InfoSafe

CISCO MARS

Реализация требований стандартов в области управления ИБ BS ISO/IEC 27001 и BS25999

Сергей Логинов | Руководитель отдела внедрения
sergey.loginov@infosafe.ua

InfoSafe

Стандарты ИБ

BS25999 и ISO/IEC 27001

25.11.2008

InfoSafe

Стандарты в области управления

На сегодняшний день существует группа стандартов, направленных на управление различными процессами.

Это:

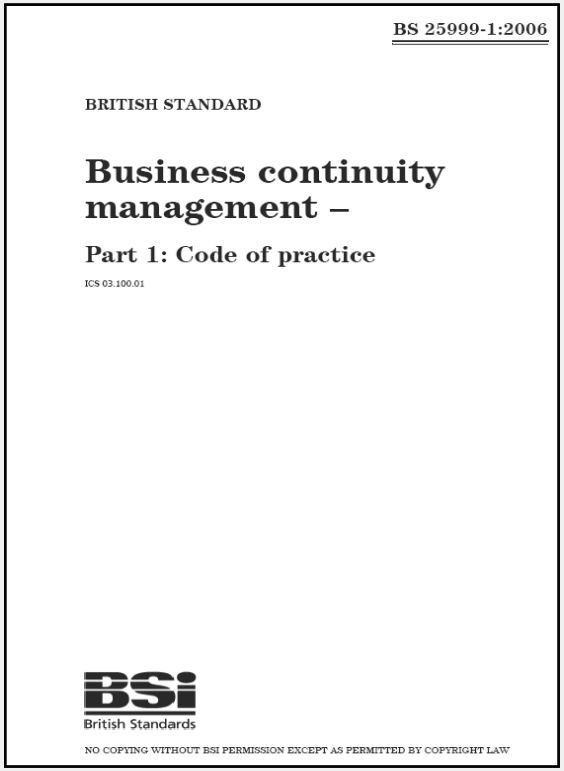
ISO/IEC 9001 – управление качеством;
ISO/IEC 27001 – управление информационной безопасностью;
ISO/IEC 20000 – управление IT инфраструктурой;
ISO/IEC 14000 – экологический менеджмент;
ISO/IEC 18000 – управление безопасностью труда;
BS25999 – управление непрерывностью бизнеса (BCM).

Стандарт **BS25999** является наиболее новым из этой группы стандартов.

Состав стандарта

Состоит из 2 частей:

- **BS25999-1:2006 – набора практик;**
- **BS25999-2:2007 – спецификации.**


BS 25999-1:2006

BRITISH STANDARD

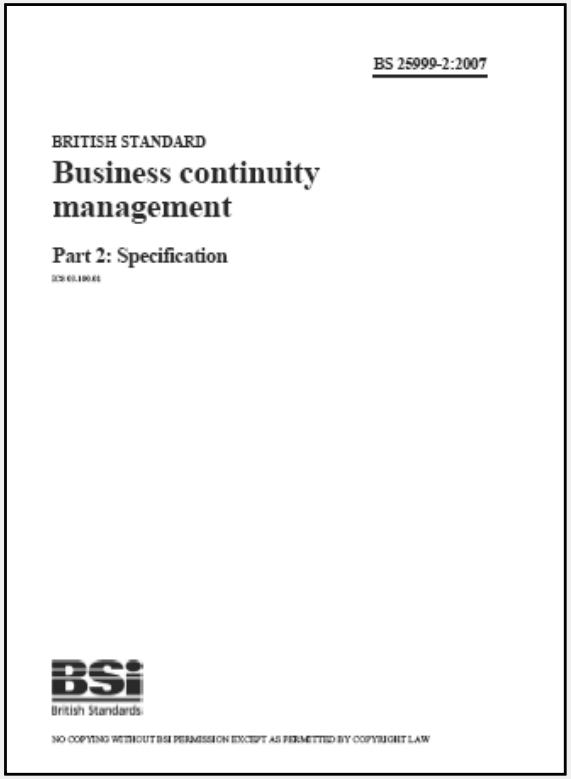
Business continuity management –

Part 1: Code of practice

ICS 03.100.01

BSI British Standards

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW


BS 25999-2:2007

BRITISH STANDARD

Business continuity management

Part 2: Specification

BSI British Standards

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Основные определение BCM

Business Continuity Management (BCM, управление непрерывностью бизнеса, согласно п.2.4 BS 25999-2:2007)

- это целостный процесс управления, который идентифицирует потенциальные угрозы организации и воздействия на бизнес процессы в случае реализации данных угроз, обеспечивает построение организационной основы для обеспечения способности организации к эффективному противодействию инцидентам, защите ключевых активов, скорейшему восстановлению основной деятельности организации удовлетворению требованиям заинтересованных сторон.

Информационная безопасность (ИБ, согласно п.3.4 ISO/IEC 27001:2005)

– это обеспечение конфиденциальности, целостности и доступности (КЦД) информации.Так же могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотказуемость и надежность.

Система управления информационной безопасностью (СУИБ, согласно п.3.7 ISO/IEC 27001:2005)

– это та часть системы управления, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Ключевые компоненты системы управления

Компоненты системы управления непрерывностью и безопасностью бизнеса:

- Политика
- Планирование
- Внедрение и поддержание
- Тестирование
- Одобрение
- Оценка руководством

Действие стандарта **ISO/IEC 27001** направленно на анализ рисков (операционный уровень), а действие **BS25999** направленно на анализ рисков (операционный уровень) и анализ бизнес инцидентов (бизнес уровень).

InfoSafe

Преимущества системы, построенной на основе международных стандартов

- Способность к проактивной оценке воздействия на бизнес в случае выхода из строя ключевых систем;
- Однозначная и эффективная реакция на инцидент, минимизирующая воздействие на основную деятельность организации, в том числе и ее **контроль**;
- Способность **контролировать** и **управлять** неструктурированными рисками;
- Развитие навыков команды ликвидации последствий инцидентов;
- Повышение репутации и получение конкурентного преимущества через демонстрацию способности защиты и контроля собственных сервисов;
- Способность продемонстрировать профессиональные действия, адекватную реакцию на инцидент, через разработанные и внедрённые процессы BCM.

InfoSafe

Cisco MARS

25.11.2008

Что такое MARS?

Cisco Monitoring, Analysis and Response System

• Сбор данных от разнородных сетевых устройств и в разных форматах:

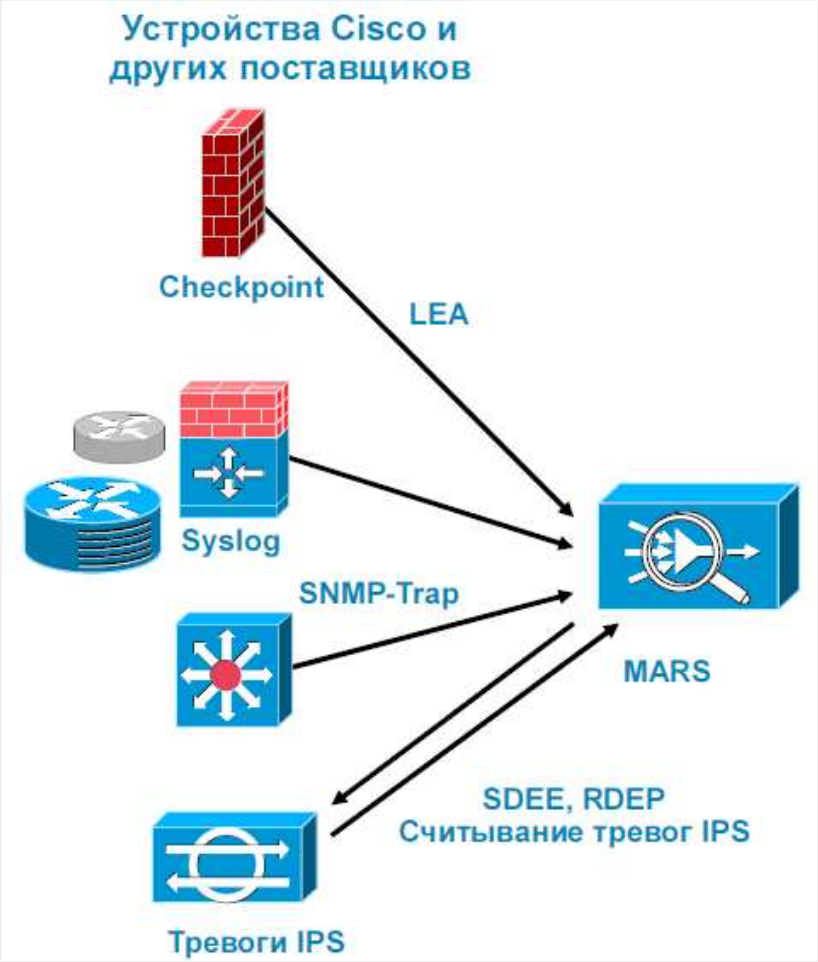
NIDS, МСЭ, маршрутизаторы, CSA;

