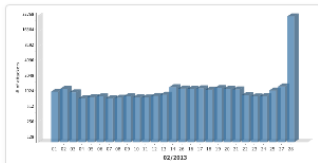
Overview of current cyber attacks (logged by 97 Sensors)



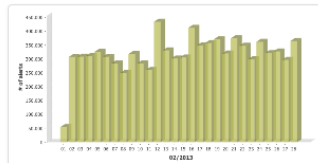
Live-Ticker

Date	Source	Attack on	Parameter
2013-03-27 20:28:17	Romania	Network services	dionaea.smbd.port.445
2013-03-27 20:28:18	Philippines	Network services	dionaea.smbd.port.445
2013-03-27 20:28:15	Romania	Network services	dionaea.smbd.port.445
2013-03-27 20:28:15	Taiwan	Network services	dionaea.smbd.port.445
2013-03-27 20:28:14	Bosnia and Herzegovina	Network services	dionaea.smbd.port.445

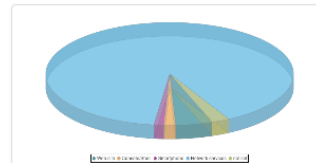
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



Top 15 of Source Countries (Last month)

Source of Attack	Number of Attacks
Russian Federation	2,402,722
Taiwan, Province of China	907,102
Germany	780,425
Ukraine	566,531
Hungary	367,966
United States	355,341
Romania	350,948
Brazil	337,977
Italy	288,607
Australia	255,777
Argentina	185,720
China	168,146
Poland	162,235
Israel	143,943
Japan	133,908

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	27,327,356
Attack on Netbios protocol	937,476
Attack on Port 33434	687,446
Attack on SSH protocol	669,589
Attack on Port 5353	522,671

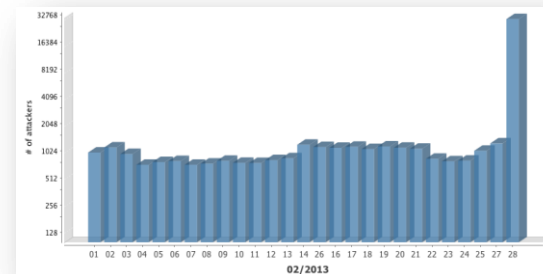
Источник: <http://www.sicherheitstacho.eu/?lang=en>

Детали центра мониторинга T-Mobile

Общий взгляд



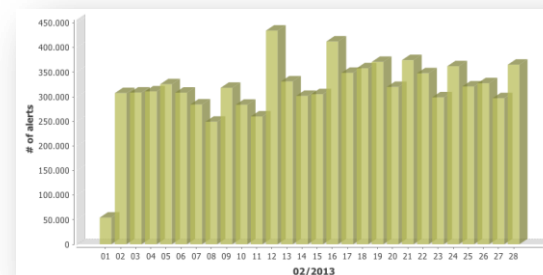
Общее число атакующих



Топ15 стран

	Quelle des Angriffes	Anzahl der Angriffe
	Russian Federation	2.178.515
	United States	1.138.420
	Taiwan, Province of China	706.478
	Romania	664.831
	Ukraine	499.931

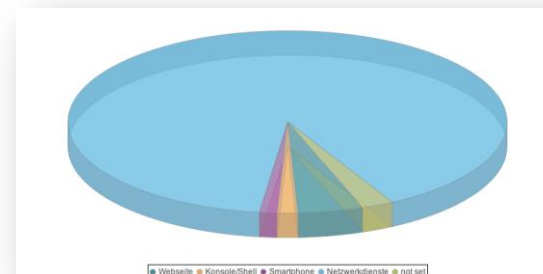
Общее число атак



Цели атак

Beschreibung	Anzahl der Angriffe
Angriff auf SMB Protokoll	22.647.453
Angriff auf Netbios Protokoll	802.221
Angriff auf Dienst an Port 33434	687.446
Angriff auf SSH Protokoll	602.557
Angriff auf Dienst an Port 5353	381.299

Распределение целей атак



Центр мониторинга Sophos: узкая специализация

[Login](#) [Register](#) | [About us](#) [Press](#) [Contact us](#) [Careers](#) [Global websites](#) [go](#)

SOPHOS

[Your Needs](#) | [Why Sophos](#) | [Products](#) | [Support](#) | [Threat Center](#) | [Security News/Trends](#) | [Partners](#)

Home » Threat Center » Threat Monitoring » Web Threats Dashboard

Web Threats Dashboard

We're constantly monitoring how many malicious requests our technology blocks. In this dashboard, you can see what we've found.

Infected website locations

Malicious web requests blocked

Top web threats

Family	Percent	Trend
Iframe	45.9%	▼
JSRedir	43.7%	▼
Badsrc	2.4%	▼
EncPk	1.0%	▲
LdlMon	1.0%	▼
ObfJS	0.8%	▲
Generic	0.8%	▼
FBJack	0.7%	▼

[Download our free Virus Removal Tool](#)
 Find what your antivirus missed.

[Login](#) [Register](#) | [About us](#) [Press](#) [Contact us](#) [Careers](#) [Global websites](#) [go](#)

SOPHOS

[Your Needs](#) | [Why Sophos](#) | [Products](#) | [Support](#) | [Threat Center](#) | [Security News/Trends](#) | [Partners](#)

Home » Threat Center » Threat Monitoring » Malware Dashboard

Malware Dashboard

We keep track of all known and emerging malware here. We've collected metrics on all the latest malware threats, and we update them as soon as we get new information. See the top threats and where they're coming from.

Viruses and Spyware

Malware detection rate per 10,000 endpoints

Top prevalent malware

Family	Percent	Trend
Agent	8.7%	▲
KeyGen	4.0%	▲
Phish	3.6%	▲
JSRedir	3.9%	▲
TDSSConf	3.7%	▲
EncPk	3.5%	▲
BredoZp	3.5%	▲

Current Vulnerabilities

Vulnerability	Definition
CVE-2013-0431	JRE JMX RCE
CVE-2013-0633	ActiveX version of Flash Player on Windows
CVE-2013-0422	Java security bypass zero-day vulnerability, Uses RMXBeanServer
CVE-2012-1535	Embedded OpenType parsing vulnerability
CVE-2012-5076	JRE JAX-WS

[Download a free Virus Removal Tool](#)

THREAT LEVEL: MEDIUM
[Learn more](#)

Security Threat Report 2013
 Our annual report explores new platforms and changing threats.
[Download now](#)

[Spicing up phishing attacks](#)
 27 Mar 2013

[The 'What's Worse Security Championships'](#)
 27 Mar 2013

[SSCC 105 - our two-weekly news podcast: HP printers, Google blocks ad blockers, Apple does the 2-step, and more.](#)
 27 Mar 2013

