



Title

# Передовые подходы к обеспечению эффективной защиты АСУ ТП в парадигме ИНДУСТРИЯ 4.0

Presenter

Станислав Бубнов

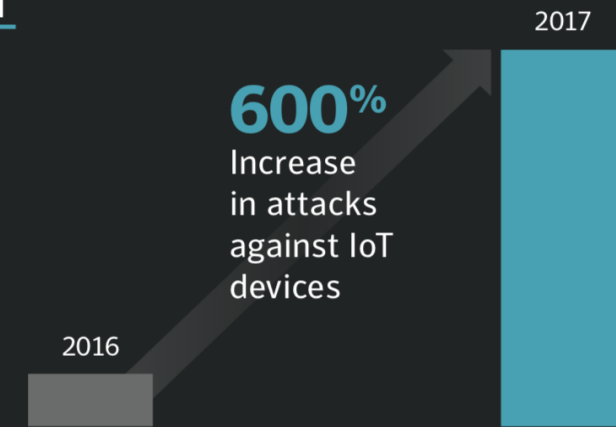
Date

18/10/2018

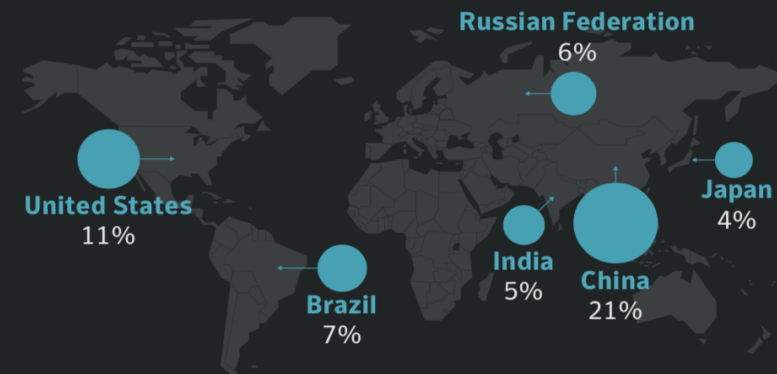
# ЦИФРОВЫЕ УГРОЗЫ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

1. Рост на 600% количества атак на IoT
2. Россия занимает лишь 4 место по количеству атак после Китая, США и Бразилии
3. Почти 50% атак на устройства Интернета Вещей имеют неизвестные ранее источники