Syslog, SNMP, RDEP, SDEE, NetFlow, XML API, системные логи;

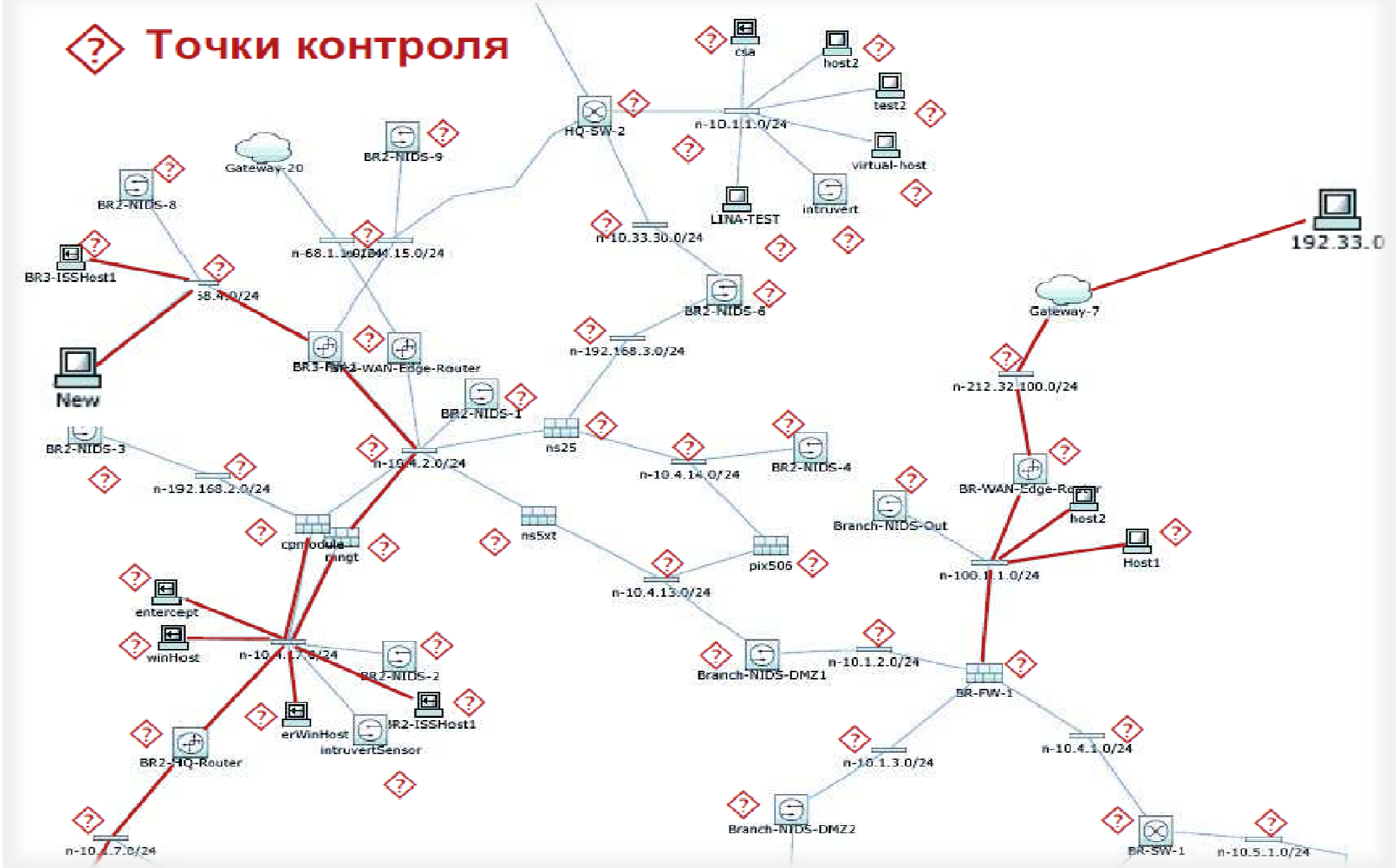
• Анализ и корреляция событий;

• Локализация и отражение атак;

• Визуализация инцидентов и их отображение на карте сети.