Проблемы

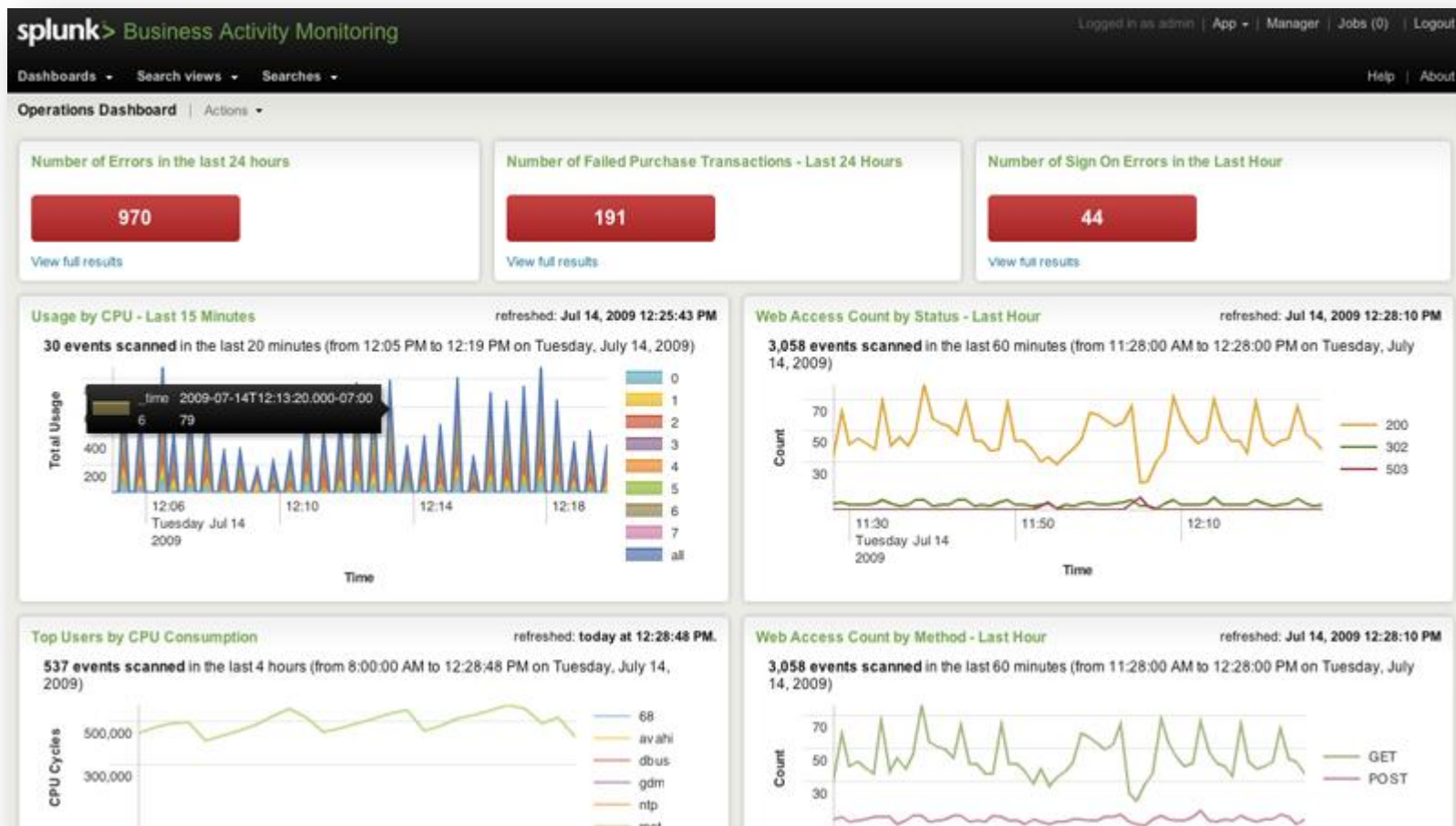
- Практически полное отсутствие собственных сенсоров
 - «Ручеек» и «Аргус» в расчет не берем
 - СОБКА?
- Активное использование разных решений по ИБ от разных производителей
- Ориентация на сетевые события или только события ИБ



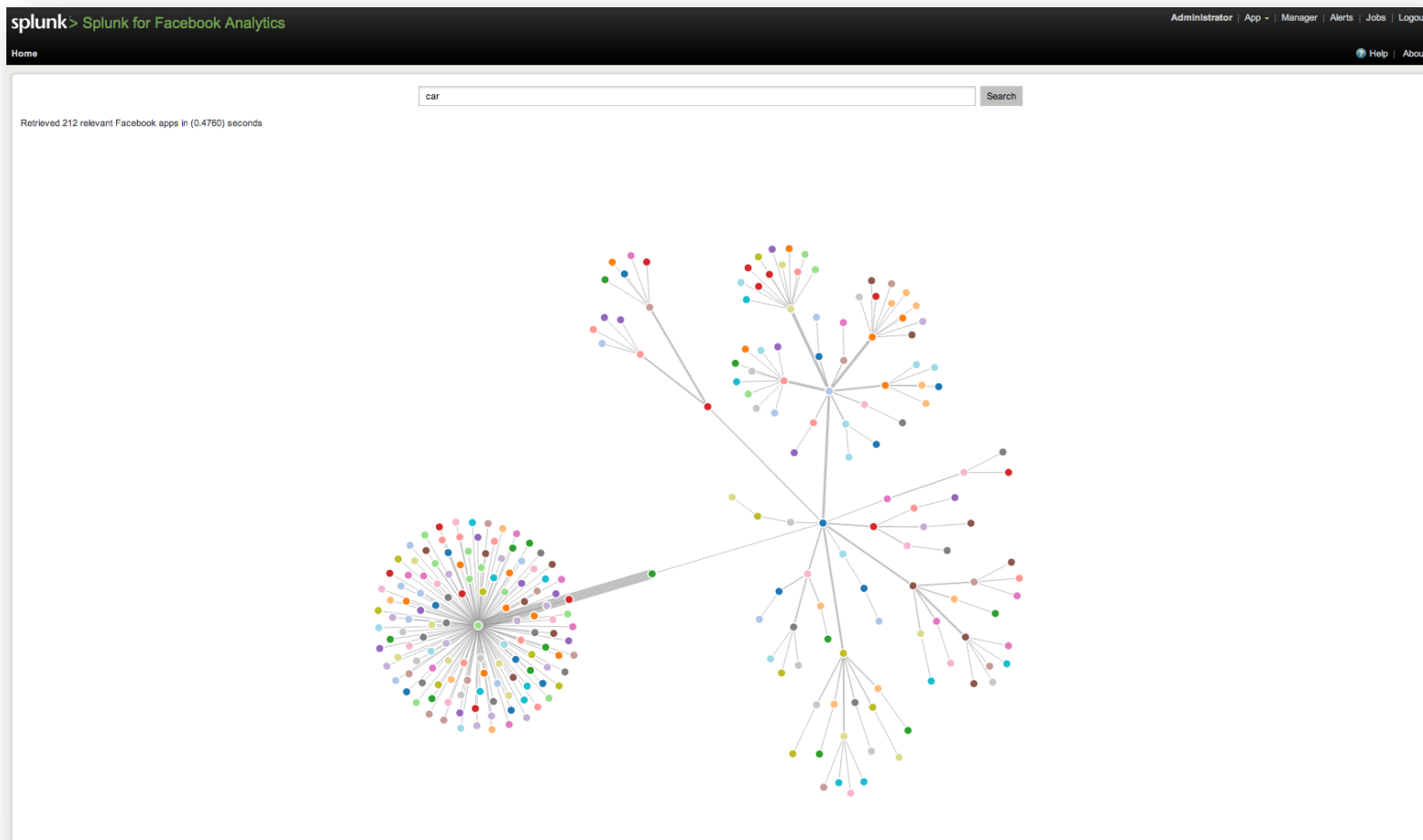
СБОР ДАННЫХ – ИСТОЧНИКИ 3-Х ЛИЦ



Анализ прикладных событий (доступ к сайту) с помощью Splunk



Анализ активности пользователей Facebook с помощью Splunk



Проблемы

- Обработка и хранение Big Data



АНАЛИЗ ДАННЫХ



Анализ трафика с помощью Maltego

The screenshot displays the Maltego Radium 3.2.0 BETA interface. The main window shows a network graph with various entities connected by lines. The entities include IP addresses (e.g., 64.124.152.50, 206.188.26.41, 206.188.26.50, 206.188.26.46, 206.188.26.32-206.188.26.63, 216.137.30.0-216), domains (mail.palantirtech.com, blog.palantirtech.com), and a website (devzone.palantirtech.com). The graph is viewed in 'Main View'.

