



TOMORROW starts here.

Межсетевые экраны следующего поколения Cisco ASA с сервисами FirePower – борьба с современными угрозами, архитектура решения и варианты применения

Руслан Иванов

Системный инженер-консультант

ruivanov@cisco.com

Проблемы с традиционной моделью «эшелонированной» безопасности

Точечные продукты

Высокая сложность,
меньшая
эффективность



Ручные и статичные механизмы

Медленная реакция,
ручное управление,
низкая
результативность



Слабая прозрачность

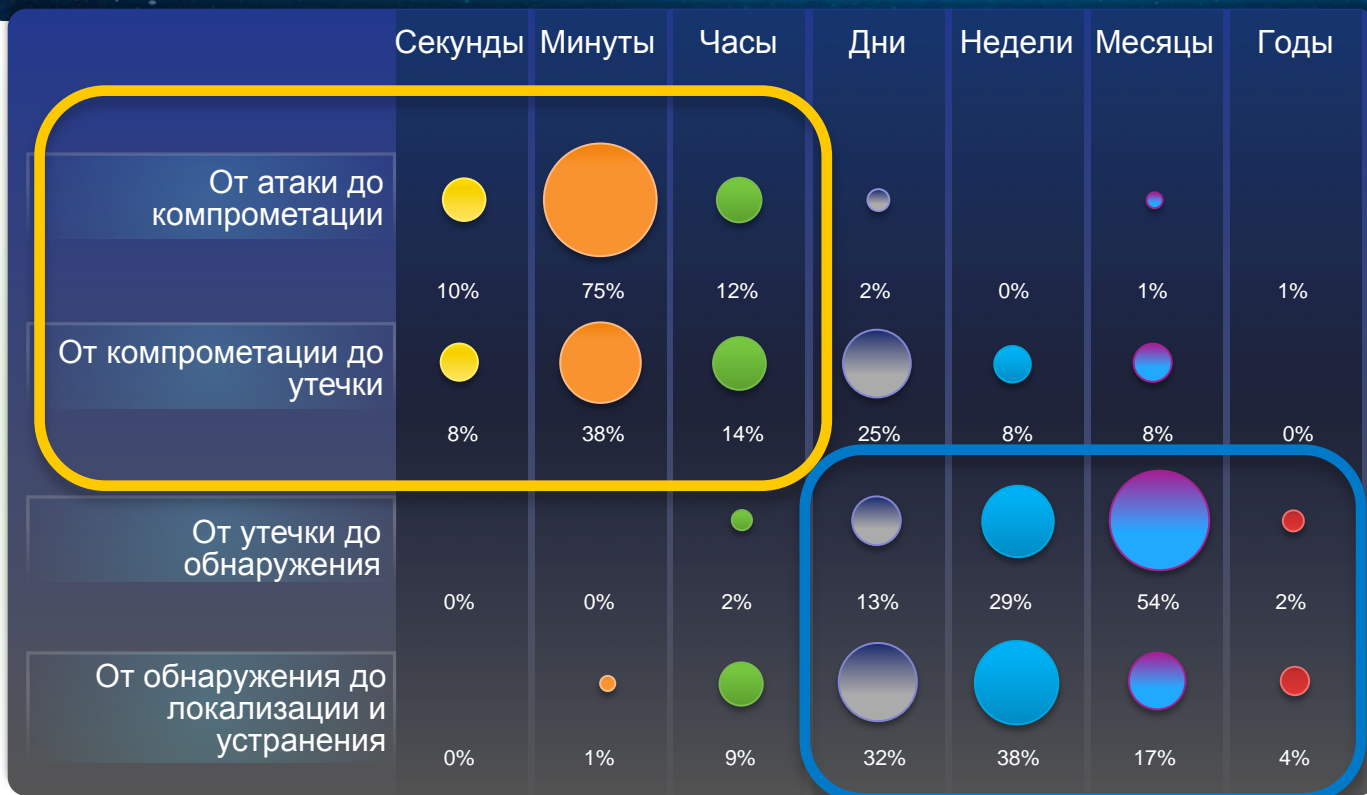
Многовекторные и
продвинутые угрозы
остаются
незамеченными



Результат печален – такая защита проигрывает

Взломы
осуществляются
за минуты

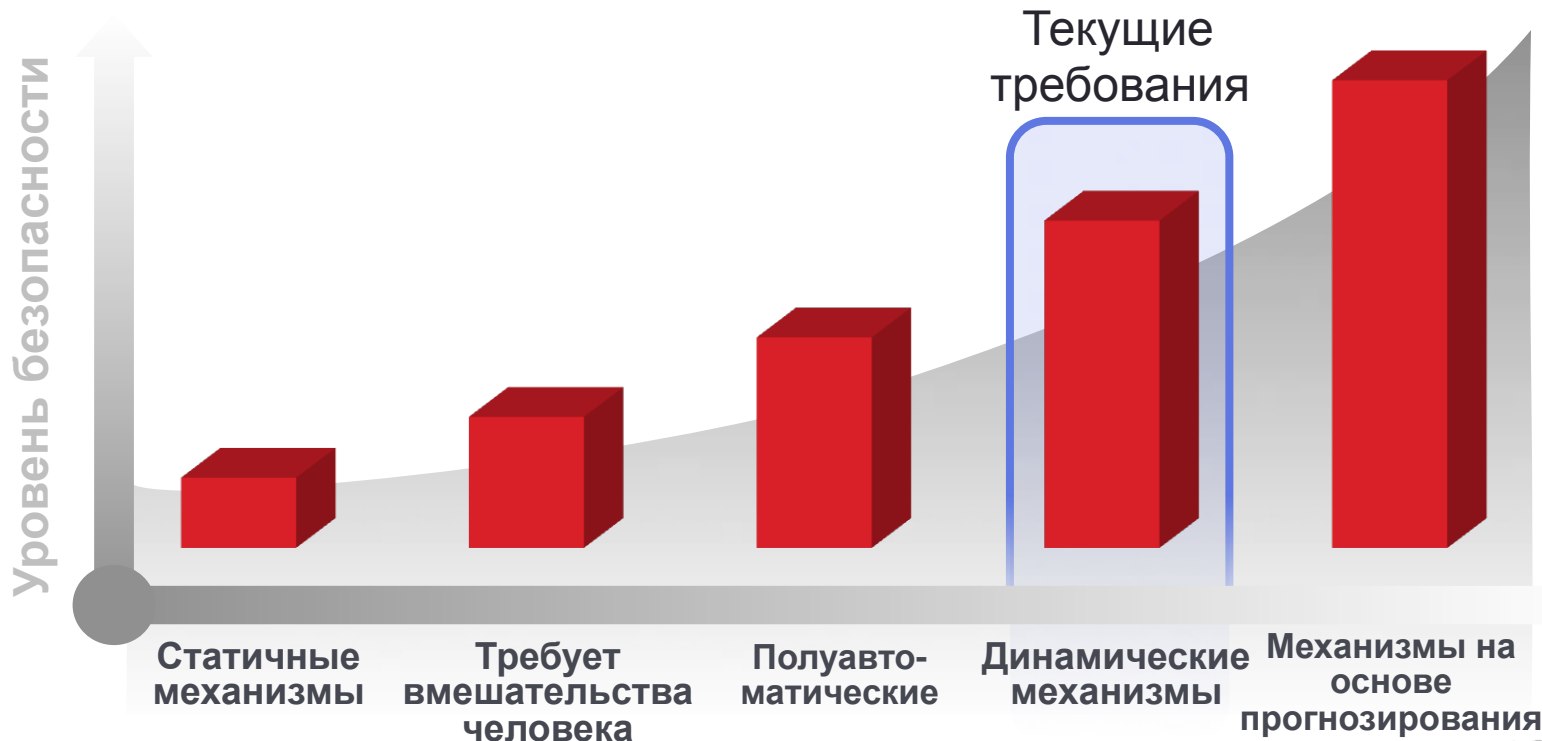
Обнаружение и
устранение
занимает недели и
месяцы



Временная шкала событий в % от
общего числа взломов

Источник: 2012 Verizon Data Breach Investigations

Эволюция механизмов безопасности



Cisco: информационная безопасность в центре внимания



Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделение Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

AMP + FirePOWER
AMP > управляемая защита от угроз

2013

2014

2015...

Cognitive + AMP



Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

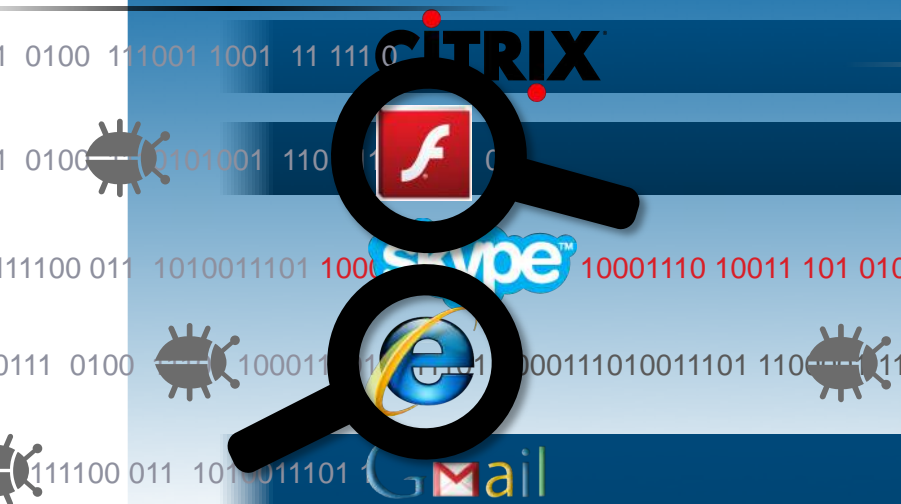
Приобретение компании ThreatGRID



- Коллективный анализ вредоносного кода
- Анализ угроз

Что не так с современными межсетевыми экранами?

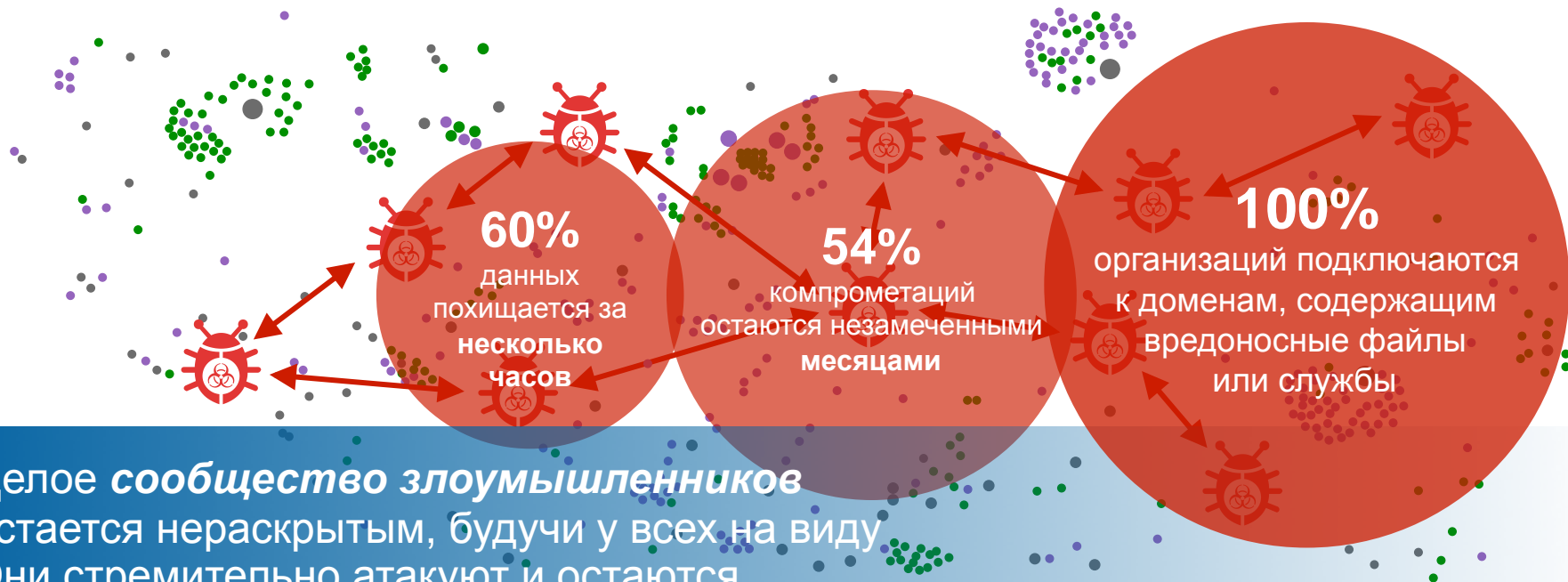
Фокусируются на приложениях...



Но полностью упускают из вида угрозы

МСЭ нового поколения могут уменьшить область атаки, но усовершенствованный вредоносный код часто обходит защитные механизмы.

