

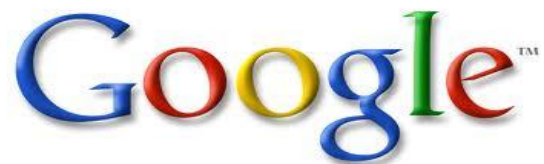


Cisco Sourcefire

Sandro Chachanidze



Обратите внимание на них...



***Все были умными. У всех была безопасность.
И всех их серьезно взломали.***

Так что же изменилось?

Хакерство изменилось.

Хакинг, 21st век

Цепочка атаки

Обследование

Обследование
защиты жертвы

Разработка

Написание специализированного софта для конкретных
условий жертвы

Тестирование

Проверяем и убеждаемся что Malware
обходит защиту жертвы

Запуск

Размещение Malware. Распространение
внутри, установление связей наружу

Завершение

Миссия: Извлечение данных,
сбор доказательств,
компрометация.

Что бы вы изменили, зная что Вас взломают?



IPS Нового Поколения!



Что делает SourceFire NGFW уникальным?

- Контекст
- Скорость
- Точность
- Гибкость
- Значимость

Figure 1. Magic Quadrant for Intrusion Prevention Systems



Каким образом SourceFire обеспечивает непревзойденную безопасность

УПРАВЛЕНИЕ

fireSIGHT™

Центр управления



fireCLOUD™

ДЕТЕКТИРОВАНИЕ И БЛОКИРОВКА

firePOWER™

NGIPS | NGFW
IPSx | Virtual | SSL



fireAMP™

Advanced Malware Protection



COLLECTIVE
SECURITY
INTELLIGENCE

Лучшие технологии для полноценной защиты

Устройства FirePOWER™

Все устройства имеют:

- Интегрированную светодиодную индикацию
- Технологии Акселерации SourceFire
- LCD дисплей

SSL8200



SSL2000

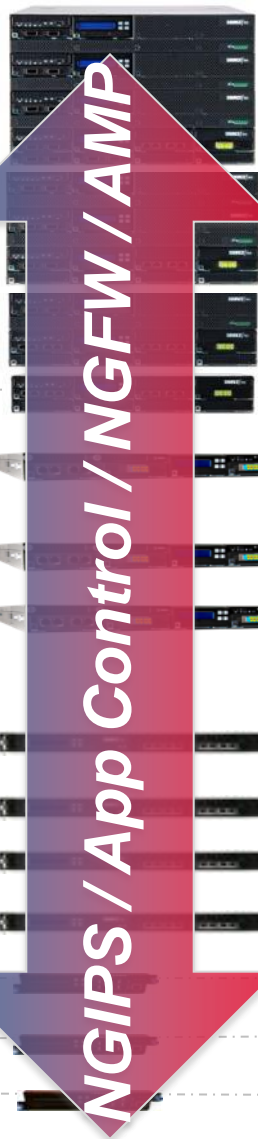


SSL1500



IPS Производительность

- 40 Gbps
- 30 Gbps
- 20 Gbps
- 10 Gbps
- 6 Gbps
- 4 Gbps
- 2 Gbps
- 1.5 Gbps
- 1.25 Gbps
- 1 Gbps
- 750 Mbps
- 500 Mbps
- 250 Mbps
- 100 Mbps
- 50 Mbps



firePOWER™

- 8290
- 8270
- 8260
- 8250
- 8140
- 8130
- 8120
- 7125
- 7120
- 7115
- 7110
- 7030
- 7020
- 7010

Фиксированные порты

Модульные порты

Стекирование

Микс / SFP

SourceFire

FirePower (NGIPS) - Архитектура решения



Архитектура развертывания

Система Sourcefire предлагает защиту от сложных (ATP) угроз, контроля доступа и приложений и фаервола. Эти функции могут быть развернуты в различных видах архитектур:

- **Single interface** конфигурация позволяет использовать устройство как inline IPS. Данный режим можно использовать совместно с коммутаторами, использующими Spanning Tree Protocol (STP).
 - **Routed** - Маршрутизируемые интерфейсы, роутинг (Static/OSPF/RIP)
 - **Switched** - Layer2 Группы портов, проброс Trunk. Использование/Отключение STP
 - **Passive** - Возможность анализа зеркальной копии трафика
- **Clustered high availability (HA)** обмен статусом позволяет устройствам или стекам в кластере синхронизировать статусы. Если любое устройство отказывает, сосед принимает работу без потери потока трафика.
- **Stacking** комбинирует два или более устройства используя сетевую конфигурацию на одном основном устройстве и CPU и RAM на остальных устройствах стека.

Системная политика

Policy Name: Initial_System_Policy 2014-01-17 10:45:35

Policy Name: Initial_System_Policy 2014-01-17 10:45:35

Policy Description: Initial System Policy

- Access Control Preferences
- Access List
- Audit Log Settings
- Authentication Profiles
- Dashboard
- Database
- DNS Cache
- Email Notification
- Intrusion Policy Preferences
- Language
- Login Banner
- SNMP
- ▶ Time Synchronization**
- User Interface
- Vulnerability Mapping

Supported Platforms: Defense Center

Serve Time via NTP: Enabled

Set My Clock: Manually in Local Configuration, Via NTP from 0.sourcefire.pool.ntp.org, 1.sourcef

Supported Platforms: Managed Device

Set My Clock: Manually in Local Configuration, Via NTP from Defense Center, Via NTP from 0.sourcefire.pool.ntp.org, 1.sourcef

Save Policy and Exit | Cancel

Supported Platforms: Defense Center

Maximum Malware Events: 1000000

Системная политика используется для настройки всех аспектов Defence Center, которые должны быть общими на всех устройствах



Мониторинг состояния (Health Monitoring)

Можно использовать SourceFire System's Health Monitor для наблюдения за статусом критически важных функций внутри системы SourceFire. Вы создаете и применяете Health Policy к вашим устройствам, которые наблюдают за важными параметрами функционирования системы, включая статусы Hardware и Software. Health Monitor выбираемые модули в политики запускают серии тестов для определения состояния системы

Health Monitor:

- Политики здоровья для устройства/системы в целом;
- Уведомление по событию для системы/устройства;
- Получение статусной информации о состоянии всех компонент системы;
- Статусный Dashboard (экран статистики) с суммарной информацией по систем;

Мониторинг состояния (Health Monitoring)

The screenshot displays a web interface for health monitoring configuration. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'FireAMP', 'Health', 'System', 'Help', and 'admin'. The 'Health' section is active, showing sub-sections: 'Health Monitor', 'Health Policy', 'Health Events', 'Blacklist', and 'Health Monitor Alerts'. The 'Active Health Alerts' panel shows a list with one entry: 'High CPU'. The 'Configure Health Alerts' panel shows a form for 'High CPU' with a severity dropdown set to 'Critical'. A table lists various modules and their associated alerts. The 'Threshold Timeout (Optional)' is set to 5 minutes.