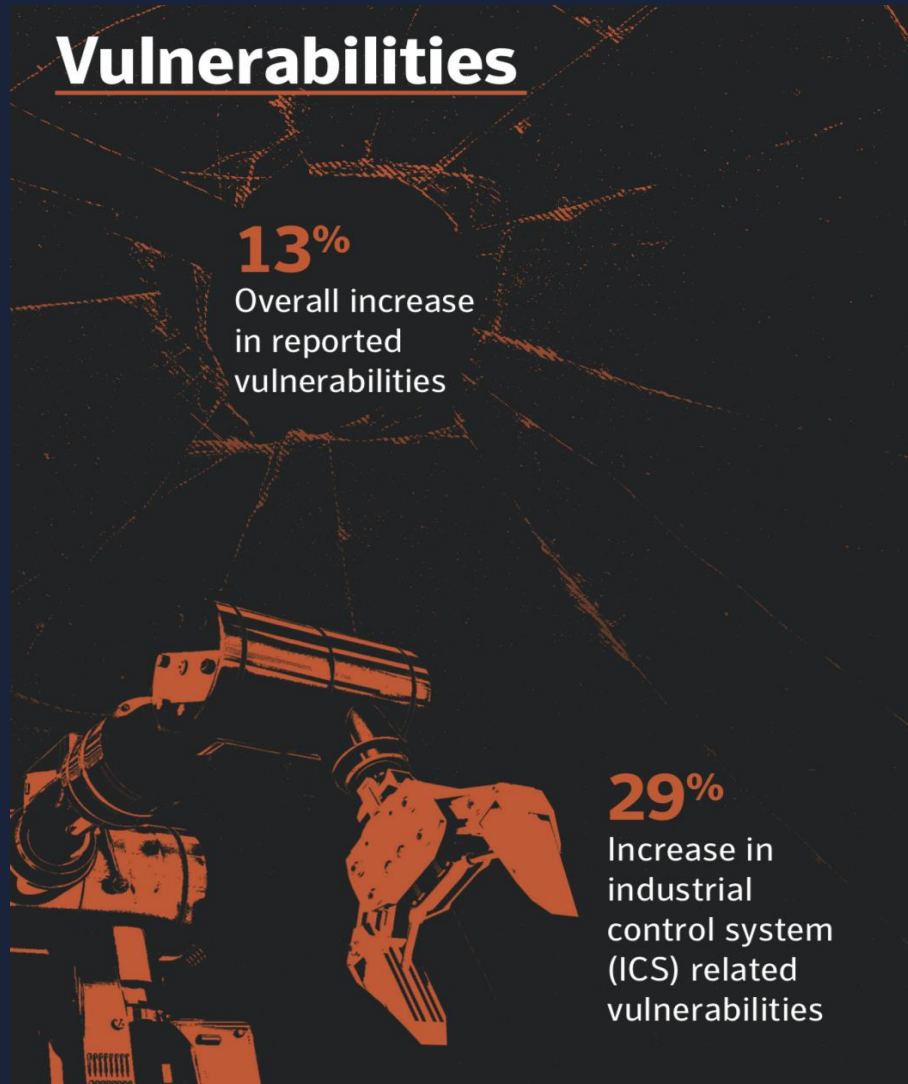
## IoT



## Attack Origin



# ЦИФРОВЫЕ УГРОЗЫ ДЛЯ ПРОИЗВОДСТВА



1. Рост количества уязвимого ПО и оборудования в 2017 году составил 13%
2. При этом рост числа уязвимостей в системах АСУ ТП составил 29%

# СТАТИСТИКА АТАК НА ИНТЕРНЕТ ВЕЩЕЙ (1)

## ТОП-10 АТАКУЮЩИХ СТРАН

Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

## ТОП-10 ПАРОЛЕЙ ДЛЯ АТАКИ

Rank	2017 Password	2017 Percent	2016 Password	2016 Percent
1	system	10.3	admin	9.5
2	sh	10.2	root	5.8
3	123456	9.1	12345	5
4	admin	3.7	123456	3.7
5	1234	3.1	password	3.2
6	password	2.5	1234	2.4
7	12345	2.5	ubnt	1.7
8		2.3	admin123	1
9	root	2.1	abc123	0.9
10	support	1.2	pass	0.7

# СТАТИСТИКА АТАК НА ИНТЕРНЕТ ВЕЩЕЙ (2)

ТОП-10 ИМЕН ПОЛЬЗОВАТЕЛЕЙ

Rank	2017 User Name	2017 Percent	2016 User Name	2016 Percent
1	root	40	root	33.5
2	admin	17.3	admin	14.1
3	enable	10.3	DUP root	6
4	shell	10.2	DUP admin	2.1
5	guest	1.5	ubnt	1.3
6	support	1.3	test	1.1
7	user	1.1	oracle	1.1
8	ubnt	0.9	postgres	0.7
9	DUP root	0.6		0.7
10	supervisor	0.5	123321	0.6

ТОП-10 ТИПОВ УСТРОЙСТВ

Rank	Device Type	Percent
1	Router	33.6
2	DVR (Digital Video Recorder)	23.2
3	Network	9.3
4	Satellite Dish	7.3
5	DSL/Cable Modem	7
6	SOHO Router	4.7
7	NAS (Network Attached Storage)	3.6
8	Camera	3.5
9	PLC (Programmable Logic Controller)	3.4
10	Alarm System	1.9

## ПОТЕНЦИАЛЬНЫЙ УРОН ОГРОМЕН В СИЛУ ВЫСОКОЙ ЗНАЧИМОСТИ ТАКИХ ЦЕЛЕЙ

- Удалённый контроль скважинных нефтяных насосов
- Система транспорта
- Энерготранспорт
- Газо- и нефтепроводы
- Водоочистка и её распределение
- Сбор и переработка сточных вод



# Атаки в кибер-реальном мире



Украинские энергосети были успешно атакованы за последние 2 года, последний раз с помощью Industroyer.