Современный ландшафт угроз требует большего, чем просто контроль приложений

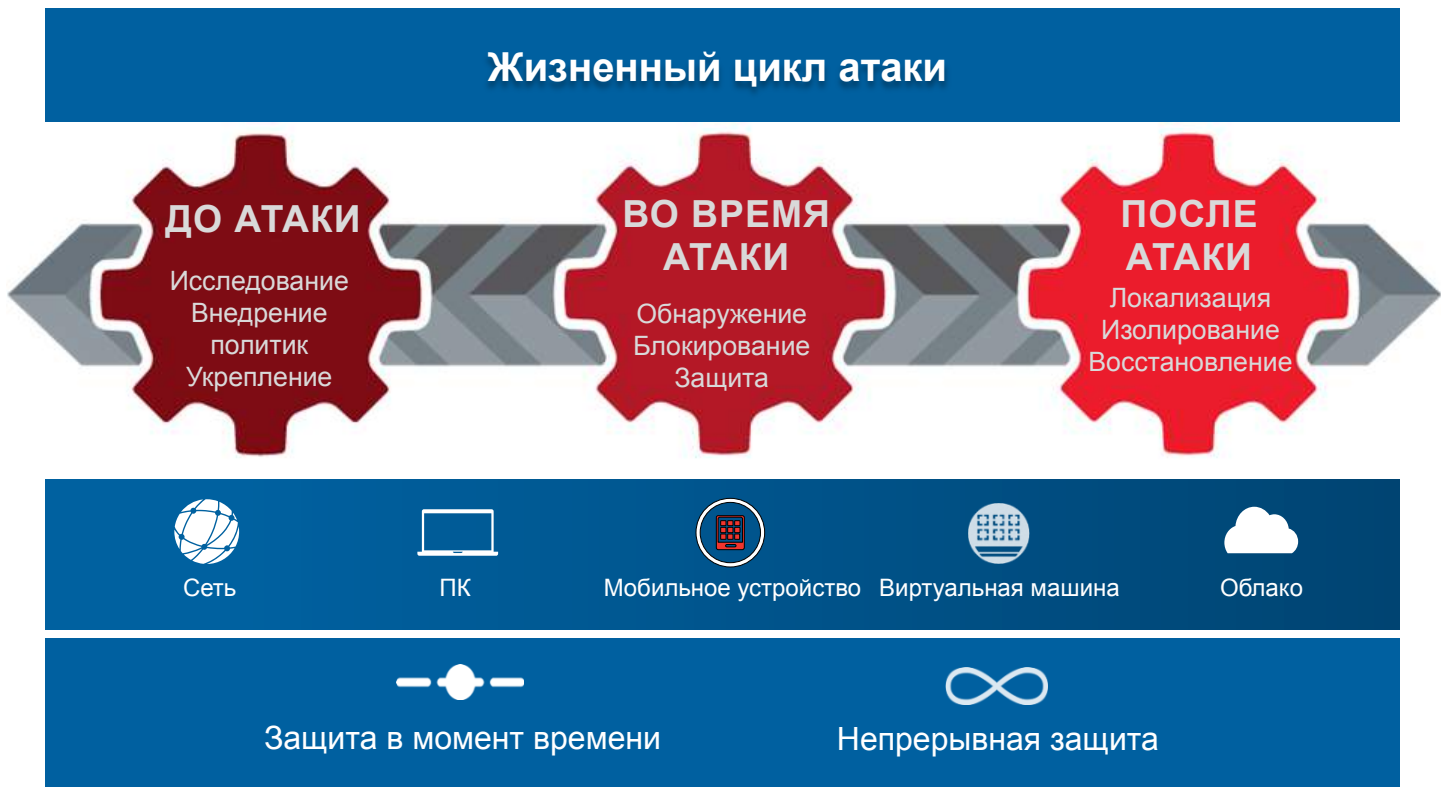


Целое сообщество злоумышленников остается нераскрытым, будучи у всех на виду. Они стремительно атакуют и остаются неуловимыми.

«Будь неуловимым, почти бесформенным.
Будь скрытным, почти беззвучным. Тогда
ты сможешь направлять судьбу врага как
тебе угодно»

Сунь Цзы. Искусство войны.

Комплексная защита от угроз для всего жизненного цикла атаки



Комплексная многоуровневая защита на основе межсетевого экрана Cisco ASA

Интеллектуальная экосистема коллективной информационной безопасности Cisco CSI



Cisco ASA

- ▶ Самый популярный межсетевой экран корпоративного класса с функцией контроля состояния соединений
- ▶ Детальный мониторинг и контроль приложений (Cisco® AVC)
- ▶ Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- ▶ Фильтрация URL-адресов на основе репутации и категоризации
- ▶ Система защиты от вредоносного кода Advanced Malware Protection с функциями ретроспективной защиты

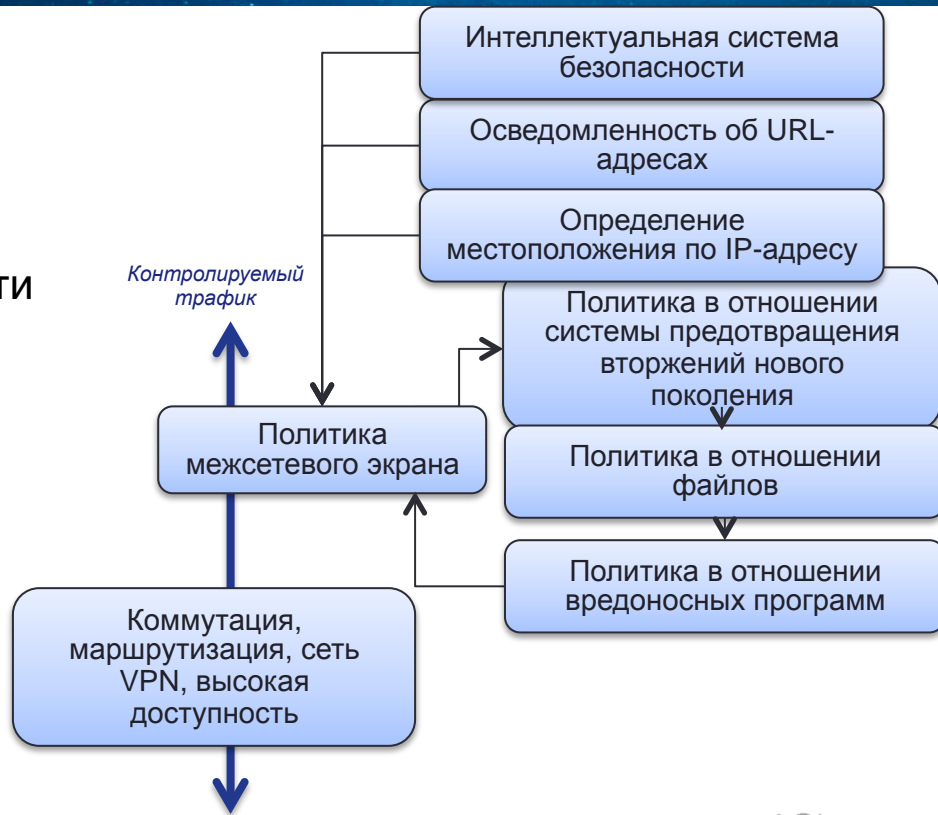
В основе лежит платформа Cisco ASA 5500-X и 5585-X



- Высокопроизводительная масштабируемая платформа
- Высокая доступность, надежность и отказоустойчивость
- Интеллектуальные сетевые сервисы
- Виртуализация, прозрачность функционирования
- Широкий модельный ряд
- Сертификация производства в ФСТЭК по 3-му и 4-му классу для МСЭ

Что такое FirePOWER Services?

- Система предотвращения вторжений нового поколения – проверка содержимого
- Учет контекста
- Интеллектуальная система безопасности – управление черными списками
- Полный контроль доступа:
 - По зоне сети, VLAN, IP, порту, протоколу, приложению, пользователю, URL-адресу
- И все эти компоненты прекрасно интегрируются друг с другом:
 - Используются политики системы предотвращения вторжений
 - Политики контроля файлов



Максимальная прозрачность сетевой активности

Категории	Технологии FirePOWER	Обычные IPS	МСЭ нового поколения
Угрозы	✓	✓	✓
Пользователи	✓	✗	✓
Веб-приложения	✓	✗	✓
Протоколы приложений	✓	✗	✓
Передача файлов	✓	✗	✓
Вредоносный код	✓	✗	✗
Серверы управления и контроля ботнета	✓	✗	✗
Клиентские приложения	✓	✗	✗
Сетевые серверы	✓	✗	✗
Операционные системы	✓	✗	✗
Маршрутизаторы и коммутаторы	✓	✗	✗
Мобильные устройства	✓	✗	✗
Принтеры	✓	✗	✗
VoIP-телефония	✓	✗	✗
Виртуальные машины	✓	✗	✗

Как выглядит пример политики NGFW?

The screenshot displays the Cisco FireAMP configuration interface for an **Inline Access Policy**. The interface includes a navigation menu at the top with tabs for Overview, Analysis, Policies, Devices, Objects, and FireAMP. Below the navigation, there are sub-tabs for Access Control, Intrusion, Files, Network Discovery, Application Detectors, Users, Correlation, and Actions. A notification bar indicates "You have unsaved changes" with buttons for Save, Cancel, and Save and Apply.

The main content area shows the **Inline Access Policy** configuration for "LAB Access-policy for Inline installations". It features a "Rules" tab and a "Filter by Device" search bar. Below the search bar is a table of rules, categorized into Administrator Rules, Standard Rules, and Root Rules.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLA...	U...	Applications	S...	De URLs	Action	Icons
Administrator Rules This category is empty												
Standard Rules												
1	Block-Bad URLs	any	any	any	any	any	any	any	any	any	Interact	Icons
2	Block Bad Applications	any	any	any	any	any	any	OpenVPN	any	any	Block wi	Icons
3	Block Facebook Games	any	any	any	any	any	any	Tags: Facebook g	any	any	Interact	Icons
4	Block Skype File Transfer	any	any	any	any	any	any	Skype File Transf	any	any	Block	Icons
5	Block High-Risk URLs (disabled)	any	any	any	any	any	any	any	any	any	Interact	Icons
6	Block High-Risk Applications (disabled)	any	any	any	any	any	any	Risk: High, Very	any	any	Interact	Icons
7	Allow Other + Inspect	any	any	any	any	any	any	any	any	any	Allow	Icons
Root Rules This category is empty												

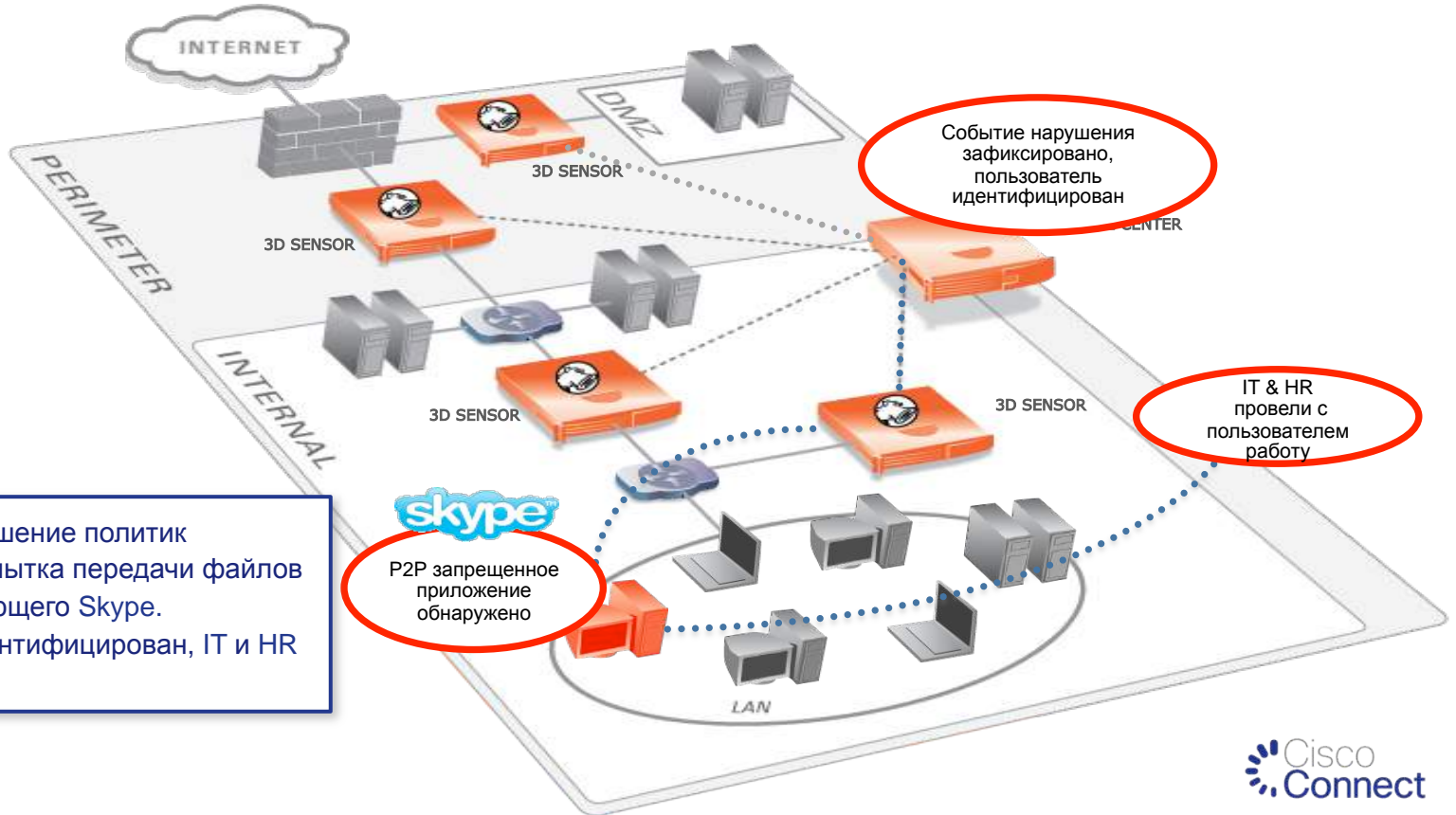
At the bottom of the interface, it shows "1 Row Selected" and "Displaying 1 - 7 of 7 rules". The footer includes the text "Last login on Thursday, 2014-06-26 at 13:20:21 PM from 192.168.100.2" and the SOURCE logo.

Распознавание приложений

- Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности
- FirePOWER for ASA распознает приложения, используемые в России:
VKontakte, Rambler, Yandex и т.д.

HTTP	Chrome	32.0.1700.102	Google		
HTTPS	SSL client		Google		
HTTPS	SSL client		Google APIs		
HTTP	Chrome	32.0.1700.102	Google Analytics		
HTTP	Firefox	26.0	Google Analytics		
HTTP	Firefox	26.0	Google Safebrowsing		
HTTPS	SSL client		Google+		
HTTPS	SSL client		Mozilla		
HTTP	Firefox	26.0	OCSF		
HTTP	Chrome	32.0.1700.102	Rambler		
HTTP	Firefox	26.0	Rambler		
HTTPS	SSL client		Rambler		
HTTPS	SSL client		Scorecard Research		
HTTPS	SSL client		ShareThis		
HTTP	Chrome	32.0.1700.102	Sourcefire.com		
HTTP	Chrome		twitter		
HTTPS	SSL client		twitter		
HTTP	Chrome	32.0.1700.102	VKontakte		
HTTPS	SSL client		WebEx		

Идентификация приложений «на лету»



Обнаружено нарушение политик безопасности: Попытка передачи файлов с хоста, использующего Skype. Пользователь идентифицирован, IT и HR уведомлены.