The 'Detail View' on the right shows the selected entity: IPv4 Address (maltego.IPv4Address) 64.124.152.35. It includes the following information:

- Relationships**
 - Incoming**
 - devzone.palantirtech.com (Website)
 - wiki.palantirtech.com (Website)
 - + Outgoing**
- Generator detail**
 - Source: devzone.palantirtech.com (Website)
 - Transform: To IP Address [DNS]
 - Result: 64.124.152.35 (IPAddress)
 - Gen. date: 2011-3-4 14:52

The 'Property View' on the right shows the following properties:

Property	Value
Type	IPv4 Address
IP Address	64.124.152.35
Internal	<input type="checkbox"/>
Graph info	
Size	210
Bookmark	★

Анализ инцидентов с помощью Maltego

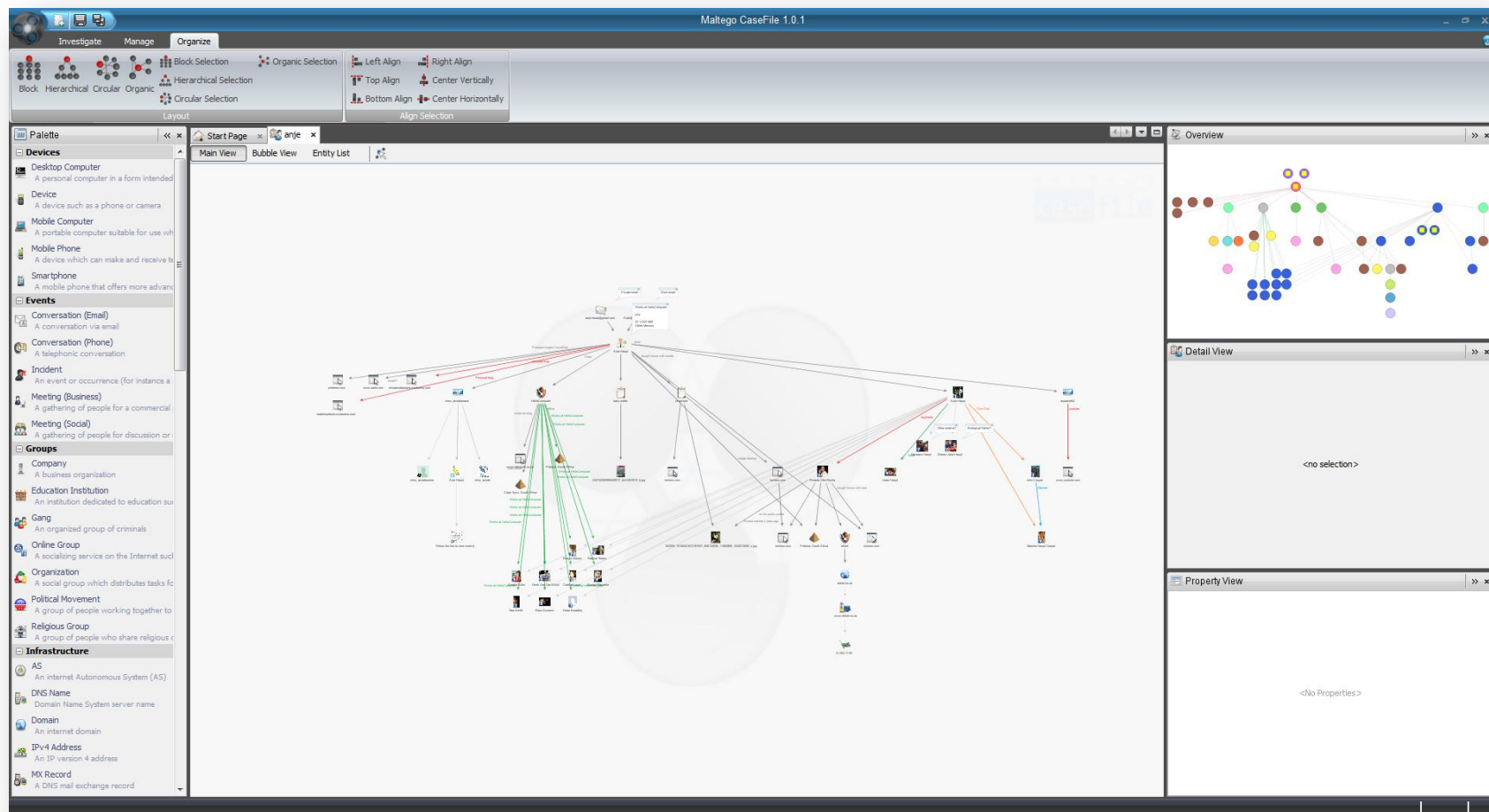
The screenshot displays the Maltego Radium 3.2.0 BETA interface. The main window shows a network graph with nodes and links. The 'Entity List' tab is active, displaying a table of nodes. The table has columns for Nodes, Type, Value, Weight, Incoming, Outgoing, and Bookmark. The node 'www.siscareers.gov.uk' is highlighted in blue.