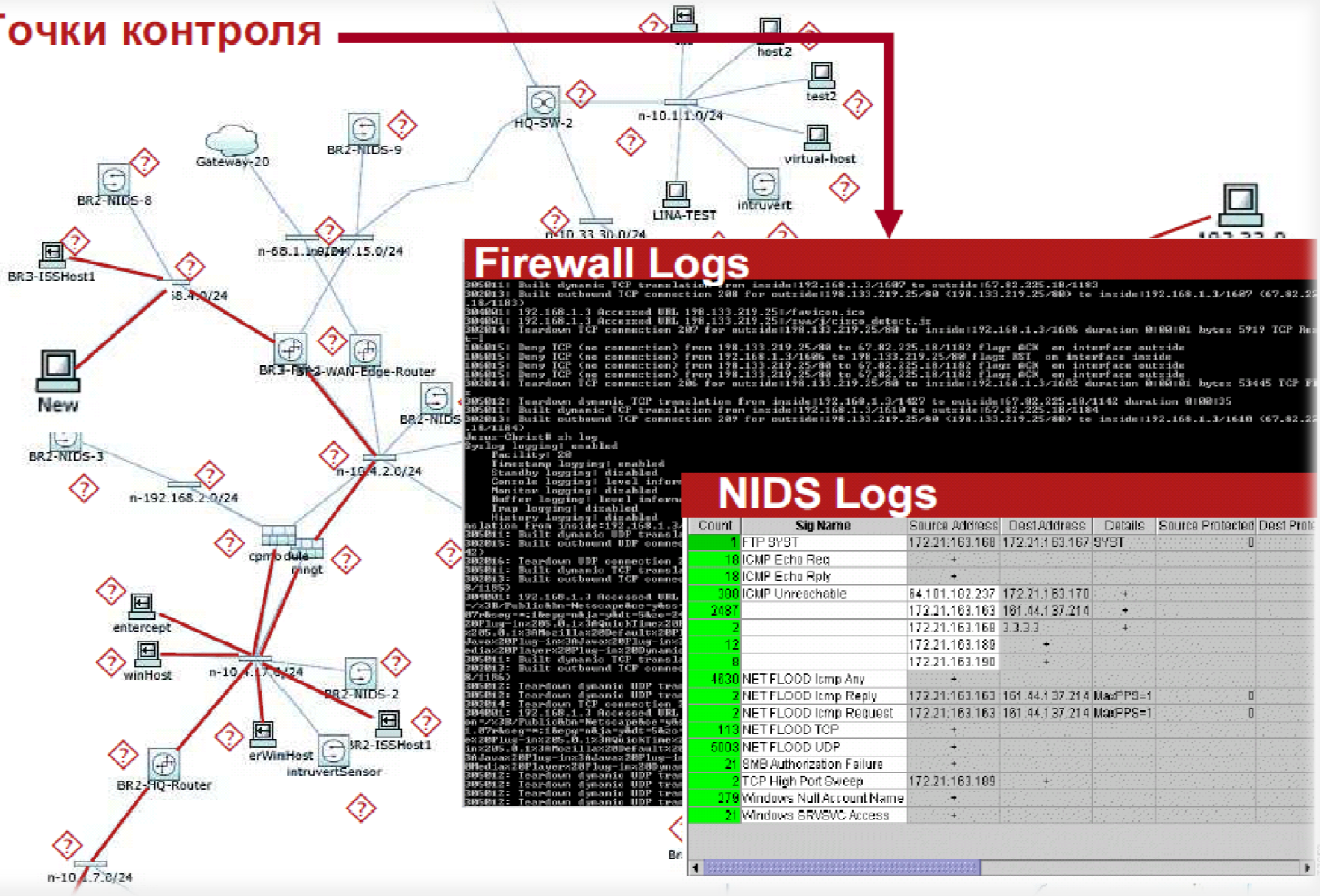


Визуализация сети



Сбор логов с разных журналов

Точки контроля



Firewall Logs

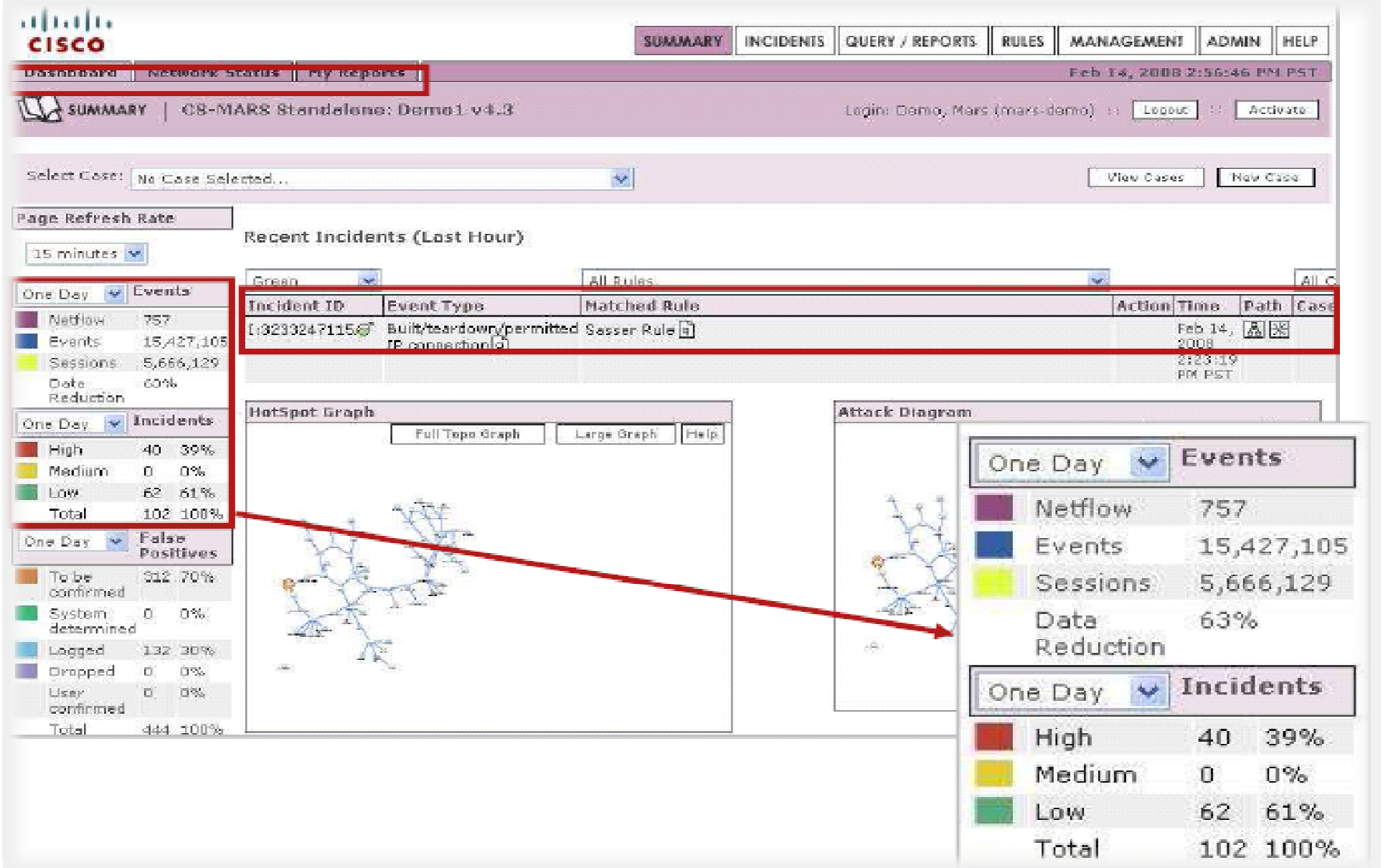
```
%SEC-6-IPACCESSLOGP: list outside_cryptomap_dyn_20 denied tcp 198.133.219.25(80) -> inside:192.168.1.3(1607), 1 packet
%ASA-6-302013: Built outbound TCP connection 288 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1607 (67.82.225.18/1183)
%ASA-6-302014: Teardown TCP connection 207 for outside:198.133.219.25/80 to inside:192.168.1.3/1606 duration 0:00:01 bytes 5919 TCP FINs
%ASA-6-106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK on interface outside
%ASA-6-106015: Deny TCP (no connection) from 192.168.1.3/1606 to 198.133.219.25/80 flags RST on interface inside
%ASA-6-106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK on interface outside
%ASA-6-106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK on interface outside
%ASA-6-302014: Teardown TCP connection 206 for outside:198.133.219.25/80 to inside:192.168.1.3/1602 duration 0:00:01 bytes 53445 TCP FINs
%ASA-6-302012: Teardown dynamic TCP translation from inside:192.168.1.3/1602 to outside:67.82.225.18/1142 duration 0:00:35
%ASA-6-302013: Built outbound TCP connection 207 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1610 (67.82.225.18/1184)
Jesus-Christ# sh log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: level inform
    Monitor logging: disabled
    Buffer logging: level informa
    Trap logging: disabled
    History logging: disabled
```

NIDS Logs

Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prot
1	FTP SYST	172.21.163.168	172.21.163.167	SYST	0	
18	ICMP Echo Req	172.21.163.163	161.44.137.214			
18	ICMP Echo Rply	161.44.137.214	172.21.163.163			
300	ICMP Unreachable	84.101.102.237	172.21.163.170			
2487		172.21.163.163	161.44.137.214			
2		172.21.163.168	3.3.3.3			
12		172.21.163.189	161.44.137.214			
8		172.21.163.190	161.44.137.214			
4630	NET FLOOD Icmp Any	172.21.163.163	161.44.137.214			
2	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
2	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
113	NET FLOOD TCP	172.21.163.163	161.44.137.214			
5003	NET FLOOD UDP	172.21.163.163	161.44.137.214			
21	SMB Authorization Failure	172.21.163.163	161.44.137.214			
2	TCP High Port Sweep	172.21.163.169	161.44.137.214			
279	Windows Null Account Name	172.21.163.163	161.44.137.214			
21	Windows SRVSVC Access	172.21.163.163	161.44.137.214			

InfoSafe

Анализ и корреляция событий



Визуализация инцидентов на карте сети

Жертва/зараженный хост

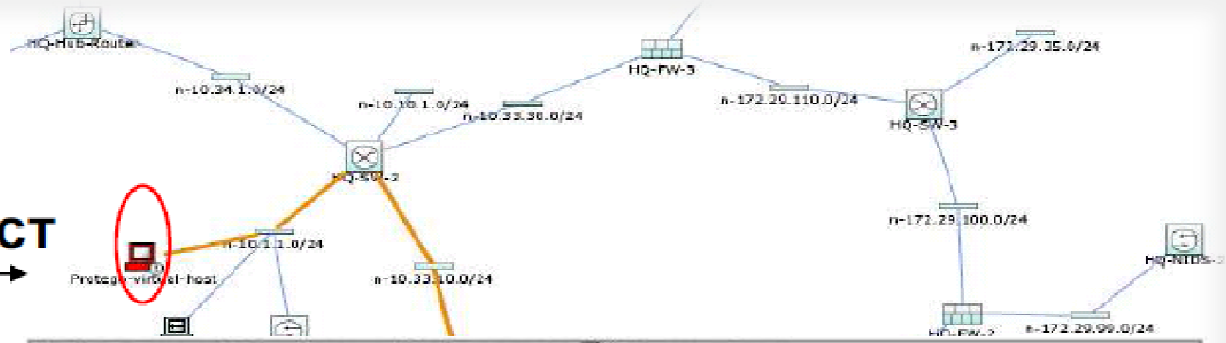
(красный)

Взломанный хост, участвующий в атаке

(сиреневый)

Источник атаки

(коричневый)



Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Cancel

- Четкое представление пути атаки на 2 и 3 уровнях
- Обнаружение устройств для отражения атаки

InfoSafe

Cisco MARS
и
стандарты ИБ

25.11.2008

Соответствие стандарту BS ISO/IEC 27001:2005

Приложение А (нормативное) – Цели и механизмы контроля

Таблица А.1 - Цели и механизмы контроля

Пункт А.10.6 – Управление сетевой безопасностью

Цель: Обеспечить сохранность информации в сетях, а так же защиту поддерживающей инфраструктуры.

Пункт А.10.10 – Мониторинг

Цель: Обнаружение несанкционированных действий по обработке информации.

Пункт А.13 – Управление инцидентами информационной безопасности (ИБ)

Пункт А.13.1. *Цель: Гарантировать, что информация о событиях ИБ и слабостях, связанных с информационными системами, доводится до сведения уполномоченных лиц в порядке, позволяющем вовремя предпринимать корректирующие действия.*

Пункт А.13.2. *Цель: Обеспечить использование последовательного и эффективного подхода к управлению инцидентами ИБ.*

Пункт А.14.1 – Аспекты управления непрерывностью бизнеса, связанные с информационной безопасностью