Блокирование передачи файлов через Skype

Editing Rule - Block Skype File Transfer

Name: Enabled Move

Action: IPS: no policies Variables: n/a Files: no inspection Logging: no logging

Zones Networks VLAN Tags Users **Applications** Ports URLs Inspection Logging Comments

Application Filters Clear All Filters Available Applications (9) Selected Applications and Filters (1)

Search by name

- User-Created Filters
 - Web Applications 1712
 - Application Protocols 851
 - Client Applications 452
- Risks (Any Selected)
 - Very Low 1048
 - Low 703
 - Medium 427
 - High 174
 - Very High 110
- Business Relevance (Any Selected)

skype

- All apps matching the filter
 - Skype
 - Skype Auth
 - Skype File Transfer
 - Skype Out
 - Skype p2p
 - Skype Probe
 - Skype Tunneling
 - Skype Video
 - Skype Voice

Add to Rule

Applications

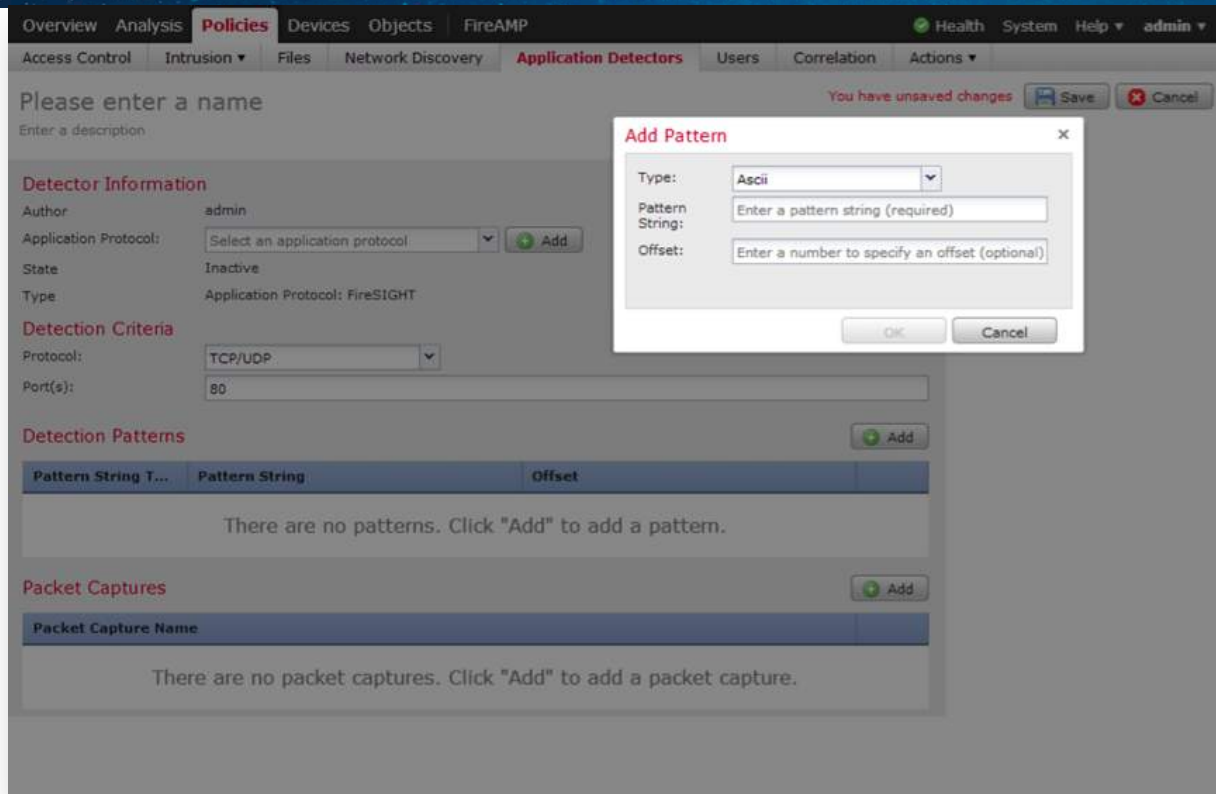
- Skype File Transfer

Save Cancel

Описание собственных приложений

Приложения могут быть описаны с помощью шаблонов следующих форматов:

- ASCII
- HEX
- PCAP-файл



The screenshot displays the Cisco FireAMP interface for configuring application detectors. The main window is titled 'Please enter a name' and contains several sections: 'Detector Information', 'Detection Criteria', 'Detection Patterns', and 'Packet Captures'. A modal dialog box titled 'Add Pattern' is open, allowing the user to specify the type of pattern (ASCII, Hex, or PCAP), the pattern string, and an optional offset. The 'Type' dropdown is currently set to 'Ascii'. The 'Pattern String' field is empty and labeled 'Enter a pattern string (required)'. The 'Offset' field is also empty and labeled 'Enter a number to specify an offset (optional)'. The 'Add' button is visible in the background interface.

Система предотвращения вторжений: Препроцессоры для отдельных протоколов

- DCE/RPC
- DNS
- FTP и Telnet
- HTTP
- Sun RPC
- SIP
- GTP
- IMAP
- POP
- SMTP
- SSH
- SSL
- Modbus / DNP3

The screenshot displays the Cisco FireAMP management interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, and FireAMP. The 'Policies' tab is active, showing a breadcrumb trail: Access Control > Intrusion > Intrusion Policy > Files > Network Discovery > Application Detectors > Users > Correlation > Actions. The main content area is titled 'Edit Policy: Inline-Security-Policy'. On the left, a sidebar lists configuration categories: Policy Information, Variables, Rules, FireSIGHT Recommendations, and Advanced Settings. Under Advanced Settings, several protocol-specific configuration options are listed, with red arrows pointing to 'DCE/RPC Configuration', 'GTP Command Channel Configuration', 'HTTP Configuration', 'Modbus Configuration', and 'SIP Configuration'. The 'HTTP Configuration' section is currently selected and expanded, showing various settings such as 'Consecutive Small Chunks' (set to 5), 'HTTP Methods' (CONNECT, DELETE, HEAD, OPTIONS, PUT, TRACE), and checkboxes for 'No Alerts', 'Normalize HTTP Headers', 'Inspect HTTP Cookies', 'Normalize Cookies in HTTP Headers', 'Allow HTTP Proxy Use', 'Inspect URI Only', 'Inspect HTTP Responses', 'Normalize UTF Encodings to UTF-8', 'Inspect Compressed Data', 'Unlimited Decompression', 'Normalize JavaScript', 'Extract Original Client IP Address', 'Log URI', 'Log Hostname', and 'Profile' (set to All). A 'Revert to Defaults' button is located at the bottom of the configuration area.

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 Configurati
 - FTP and Telnet Configur
 - Global Rule Thresholdin
 - GTP Command Channel
 - HTTP Configuration

Rules

- Rule Configuration
- Rule Content
- Category
- Classifications
- Microsoft Vulnerabilities**
 - MS00-006
 - MS00-019
 - MS00-021
 - MS00-025
 - MS00-028
 - MS00-031**
 - MS00-040
 - MS00-044
 - MS00-049
 - MS00-060
 - MS00-063
 - MS00-075
 - MS00-078
 - MS00-082
 - MS00-085
 - MS00-092
 - MS00-094
- Microsoft Worms
- Platform Specific
- Preprocessors
- Priority
- Rule Update

Filter: MicrosoftVulnerabilities:"MS00-031" Filter returned 1 result

Rule State
 Event Filtering
 Dynamic State
 Alerting
 Comments

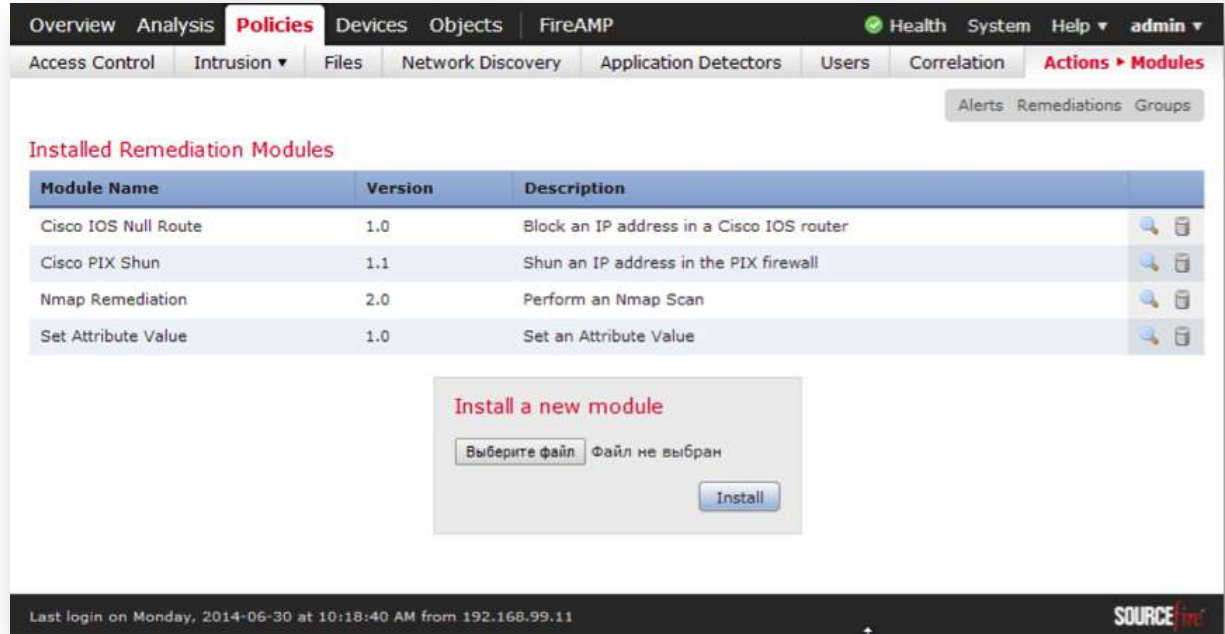
GID	SID	Message
1	1021	SERVER-IIS ism.dll attempt

Hide details 1 of 1








Case of Attack	Simple. No exploit software required.
False Positives	None Known
False Negatives	None known
Corrective Action	Check server logs for signs of compromise.
Contributors	Original rule writer unknown Original document author unknow Sourcefire Vulnerability Research Team Nigel Houghton <nigel.houghton@sourcefire.com>
References	<ul style="list-style-type: none"> Bugtraq page Common Vulnerabilities and Exposures Page Nessus Page Microsoft security bulletin
SRU	Sourcefire Rule Update 2013 06 17 001 vrt

Реагирование на события

- Запуск сканирования NMAP с заданными параметрами на источник/направление атаки;
- Блокировка нарушителя на маршрутизаторе Cisco (RTBH);
- Блокировка нарушителя на МСЭ Cisco ASA;
- Установка необходимого атрибута на хост;
- Уведомление администратора посредством Email/SNMP/Syslog;
- Выполнение самописной программы, написанной на C, BASH, TCSH, Perl, с возможностью передачи переменных из события.



The screenshot displays the Cisco FireAMP web interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, and FireAMP. Below this are sub-tabs for Access Control, Intrusion, Files, Network Discovery, Application Detectors, Users, Correlation, and Actions > Modules. A secondary bar contains Alerts, Remediations, and Groups. The main content area is titled 'Installed Remediation Modules' and contains a table with the following data:

Module Name	Version	Description	
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router	 
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall	 
Nmap Remediation	2.0	Perform an Nmap Scan	 
Set Attribute Value	1.0	Set an Attribute Value	 

Below the table is a dialog box titled 'Install a new module'. It contains a text input field with the placeholder 'Выберите файл' (Select file) and the text 'Файл не выбран' (File not selected). An 'Install' button is located at the bottom right of the dialog. At the bottom of the interface, a status bar shows 'Last login on Monday, 2014-06-30 at 10:18:40 AM from 192.168.99.11' and the SOURCEfire logo.

Фильтрация URL

Editing Rule - Web Block List

The screenshot displays the 'Editing Rule - Web Block List' configuration window. At the top, the rule name is 'Web Block List', it is 'Enabled', and the action is set to 'Block'. Below this are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Services', 'URLs', 'Policy', 'Logging', and 'Comments'. The 'URLs' tab is active, showing three main sections: 'Categories and URLs', 'Reputations', and 'Selected URLs'.
1. 'Categories and URLs': A search bar 'Search by name or value' is at the top. Below it is a list of categories including 'Any', 'Abortion', 'Abused Drugs', 'Adult and Pornography', 'Alcohol and Tobacco', 'Auctions', 'Bot Nets', 'Business and Economy', 'CDNs', 'Computer and Internet Info', and 'Computer and Internet Security'.
2. 'Reputations': A list of risk levels from 1 to 5: 'Any', '5 - Well known', '4 - Benign sites', '3 - Benign sites with security risks', '2 - Suspicious sites', and '1 - High risk'. An 'Add to Rule' button with a green arrow is positioned between this list and the 'Selected URLs' list.
3. 'Selected URLs': A list of selected categories with checkboxes and copy icons, including 'Adult and Pornography (Any Reputation)', 'Bot Nets (Any Reputation)', 'Confirmed SPAM Sources (Any Reputation)', 'Gambling (Any Reputation)', 'Keyloggers and Monitoring (Any Reputation)', 'Malware Sites (Any Reputation)', 'Marijuana (Any Reputation)', 'Nudity (Any Reputation)', 'Open HTTP Proxies (Any Reputation)', 'Parked Domains (Any Reputation)', and 'Pay to Surf (Any Reputation)'. Below this list is an 'Enter URL' input field and an 'Add' button.
At the bottom right of the window are 'Save' and 'Cancel' buttons.