Active Health Alerts

Name
High CPU

Configure Health Alerts

Health Alert Name: High CPU

Severity	Module	Alert
Critical	Advanced Malware Protection	CPU Alert Health Monitoring (Email)
Warning	Appliance Heartbeat	
Normal	Automatic Application Bypass Status	
Error	CPU Usage	
Recovered	Card Reset	
	Discovery Event Status	
	Disk Status	
	Disk Usage	
	FireAMP Status Monitor	
	FireSIGHT Host License Limit	
	Hardware Alarms	
	Health Monitor Process	
	Intrusion Event Rate	
	License Monitor	
	Link State Propagation	
	Memory Usage	
	Power Supply	
	Process Status	
	RRD Server Process	
	Security Intelligence	

Threshold Timeout (Optional): 5 (in minutes)

Buttons: Load, Delete, Save

Управление объектами























Overview Analysis Policies Devices **Objects** FireAMP

Health System Help admin

Object Management

[+ Add Port](#)







- Network
 - Individual Objects
 - Object Groups
- Security Intelligence
 - Port
 - Individual Objects
 - Object Groups
- VLAN Tag
 - Individual Objects
 - Object Groups
- URL
 - Individual Objects
 - Object Groups
- Application Filters
- File List
- Security Zones

Name	Value	
AOL	TCP (6)/5190	 
Bittorrent	TCP (6)/6881-6889	 
DNS over TCP	TCP (6)/53	 
DNS over UDP	UDP (17)/53	 
FTP	TCP (6)/21	 
HTTPS	TCP (6)/443	 
HTTP	TCP (6)/80	 
IMAP	TCP (6)/143	 
LDAP	TCP (6)/389	 
NFSD-TCP	TCP (6)/2049	 
NFSD-UDP	UDP (17)/2049	 

Security Intelligence

Object Management

Update Feeds Add Security Intelligence Filter

Name	Type	
Global Blacklist	List	 
Global Whitelist	List	 
Sourcefire Intelligence Feed <i>Last Updated: 2014-02-03 21:18:57</i>	Feed	 

- Network
 - Individual Objects
 - Object Groups
- Security Intelligence
- Port
 - Individual Objects
 - Object Groups
- VLAN Tag
 - Individual Objects
 - Object Groups
- URL
 - Individual Objects
 - Object Groups
- Application Filters
- File List
- Security Zones

Security Intelligence

Name:

Type:

Feed URL:

MD5 URL:

Update Frequency:

Save Cancel

Объекты фильтров приложений

Overview Analysis **Policies** Devices Objects FireAMP

Health System Help admin

Access Control Intrusion Files Network Discovery **Application Detectors** Users Correlation Actions

Please enter a name

You have unsaved changes

Save Cancel

Enter a description

Detector Information

Author: admin
Application Protocol: Cisco SYSMANT
State: Inactive
Type: Application Protocol: FireSIGHT

Detection Criteria

Protocol: TCP/UDP
Port(s): 8080

Detection Patterns

Pattern String Type	Pattern String
There are no patterns.	

Packet Captures

Packet Capture Name
ingress-capture.pcap

Add Pattern [X]

Type: Ascii [v]
Pattern String: custom_app
Offset: 121

OK Cancel

Политика доступа (Access Control Policy)

Overview Analysis **Policies** Devices Objects FireAMP Health System Help admin

Access Control Intrusion **Files** Network Discovery Application Detectors Users Correlation Actions

File Malware protection

Monitor Executables

You have unsaved changes

Save Cancel

Used by 2 access control policies

Add File Rule

File Types	Application Protocol	Direction	Action
------------	----------------------	-----------	--------

- JARPACK
- MSEXE
- ACCDB
- JAR
- (8 more...)

Edit File Rule

Application Protocol: Any | Direction of Transfer: Any | Action: Malware Cloud Lookup Reset Connection

File Type Categories	File Types	Selected File Categories and Types
<input type="checkbox"/> Office Documents 7	<input type="text" value="Search name and description"/>	<input type="checkbox"/> JARPACK (Jar pack file)
<input type="checkbox"/> Archive 1	<input type="checkbox"/> ACCDB (Microsoft Access 2007 file)	<input type="checkbox"/> MSEXE (Windows/DOS executable file)
<input type="checkbox"/> Multimedia 1	<input type="checkbox"/> JAR (Java archive file)	<input type="checkbox"/> ACCDB (Microsoft Access 2007 file)
<input type="checkbox"/> Executables 2	<input type="checkbox"/> JARPACK (Jar pack file)	<input type="checkbox"/> JAR (Java archive file)
<input type="checkbox"/> PDF files 1	<input type="checkbox"/> MDB (Microsoft Access file)	<input type="checkbox"/> MDB (Microsoft Access file)
<input type="checkbox"/> Encoded 0	<input type="checkbox"/> MNY (Microsoft Money file)	<input type="checkbox"/> MNY (Microsoft Money file)
<input type="checkbox"/> Graphics 0	<input type="checkbox"/> MSEXE (Windows/DOS executable file)	<input type="checkbox"/> MSOLE2 (Microsoft Office applications)
<input type="checkbox"/> System files 0	<input type="checkbox"/> MSOLE2 (Microsoft Office applications)	<input type="checkbox"/> MSWORD_MAC5 (Microsoft Word for Mac)
	<input type="checkbox"/> MSWORD_MAC5 (Microsoft Word for Mac)	<input type="checkbox"/> NEW_OFFICE (Microsoft Office Open XML Document)
	<input type="checkbox"/> NEW_OFFICE (Microsoft Office Open XML Document)	<input type="checkbox"/> PDF (PDF file)

My Inline policy

Save Cancel Save and Apply

Logging

Log at Beginning of Connection

Log at End of Connection

Send Connection Events to:

Defense Center

Syslog

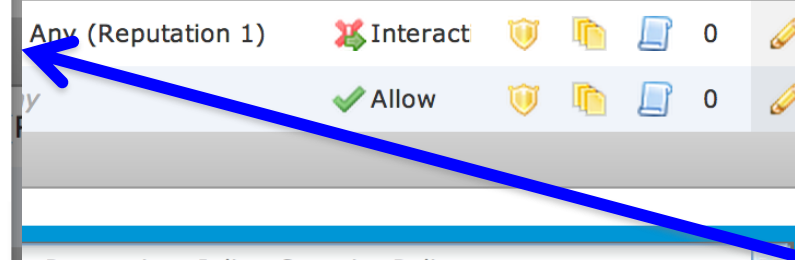
SNMP Trap

OK Cancel

Category Add Rule Search Rules

RLs	Action					
Any (Reputation 1)	Interact				0	
	Allow				0	

Intrusion Prevention: Inline-Security-Policy



- Sourcefire Authored Policies--
- Access Control: Block All Traffic
 - Access Control: Trust All Traffic
 - Network Discovery Only
 - Intrusion Prevention: Experimental Policy 1
 - Intrusion Prevention: Connectivity Over Security
 - Intrusion Prevention: Balanced Security and Connectivity
 - Intrusion Prevention: Security Over Connectivity
- User Created Policies--
- Intrusion Prevention: Passive-Secure-Policy
 - Intrusion Prevention: Initial Inline Policy - SourceFireDC.ashes.cc
 - Intrusion Prevention: Inline-Security-Policy**

HTTP Ответы

Overview Analysis **Policies** Devices Objects FireAMP

Health System Help admin

Access Control Intrusion Files Network Discovery Application Detectors Users Correlation Actions

My Inline policy

Save Cancel Save and Apply

LAB Policy for Inline

Rules Targets (1) Security Intelligence **HTTP Responses** Advanced

Block Response Page

This page will be displayed when HTTP traffic is blocked.

Custom...

Interactive Block Response Page

This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.

Sourcefire-provided

Edit Block Response Page

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;padding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {color:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong>
<br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

506 of 1353 characters used

Save Cancel

Sourcefire FireSIGHT® Technology



FireSight!

Система SourceFire вошла в эру, где обнаружение тесно связано с знанием окружения с целью обеспечения более точного и релевантного предупреждения. Коллекция технологий, которые это обеспечивают называется FireSight. FireSight применяет 3 основных типа обнаружения для понимания сети, которую защищает SourceFire:

- **Discovery** – Тип обнаружения, который сообщает информацию о хостах, операционных системах, сервисах, протоколах и приложениях в выделенном окружении.
- **Connection** – Этот тип обнаружений является мониторингом соединений и хранит все что происходит, все связи хостов, как много данных прошло за время соединений и если применимо, какие URL запрашивались.
- **Users** – Этот тип обнаружения и мониторинга Ваших сетей за пользовательской активностью и записи их IP адресов. Также интегрируется с LDAP серверами для предоставления большей информации о обнаруживаемых пользователях. Также может интегрироваться с Microsoft Active Directory серверами для записи пользователей.