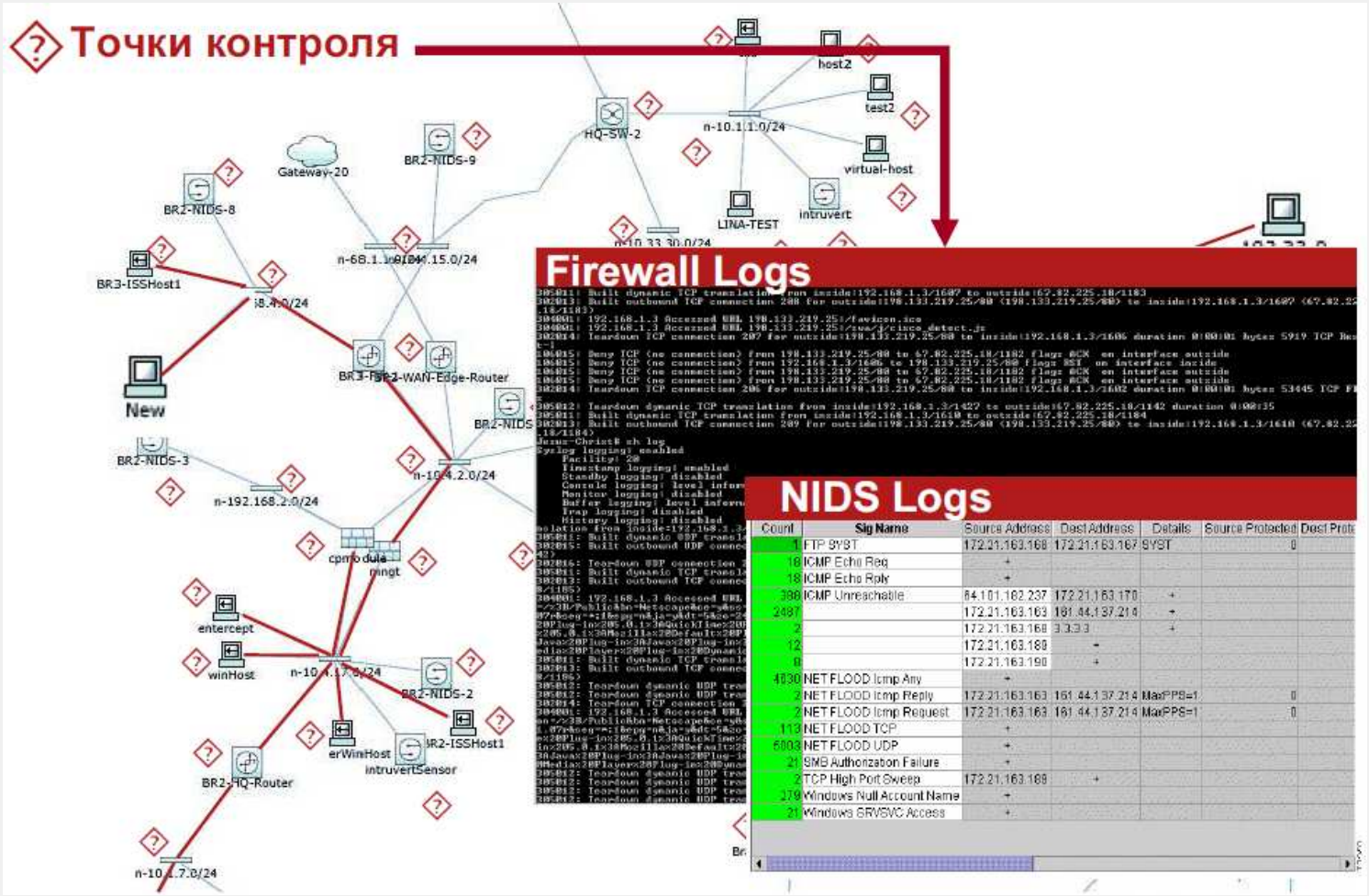
Цель: Препятствовать прерываниям хозяйственной деятельности и защищать критически важные бизнес-процессы от влияния крупных сбоев информационных систем или аварий и обеспечить их своевременное возобновление.

A.10.6.1 – Сетевые механизмы контроля

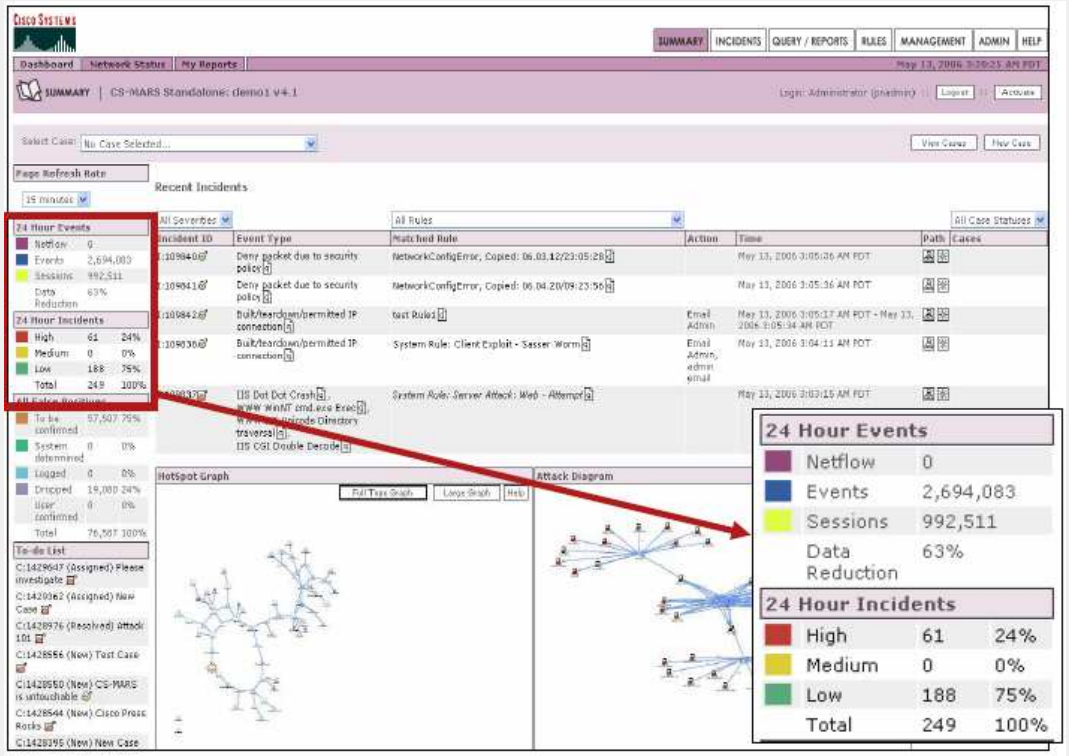
Должны быть обеспечены адекватное управление и контроль сети для защиты от угроз и обеспечения безопасности систем и приложений при использовании сети, включая передаваемую информацию.

A.10.10 – Мониторинг

A.10.10.1 – Регистрация событий аудита
A.10.10.2 – Мониторинг использования системы
A.10.10.3 – Защита журналов аудита ?
A.10.10.4 – Журналы администратора и оператора
A.10.10.5 – Протоколирование сбоев
A.10.10.6 – Синхронизация часов ?



A.13 – Управление инцидентами информационной безопасности



2 694 083 событий

↓

992 511 сеансов

↓

249 инцидентов

↓

61 серьезный инцидент

ЭФФЕКТИВНАЯ СИСТЕМА

ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ ИНЦИДЕНТОВ ИБ

InfoSafe

Пример инцидента – червь Sasser-D (сигнатуры отсутствуют)

hed Rule: System Rule: Sudden Traffic Increase To Port
ription: This rule detects scans statistically significant increase in traffic to a particular port.

pen (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
	ANY	ANY	ANY	System Rule: Sudden Traffic Increase To Port	ANY	ANY	1				0hh:10mm:0ss