Различные категории URL
URLs категорированы по уровню рисков

Контроль по типам файлов и направлению передачи

Add File Rule

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

File Type Categories

<input type="checkbox"/>	Office Documents	7
<input type="checkbox"/>	Archive	1
<input type="checkbox"/>	Multimedia	1
<input checked="" type="checkbox"/>	Executables	2
<input type="checkbox"/>	PDF files	1
<input type="checkbox"/>	Encoded	0
<input type="checkbox"/>	Graphics	0
<input type="checkbox"/>	System files	0

File Types

Search name and description

- All types in selected Categories
- MSEXE
- JARPACK




















Selected File Categories and Types

- MSEXE
- JARPACK

Buttons: Add, Save, Cancel

Геолокация и визуализация местонахождения атакующих



Initiator IP	Initiator Location	Responder IP
 76.100.209.66	 USA	 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.10.131		 10.4.32.112
 10.4.33.95		 10.5.32.206
 89.188.101.82	 ISR	 10.5.32.206
 200.189.215.85	 BRA	 10.4.33.44
 10.4.31.237		 10.5.32.206
 10.4.11.216		 10.5.39.206

Визуализация карт, стран и городов для событий и узлов

Детальная геолокация

- IP –адреса должны быть маршрутизируемыми
- Два типа геолокационных данных
 - Страна – включено по умолчанию
 - Full – Может быть загружено после установки:
 - Почтовый индекс, координаты, TZ, ASN, ISP, организация, доменное имя и т.д.
 - Ссылки на карты (Google, Bing и другие)
- Страна сохраняется в запись о событии
 - Для источника & получателя

Geolocation for 94.236.27.33

Country	United Kingdom  (Europe)
Region	Lnd
City	London
Postal Code	wc2n 5
Latitude/Longitude	51.5073, -0.12601
Maps	   
Timezone	GMT:+0

▼ **Additional Information**

ASN	15395 (Uk Rackspace)
ISP	Cogent Communications
Home/Business	Business
Domain Name	hayward.co.uk
Connection Type	Broadband

«Черные списки»: как свои, так и централизованные

Blacklist (13)

- Global Blacklist (Any Zone) ❌
- Attackers (Any Zone) ❌
- Bogon (Any Zone) ❌
- Bots (Any Zone) ❌
- CnC (Any Zone) ❌
- Google-Monitor (Any Zone) ❌
- Google-Not (Any Zone) ❌
- Malware (Any Zone) ❌
- Open_proxy (Any Zone) ❌
- Open_relay (Any Zone) ❌
- Phishing (Any Zone) ❌
- Spam (Any Zone) ❌
- Tor_exit_node (Any Zone) ❌

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

Access Control Intrusion Files Network Discovery Application Detectors Users Correlation Actions

Inline Access Policy

LAB Access-policy for Inline installations

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

Available Objects Available Zones Whitelist (1) Blacklist (11)

Search by name or value

Any
External
Internal
Passive

Global Whitelist (Any Zone)

Global Blacklist (Any Zone) ❌
Attackers (Any Zone) ❌
Bogon (Any Zone) ❌
Bots (Any Zone) ❌
CnC (Any Zone) ❌
Malware (Any Zone) ❌
Open_proxy (Any Zone) ❌
Open_relay (Any Zone) ❌
Phishing (Any Zone) ❌
Spam (Any Zone) ❌
Suspicious (Any Zone) ❌

Attackers
Bogon
Bots
CnC
Malware
Open_proxy
Open_relay
Phishing
Spam
Suspicious
Tor_exit_node
Global Blacklist
Global Whitelist
Home-Network
Parents-Network

Add to Whitelist
Add to Blacklist

Last login on Friday, 2014-06-27 at 15:50:05 PM from 192.168.100.2

Создание «белых списков» / «списков соответствия»

- Разрешенные типы и версии ОС
- Разрешенные клиентские приложения
- Разрешенные Web-приложения
- Разрешенные протоколы транспортного и сетевого уровней
- Разрешенные адреса / диапазоны адресов
- И т.д.

The screenshot displays the Cisco FireAMP interface for configuring a 'White List'. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The secondary navigation bar shows 'Access Control', 'Intrusion', 'Files', 'Network Discovery', 'Application Detectors', 'Users', 'Correlation', and 'Actions'. The current page is 'Policy Management' > 'Rule Management' > 'White List' > 'Traffic Profiles'. The left sidebar shows a tree view with 'Client DHCP devices', 'Target Networks' (containing '192.168.99.0/25'), and 'Allowed Host Profiles' (containing 'Any Operating System', 'Apple Mac OS X 10.5, 10.6, 10.8, ...', 'Apple Mac OS X 10.9, Server 10.9', 'Apple IOS 5.1.1', 'Apple IOS 5.x, 6.x, 7.0, 7.0.2, ...', 'Apple IOS 7.1', 'Microsoft Windows 7', and 'Sony Playstation 2'). The main content area is titled 'Host Profile: Microsoft Windows 7' and contains the following configuration fields:

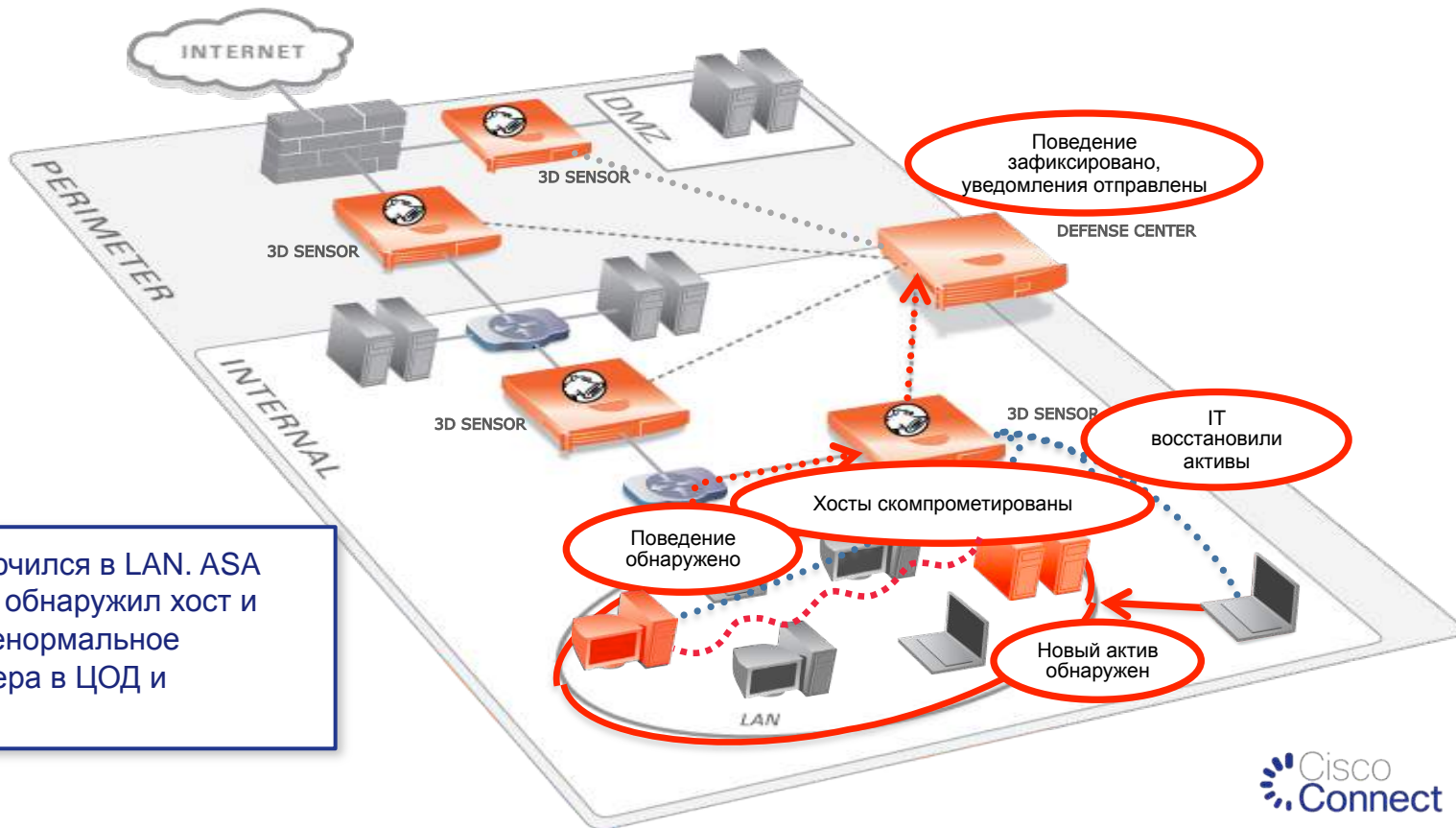
- Name: Microsoft Windows 7
- OS Vendor: Microsoft
- OS Name: Windows
- Version: 7

Below these fields are three expandable sections:

- Allowed Application Protocols:** No Application Protocols are allowed. Allow all Application Protocols.
- Allowed Clients:** A list of clients including BITS, Firefox, Jabber, Microsoft CryptoAPI, RDP, SSL client, and Windows Update.
- Allowed Web Applications:** A list of web applications including Cisco and Doubleclick.

At the bottom of the left sidebar, there are 'Save White List' and 'Cancel' buttons.

Обнаружение «посторонних» / аномалий / несоответствий



Новый хост включился в LAN. ASA with FirePOWER обнаружил хост и последующее ненормальное поведение сервера в ЦОД и уведомил IT.

Инвентаризация и профилирование узлов

- Профиль хоста включает всю необходимую для анализа информацию
 - IP-, NetBIOS-, MAC-адреса
 - Операционная система
 - Используемые приложения
 - Зарегистрированные пользователи
 - И т.д.
- Идентификация и профилирование мобильных устройств

The screenshot displays the FireAMP interface with the 'Hosts' tab selected. The left sidebar shows a tree view of hosts, including a list of IP addresses under 'Hosts [IPv4] (26)'. The main content area shows the 'Host Profile' for IP address 192.168.99.16, detailing its NetBIOS name, device hops, MAC addresses, host type, and last seen time. Below this, the 'Operating System' section identifies the host as a Google Android 4.0.3. The 'Servers (2)' section lists active connections for protocols like HTTP and SSH. The 'User History' section shows a user named 'Yi Lu (ylu, LDAP)' active on 2012-07-05 and 2012-07-06.

Vendor	Product	Version	Source
Google	Android	4.0.3	FireSIGHT

Protocol	Port	Application Protocol	Vendor and Version
tcp	443	HTTP	
tcp	22	SSH	OpenSSH 5.3

Users	2012-07-05 18:49:06	2012-07-06 18:49:06
Yi Lu (ylu, LDAP)		

Профилирование трафика

- Профиль трафика может включать до 30 параметров соединения:
 - IP-, NetBIOS-, MAC-адреса
 - Сетевой протокол
 - Транспортный протокол
 - Прикладной протокол
 - И т.д.
- Позволяет устанавливать флаги состояний и т.д.

The screenshot displays the Cisco FireAMP web interface for configuring a traffic profile. The navigation menu includes Overview, Analysis, Policies, Devices, Objects, and FireAMP. The main menu has Access Control, Intrusion, Files, Network Discovery, Application Detectors, Users, Correlation, and Actions. The sub-menu includes Policy Management, Rule Management, White List, and Traffic Profiles.

Profile Information

Profile Name: My traffic profile, data leakage
Profile Description: Профиль трафика, утечка данных

Profile Conditions [Copy Settings](#)

Collect connection information for all traffic that matches the following conditions:

Initiator IP is in 192.168.0.0/16

OR

Application Protocol is Skype File Transfer

OR

Application Protocol is Google Talk File Exchange

Host Profile Qualification

Only collect connection information with the following properties:

Initiator Host Default White List is Compliant

Profile Options

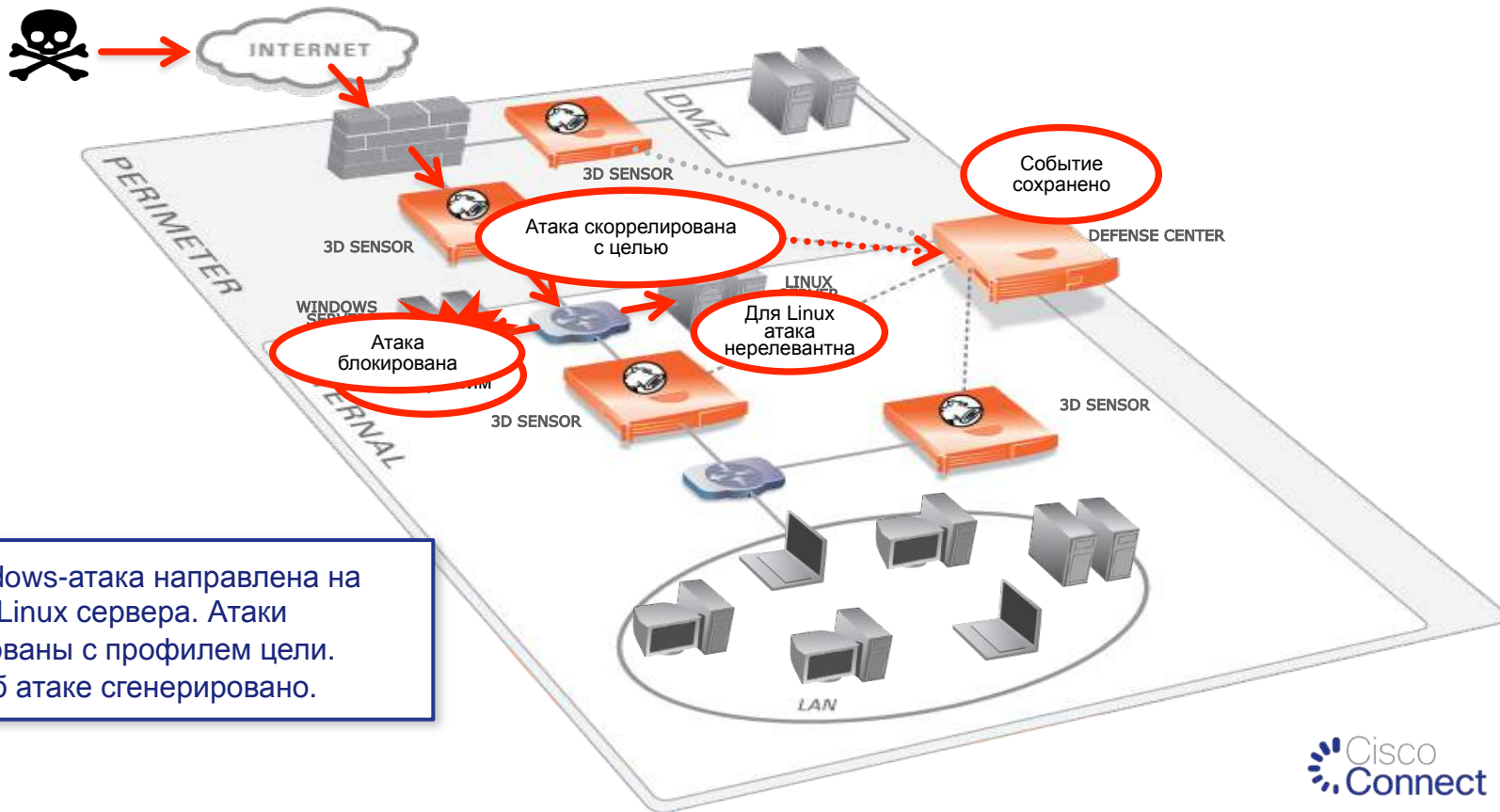
Profiling Time Window: Maintain data for this profile for the last 1 week(s)

Sampling Rate: Sample data every 05 minutes

Last login on Monday, 2014-06-30 at 13:59:42 PM from dkazakov-pc.ashes.cc

SOURCEfire

Встроенная корреляция событий безопасности



Новая Windows-атака направлена на Windows и Linux сервера. Атаки скоррелированы с профилем цели. Событие об атаке сгенерировано.