230,000  
Customers lost  
power<sup>1</sup>

30  
Substations  
Disconnected<sup>1</sup>

8  
Provinces  
Without  
Power<sup>1</sup>

Dragonfly 2.0

## Cyber Attacks on the Energy Sector

Группа DragonFly произвела ряд успешных атак на энергетический сектор США и ряда европейских стран

7  
Individual  
Toolsets

5+  
hacked  
websites

X  
Attacked  
Orgs.

## Профиль атаки

Суть атак очень просты. Используются врождённые уязвимости атакуемых систем :

- Старые ОС снятых с поддержки вендора
- Антивирусная защита не работает должным образом
- Сообщения протоколов операционных технологии

# Анатомия типовой атаки

1

.\*

2

wannacry

3

4

triton

stuxnet

industroyer

## Компрометация внутренних систем

- Взлом почты
- Watering Hole
- ПО с троянами
- Безфайловые атаки

## Переход к операционным технологиям

- Доступ к L2/L3 контроллерам
- Обычно через USB, сеть или иным способом
- Активность не привязана ко времени

## Доступ к PLC

- Логику можно перенастроить без идентификации
- Использование протокола против него же самого
- $f(X,Y)=z$

## Выгода

- Все под внешним управлением
- Устройства могут быть полностью отключены или изменены
- оповещения могут быть отключены