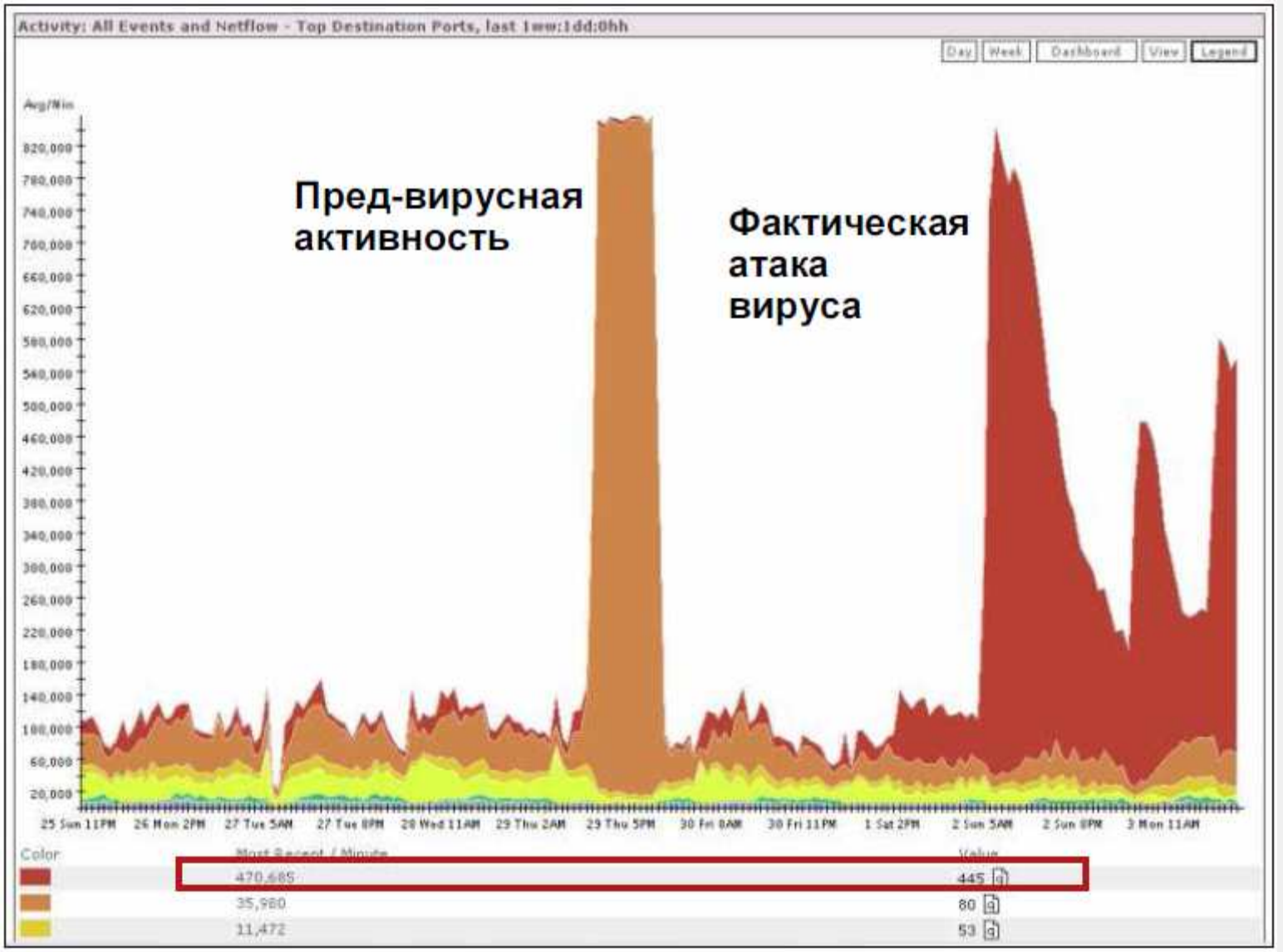
473601390

Escalate | Expand All | Collapse All

/ ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Device	Graph	False Positive	Mitigati
0316, 1390	Sudden increase of traffic to a port	0.0.0.0		0.0.0.0	445	IP	May 3, 2004 6:00:03 AM EDT				Tune	Mitigate
	AAA authorization denied due to no prior authentication	Total: 25										
	AAA authorization denied due to no prior authentication	[redacted]120		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].142		Total: 2								
6544, 1390	AAA authorization denied due to no prior authentication	[redacted].85	4049	[redacted]128	445	N/A	May 3, 2004 5:40:05 AM EDT		[redacted]2		Tune	Mitigate
	AAA authorization denied due to no prior authentication	[redacted].104		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].205		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted].132		Total: 2								
	AAA authorization denied due to no prior authentication	[redacted].174		Total: 3								
	AAA authorization denied due to no prior authentication	[redacted].89		Total: 6								
	AAA authorization denied due to no prior authentication	[redacted].95		Total: 3								
6538, 1390	Built/teardown/permitted IP connection	[redacted]70	2503	[redacted]2.164	445	TCP	May 3, 2004 5:40:05 AM EDT - May 3, 2004 5:42:07 AM EDT		[redacted]1		Tune	Mitigate
	Denied packet - no translation group	Total: 4										
6547, 1390	Denied packet - no translation group	[redacted].85	4050	[redacted]80.35	445	TCP	May 3, 2004 5:40:05 AM EDT		[redacted]2		Tune	Mitigate