Автоматизированная, комплексная защита от угроз

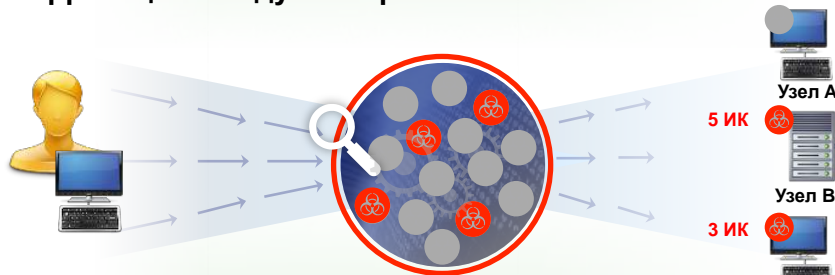
Максимальная защита во время всего жизненного цикла атаки

Корреляция между контекстом и угрозами



Оценка вредоносного воздействия

Корреляция между векторами атаки



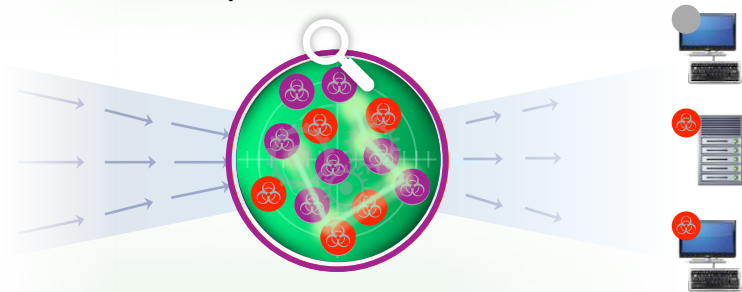
Раннее предупреждение о современных типах угроз

Динамические механизмы безопасности



Адаптация политик к рискам

Ретроспективная защита



Сокращение времени между обнаружением и нейтрализацией

Встроенная система корреляции событий

- Правила корреляции могут включать любые условия и их комбинации на базе идентифицированных в сети данных

- Приложения
- Уязвимости
- Протоколы
- Пользователи
- Операционные системы
- Производитель ОС
- Адреса
- Место в иерархии компании
- Статус узла и т.п.

Rule Information ➕ Add Connection Tracker

Rule Name: Critical phone Attacks
Rule Description: Attacks on Executives Android-based phones
Rule Group: Executive Attacks

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

➕ Add condition ➕ Add complex condition

✖ Impact Flag is 1 - red (Vulnerable)

AND

➕ Add condition ➕ Add complex condition

✖ Inline Result is not dropped

Host Profile Qualification ✖ Remove Host Profile Qualification

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

➕ Add condition ➕ Add complex condition

✖ Destination Host has the following properties:

- OS Vendor is Google
- OS Name is Android
- OS Version is any

✖ Destination Host is Jailbroken is Yes

User Identity Qualification ✖ Remove User Qualification

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

➕ Add condition ➕ Add complex condition

✖ Identity on Destination Department is Executives

Встроенная система корреляции событий

- Различные типы события для системы корреляции
 - Атаки / вторжение
 - Активность пользователя
 - Установлено соединение
 - Изменение профиля трафика
 - Вредоносный код
 - Изменение инвентаризационных данных (например, появление нового узла в сети или ОС на узле)
 - Изменение профиля узла
 - Появление новой уязвимости

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

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

Alerts Remediations Groups

Policy Management **Rule Management** White List Traffic Profiles

Rule Information

Rule Name

Rule Description

Rule Group

Select the type of event for this rule

If and it meets the following conditions:

Rule

Snooze generates an event, snooze for hours

Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Встроенная система корреляции событий

- В зависимости от типа события могут быть установлены дополнительные параметры системы корреляции
- Возможность создания **динамических** политик безопасности

Select the type of event for this rule

If a host input event occurs

+ Add condition

X

Rule Options

Snooze If this rule g

Inactive Periods There are no

a client is deleted

an address is deleted

an attribute value is deleted

an attribute value is set

a client is added

a client is deleted

host criticality is set

a host is added

an OS definition is set

a protocol is added

a protocol is deleted

a scan result is added

a server definition is set

a server is added

a server is deleted

a vulnerability is marked invalid

a vulnerability is marked valid

and it me

hours

inactive perio

Автоматизация создания и настройки политик

The screenshot displays a network security management interface. On the left, a window titled "Intrusion Events" shows a "Last 1 hour" view with a bar chart and a list of event categories (1-4 and All). On the right, a "Policy Information" dialog box is open, showing details for a policy named "Default Production Demo Lab IPS Policy".

Policy Information

Name: Default Production Demo Lab IPS Policy

Description: Sourcefire Provided. For best results, do not modify.

Drop when Inline:

Base Policy: Security Over Connectivity
The base policy is up to date (Rule Update 2013-10-09-004-vrt)

This policy defines 0 variables

This policy has 9038 enabled rules

- 558 rules generate events
- 8480 rules drop and generate events

FireSIGHT recommends 7154 rule state settings for 7430 hosts

- Set 214 rules to generate events
- Set 3550 rules to drop and generate events
- Set 3390 rules to disabled

Policy is not using the recommendations. Click to change recommendations

Last generated: 2013 Oct 10 10:15:33

Buttons: Commit Changes, Discard Changes

Анализ сети, протоколов, приложений, сервисов, устройств, ОС, уязвимостей и др. позволяет автоматизировать создание политик и правил МСЭ и IPS

Оценка вредоносного воздействия



Каждой попытке вторжения или событию присваивается уровень воздействия атаки на объект

УРОВЕНЬ ВОЗДЕЙСТВИЯ

ДЕЙСТВИЯ АДМИНИСТРАТОРА

ПРИЧИНЫ



1

Немедленно принять меры, опасность

Событие соответствует уязвимости, существующей на данном узле



2

Провести расследование, потенциальная опасность

Открыт соответствующий порт или используется соответствующий протокол, но уязвимости отсутствуют



3

Принять к сведению, опасности пока нет

Соответствующий порт закрыт, протокол не используется



4

Принять к сведению, неизвестный объект

Неизвестный узел в наблюдаемой сети



0

Принять к сведению, неизвестная сеть

Сеть, за которой не ведется наблюдение

Использование информации об уязвимостях

Users (no user history available)

Attributes ▾

Host Criticality None

Host Protocols ▾

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

Vulnerabilities (362) ▾

Name	Remote	Component
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability	Yes	Mac OS X 10.5, 10.6, Server 10.5, Server 10.6
Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability	Yes	Mac OS X 10.5, 10.6, Server 10.5, Server 10.6
Adobe Flash Player and AIR (CVE-2009-1866) Stack Buffer Overflow Vulnerability	Yes	Mac OS X 10.5, 10.6, Server 10.5, Server 10.6

Vulnerability Detail

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
CVE ID	2009-1862
Title	Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Impact Qualification	Enabled ▾
Date Published	2009-07-21
Vulnerability Impact	8
Remote	TRUE
Available Exploits	
Description	Multiple Adobe products are prone to a remote code-execution vulnerability.
Technical Description	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

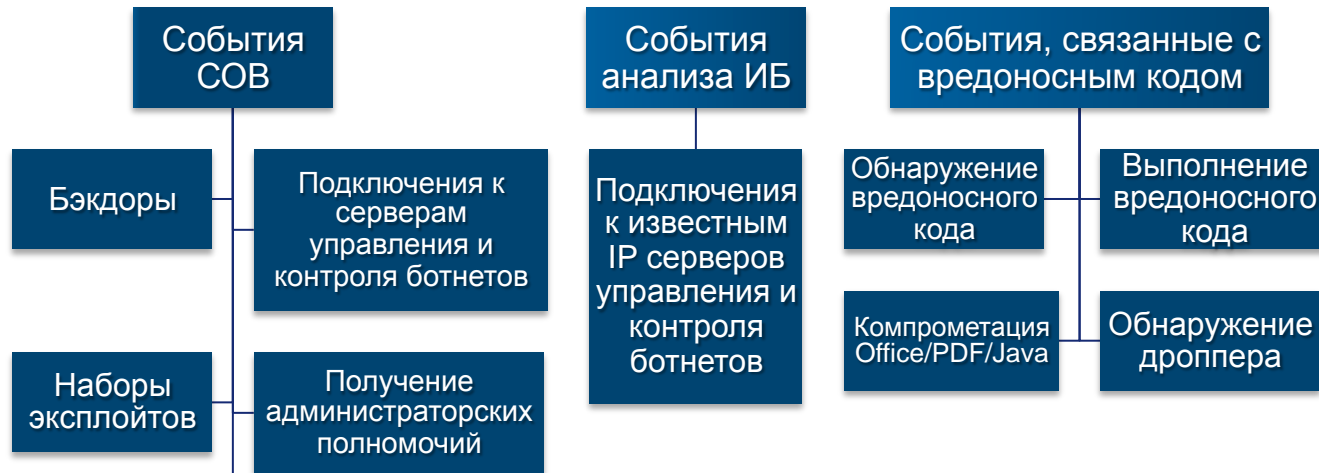
Updates are available. Please see the references for details.

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	Intel Download
Patch SecUpd2009-005PPC.dmg	PPC Download

Признаки компрометации



Indications of Compromise (3)

Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Анализ траектории движения вредоносных программ



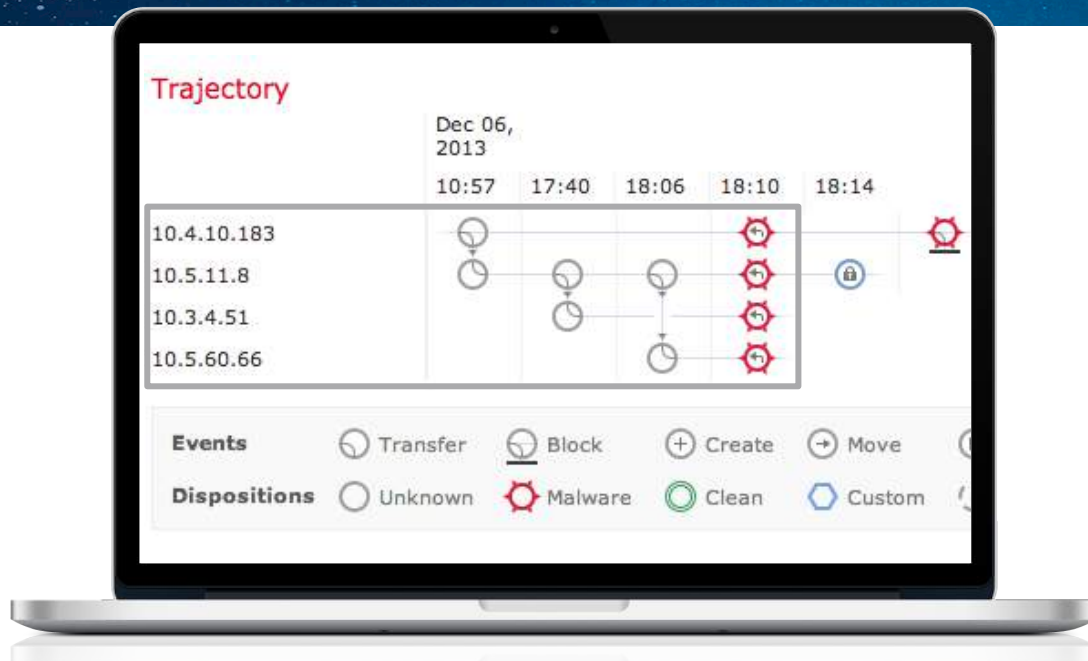
Сеть



Конечные
устройства



Контент



- Сетевая платформа использует признаки компрометации, анализ файлов и траекторию движения файла для того, чтобы показать, как вредоносный файл перемещается по сети, откуда он появился, что стало причиной его появления и кто еще пострадал от него

Обнаружение вредоносного кода с помощью AMP

Фильтрация по репутации

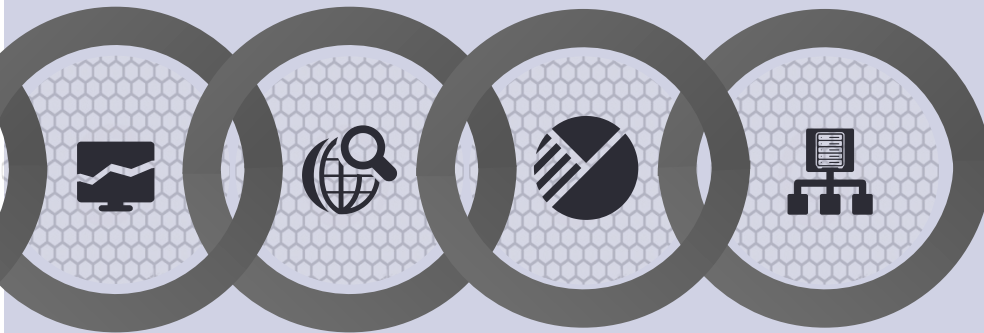


Идентичная
сигнатура

Нечеткие
идентифицирующие
метки

Машинное
обучение

Поведенческое обнаружение



Признаки
компрометации

Динамический
анализ

Расширенная
аналитика

Сопоставление
поточков данных с
устройств

Блокирование вредоносного кода

Bad Guys

The screenshot shows the Cisco FireAMP interface for configuring a file policy. The main window is titled "My File Policy" and is in the "Rules" tab. It shows a table with columns for File Types, Application Protocol, Direction, and Action. The current rule is set to "Any" for both Application Protocol and Direction, with the action "Block Malware with Reset".

An "Edit File Rule" dialog box is open, showing the following configuration:

- Application Protocol: Any
- Direction of Transfer: Any
- Action: Block Malware
- Selected actions: Spero Analysis for MSEXE, Dynamic Analysis, Reset Connection
- Store Files: Malware (checked), Unknown, Clean, Custom
- File Type Categories (left): System files (1), Graphics (0), Encoded (0), PDF files (1), Executables (6), Multimedia (2), Archive (17), Office Documents (16), Dynamic Analysis Capable (1)
- File Types (middle): Search name and description, 7Z (7-Zip compressed file), ACCDB (Microsoft Access 2007 file), ARJ (Compressed archive file), BINARY_DATA (Universal Binary/3), BINHEX (Macintosh BinHex 4 Com), BZ (bzip2 compressed archive), CPIO_CRC (Archive created with t), CPIO_NEWC (Archive created with t), CPIO_ODC (Archive created with t)
- Selected File Categories and Types (right): Category: Dynamic Analysis Capable, Category: Office Documents, Category: Archive, Category: Multimedia, Category: Executables, Category: PDF files, Category: Encoded, Category: Graphics, Category: System files

Buttons for "Save" and "Cancel" are visible at the bottom of the dialog box.