ICSP, CSP

CSP



# a **trusted** strategy.

**Rockwell  
Automation**

DAIMLER



**AMTRAK**



**Walmart**

**WELLS  
FARGO**

**Andersen**  
CORPORATION

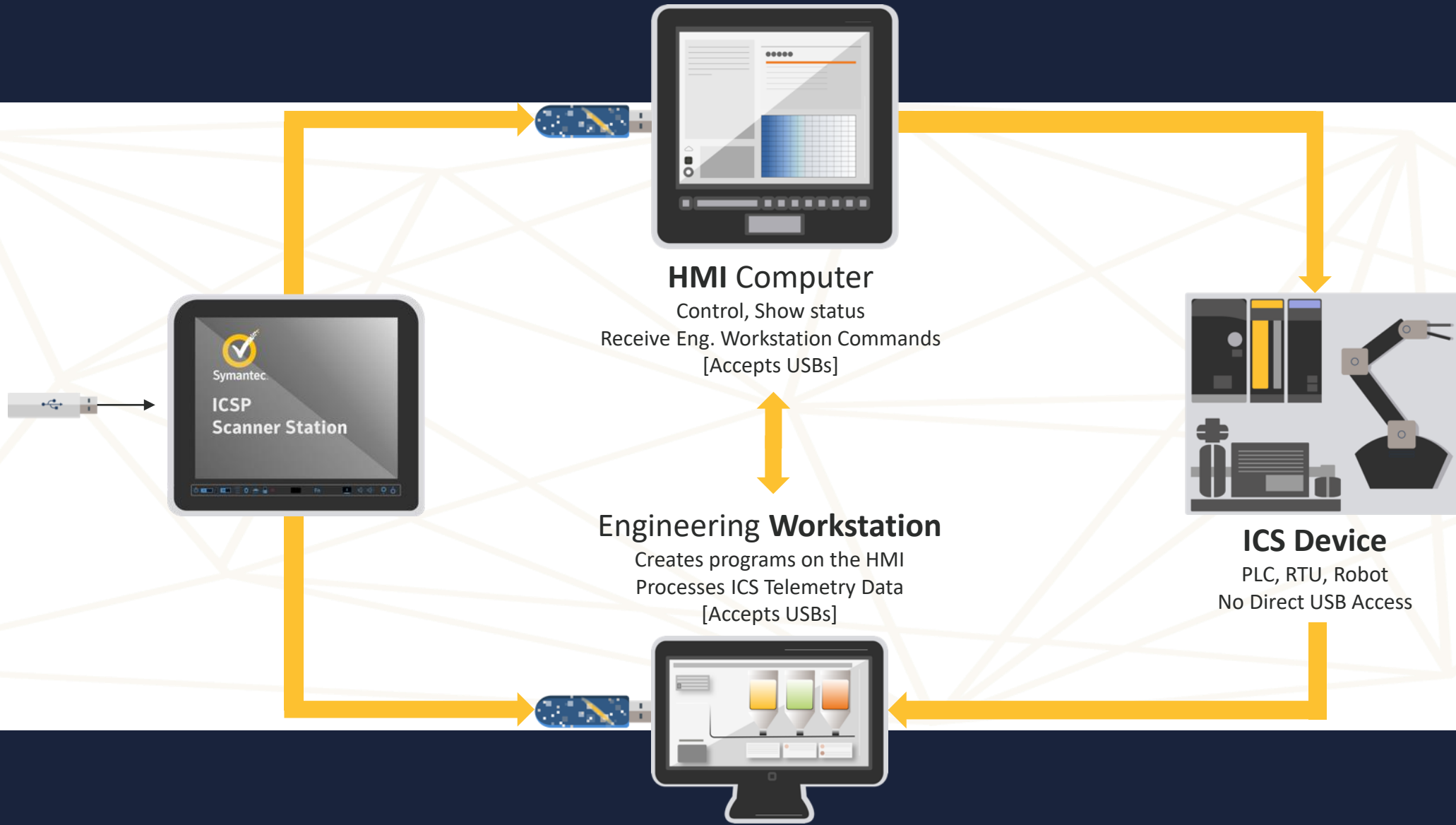
# USB Scanning

Section

## ICSP (Sheepdip)



# Industrial Control System Protection (ICSP)





## Лучшее USB сканирование на наличие вредоноса – Powered by Symantec STAR

- Определение без сигнатур
- Высочайшая эффективность модели, наученной 7 триллионами точек измерения
- Атрибуты, анализ поведения, машинное обучение
- Постоянное обучение

- 200M+ рабочих мест для оценки репутации файлов
- “Мудрость толпы”

- Легкие сигнатуры
- Продвинутое сигнатурные техники проверки (не только проверка по хэш)

- Эмуляция X86
- Эмуляция java script
- Эмуляция VBS/VBA
- Unrar/UnZip
- PE/Non-PE

Машинное обучение

Репутация

Сигнатуры

Эмуляция

STAR

ICSP (IOT)

[AVTest 2017 Results](#)

# The Endpoint

Section

## Critical System Protection





### Компактность

Программа работает на уровне ядра ОС и занимает ~20MB на Windows и использует менее 1% CPU ресурса.



### Изоляция приложений

Понижение уровня привилегий каждого приложения в отдельности, без изменения кода или ограничения функциональности.

Изоляция также известна как песочница.



### Контроль за поведением

IoT устройства имеют конкретную функцию и не обладают динамикой конечных пользователей, хоть и похожи на них

Можно создавать и редактировать политики для каждого приложения, файла, памяти, сети и общего хранилища.

# Изоляция приложений



Explicitly allowed by CSP?

Конечный итог - “песочница” или “клетка” для одной или более программ (процесса), используя наименьшие привилегии управления или “приемлемый” уровень доступа к ресурсам

## Granular Resource Constraints

<b>Files</b>	Read/Write Data Files
<b>Registry</b>	Read Only Configuration Information
<b>Memory</b>	
<b>Network</b>	Usage of Selected Ports and Devices
<b>Devices</b>	



# Лучшая в мире защита критических систем

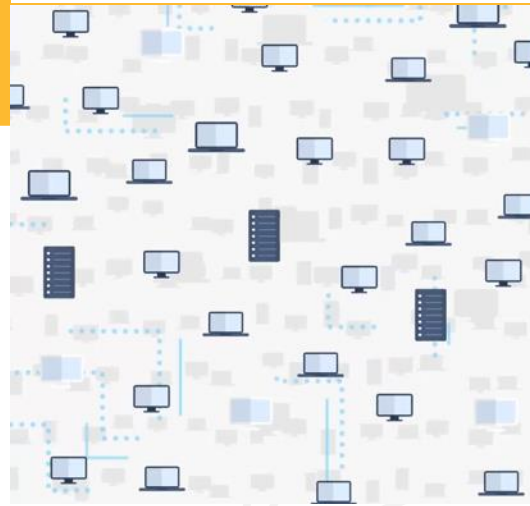
## авто-изоляция

- главная особенность и отличие Symantec
- ограничивает процессы, систему, память, ОС, регистр, командную строку, сеть



## широкая совместимость

- любая OS Windows с версии 2000, linux, qnx
- режим работы с центральной консолью управления и без



## полная защита

- защита от многоуровневых атак нулевого дня
- IPS/IDS
- масштабируемое и зрелое решение