InfoSafe

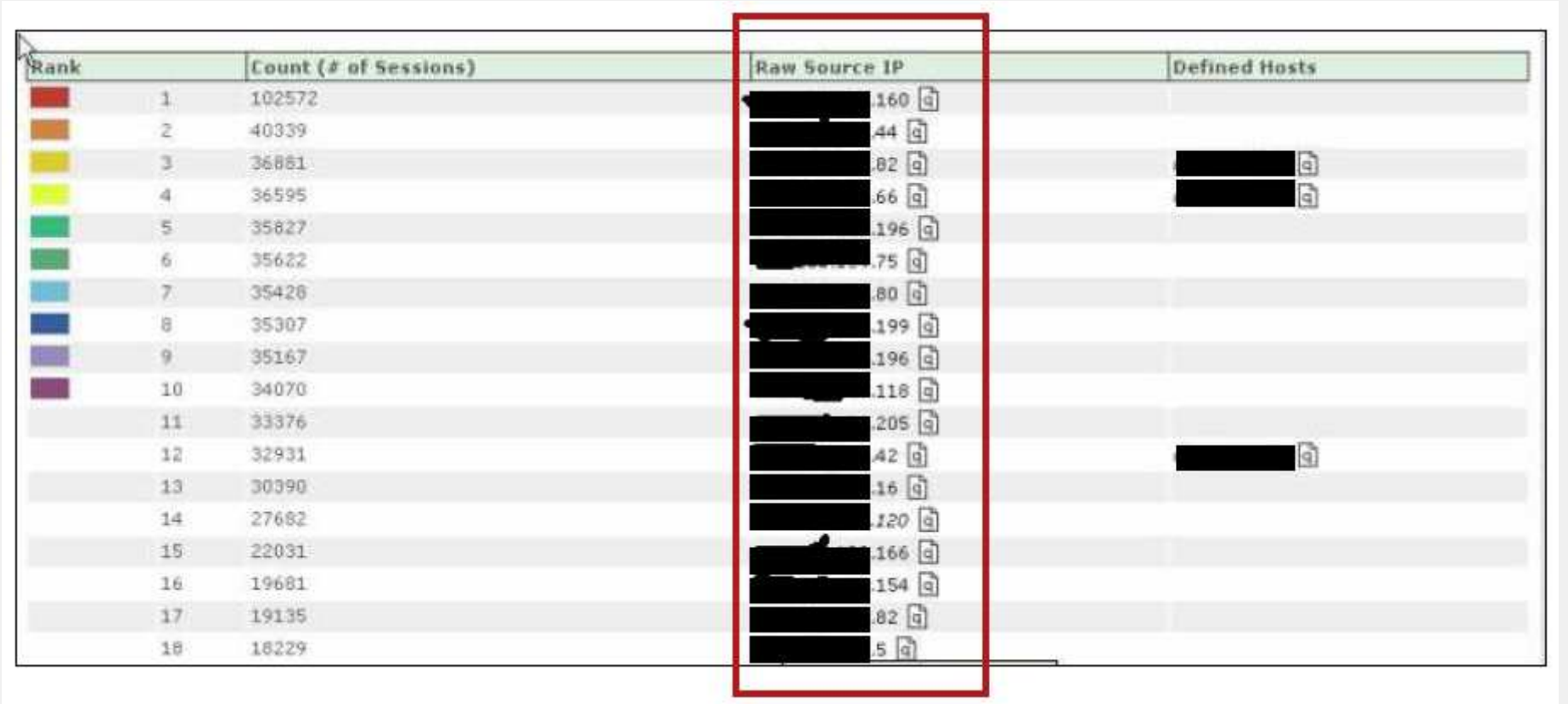
График активности вируса



InfoSafe

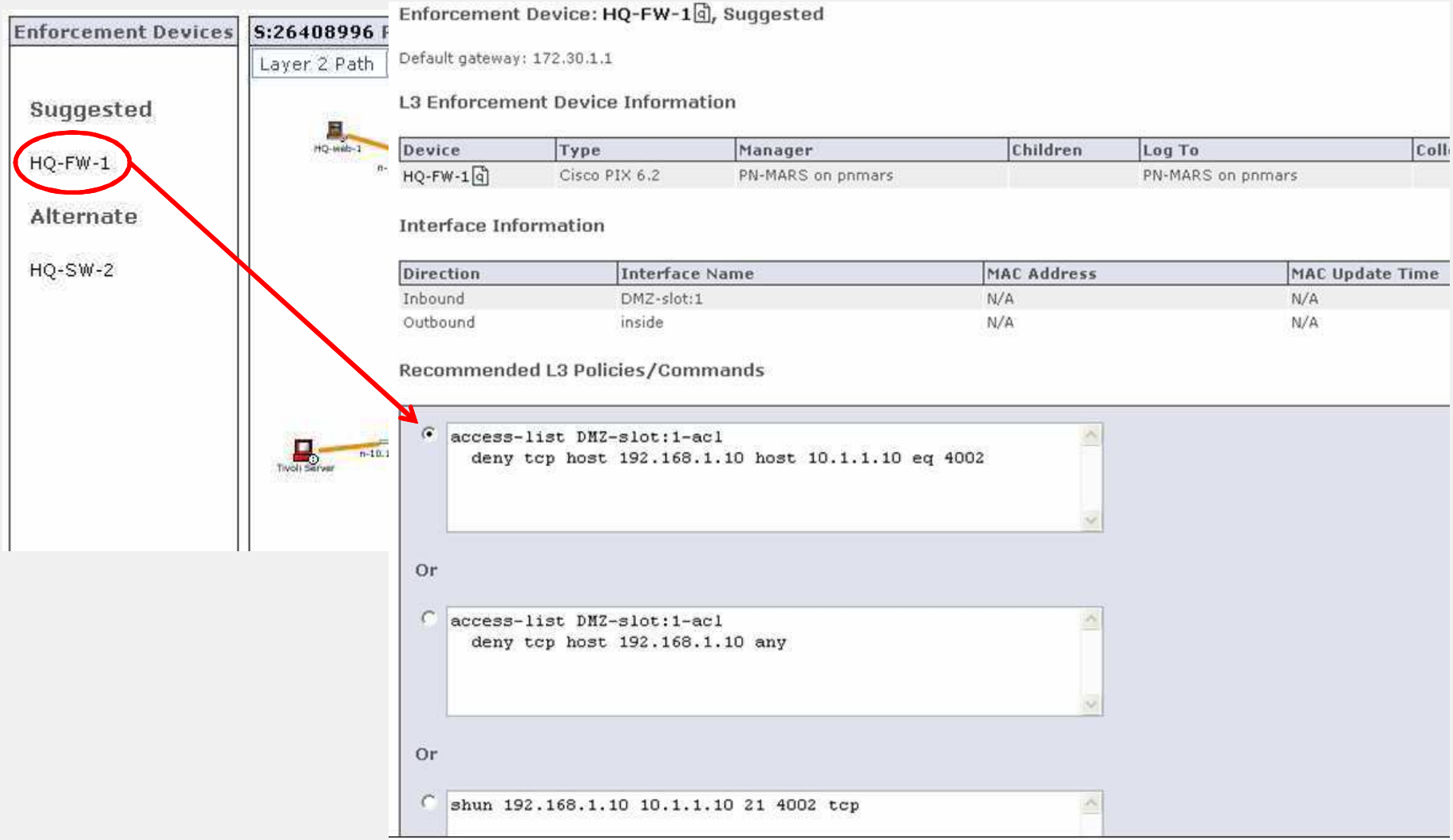
Зараженные компьютеры

Покажите мне кто генерирует траффик по порту 445?



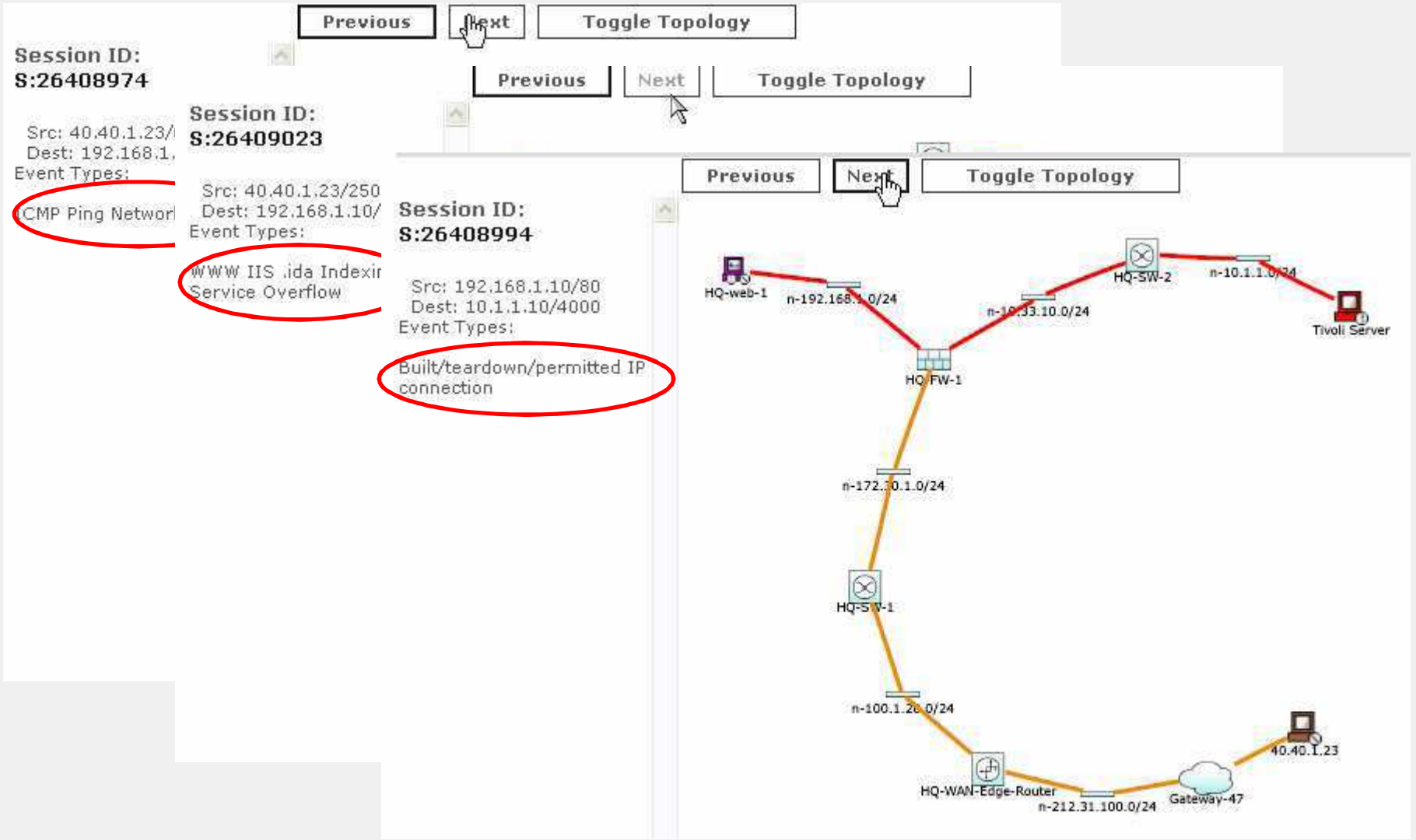
Rank	Count (# of Sessions)	Raw Source IP	Defined Hosts
1	102572	[redacted].160	
2	40339	[redacted].44	
3	36881	[redacted].82	[redacted]
4	36595	[redacted].66	[redacted]
5	35827	[redacted].196	
6	35622	[redacted].75	
7	35426	[redacted].80	
8	35307	[redacted].199	
9	35167	[redacted].196	
10	34070	[redacted].118	
11	33376	[redacted].205	
12	32931	[redacted].42	[redacted]
13	30390	[redacted].16	
14	27682	[redacted].120	
15	22031	[redacted].166	
16	19681	[redacted].154	
17	19135	[redacted].82	
18	18229	[redacted].5	

Автоматическая реконфигурация сетевого оборудования L2/L3



Расследование инцидента

В рамках инцидента можно отследить последовательность сеансов:



A.14.1 – Аспекты управления непрерывностью бизнеса, связанные с информационной безопасностью

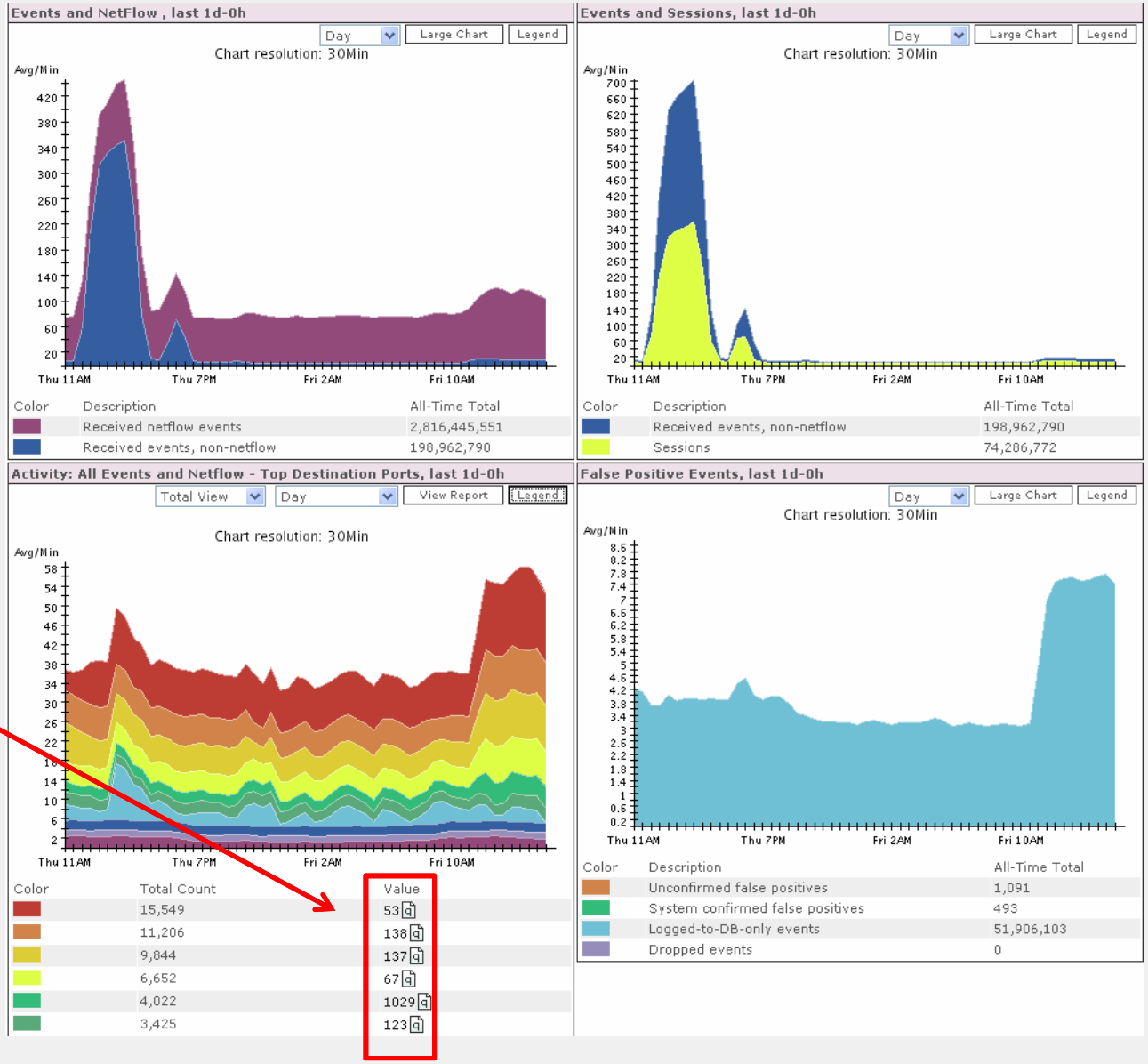
Обнаружение аномалий:

- События / NetFlow;
- События / сеансы;
- Ложные срабатывания;

и лучшее место поиска аномалий:

- основные целевые порты

Настроенные оповещения сообщат по e-mail или sms о резком всплеске активности, появлении появлении аномалий или инциндентов.

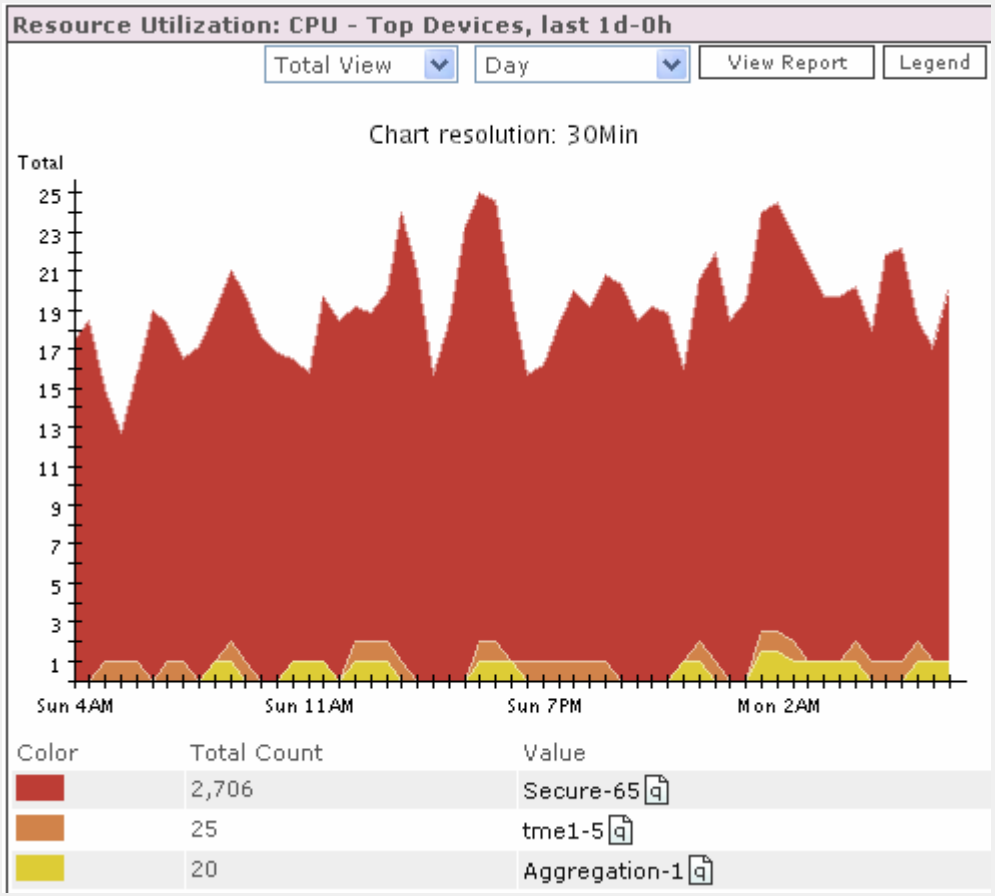


Атаки на средства защиты (Cisco IOS, PIX, ASA)

Доступна информация:

1. Загрузка процессора
2. Загрузка памяти
3. Количество соединений
4. IO kbps

и др.



Глава 7– Анализ СУИБ руководством

Руководство должно анализировать СУИБ организации через запланированные интервалы времени, чтоб убедиться в ее постоянной пригодности, адекватности и эффективности.

Бльше 100 встроенных отчетов

Настраиваемые пользовательские отчеты

Инциденты

TOP 10 атак

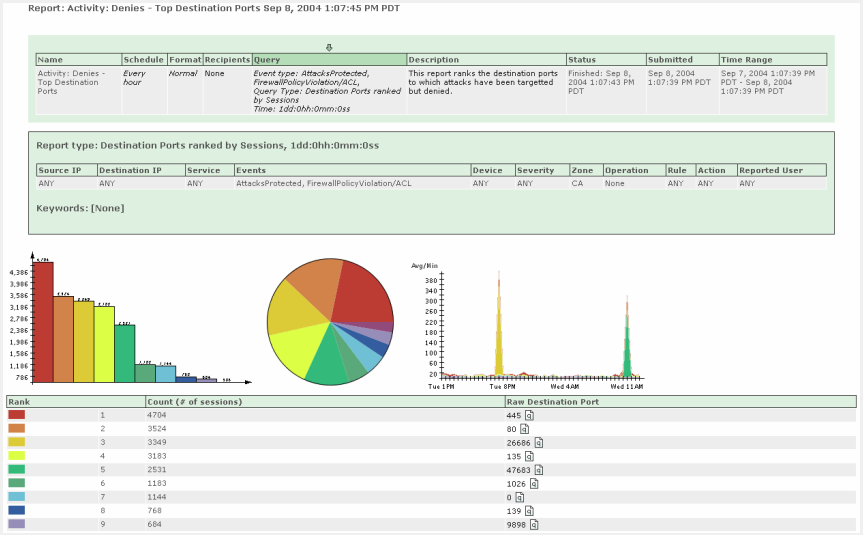
TOP 10 атакуемых устройств

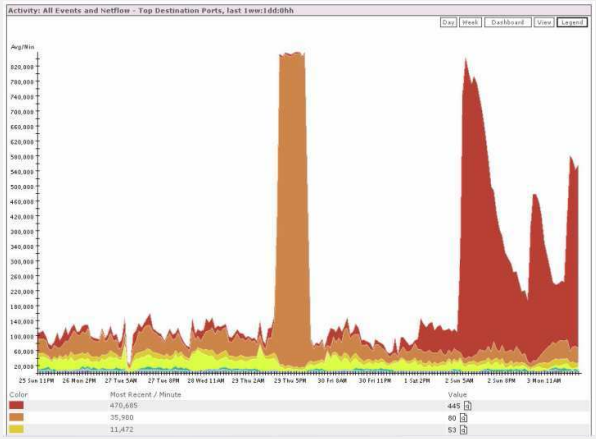
TOP 10 хакеров

Экспорт отчетов в CSV и HTML

Фильтрация по:

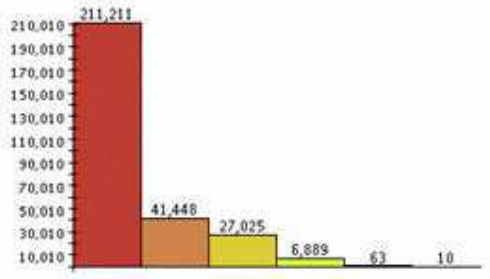
зонам, времени, адресам, портам, событиям, устройствам.