Nodes	Type	Value	Weight	Incoming	Outgoing	Bookmark
www.tsol.gov.uk	DNS Name	www.tsol.gov.uk	100	2	1	★
www.gls.gov.uk	DNS Name	www.gls.gov.uk	100	2	1	★
w1.mi5.gov.uk	DNS Name	w1.mi5.gov.uk	100	2	1	★
www.treasury-solicitor.gc	DNS Name	www.treasury-solicitor.gov.uk	100	2	1	★
test.gls.gov.uk	DNS Name	test.gls.gov.uk	100	2	1	★
www.siscareers.gov.uk	DNS Name	www.siscareers.gov.uk	100	2	1	★
www.pppaservices.qineti	DNS Name	www.pppaservices.qinetiq-tim.com	100	2	1	★
webdev.qinetiq-tim.net	DNS Name	webdev.qinetiq-tim.net	100	2	1	★
daisy.qinetiq-tim.com	DNS Name	daisy.qinetiq-tim.com	100	2	1	★
sorry.aegate.com	DNS Name	sorry.aegate.com	100	2	1	★
w2.mi5.gov.uk	DNS Name	w2.mi5.gov.uk	100	2	1	★
mail.mi5.gov.uk	DNS Name	mail.mi5.gov.uk	100	2	1	★
stats.mi5.gov.uk	DNS Name	stats.mi5.gov.uk	100	2	1	★
search01.mi5.gov.uk	DNS Name	search01.mi5.gov.uk	100	2	1	★
www.mi5careers.gov.uk	DNS Name	www.mi5careers.gov.uk	100	2	1	★
preview.mi5.gov.uk	DNS Name	preview.mi5.gov.uk	100	2	1	★
vmi.mi5.gov.uk	DNS Name	vmi.mi5.gov.uk	100	2	1	★
search.mi5.gov.uk	DNS Name	search.mi5.gov.uk	100	2	1	★
www.mi5.gov.uk	DNS Name	www.mi5.gov.uk	100	2	1	★
www.securityservice.gov	DNS Name	www.securityservice.gov.uk	100	2	1	★
208.73.210.29	IPv4 Address	208.73.210.29	100	3	0	★
portal2.qinetiq-tim.net	DNS Name	portal2.qinetiq-tim.net	100	1	0	★
portal2.qinetiq-tim.com	DNS Name	portal2.qinetiq-tim.com	100	1	0	★
www.sdc-test.qinetiq-tim	DNS Name	www.sdc-test.qinetiq-tim.net	100	1	0	★
mi5careers.co.uk	DNS Name	mi5careers.co.uk	100	1	0	★
mi5careers.org.uk	DNS Name	mi5careers.org.uk	100	1	0	★
mrw3.qinetiq-tim.com	DNS Name	mrw3.qinetiq-tim.com	100	1	0	★

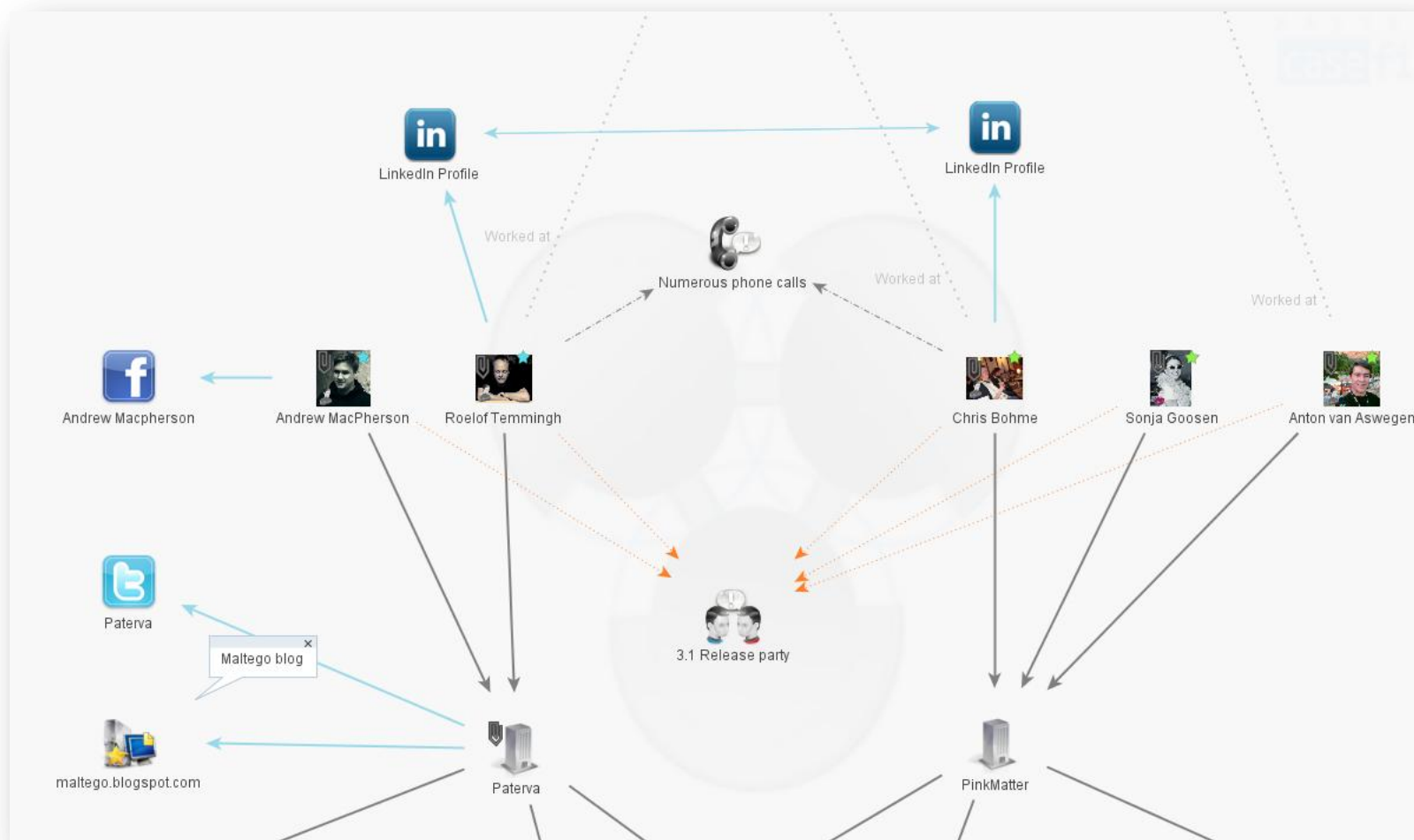
The right-hand side of the interface shows the 'Detail View' for the selected entity 'www.siscareers.gov.uk'. It displays the following information:

- Generator detail:**
 - Source: 194.61.183.100 (IPAddress)
 - Transform: To DNS Name [Reverse DNS]
 - Result: www.siscareers.gov.uk (DNSName)
 - Gen. date: 2011-8-22 16:16
- Generator detail:**
 - Source: 194.61.183.100 (IPAddress)
 - Transform: To DNS Name [Other DNS names]
 - Result: www.siscareers.gov.uk (DNSName)
 - Gen. date: 2011-8-22 16:36
- Property View:**
 - Type: DNS Name
 - DNS Name: www.siscareers.gov.uk
 - Weight: 100
 - Incoming: 2
 - Outgoing: 1
 - Bookmark: ★

Анализ взаимосвязей между пользователями с помощью Maltego



Анализ взаимосвязей между пользователями с помощью Maltego



Анализ событий в рамках ОРД с помощью Maltego

The screenshot displays the Maltego Radium 3.2.0 BETA interface. The main window shows a network graph with several entities and their relationships. The entities include:

- RT @kylemaxwell: I wrote some pretty terrible...** (Yellow bubble)
- RT @kylemaxwell: The sample Python library fo...** (Blue bubble)
- I wrote some pretty terrible prototype code...** (Blue bubble)
- #maltego** (Black bubble)
- maltego - Additional Footprinting Tool...** (Blue bubble)
- RT @kylemaxwell: I wrote some pretty terrible...** (Blue bubble)

The graph shows relationships between these entities, with arrows indicating the direction of the connections. A central yellow bubble is connected to several other entities, including the blue bubbles and the black bubble. The interface also features a left sidebar with a 'Palette' of entity types, a top menu bar with 'Investigate', 'Manage', 'Organize', and 'Machines', and a right sidebar with 'Running Machines', 'Detail View', and 'Property View'.