# Analysis

Section

## Security Analytics



# Symantec Security Analytics

## КАМЕРА БЕЗОПАСНОСТИ И ЦИФРОВОЙ РЕГИСТРАТОР ДЛЯ ВАШЕЙ СЕТИ

Предание контекста сложным вещам



Анализ в реальном режиме времени и полная визуализация всего, что происходит внутри и снаружи вашей сети

Записывает, классифицирует и индексирует все пакеты и потоки данных в сети

DPI классифицирует более 3,200 приложений и тысячи мета атрибутов

Визуализация и анализ на полной скорости подключения, в реальном режиме времени

Контекст опасности, включая информацию о репутации, пользователей и артефактах

‘Черный ящик’ для расследования инцидентов, аналитики, первопричин и анализ воздействия

**ВИДЕТЬ ВСЁ. ЗНАТЬ БОЛЬШЕ. РЕАГИРОВАТЬ БЫСТРЕЕ.**

# Security Analytics SCADA Analysis

Полная визуализация угроз нацеленных на SCADA и ICS системы в реальном режиме времени



Индикаторы, правила и определение аномалий по индексированным SCADA атрибутам

Полное понимание уровня приложения и визуализация Modbus и DNP3 протоколов

Конфигурируемый срок хранения трафика предоставляет ретроспективный анализ

# Расширенная поддержка протоколов

- Поддержка 100 новых протоколов— более 3,200 в общем
- New ICS/SCADA Protocol Highlights
  - Modbus (new implementation)
  - DNP3 (new implementation)
  - CIP
  - Ethernet/IP (Rockwell)
  - GOOSE/IEC 61850-5
  - IEC 60870-6/TASE 2 (ICCP)
  - IEC 61784-2 (Yokogawa Vnet/IP)
  - iFIX (Proficy)
  - ISO 16484-5 (BACnet network, application, and virtual link control layers)
  - ISO 9506 (MMS)
  - OPC-UA
  - OSI PI Analysis Framework and Data Archive
  - Profinet
  - S7comm (Siemens System7)

# Security Analytics:

## МГНОВЕННАЯ РЕАКЦИЯ НА ИНЦИДЕНТ

### Sample Workflow

#### Начинаем расследование

- Обзор SIEM, endpoint, DLP, и других алертов
- Анализ результата песочницы
- Реакция на алерты прямо из Security Analytics
- Сторонний телефонный звонок
- Проведение проактивного поиска



#### Переходим к Security Analytics

- Начинаем расследования с точки
- Получения алерта
- Быстрый поиск по метаданным
- Доступ к полной “системе записи” – до / вовремя / после алерта
- Расширить или сузить временные рамки, критерии поиска или вердикт отчёта



#### Определяем источник

- Определяем первоисточник проблемы по отчётам для IOC или аномалиям
- Прослеживаем подозрительные файлы до их точки входа
- Анализ репутации файла с помощью GIN
- Извлекаем другие артефакты расследования и формируем их в кейс