FireSight!

С настолько детальным представлением окружений SourceFire может подставлять IPS события в контекст где они происходят и мониторить подозрительную активность. Комбинация враждебной активности, сетевого поведения и детальное знание окружения позволяет SourceFire проводить корреляцию событий для достижения следующих результатов:

События по уровню воздействия – Хост, который пытается использовать уязвимость актуальную для жертвы произведет высокий приоритет события; Если же жертва не имеет используемой в атаке уязвимости, событие все еще будет выдаваться, однако уровень угрозы будет ниже в силу невозможности нанести урон жертве.

Автоматическая подстройка – может быть достигнута в силу того, что система может выбирать правила и опции конфигурации основываясь на известном окружении. Это динамический процесс, в котором обнаруживаемые изменения в окружении детектируются и рапортуются как только обнаруживаются. Таким образом политики и конфигурация может обновляться самостоятельно без привлечения администратора.

Сетевое поведение – автоматически анализирует отклонение от нормального поведения хоста и на основании отклонений может вызвать событие.

Compliance - соответствие с Вашей корпоративной политикой безопасности может отслеживаться и рапортваться.

User awareness – позволяет понимать что ваши пользователи делают в сети. Также можно отследить в какие атаки и активности были вовлечены пользователи и использовать эти знания в политике корреляции.

Discovery

Данная компонента SourceFire отвечает за пассивный мониторинг вашей сети. **Может быть дополнено активными сетевыми сканерами, либо прямым импортом информации об окружении через выделенный API.**

Следующая информация собирается об окружении:

- Хосты
- Операционные системы
- Сервисы
- Клиентские приложения
- Уязвимости, которые могут присутствовать
- Сетевое мапирование

Хостовые профили

- **Host** – Первый информационный блок на хостовом профиле и он содержит базовую информацию: Имя, операционную систему, IP address, MAC address и тип хоста.
- **Operating System** – Если прошло достаточно трафика до и от машины, определяется его ОС.
- **Servers** – Все сервисы, обнаруженные на хосте.
- **Applications** – Все приложения, обнаруженные на хосте.
- **Users** – Все пользователи, ассоциированные с хостом .
- **Attributes** – Атрибуты, ассоциированные с хостом.
- **Host Protocols** – Протоколы замеченные на хосте.
- **Vulnerabilities** – Уязвимости, основываясь на сервисах, клиентских приложениях, протоколах и операционной системе хоста система может заключить об их актуальности и перечислит их в профиле;

Context Ex **Sourcefire Vulnerability ID** 94754
Snort ID 15728, 15729, 15727, 19268, 19269, 19270, 19271, 19272, 19273, 19274, 19275, 19276, 19277, 19278, 19279, 19280
BugTraq ID 35759, 44503
WebPage title,OoApp Guestbook XSS vuln. || author,rakstija r0t3d3Vil || url,http://pridels0.blogspot.com/2005/12/ooapp-guestbook-xss-vuln.html

Hosts

Filter by

CVE ID 2009-1862
Title Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Impact Qualification Enabled ▾

Hosts [IP]
 192 (26)
 192.
 19

Date Published 2009-07-21
Vulnerability Impact 8
Remote TRUE

Available Exploits
Description
Technical Description

Multiple Adobe products are prone to a remote code-execution vulnerability.

Adobe Acrobat and Reader are applications for handling PDF files. Adobe Flash Player is a multimedia application. The applications are available for multiple platforms.

Acrobat, Reader, and Flash Player are prone to a remote code-execution vulnerability that arises in the Adobe ActionScript Virtual Machine and affects the 'flash9f.dll' and 'authplay.dll' modules. Specifically, an arbitrary value for an object scope can be placed on the stack as a memory address and then later referenced by a call to 'MethodEnv::findproperty'. This call will reference heap memory containing arbitrary code specified by the attacker and will allow code execution in the context of the user running the affected application.

The attacker can exploit this issue by supplying a malicious Flash ('.swf') file or by embedding a malicious Flash application in a PDF file.

Failed attempts will likely result in denial-of-service conditions.

The issue affects the following:

Reader and Acrobat 9.1.2
 Flash Player 9 and 10

Solution
 Updates are available. Please see the references for details.

Additional Information ▶

Fixes ▾

- Upgrade Flash-player-10.0.32.18-1.i586.rpm [Download](#)
- Patch MacOSXUpd10.6.1.dmg [Download](#)
- Patch MacOSXServerUpd10.6.1.dmg [Download](#)
- Patch SecUpd2009-005.dmg [Download](#)
- Patch SecUpdSrvr2009-005.dmg [Download](#)
- Patch SecUpd2009-005Intel.dmg [Download](#)
- Patch SecUpd2009-005PPC.dmg [Download](#)



onent Port

5X	0.6, 10.5, 10.6
5X	0.6, 10.5, 10.6
5X	0.6, 10.5, 10.6
5X	0.6, 10.5, 10.6

Профили соединений

События соединений это записи происходящих соединений и если не записываются сами передаваемые данные, то фиксируются метаданные соединений время, source-destination, протоколы и количество переданных данных

Отслеживание активных соединений дает системе возможность мониторинга сетевого поведения и уведомления с исправлением подохрительной активности.

- First Packet
- Initiator User
- Client
- Initiator Packets
- URL Category
- Egress Security Zone
- Last Packet
- Initiator Port
- Version
- Responder Packets
- URL Reputation
- Device
- Action
- Responder Port
- TCP Flags
- Initiator Bytes
- Source Device
- Ingress Interface
- Initiator IP
- Protocol
- Connection Type
- Responder Bytes
- Access Control Policy
- Egress Interface
- Responder IP
- Application
- NetBIOS Domain
- URL
- Ingress Security Zone

Connection Summary

Provides tables and charts of the activity on your monitored network segment organized by different criteria

Connections x **Traffic** x **Geolocation** x +

Show the Last 1 hour

+ Add Widgets

Traffic by Application [\(switch workflow\)](#)

Top 10 Applications by Traffic > [Table View of Connection Events](#)