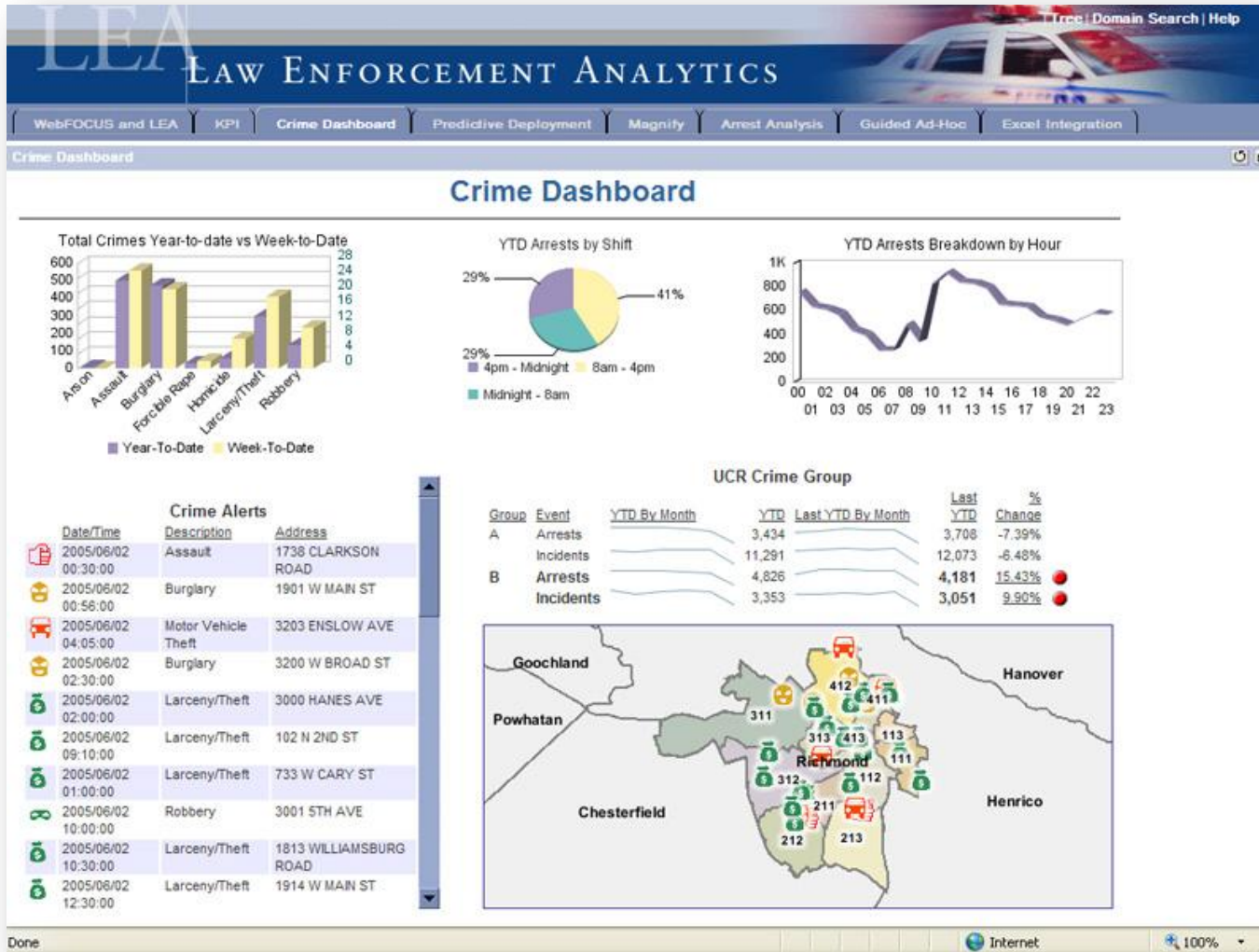
The 'Detail View' shows the following information for the selected entity:

Twitter info	
Content	RT @kylemaxwell: I wrote some pretty terrible prototype code tonight to integrate CIF and #Maltego. https://t.co/hQrOks6C/jc @Paterva @Barely3am
Date	2012-08-16T10:43:40Z
Author	Barely3am (Barely3am)

The 'Property View' shows the following properties for the selected entity:

Properties	
Type	Twit
Twit	RT @kylemaxwell: I wrote som...
Twit ID	tag:search.twitter.com,2005:...
Author	Barely3am (Barely3am)
Author URI	http://twitter.com/Barely3am
Content	RT @<a class="" href="https...
Image Link	http://a0.twimg.com/profile_j...
Date published	2012-08-16T10:43:40Z
Title	RT @kylemaxwell: I wrote som...
Dynamic properties	
Image	http://a0.twimg.com/profile_i...

Прогнозирование с помощью WebFOCUS



Проблемы

- Необходимое количество аналитиков
- Кто расследует инциденты?
- Отсутствие моделей для анализа
- Отсутствие моделей для прогнозирования



РЕАГИРОВАНИЕ



Центр мониторинга Cisco SIO

The screenshot displays the Cisco SIO portal interface. At the top, there is a navigation bar with the Cisco logo and links for Products & Services, Support, How to Buy, Training & Events, and Partners. A search bar is located on the right side of the navigation bar. Below the navigation bar, the main heading is "Security Intelligence Operations" with the tagline "Inform, Protect, Respond" and a brief description of the center's mission. There are social media icons and search boxes for "Search Security" and "URL Reputation Lookup". A horizontal menu contains categories: Latest Threat Information, Resources, Cisco Products and Services, Cisco Emergency Response, and Notification Registration. A large banner features a photo of people working at computers with the text "Cisco SIO Portal Customer Survey Help us improve this site by taking our survey!". Below the banner, there are tabs for "Security Highlights", "Security Alerts", "Upcoming Security Events", and "Security Blog". The "Security Alerts" tab is active, showing a table of security updates. To the right, there are two featured content boxes: "Cisco IOS Software Bundled Publication for March 2013" with a video player and "Cisco Event Response: Cisco IOS Software Bundled Publication" with a text snippet.

Worldwide | Log In | Account | Register

Products & Services | Support | How to Buy | Training & Events | Partners

Security Intelligence Operations

Inform, Protect, Respond
Early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks

Search Security [Advanced Search](#)





URL Reputation Lookup

Latest Threat Information | Resources | Cisco Products and Services | Cisco Emergency Response | Notification Registration


Cisco SIO Portal Customer Survey

Help us improve this site by taking our survey!

Security Highlights | **Security Alerts** | Upcoming Security Events | Security Blog

Title	Last Updated
 Cisco Event Response: March 2013 Semiannual Cisco IOS Software Advisory Bundled Publication	2013 Mar 27
 Apple Mac OS X Security Update for March 2013	2013 Mar 15
 Oracle Java SE Critical Patch Update Advisory for February 2013 Urgent	2013 Mar 05
 Today's the Day: Announcing the Cisco IOS Software Security Advisory Bundle	2013 Mar 27

Cisco IOS Software Bundled Publication for March 2013




This is a summary video of the Cisco IOS Software Bundled Publication for March 2013.