Last login on Friday, 2014-06-27 at 16:41:02 PM from 192.168.100.2

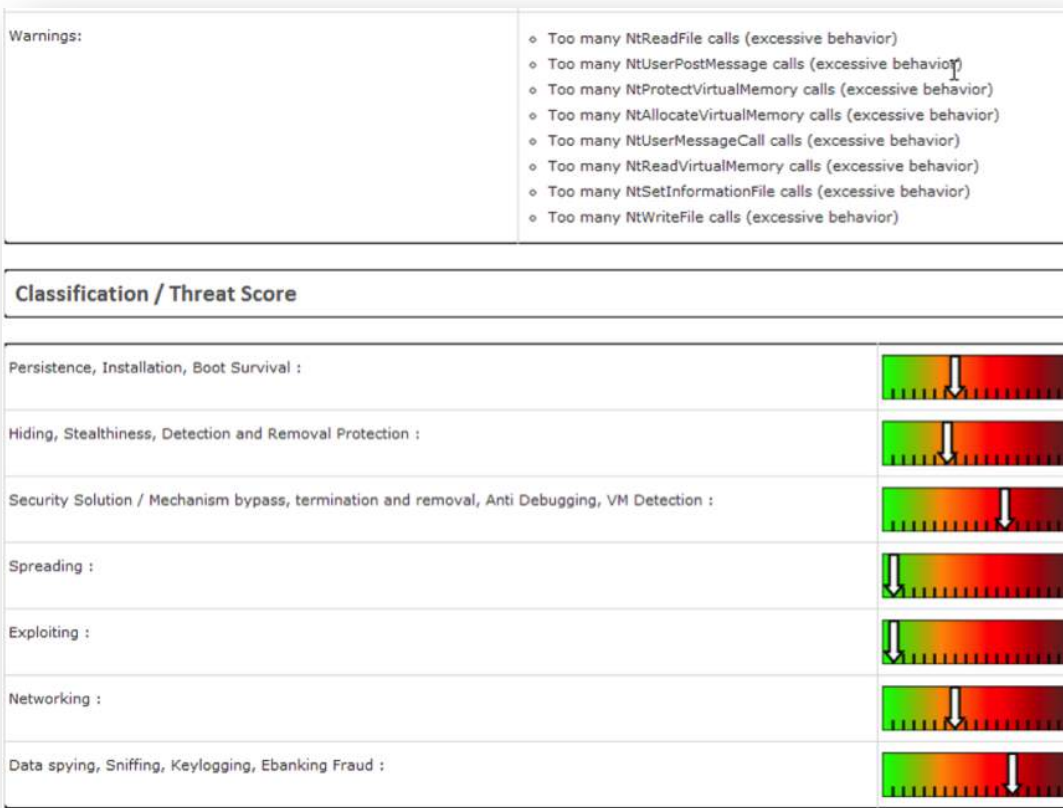
Обнаружение известного вредоносного кода

Bad Guys

Context Explorer	Connections	Intrusions	Files	Hosts	Users	Vulnerabilities	Correlation	Custom
			Boonex.exe	4c136a95...271b4828		MSEXE	2	
W32.Trojan.Breach.VRT			skunk-straddling.pdf	f02e1bb1...3b483a04		PDF	1	
W32.Trojan.Breach.VRT			repair-cadets.pdf	f02e1bb1...3b483a04		PDF	1	
W32.Trojan.Breach.VRT			ankles-bushiest.pdf	f02e1bb1...3b483a04		PDF	1	
W32.Spy:Malwaregen.17db.1201			Weelsof.exe	e32ecc71...881078ce		MSEXE	1	
W32.Spy:Malwaregen.17db.1201			IRCBot.exe	e32ecc71...881078ce		MSEXE	1	
W32.Spy:Malwaregen.17db.1201			InternetAntivirus.exe	e32ecc71...881078ce		MSEXE	1	
W32.Spy:Malwaregen.17db.1201			Dofoil.exe	e32ecc71...881078ce		MSEXE	1	
W32.Banker:Spy.16hi.1201			Korgo.exe	b73b0e49...b67c0409		MSEXE	1	
W32.Banker:Spy.16hi.1201			Hacker_Defender.exe	b73b0e49...b67c0409		MSEXE	1	
W32.8BBFF65DB8-100.SBX.VIOC			Helompy.exe	8bbff65d...75dc60d6		MSEXE	1	
W32.8BBFF65DB8-100.SBX.VIOC			Bofra.exe	8bbff65d...75dc60d6		MSEXE	1	
W32.7FF810938B-100.SBX.VIOC			Pramro.exe	7ff81093...293edc5c		MSEXE	1	
W32.7FF810938B-100.SBX.VIOC			Oficla.exe	7ff81093...293edc5c		MSEXE	1	
W32.7FF810938B-100.SBX.VIOC			Dishiqv.exe	7ff81093...293edc5c		MSEXE	1	
W32.7FF810938B-100.SBX.VIOC			Conhook.exe	7ff81093...293edc5c		MSEXE	1	
W32.7AF5A19B73-100.SBX.VIOC			Sefnit.exe	7af5a19b...5b44869b		MSEXE	1	
W32.7AF5A19B73-100.SBX.VIOC			Blat.exe	7af5a19b...5b44869b		MSEXE	1	

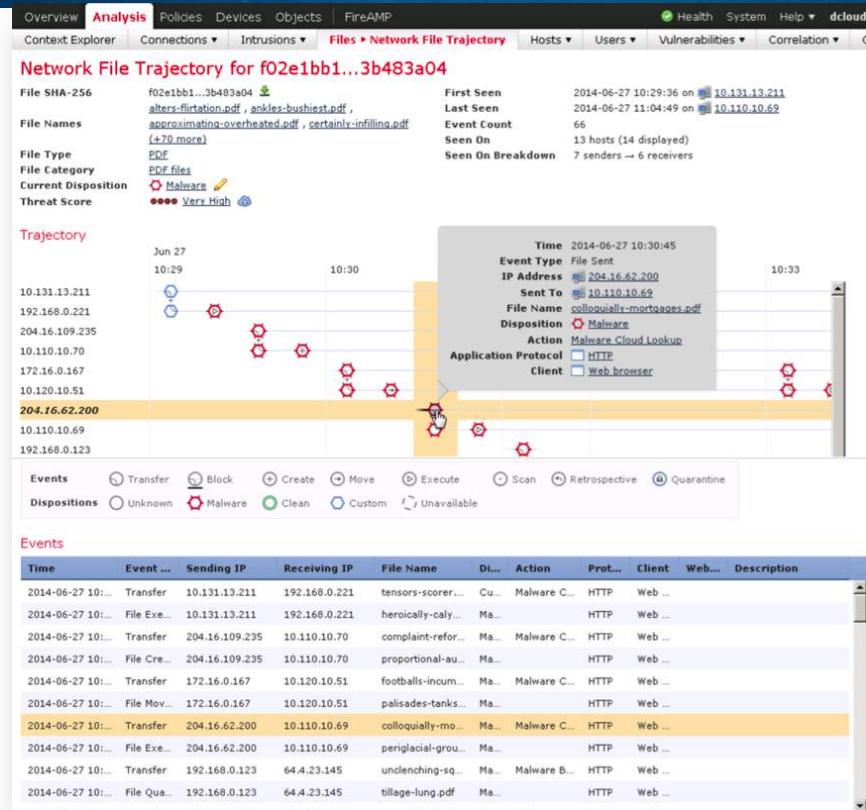
Если статус файла неизвестен, он отправляется в песочницу

Bad Guys



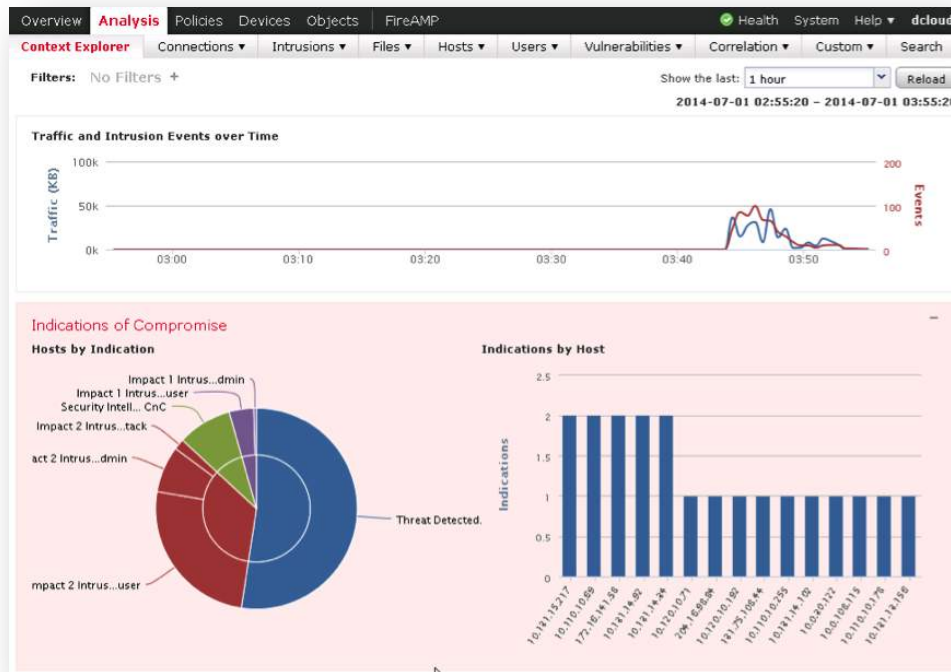
Анализ траектории вредоносного кода

- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс был отправной точкой?
- Почему это произошло?
- Когда это произошло?
- Что еще произошло?



Мониторинг общей информации о сети

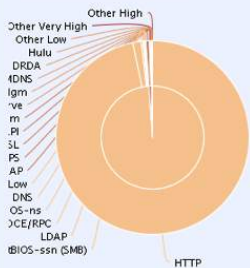
- Корреляция событий безопасности, трафика и вредоносного кода
- Активность конкретных пользователей и их приложений
- Используемые ОС и активность сетевого обмена
- Оценка событий по уровню воздействия и приоритета
- Статистика по вредоносному коду и зараженным файлам
- Геолокационные данные
- Категории сайтов и посещаемые URL



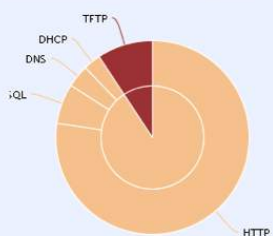
Мониторинг общей информации о сети

Application Protocol Information

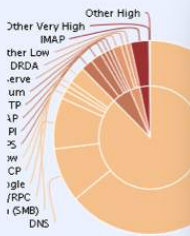
Traffic by Risk and Application



Intrusion Events by Risk and Application



Hosts by Risk and Application

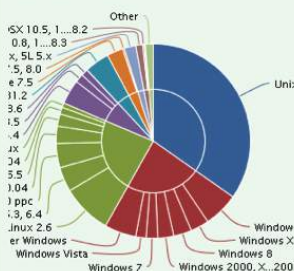


Application Details

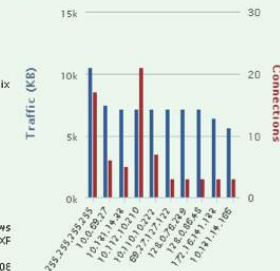
Application	Risk	Business Relevance	Category	Hosts
HTTP	Very Low	Medium	network protocols/services	915
DNS	Very Low	Very High	network protocols/services	129
NetBIOS-ssn (SMB)	Very Low	High	network protocols/services	122
IMAP	Very High	Medium	email	44
HTTPS	Medium	Medium	network protocols/services	28
MAPI	Medium	Very High	email	27
ARCServe	Low	Very High	network utilities, remote file st	22
DCE/RPC	Very Low	High	network protocols/services	20

Network Information

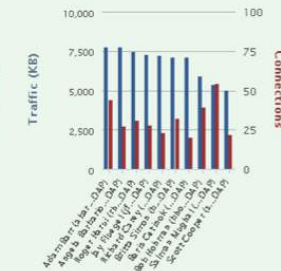
Operating Systems



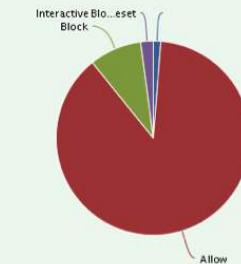
Traffic by Source IP



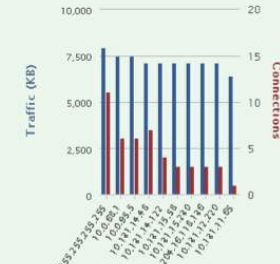
Traffic by Source User



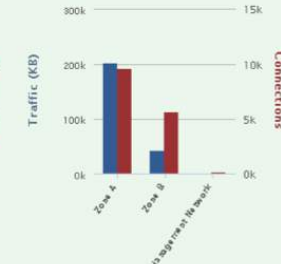
Connections by Access Control Action



Traffic by Destination IP

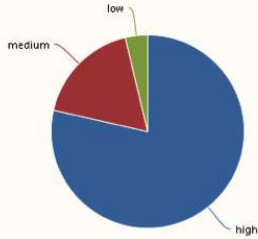


Traffic by Ingress Security Zone

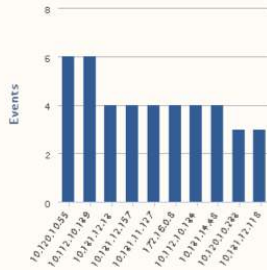


Мониторинг общей информации о сети

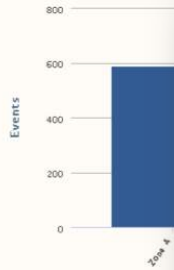
Intrusion Events by Priority



Top Targets



Top Ingress Security Zones

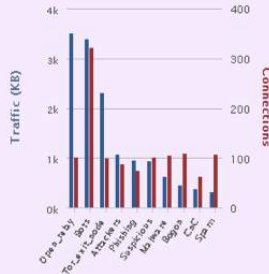


Intrusion Event Details

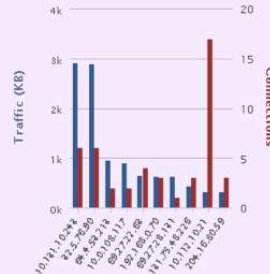
Event	Classification	Priority	Events
PROTOCOL-TFTP GET filename overflo	Attempted Administrator Privilege Gain	high	32
INDICATOR-SHELLCODE x86 OS agno	Executable Code was Detected	high	29
SERVER-OTHER Wireshark LWRES Dis	Attempted Denial of Service	medium	26
SERVER-WEBAPP OpenView Network	Attempted User Privilege Gain	high	14
OS-WINDOWS Microsoft Windows java	Attempted User Privilege Gain	high	14
SERVER-WEBAPP HP OpenView Netwo	Attempted User Privilege Gain	high	14
SERVER-MAIL Microsoft Windows Exch	Attempted Denial of Service	medium	13
SERVER-OTHER ISC BIND RRSIG quer	Attempted Denial of Service	medium	13