2014-02-03 01:14:00 - 2014-02-04 01:25:27

Expanding

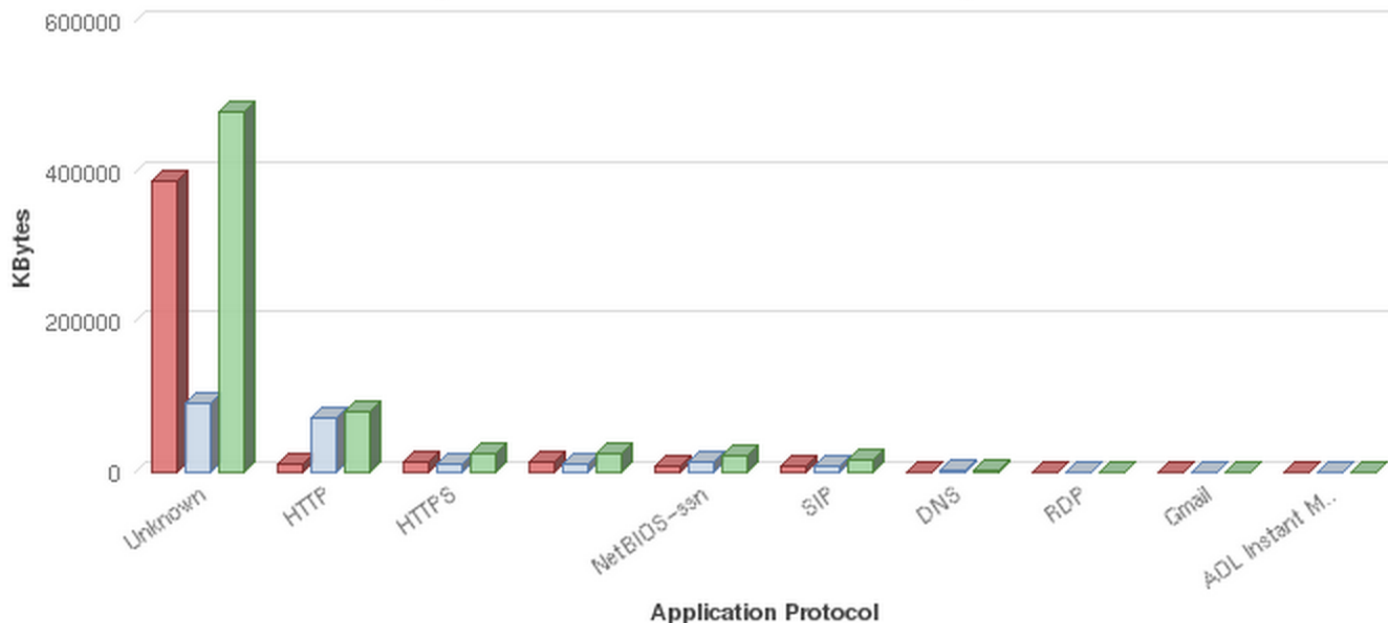
No Search Constraints [\(Edit Search\)](#)

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Servers | Host Attributes | More ▾

X-Axis | Y-Axis | Datasets | Switch to Pie

Export Data | Detach

KBytes by Application Protocol (top 10)
(2014-02-03 01:10:00 - 2014-02-04 01:25:00)



Initiator KBytes | Responder KBytes | Total KBytes

Обнаружение пользователей

Данная функция дает возможность коррелировать угрозы с хостами и пользователями. Сенсоры идентифицируют источник угроз, нарушения политик и сетевых уязвимостей. Путем связывания сетевого поведения, трафика и событий напрямую с пользователями, система SourceFire помогает бороться с угрозами, блокировать пользователей или их активности, а также защищать других от воздействия.

LDAP User Metadata Collection - Соединение с MS AD сервером или сервером, поддерживающим LDAP (Sun Directory Services or OpenLDAP) для сбора списка пользователей и их метаданных.

Следующая информация включается в обнаружение:

- first name
- last name
- email
- department
- phone number

Правила и политики корреляции

Defence Center можно настроить на запуск различных действий в ответ на нарушение политики или событие Network Discovery.

Эти действия включают ремедиацию, такую как блокирование хоста на фаерволе при обнаружении атаки. Когда срабатывает действие, генерируется событие о ремедиации.

Компонента ремедиации политики и соответствующие действия предоставляют гибкий API, который позволяет создавать и загружать собственные модули ремедиации и отвечать на события безопасности.

Еще один вариант ответа – это запуск уведомления.

- Email
- SNMP
- Syslog

Также есть возможность добавить атрибут на хост, атрибуты и их типы можно задавать самостоятельно.

Собственный модуль ремедиации

В дополнение к стандартным модулям, которые поставляются с системой можно применять свои собственные модули. Модуль ремедиации это программа или скрипт, упакованный с ассоциированными файлами, который написан с целью совершения действий в ответ на определенные условия.

Скрипт ремедиации может быть написан на любом из указанных языков:

- Bash
- Tcsh
- Perl
- C - If you write your remediation module program in C, it must be pre-compiled and statically linked, with the exception of links to routines

Rule Information

[+ Add Connection Tracker](#)

Rule Name

Rule Description

Rule Group

Select the type of event for this rule

If and it meets the following conditions:

100,000 events

[+ Add condition](#) [+ Add complex condition](#)

is

5,000 events

AND

[+ Add condition](#) [+ Add complex condition](#)

is not

500 events

Host Profile Qualification

[X Remove Host Profile Qualification](#)

Only generate an event if the host(s) involved have the following properties:

[+ Add condition](#) [+ Add complex condition](#)

has the following properties

OS Vendor is

OS Name is

OS Version is

OR

20 events

is

+10 events

User Identity Qualification

[X Remove User Qualification](#)

Only generate an event if the user(s) involved have the following properties:

[+ Add condition](#) [+ Add complex condition](#)

is

3 events

Edit Policy: Inline-Security-Policy

Policy Information

- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings
- Policy Layers
 - My Changes
 - Rules
 - DNP3 Configuration
 - Modbus Configuration
 - FireSIGHT Recommendation
 - Rules
 - Security Over Connectivity
 - Rules
 - Back Orifice Detection
 - Checksum Verification
 - DCE/RPC Configuration
 - DNS Configuration
 - Event Queue Configuration
 - FTP and Telnet Configuration
 - Global Rule Thresholding
 - GTP Command Channel
 - HTTP Configuration

Rules < Back

Rule Configuration Filter: X ?

Rule Content

Category

Classifications

Microsoft Vulnerabilities

Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input type="checkbox"/>				
GID SID	Message			
1 1021	SERVER-IIS ism.dll attempt			

Filter returned 1 result

1 of 1

MS00-031

Attack: Simple. No exploit software required.

Positives: False
Negatives: False

Action: Corrective
Check server logs for signs of compromise.

Contributors: Original rule writer unknown
Original document author unknown
Sourcefire Vulnerability Research Team
Nigel Houghton <nigel.houghton@sourcefire.com>

References: [Bugtraq page](#)
[Common Vulnerabilities and Exposures Page](#)
[Nessus Page](#)
[Microsoft security bulletin](#)

SRU: [Sourcefire Rule Update 2013 06 17 001 vrt](#)

Edit Policy: Inline-Security-Policy

- Policy Information
- Variables
- Rules
- FireSIGHT Recommendations
- Advanced Settings
 - Back Orifice Detection
 - Checksum Verification
 - DCE/RPC Configuration
 - DNP3 Configuration
 - DNS Configuration
 - Event Queue Configuration
 - FTP and Telnet Configurati
 - Global Rule Thresholding
 - GTP Command Channel Co
 - HTTP Configuration**
 - IP Defragmentation
 - Latency-Based Rule Handlin
 - Modbus Configuration
 - Packet Decoding
 - Performance Statistics Con
 - Regular Expression Limits
 - Rule Processing Configurati
 - SIP Configuration

HTTP Configuration < Back

Consecutive Small Chunks	<input type="text" value="5"/>	(0 - 255. When Small Chunk Size > 0, number of consecutive small chunks that is excessive.)
HTTP Methods	<input type="text" value="CONNECT, DELETE, HEAD, OPTIONS, PUT, TRACE"/>	
No Alerts	<input type="checkbox"/>	
Normalize HTTP Headers	<input checked="" type="checkbox"/>	
Inspect HTTP Cookies	<input checked="" type="checkbox"/>	
Normalize Cookies in HTTP Headers	<input type="checkbox"/>	
Allow HTTP Proxy Use	<input type="checkbox"/>	
Inspect URI Only	<input type="checkbox"/>	
Inspect HTTP Responses	<input checked="" type="checkbox"/>	
Normalize UTF Encodings to UTF-8	<input checked="" type="checkbox"/>	
Inspect Compressed Data	<input checked="" type="checkbox"/>	
Unlimited Decompression	<input type="checkbox"/> (Enabling this option sets Maximum Compressed Data Depth and Maximum Decompressed Data Depth to 65535 during commit)	
Normalize JavaScript	<input type="text"/>	(Maximum allowed consecutive encoded spaces inside JavaScript)
Extract Original Client IP Address	<input checked="" type="checkbox"/>	
Log URI	<input checked="" type="checkbox"/>	
Log Hostname	<input checked="" type="checkbox"/>	
Profile	<input checked="" type="radio"/> All <input type="radio"/> Apache <input type="radio"/> IIS <input type="radio"/> Custom	

This configuration is contained in the base policy: Security Over Connectivity

Препроцессоры транспортного/сетевого уровней

SourceFire предоставляет препроцессоры, которые детектируют эксплоиты на сетевом и транспортных уровнях. Эти препроцессоры детектируют атаки, направленные на IP фрагментацию, валидацию чексуммы, TCP и UDP обработку сессий. До отсылки пакета в препроцессор пакетный декодер конвертирует заголовки пакета и данные в формат, доступный препроцессору и движку правил, далее детектирует аномальное поведение в заголовках пакетов.