Cisco Event Response: Cisco IOS Software Bundled Publication

Intelligence to help identify and mitigate vulnerabilities in the

Рекомендации SecurityLab.ru




SecurityLab
by Positive Technologies



ВЕБИНАР
04.04.2013 / 14:00

Особенности сканирования сетевых устройств с помощью MaxPatrol



POSITIVE TECHNOLOGIES


Блоги | Уязвимости | Новости | Статьи | Софт | Проекты партнеров | Форум

RSS • Вход • Поиск


Уязвимости

Важные уязвимости

01 марта, 2013




✓ **Компрометация системы в Java**
Удаленный пользователь может скомпрометировать целевую систему. / просмотров: 2025



28 февраля, 2013

✓ **Компрометация системы в JustSystems Ichitaro**
Удаленный пользователь может скомпрометировать целевую систему. / просмотров: 717



27 февраля, 2013

✓ **Множественные уязвимости в Adobe Flash Player**
Удаленный пользователь может выполнить произвольный код на целевой системе. / просмотров: 1644

Новые уведомления

27 марта, 2013

- ✓ **Обход ограничений безопасности в McAfee Virtual Technician** / (просмотров: 93)
- ✓ **Повышение привилегий в Linux Kernel** / (просмотров: 163)
- ✗ **Компрометация системы в MongoDB** / (просмотров: 87)
- ✗ **Межсайтовый скриптинг в zClip** / (просмотров: 83)
- ✓ **Межсайтовый скриптинг в Splunk** / (просмотров: 82)
- ✓ **Обход ограничений безопасности в Cerb** / (просмотров: 89)
- ✗ **Раскрытие важных данных в roundcube** / (просмотров: 223)

Transferring data from www.securitylab.ru... в Microsoft Windows Modern Mail / (просмотров: 76)

ТОП Новости

НАТО: Убивать хакеров – это нормально 18
21 марта, 2013
Альянс представил ряд предложений, призванных сделать кибервойны более цивилизованными.

В Сеть утекла сборка Windows Blue 23
25 марта, 2013
Теперь настраивать персонализацию можно из боковой панели, не открывая приложение настроек.

Китай создаст собственную ОС 25
22 марта, 2013
Речь идет о версии ОС Ubuntu от Canonical, которая получила название Kylin.

Windows 7 Service Pack 1 будет автоматически устанавливаться с обновлениями ОС 22
19 марта, 2013
Ранее пользователям предоставлялся выбор, устанавливать или нет новую версию SP1.

Эксперты: Большинство российских пользователей загружают пиратское ПО из интернета 16
21 марта, 2013
Исследователи установили, что другие способы передачи контрафактного ПО намного уступают всемирной Сети.

Организации Южной Кореи пострадали от вируса, который удалял критические файлы на Linux машинах 15
22 марта, 2013
Компонент для удаления системных файлов Linux встроен во вредоносный инструмент, предназначенный для...

Работающие на правительство Китая хакеры изменили свою

Проблемы

- Кто будет **оперативно** разрабатывать методические рекомендации по отражению атак?
 - Будет ли на них навешиваться гриф секретности?
- Кто будет реагировать на местах?
- Автоматическое реагирование
 - Проблема ложных срабатываний



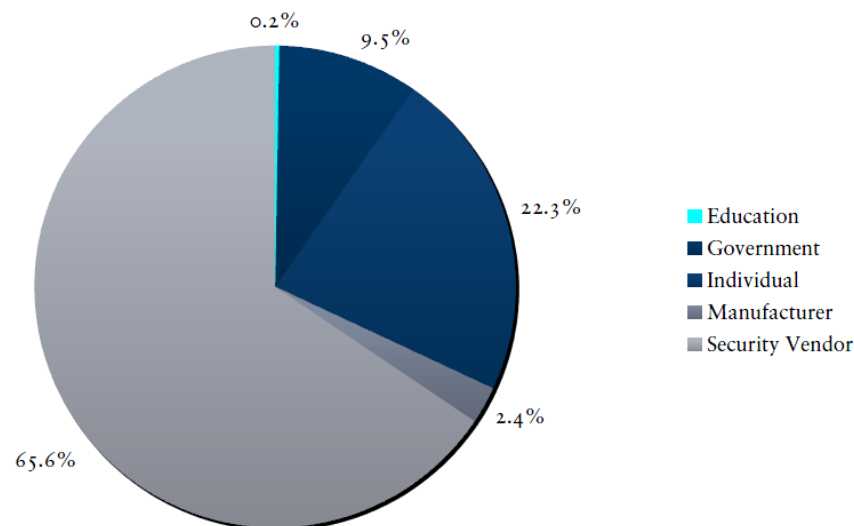
ОБМЕН ИНФОРМАЦИЕЙ



Проблемы

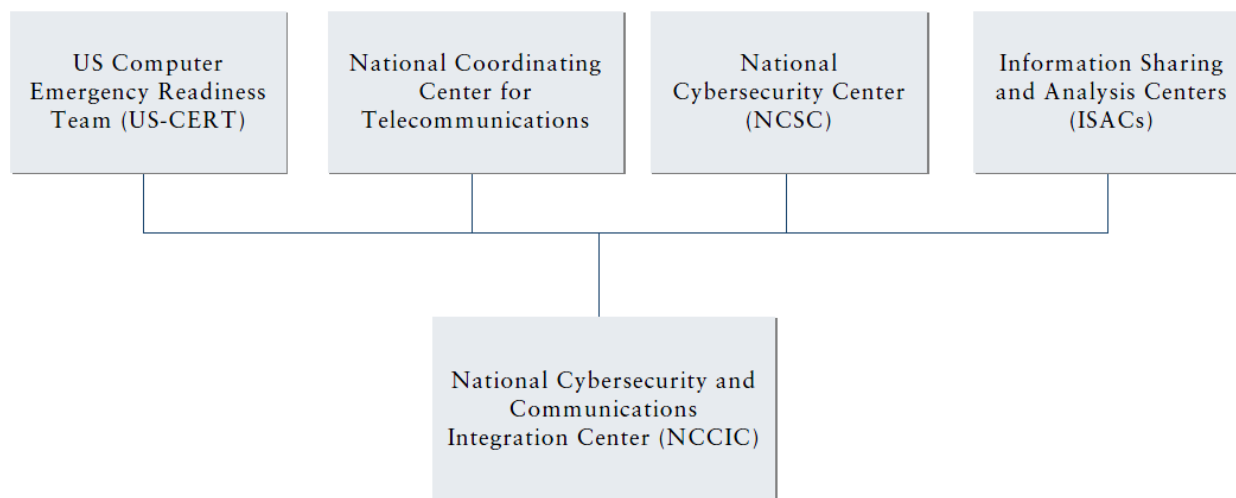
- Как обмениваться средствами защиты ФОИВов между собой информацией об атаках?
- Как обмениваться ФОИВам между собой информацией об инцидентах, атакующих и т.п.?
- Как обмениваться этой информацией с международными организациями?

Кто сообщает об уязвимостях в США?