Security Intelligence

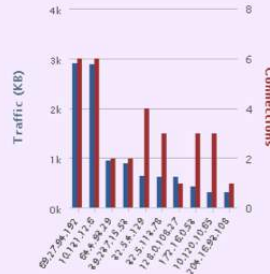
Security Intelligence Traffic by Category



Security Intelligence Traffic by Source IP

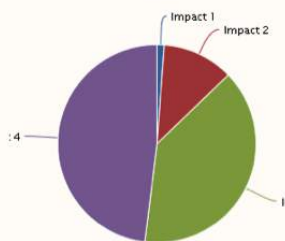


Security Intelligence Traffic by Destination IP

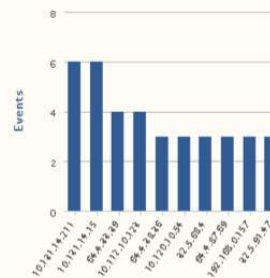


Intrusion Information

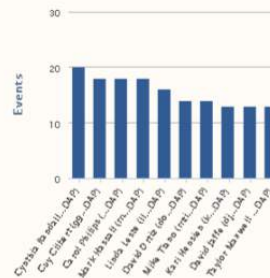
Intrusion Events by Impact



Top Attackers



Top Users



Intrusion Events by Priority

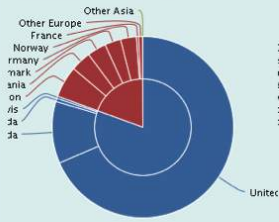
Top Targets

Top Ingress Security Zones

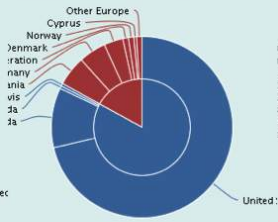
Мониторинг общей информации о сети

Geolocation Information

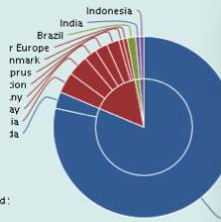
Connections by Initiator Country



Intrusion Events by Source Country

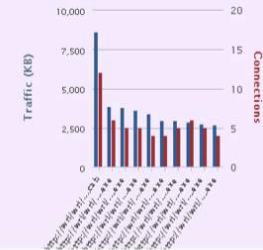


File Events by Sending Country

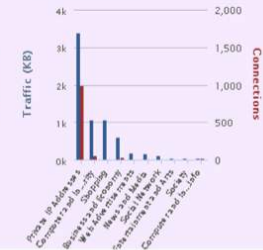


URL Information

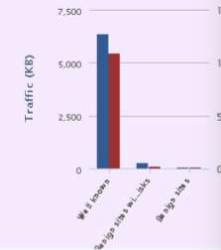
Traffic by URL



Traffic by URL Category



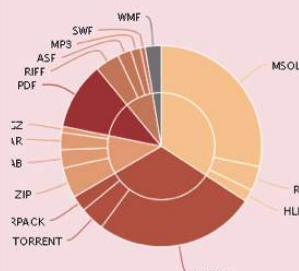
Traffic by URL Reputation



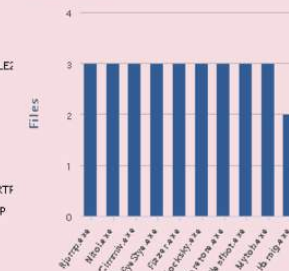
Last login on Tuesday, 2014-05-27 at 15:15:08 PM from 10.117.255.90

File Information

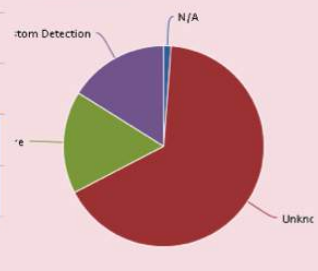
Top File Types



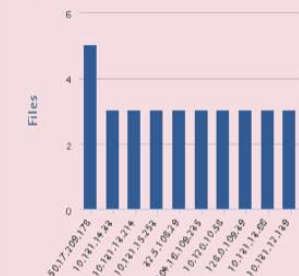
Top File Names



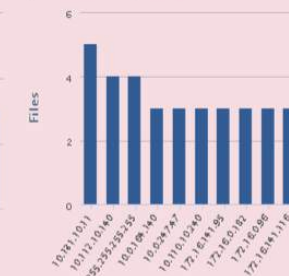
Files by Disposition



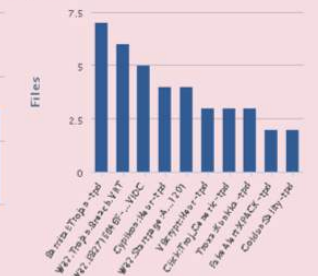
Top Hosts Sending Files



Top Hosts Receiving Files

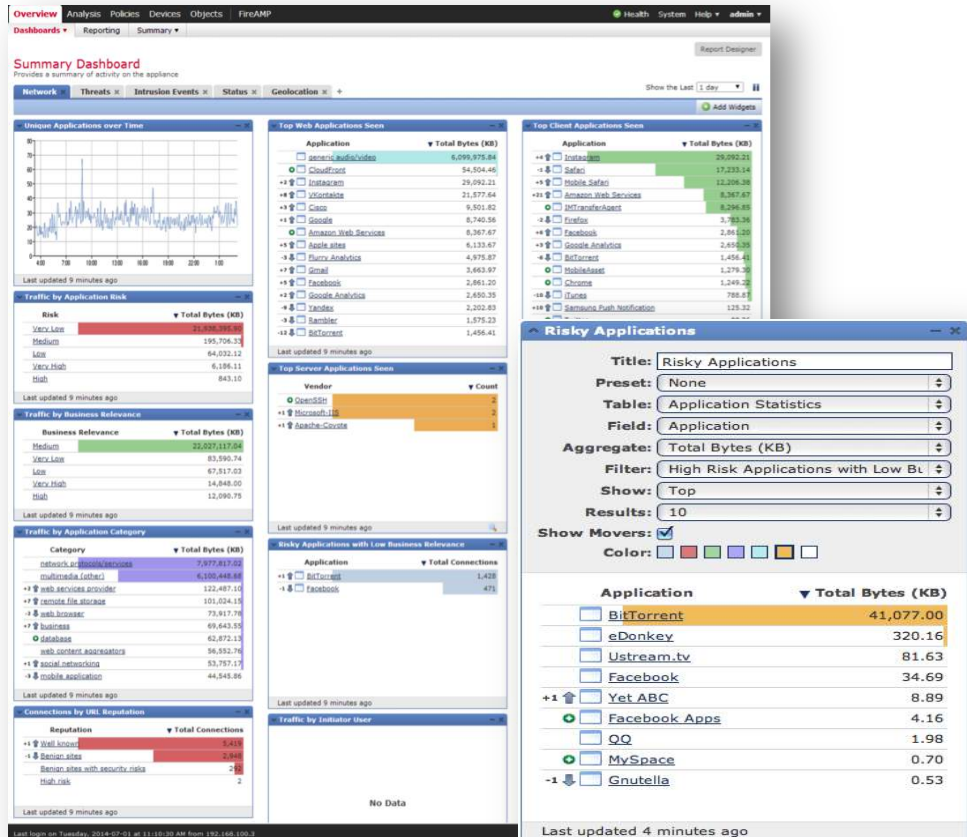


Top Malware Detections



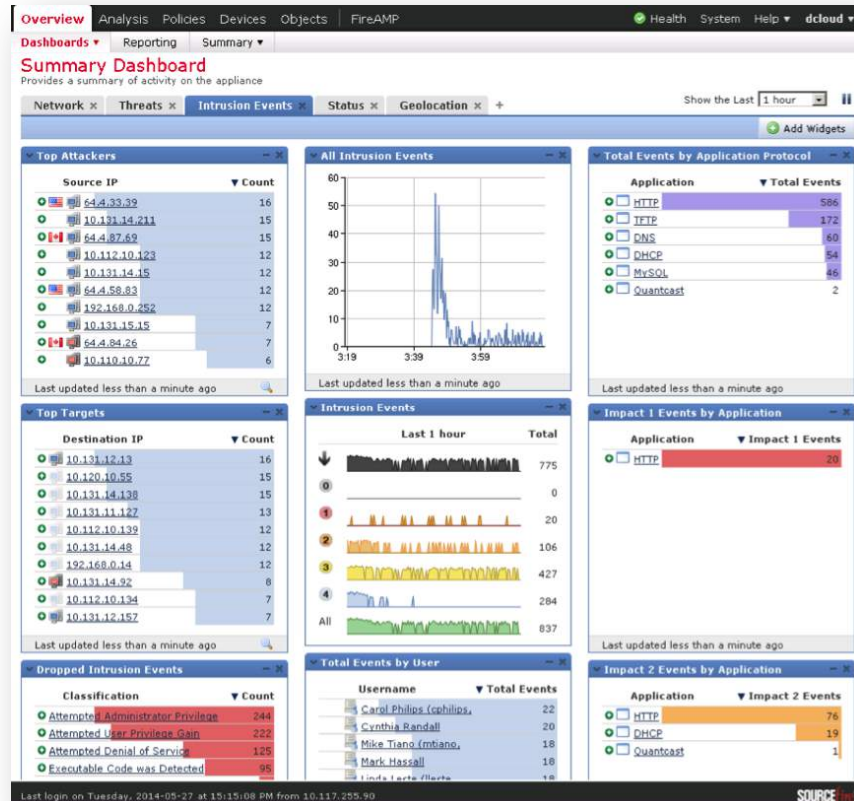
Мониторинг сетевых событий

- Использование сервисов
- Использование приложений
- Использование операционных систем
- Распределение соединений
- Активность пользователей
- Уязвимые узлы и приложения
- И т.д.



Мониторинг событий безопасности

- Основные нарушители
- Основные атаки
- Заблокированные атаки
- Основные цели
- Приоритет событий
- Уровень воздействия



Детализация событий безопасности

- Подробная информация о событии безопасности
- Возможность изменения правил реагирования
- Возможность тюнинга правила / сигнатуры
- Сетевой дамп

The screenshot displays the Cisco FireAMP web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The main menu shows 'Context Explorer', 'Connections', 'Intrusions', and 'Events'. The current view is 'Events By Priority and Classification' for the date range '2014-07-01 05:57:07 - 2014-07-01 06:57:21'. The event details are as follows:

Event	EXPLOIT Microsoft IIS ASP handling buffer overflow attempt (3:15974)
Timestamp	2014-07-01 06:02:05
Classification	Web Application Attack
Priority	high
Ingress Security Zone	Zone A
Device	198.18.133.11
Ingress Interface	eth1
Source IP	10.131.10.108
Source Port / ICMP Type	52914 / tcp
Destination IP	10.131.12.163
Destination Port / ICMP Code	80 (http) / tcp
Intrusion Policy	Cisco Security BG - Production Demo IPS Policy
Access Control Policy	Cisco Security BG - Production Demo AC Policy
Rule	alert top \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"EXPLOIT Microsoft IIS ASP handling buffer overflow attempt"; sid:15974; gid:3; rev:3; classtype:web-application-attack; reference:bugtraq,27676; reference:cve,2008-0075; reference:url,technet.microsoft.com/en-us/security/bulletin/ms08-006; metadata:engine shared, soid 3 15974, service http, policy balanced-ips drop, policy security-ips drop;)
Summary	This event is generated when an attempt is made to exploit a known vulnerability in Internet Information Server.

Actions

Rule Actions

- [Edit](#)
- [View Documentation](#)
- [Rule Comment](#)
- [Disable in current policy \(Cisco Security BG - Production Demo IPS Policy \)](#)
- [Set this rule to drop the triggering packet and generate an event in current inline intrusion policy \(Cisco Security BG - Production Demo IPS Policy \)](#)
- [Set this rule to generate events in all locally created policies](#)
- [Disable this rule in all locally created policies](#)
- [Set this rule to drop the triggering packet and generate an event in all locally created inline intrusion policies](#)

Set Thresholding Options

- ▶ in the current policy (Cisco Security BG - Production Demo IPS Policy)
- ▶ in all locally created policies

Set Suppression Options

- ▶ in the current policy (Cisco Security BG - Production Demo IPS Policy)
- ▶ in all locally created policies

Packet Information

FRAME 1 (Expand All)

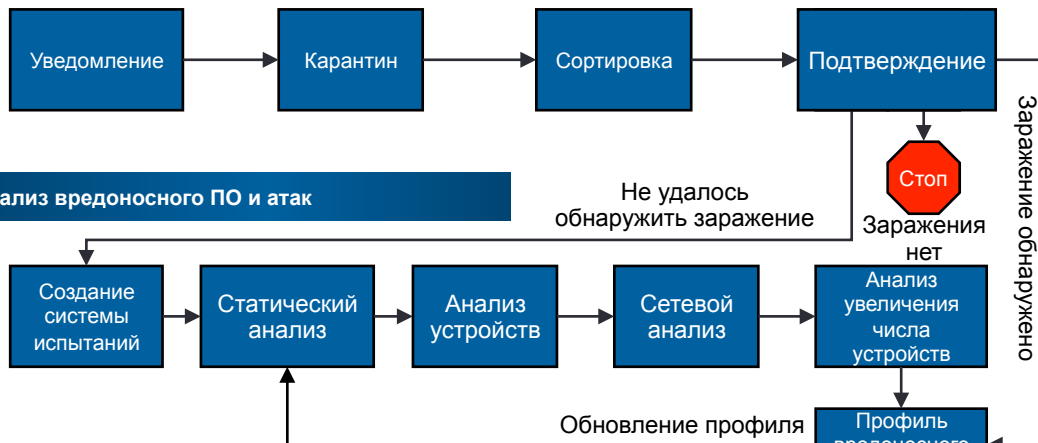
ASA с сервисами FirePOWER объединяет все вместе



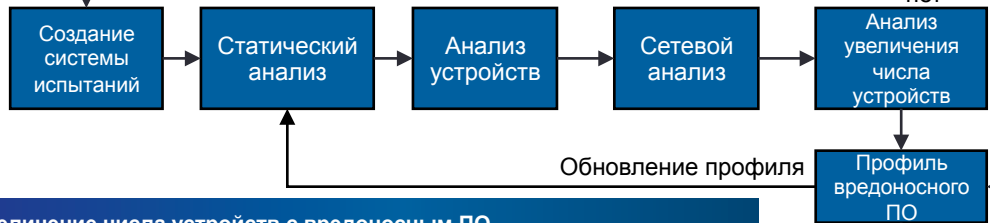
Вопрос не в том, произойдет ли заражение, а как скоро мы его обнаружим, устраним и поймем причины

- С чего начать?
- Насколько тяжела ситуация?
- Какие системы были затронуты?
- Какой ущерб нанесла угроза?
- Как можно восстановить?
- Как можно предотвратить ее повторение?