Имеются следующие advanced configuration опции:

- Checksum Verification
- Detection Settings
- Inline Normalization
- IP Defragmentation
- Packet Decoding
- TCP Stream Configuration
- UDP Stream Configuration

Управление пользователями

Доступна внешняя и внутренняя база аутентификации пользователей

На странице логина пользователь вводит свои учетные данные:

- Если пользователь настроен как внутренний пользователь, устройство проверяет свою локальную базу пользователей со всеми сопутствующими атрибутами.
- Если пользователь заведен как внешний, система проверяет существует ли логин во внутренней базе и находит атрибуты, которые надо применить. Если пользователя нет во внутренней базе, система идет во внешний репозиторий, LDAP и RADIUS поддерживаются. Проверяются учетные данные и если они верны, предоставляется доступ.

Пользовательские роли

Overview Analysis Policies Devices Objects FireAMP

Health System Help admin

Local User Management Updates Licenses Monitoring Tools

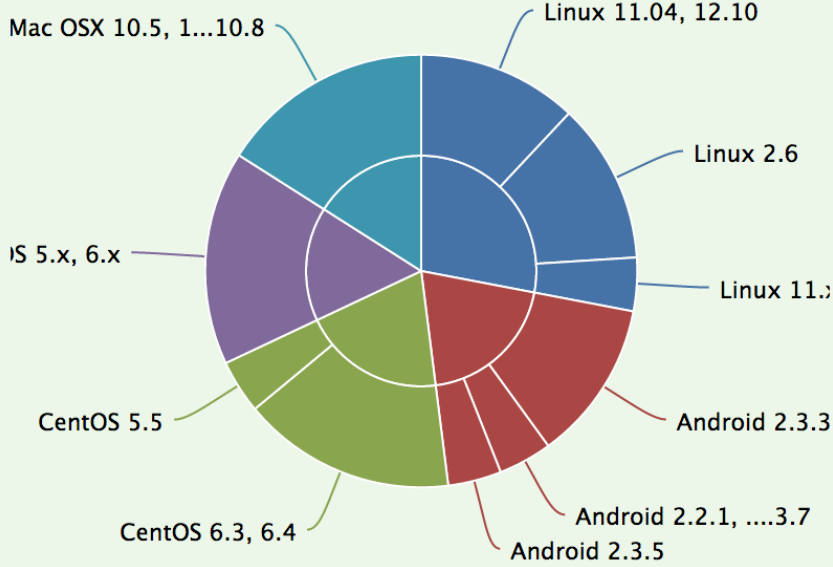
Users User Roles Login Authentication

Configure Permission Escalation Create User Role

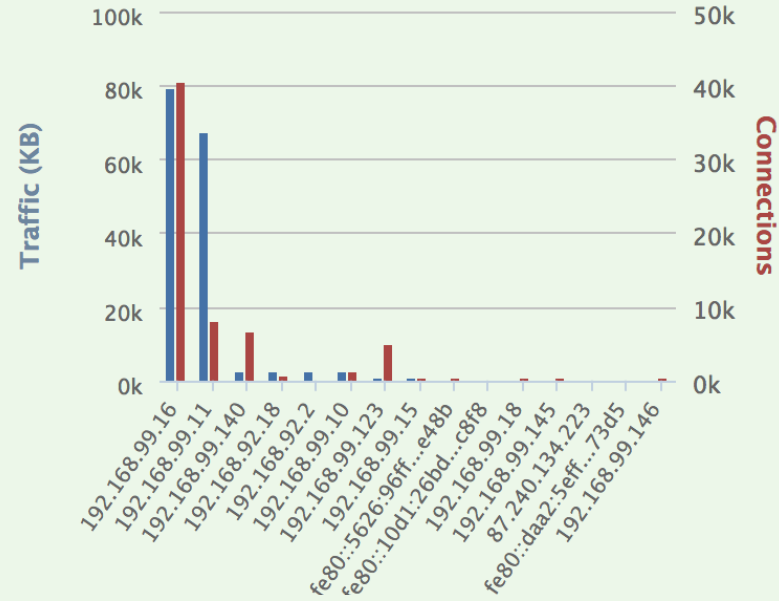
User Role	Enabled	Actions
Access Admin Sourcefire-provided	<input checked="" type="checkbox"/>	   
Administrator Sourcefire-provided	<input checked="" type="checkbox"/>	   
Discovery Admin Sourcefire-provided	<input checked="" type="checkbox"/>	   
External Database User Sourcefire-provided	<input checked="" type="checkbox"/>	   
Intrusion Admin Sourcefire-provided	<input checked="" type="checkbox"/>	   
Maintenance User Sourcefire-provided	<input checked="" type="checkbox"/>	   
Network Admin Sourcefire-provided	<input checked="" type="checkbox"/>	   
Security Analyst Sourcefire-provided	<input checked="" type="checkbox"/>	   
Security Analyst (Read Only) Sourcefire-provided	<input checked="" type="checkbox"/>	   
Security Approver Sourcefire-provided	<input checked="" type="checkbox"/>	   