Пример: Electric Sector Industry Sector Advisory Committee (ES-ISAC)

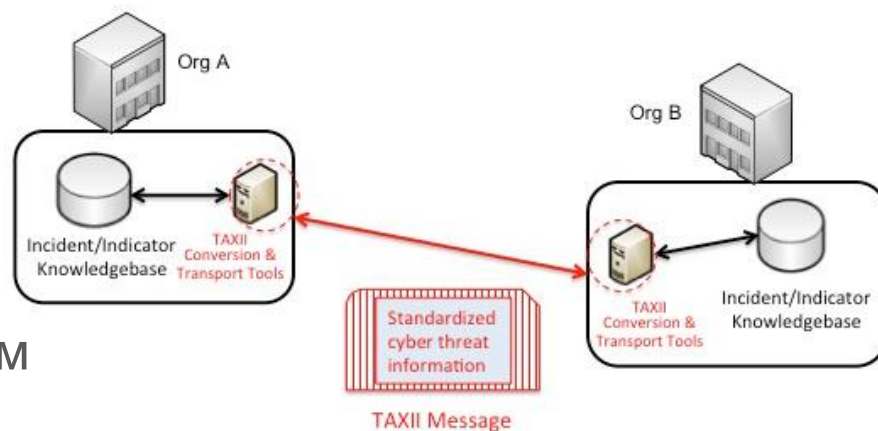
- Получение данных об инцидентах от электрокомпаний
- Взаимодействие с National Infrastructure Protection Center (NIPC)
- Связь с другими ISAC
- Распространение лучших практик и извлеченных уроков
- Взаимодействие с другими секторами экономики
- Участие в киберучениях



Автоматизация процесса обмена: протоколы STIX и TAXII

- Протокол STIX позволяет унифицировать описание различных угроз и связанных с ними параметров - индикаторы атаки, информация об инциденте, используемый для атаки инструментарий или уязвимости, предполагаемые меры нейтрализации атаки, информация о предполагаемом противнике/нарушителе и т.п.
- Протокол TAXII унифицирует способы обмена информацией об угрозах, описанных с помощью STIX

Structured Threat Information eXpression



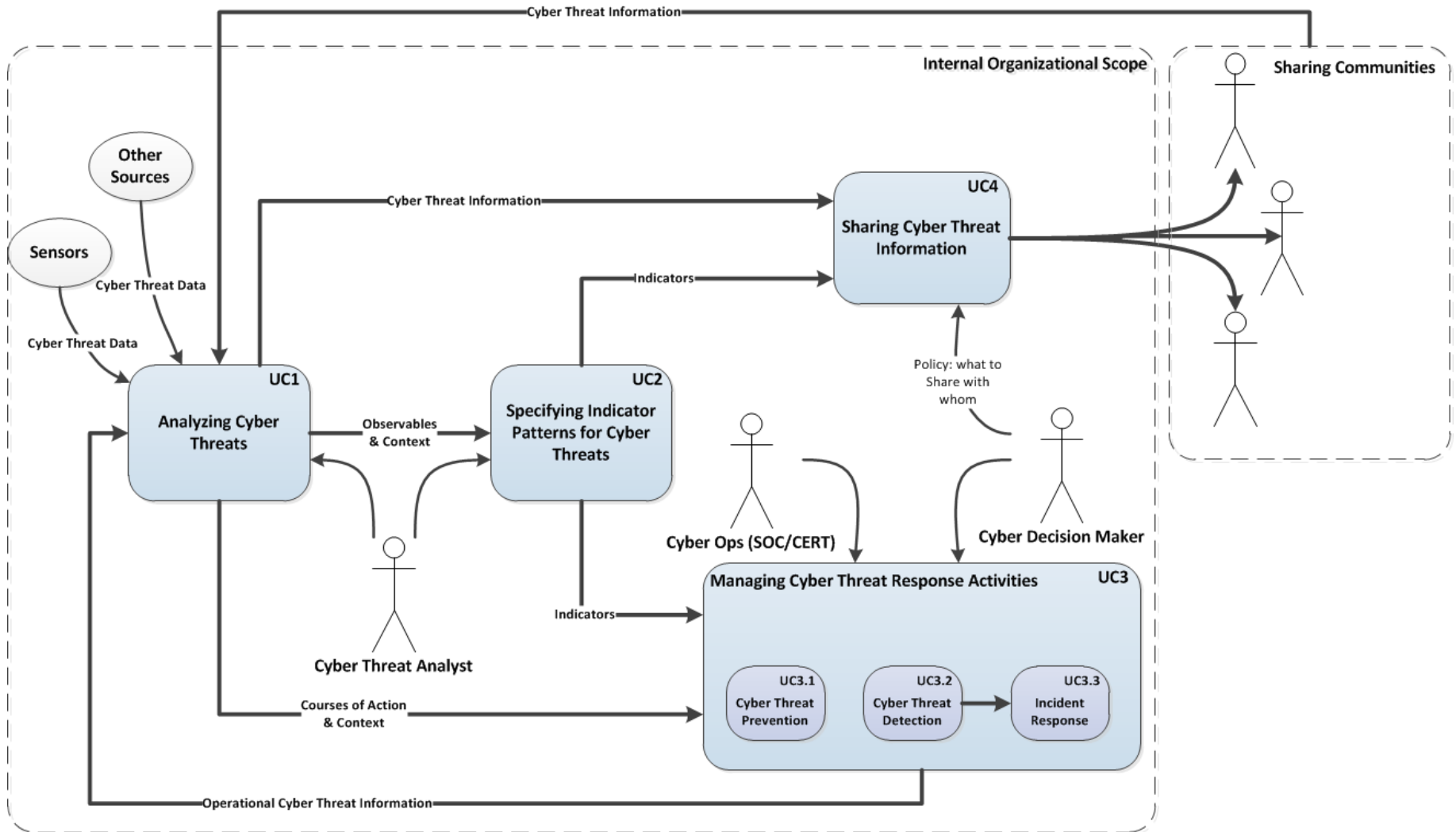
Trusted Automated eXchange of Indicator Information