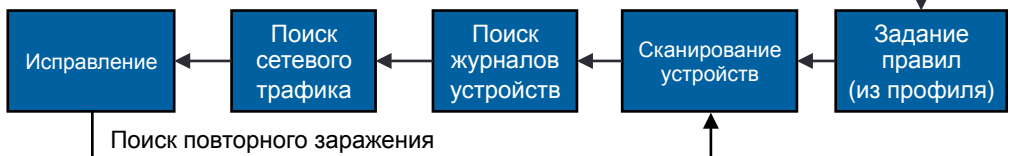
Подтверждение атаки и заражения



Анализ вредоносного ПО и атак



Увеличение числа устройств с вредоносным ПО



Объединяя все вместе, ASA с сервисами FirePOWER...

Все компоненты –
контрольные точки



Эл. почта



Оконечные устройства



Интернет



Сеть



Система
предотвращения
вторжений IPS



Устройства

Поток
телеметрических
данных



Идентифицирующие метки
и метаданные файла



Файловый и сетевой ввод/вывод



Информация о процессе

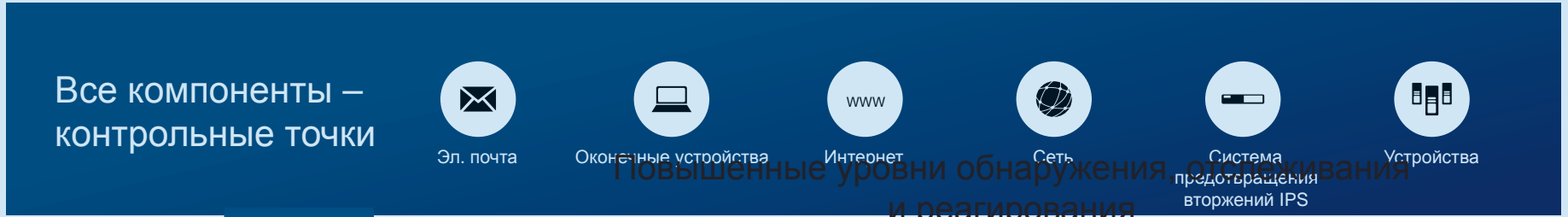
Непрерывная передача

000111010011101 1100001110001110 1001 1101 1110011 011001
001110 1001 1101 1110011 0110011 101000 0110 00 011100
01100001 1100 0111010011101 1100001110001110 1001 1101



Непрерывный анализ

...позволяет непрерывно анализировать широкий спектр угроз и реагировать на них...



...и даёт понимание того, что именно следует делать, чтобы решить проблему.



Кто



Сфокусируйтесь сначала на этих пользователях



Что



Эти приложения пострадали



Где



Взлом затронул эти области сети



Когда



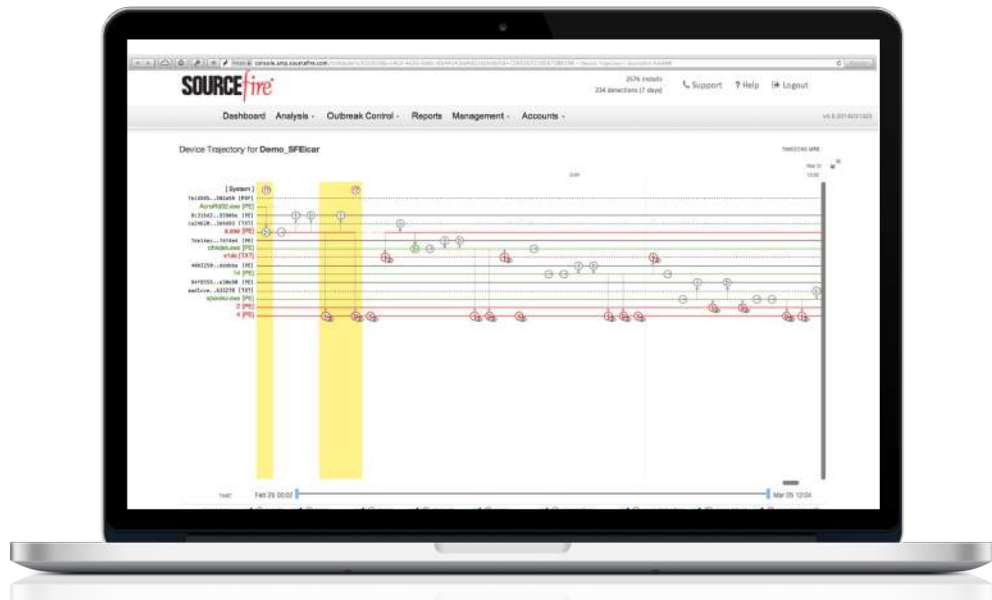
Такова картина атаки по времени



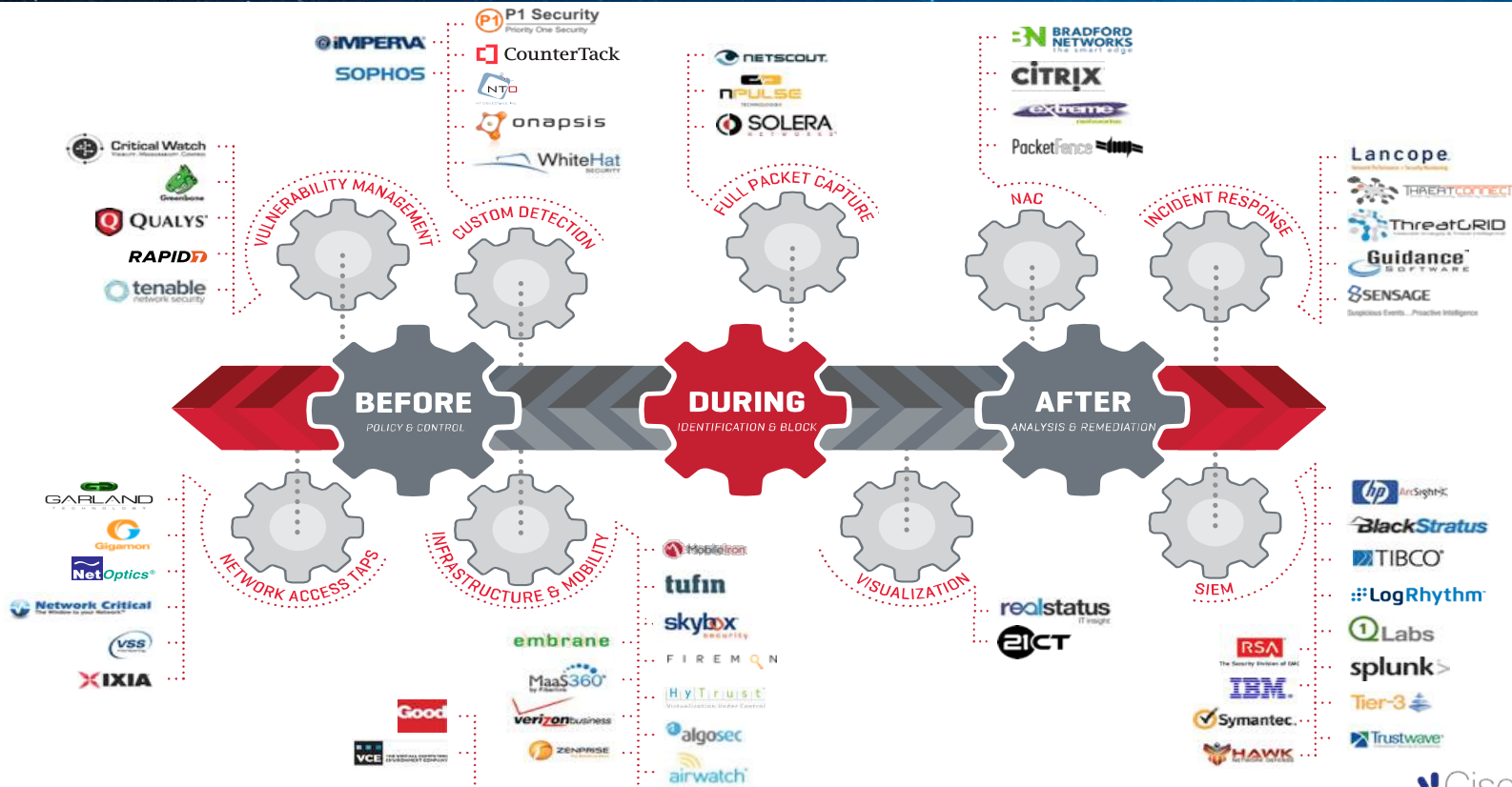
Как



Это источник угрозы и путь ее распространения



Экосистема Cisco ASA with FirePOWER



Варианты исполнения Cisco ASA with FirePOWER

FirePOWER Services for 5500-X
(ПО)



ASA 5512-X, 5515-X, 5525-X,
5545-X, 5555-X

FirePOWER Services for 5585-X
(модуль)

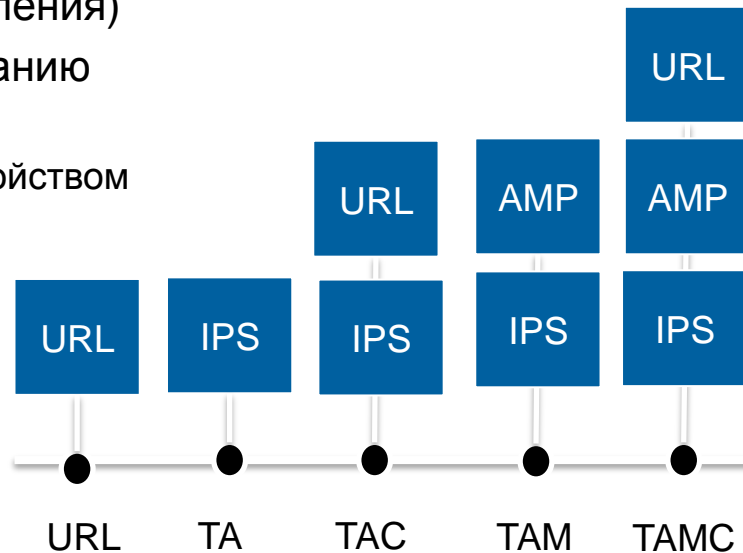


ASA 5585-X

Модульная функциональность

5 вариантов заказа защитных функций:

- Подписка на 1 или 3 года (включая обновления)
- Функция AVC (NGFW) включена по умолчанию
 - Активирует функции FirePOWER Services
 - Постоянная и поставляется вместе с устройством
- Обновления AVC включены в SMARTnet



Что используется для управления ASA с сервисами FirePower?

NetOPS Workflows - CSM 4.6/7 или ASDM-ASA-On-Box



FireAMP Connector (Управляется облачной FMC)

SecOPS Workflows - FireSIGHT Management Center

Управление NGFW/NGIPS

Forensics / Управление логами

Network AMP / Trajectory

Управление уязвимостями

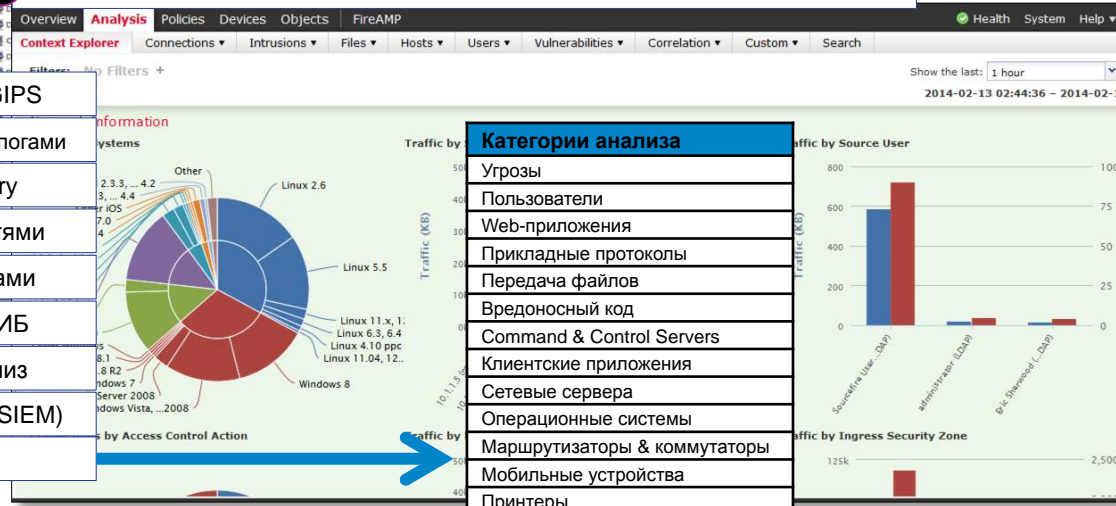
Управление инцидентами

Адаптивная политика ИБ

Ретроспективный анализ

Корреляция событий (SIEM)

Распознавание



Категории анализа

- Угрозы
- Пользователи
- Web-приложения
- Прикладные протоколы
- Передача файлов
- Вредоносный код
- Command & Control Servers
- Клиентские приложения
- Сетевые сервера
- Операционные системы
- Маршрутизаторы & коммутаторы
- Мобильные устройства
- Принтеры
- VoIP-телефоны
- Виртуальные машины

Cisco ASA с функциями FirePOWER

Реальная борьба с угрозами

Полная информация о происходящих в сети процессах

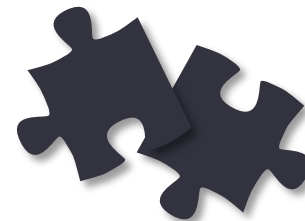
- ▶ Полная осведомленность о сетевом контексте для устранения уязвимостей

Комплексная защита от угроз

- ▶ Лучшая в своем классе многоуровневая защита в одном устройстве

Автоматизация

- ▶ Простота управления, динамическое реагирование и восстановление



«Поэтому сказано, что тот, кто знает врага и знает себя, не окажется в опасности и в ста сражениях. Тот, кто не знает врага, но знает себя, будет то побеждать, то проигрывать. Тот, кто не знает ни врага, ни себя, неизбежно будет разбит в каждом сражении.»

Сунь Цзы. Искусство войны.

Спасибо за внимание!
Пожалуйста, используйте код для оценки
доклада:

3345

Руслан Иванов
Системный инженер-консультант
+7 (495) 961-1467
ruivanov@cisco.com



CiscoRu



Cisco



CiscoRussia