Network Information

Operating Systems



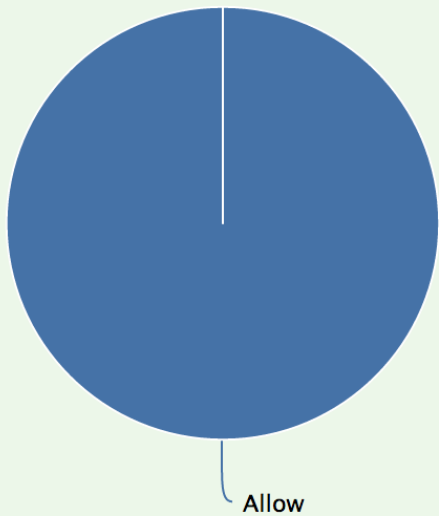
Traffic by Source IP



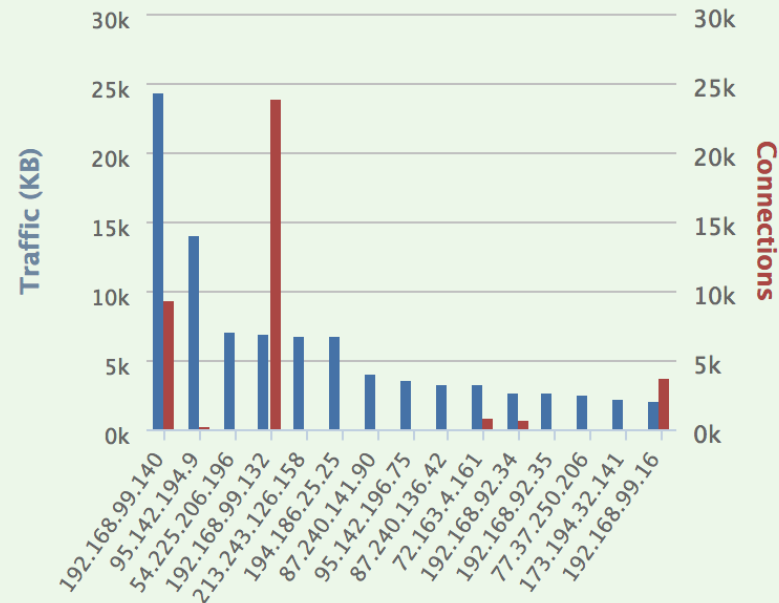
Traffic by Source User

No Data

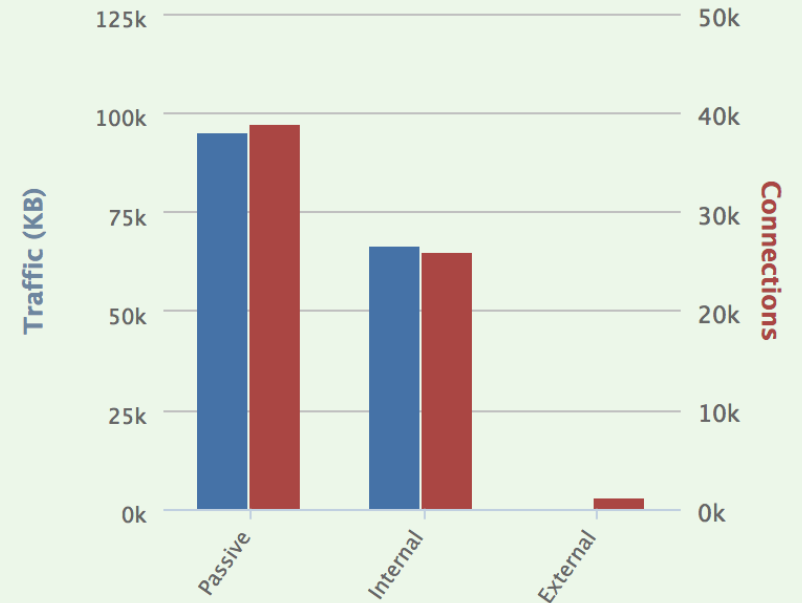
Connections by Access Control Action



Traffic by Destination IP



Traffic by Ingress Security Zone



Браузер контекста (Context Explorer)

Статистика приложений

Секция информации о приложениях в браузере контекста состоит из трех интерактивных графиков и таблицы-списка:

-- Траффик

-- События безопасности

-- Хосты ассоциированные с приложениями и организованные по риску для бизнеса.

Application Protocol Information

Application Protocol Client Application Web Application

Traffic by Risk and Application

Intrusion Events by Risk and Application

Hosts by Risk and Application

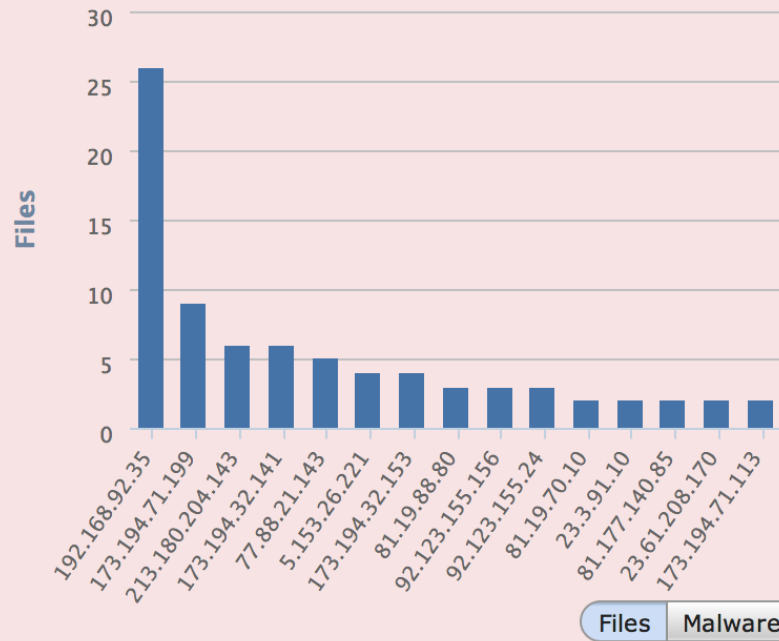
Intrusion Event Details

Event	Classification	Priority	Events
HI_CLIENT_IIS_UNICODE (119:7)	Unknown Traffic	low	246
MALWARE-OTHER self-signed SSL certificate with c	Potential Corporate Policy Violation	high	151
HI_CLIENT_DOUBLE_DECODE (119:2)	Not Suspicious Traffic	low	55
HI_CLIENT_BARE_BYTE (119:4)	Not Suspicious Traffic	low	28
HI_CLIENT_OVERSIZE_DIR (119:15)	Potentially Bad Traffic	medium	26
SSH_EVENT_PROTOMISMATCH (128:4)	Detection of a Non-Standard Protocol or Event	medium	12
SERVER-WEBAPP Oracle Java Web Server WebDA'	Attempted Administrator Privilege Gain	high	10
FILE-IMAGE Microsoft Kodak Imaging large offset	Attempted User Privilege Gain	high	8
PROTOCOL-FTP DELE overflow attempt (1:1975)	Attempted Administrator Privilege Gain	high	8

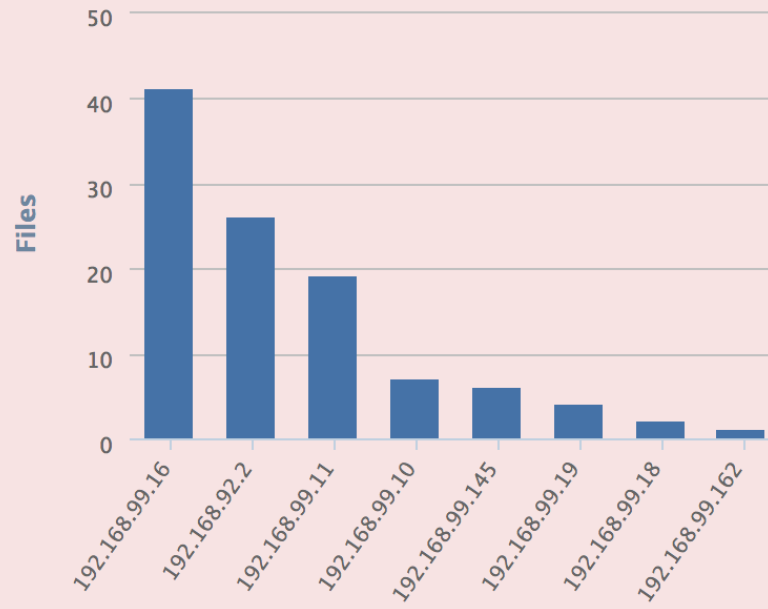
Браузер контекста (Context Explorer)