ОБЪЕДИНЯЯ ВСЕ ВМЕСТЕ

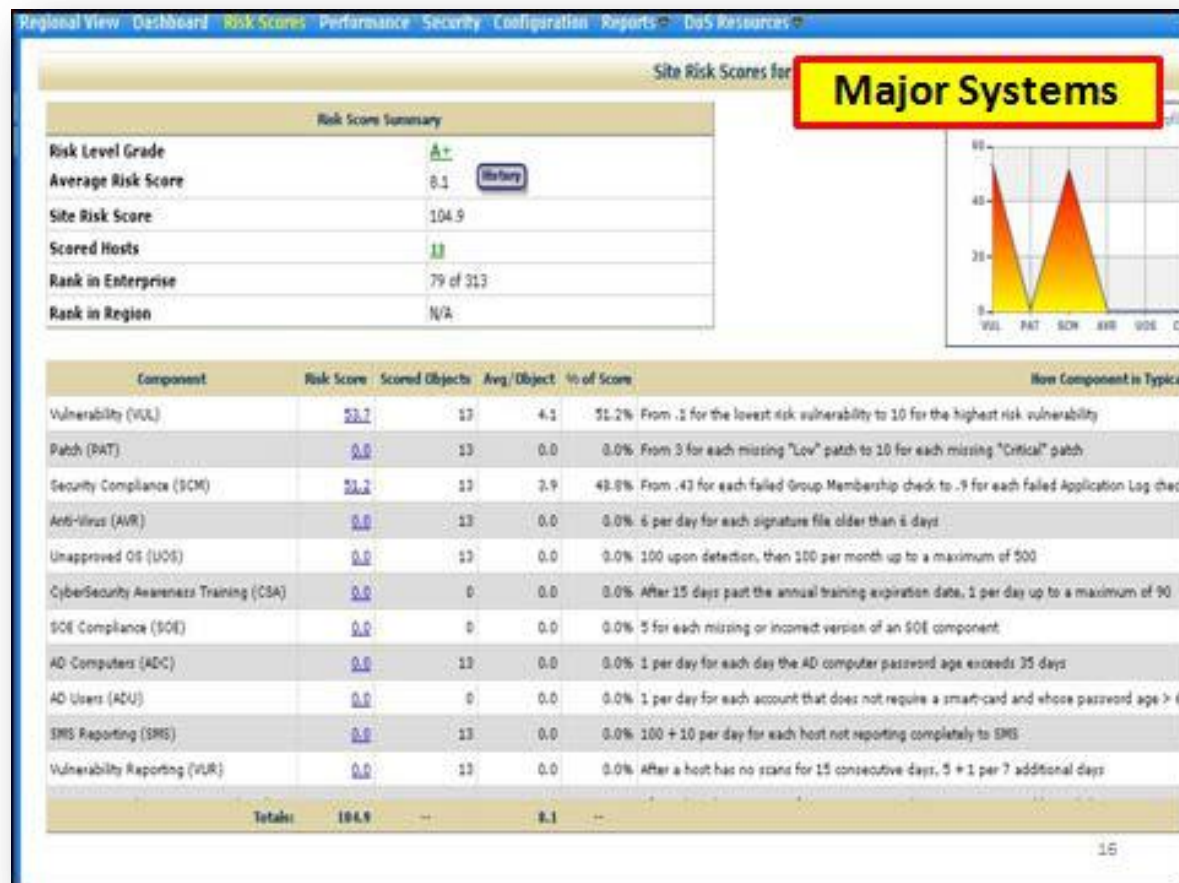


Как пытаются построить такую систему в мире?



Система визуализации уровня ИБ в Госдепартаменте США

- Сканирование каждые 36-72 часа
- Фокус на готовности к атакам
- Ежедневное устранение критичных проблем
- Привязка к ответственности руководителей



100000 узлов

Cisco Security Intelligence Operations

24x7x365
ОПЕРАЦИИ

40+
ЯЗЫКОВ

\$100M+
ТРАТИТСЯ НА ИССЛЕДОВАНИЯ И
РАЗРАБОТКИ

600+
ИНЖЕНЕРОВ И ИССЛЕДОВАТЕЛЕЙ

80+
PH.D.S, CCIE, CISSP, MSCE

0010 010 10010111001 10 100111 010 000100101 110011 01100111010000110000111000111010011101 1100001110001110 1001 1101 1110011 0110011 101000
0010 010 10010111001 10 100111 010 000100101 110011 01100111010000110000111000111010011101 1100001110001110 1001 1101 1110011 0110011 101000

Cisco SIO



Email



Устройства



Web



IPS



Сети



Endpoints

Обзор



Действия



CWS



IPS



AnyConnect



ESA



ASA



WWW

WSA

Контроль

1.6M
ГЛОБАЛЬНЫХ СЕНСОРОВ

35%
МИРОВОГО EMAIL ТРАФИКА

75TB
ДАННЫХ ЕЖЕДНЕВНО

13B
WEB-ЗАПРОСОВ

150M+
УСТАНОВЛЕННЫХ ENDPOINT

От 3 до 5
МИНУТ ИНТЕРВАЛ МЕЖДУ
ОБНОВЛЕНИЯМИ

5,500+
IPS СИГНАТУР ВЫПУЩЕНО

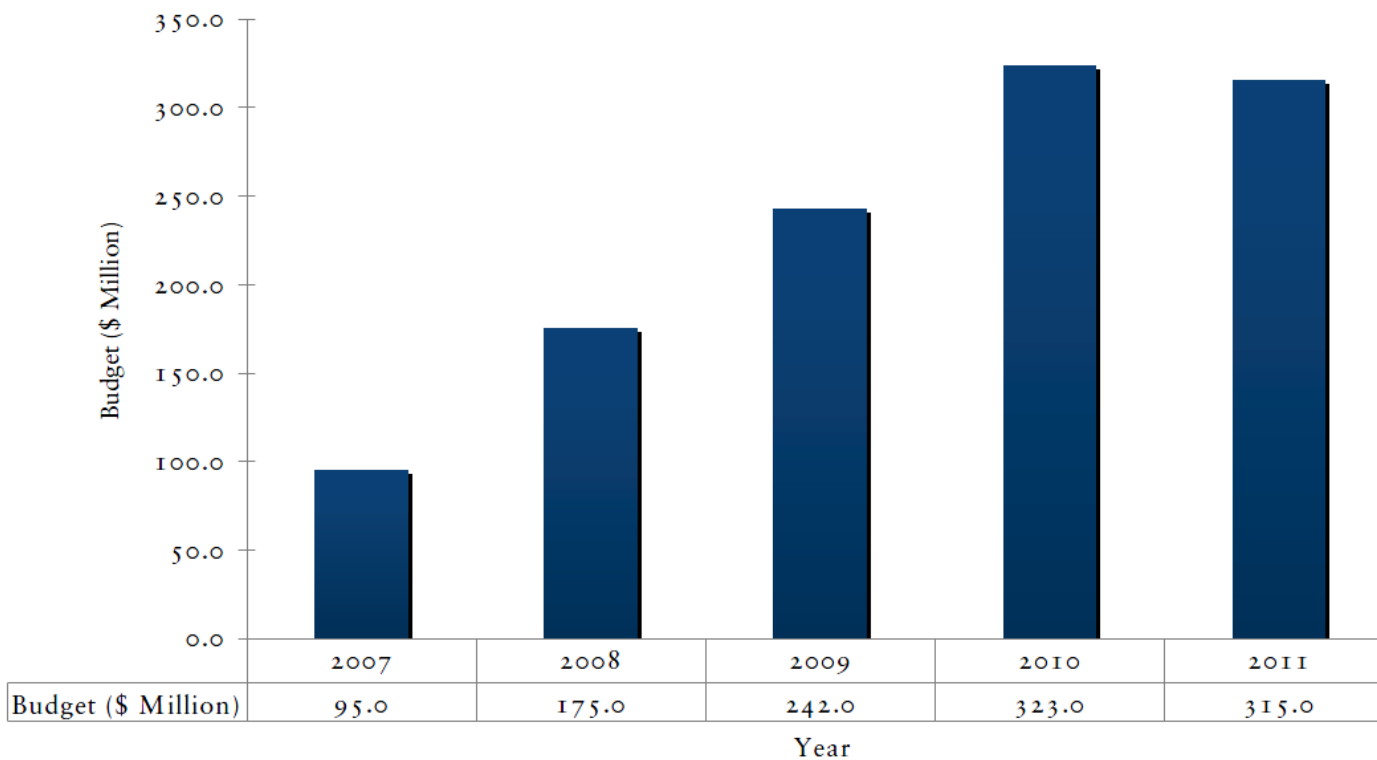
8M+
ПРАВИЛ В ДЕНЬ

200+
ПАРАМЕТРОВ ОТСЛЕЖИВАЕТСЯ

70+
ПУБЛИКАЦИЙ ВЫПУЩЕНО

Сколько это может стоить?

Финансирование US-CERT, 2007-2011



security-request@cisco.com

Благодарю вас
за внимание