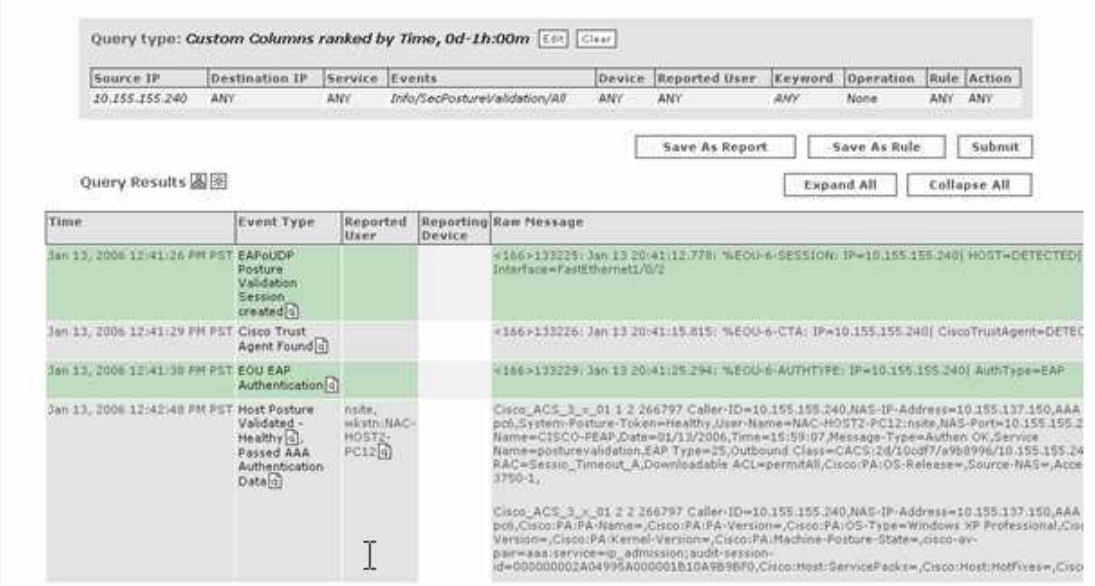


Отчеты

От отчетов высокого уровня для быстрого чтения и простого анализа...



Rank	Count (# of Sessions)	Raw Destination IP	Defined Hosts
1	211211	10.177.10.21	NAC-7200-1
2	41448	10.155.165.150	nac-6500-1
3	27025	10.155.137.150	nac-3750-1
4	6889	10.155.145.150	NAC-4500-1.nsitenac.com
5	63	10.177.10.25	
6	10	10.155.235.150	

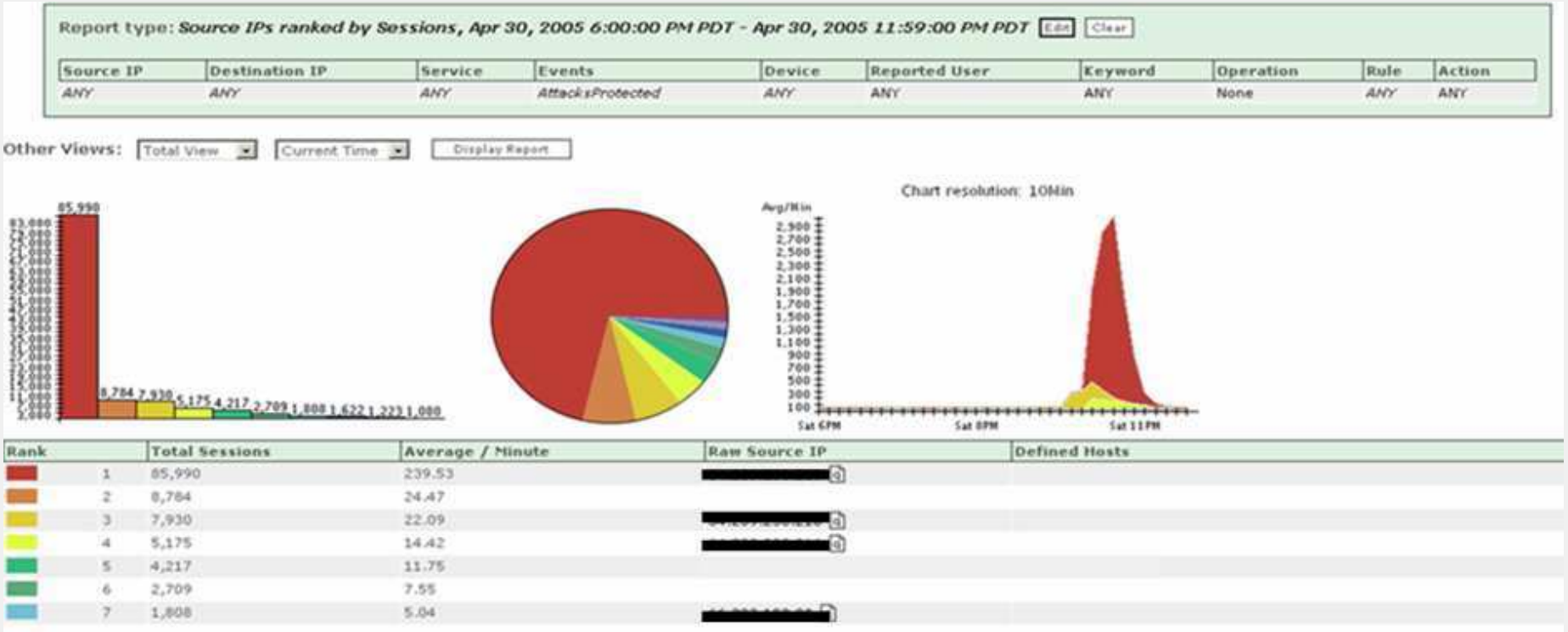


... до деталей конкретного исходного сообщения, полученного консолью.

Пользовательские отчеты

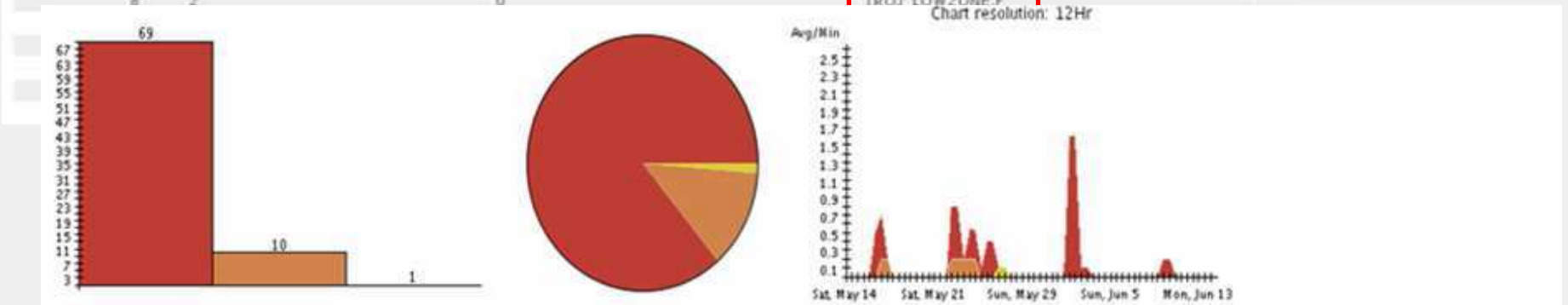
Я плачу за то, чтобы сканировали мою сеть и мои компьютеры.
Покажите мне что это действительно делается.

Настраиваемый отчет:



Отчеты о вирусах в сети

Rank		Total Sessions	Average / Minute	Name	Wor
	1	19	0	JAVA_BYTEVER.A	
	2	9	0	TROJ_STERVIS.C	
	3	7	0	TROJ_BUDDY.F	
	4	6	0	TROJ_DYFUCA.DE	
	5	4	0	TROJ_DLOADER.FN	
	5	4	0	TROJ_AGENT.QJ	
	5	4	0	TROJ_AGENT.RV	
	8	2	0	HTML_REDIR.A	
	8	2	0	TROJ_AGENT.KR	
	8	2	0	BKDR_SANDBOX.A	
	8	2	0	TROJ_LOWZONE.F	



Rank	Total Sessions	Average / Minute	Event ID	Description	CVE Name	Severity	Device Event ID	Gro
1	69	0	Virus Alert virus deleted	Virus Alert virus deleted			Trend Micro Office Scan 6.5: Trend Micro Virus Alert virus deleted	
2	10	0	Virus Alert virus not cleaned	Virus Alert virus not cleaned			Trend Micro Office Scan 6.5: Trend Micro Virus Alert not cleaned	
3	1	0	Virus Alert virus cleaned	Virus Alert virus cleaned			Trend Micro Office Scan 6.5: Trend Micro Virus Alert virus cleaned	

Соответствие стандарту BS ISO/IEC 27001:2005

Приложение А, Таблица А.1 - Цели и механизмы контроля.

Пункт А.10.1.3 – Разделение обязанностей

Обязанности и области ответсвенности должны быть разделены с целью снижения возможностей несанкционированного изменения или злоупотребления ресурсами организации.

Пункт А.10.2 – Управление сервисами, предоставляемыми третьей стороной

Цель: Реализация и поддержание необходимого уровня ИБ и предоставления сервиса в соответствии с соглашениями о предоставлении сервисов, заключаемыми с третьей стороной.

Пункт А.6.2 – Внешние стороны

Цель: Обеспечить безопасность информации организации и средств ее обработки , доступ, обработка, передача или управление которыми осуществляется третьими сторонами.

Пункт А.10.4 – Защита от вредоносного мобильного кода

Цель: Обеспечить целостность информации и программного обеспечения.

Пункт А.16.6 – Управление техническими уязвимостями

Цель: Уменьшение рисков, связанных с использованием опубликованных технических уязвимостей.

InfoSafe

Спасибо за внимание!

Сергей Логинов | Руководитель отдела внедрения
sergey.loginov@infosafe.ua