Статистика файлов

Top Hosts Sending Files



Top Hosts Receiving Files



Top Malware Detections

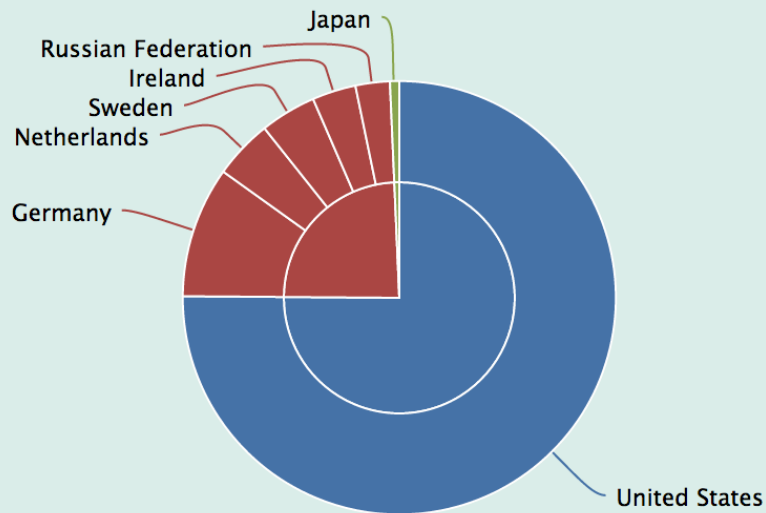
No Data

Браузер контекста (Context Explorer)

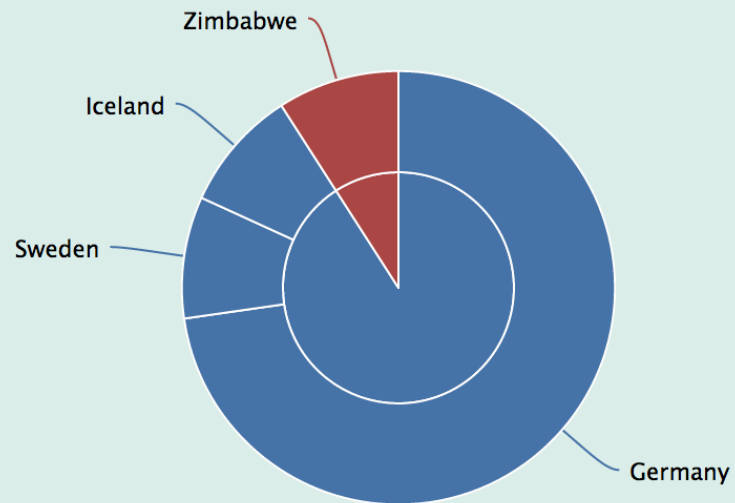
Геолокация

Geolocation Information

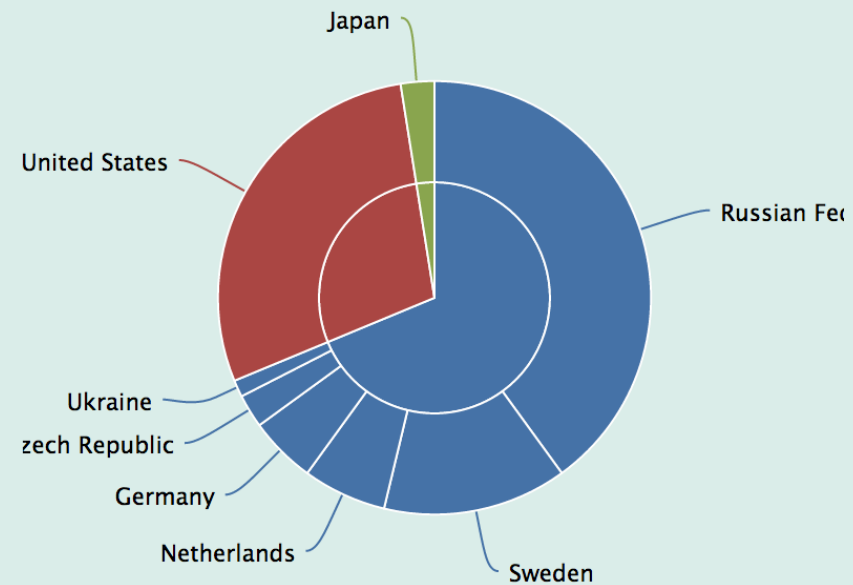
Connections by Initiator Country



Intrusion Events by Source Country



File Events by Sending Country



Advanced Malware Protection



Антивирус как средство от Malware

- **Весьма ограничено:**
 - Может использовать 2-5% от имеющегося CPU.
 - Ограниченный набор правил
 - Ограничено покрытие
 - Оперирует в точке времени.
- **Зачем доверять безопасности 386-му компьютеру?**



To your AV, this ...



... looks like this.

Что если защита от Malware реализуется так?

- Петафлопы производительности
- Петабайты хранилища
- Big data аналитика
- Постоянный анализ
- Интеллектуальные алгоритмы поиска Malware



“Now, *that’s* what I’m talkin’ about!”

Детектирование malware дело не легкое....

- Не рассматривайте разрозненные объекты.
- Думайте об **экосистеме Malware**, смотрите за сцену, ищите **скрытых актеров**
- Отслеживайте праекторию Malware до пациента 9, в другом случае вы снова заразитесь

Диспозиция файлов:

- Known bad
- Known good
- Unknown



Unknown drops
known bad
75%

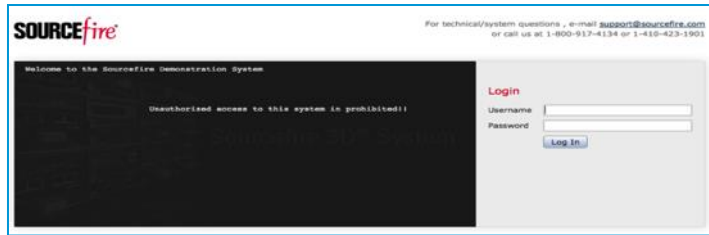


Known bad
drops unknown
70%



Наш подход к advanced malware protection

AMP for Networks



FireSIGHT Management Center



Sourcefire Sensor



AMP Malware license



Detection Services & Big Data analytics



SSL:443 | 32137

Heartbeat: 80

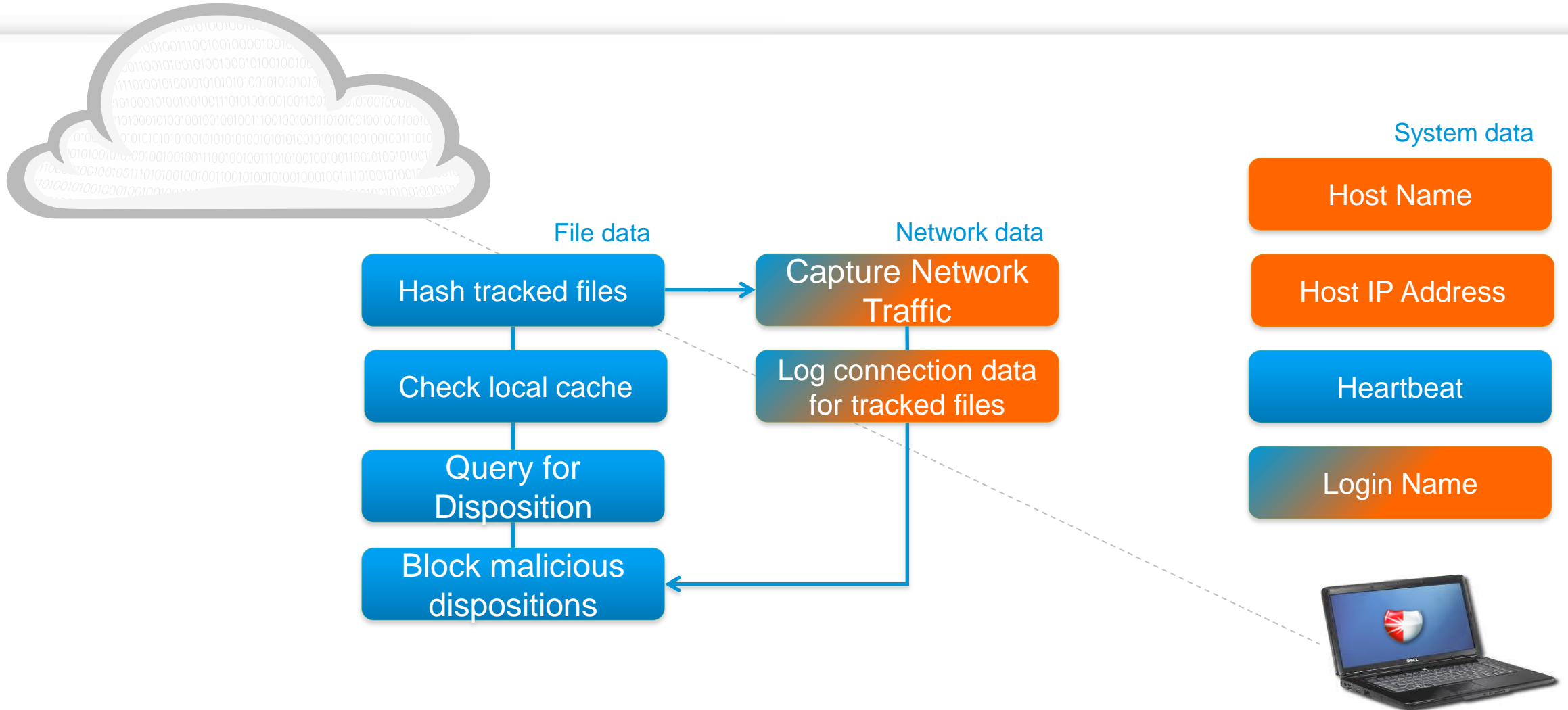


AMP for Endpoints



SaaS Manager

Модель работы Endpoint



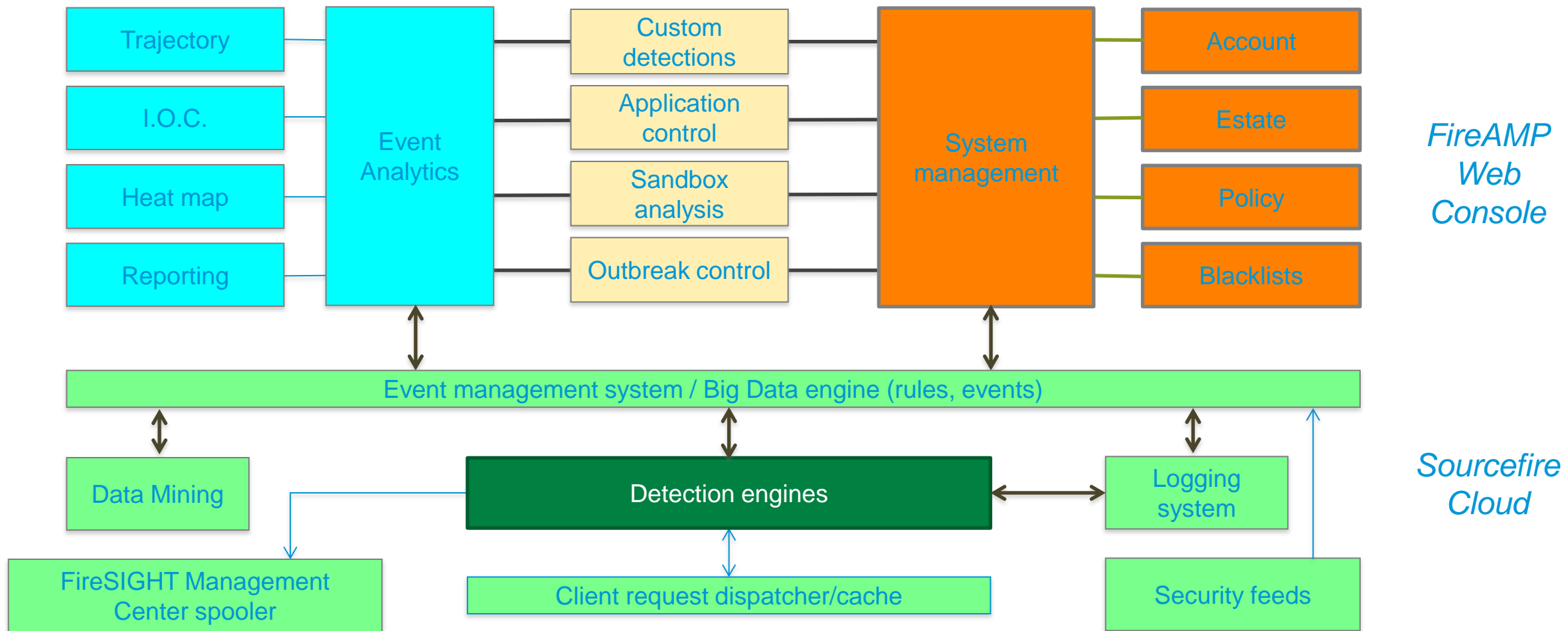
Legend

No Personally Identifiable Information (PII)

Optional PII

PII

Все самое умное находится в облаке



Движки детектирования в AMP

ADVANCED ANALYTICS

Integrates heuristics from the malware environment, the Big Data store, ETHOS and SPERO to clarify the outcome of a marginal conviction

~~Generic
ETHOS~~

~~Decision Tree
(SPERO)~~

ETHOS

Catches families of malware through use of “fuzzy hashes” embedded in the Feature Print. Counters malware evasion by “bit-twiddling”.

Primary Hash

Feature Print

Detection torque

(•)

{...}



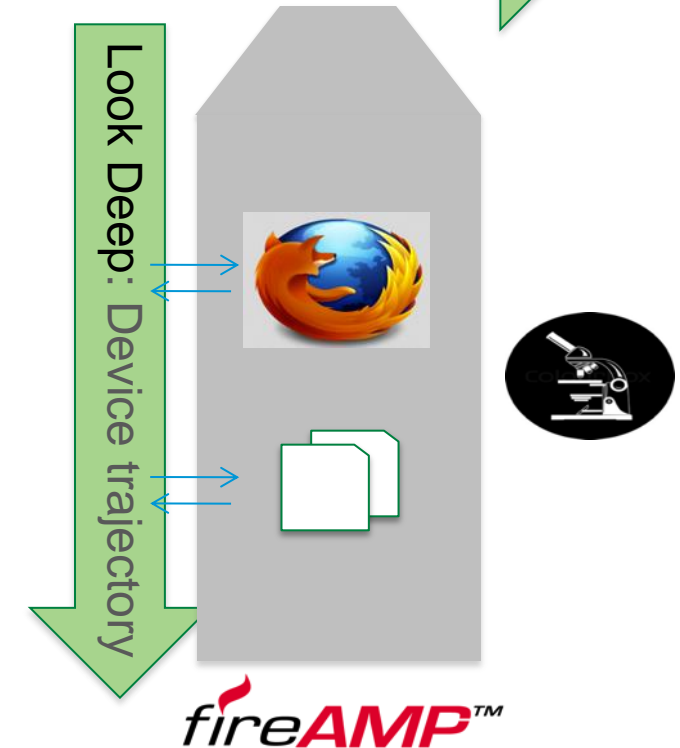
∫ users, engines
1

Поиск пациента 0: Анализ Траектории

Смотрите шире (AMP for Networks), глубже (AMP for Endpoints)



- Какие системы заражены?
- Когда это произошло?
- Где пациент №0?
- Что еще он с собой принес?



Thank you.

Questions ?

Sandro Chachanidze
achachan@cisco.com