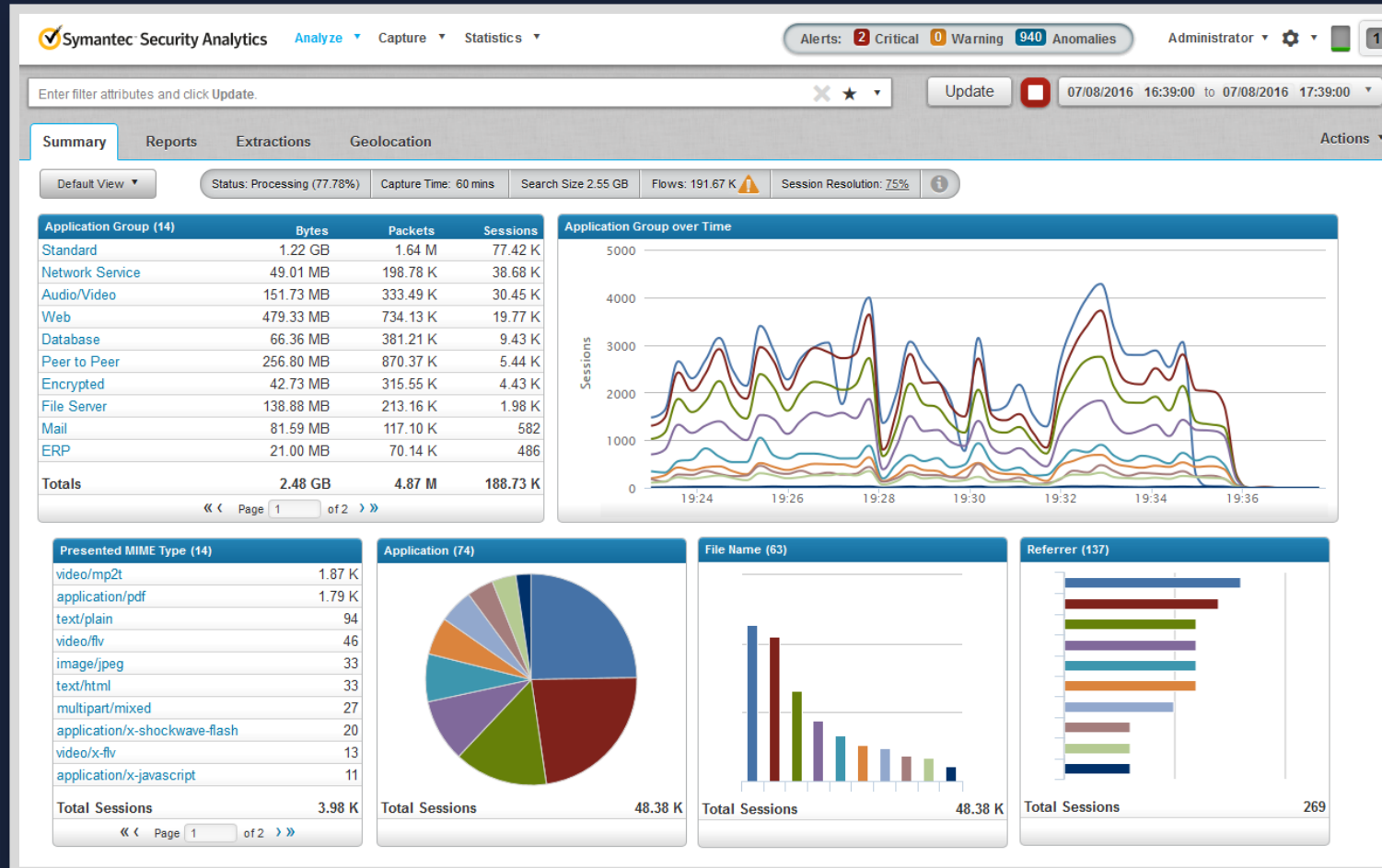
#### Исправление и защита

- Проверка endpoint, затем изоляция / блокирование / исправление через ATP: Endpoint или EDR
- Обновление базы знаний новой информацией
- Создание алерта для реакции на схожие атаки
- Обновление процессов и учебных методов





# Pivot Into Security Analytics



Глубокий анализ каждого сетевого события

Начало расследования с деталей алерта (IP / timeframe)

Интерфейс может быстро сузить или расширить рамки поиска по времени или другим критериям

Интерактивные отчёты по метаданным Уровней 2-7

# Обзор / Анализ отчетов

Множество настраиваемых отчетов для мгновенного отображения деталей по каждому событию

Summary Reports Extractions Geolocation

App: Application Status: Finished

- Application Reports
- Custom Analytics
- Email
- Encrypt
- File Reports
  - File Name
  - Fuzzy Hash
  - MD5 Hash
  - MIME Type
  - SHA1 Hash
  - VLAN ID
  - VoIP ID
- Geographical
- Network Layer
- SCADA
- Social Persona
- Threat Intel
- Web

tcp > http

tcp > ssl > https

Symantec Security Analytics Analyze Capture Statistics Alerts: 2 Critical 0 Warning 940 Anomalies Administrator

Enter filter attributes and click Update. Update 07/08/2016 16:39:00 to 07/08/2016 17:39:00

Summary Reports Extractions Geolocation Actions

Web: HTTP Server Status: Finished (100.00%) Capture Time: 15 mins Search Size 4.83 GB Flows: 23.38 K Session Resolution: Full

Report Summary

Selected Totals Settings Total Sessions over Time

Results (856)

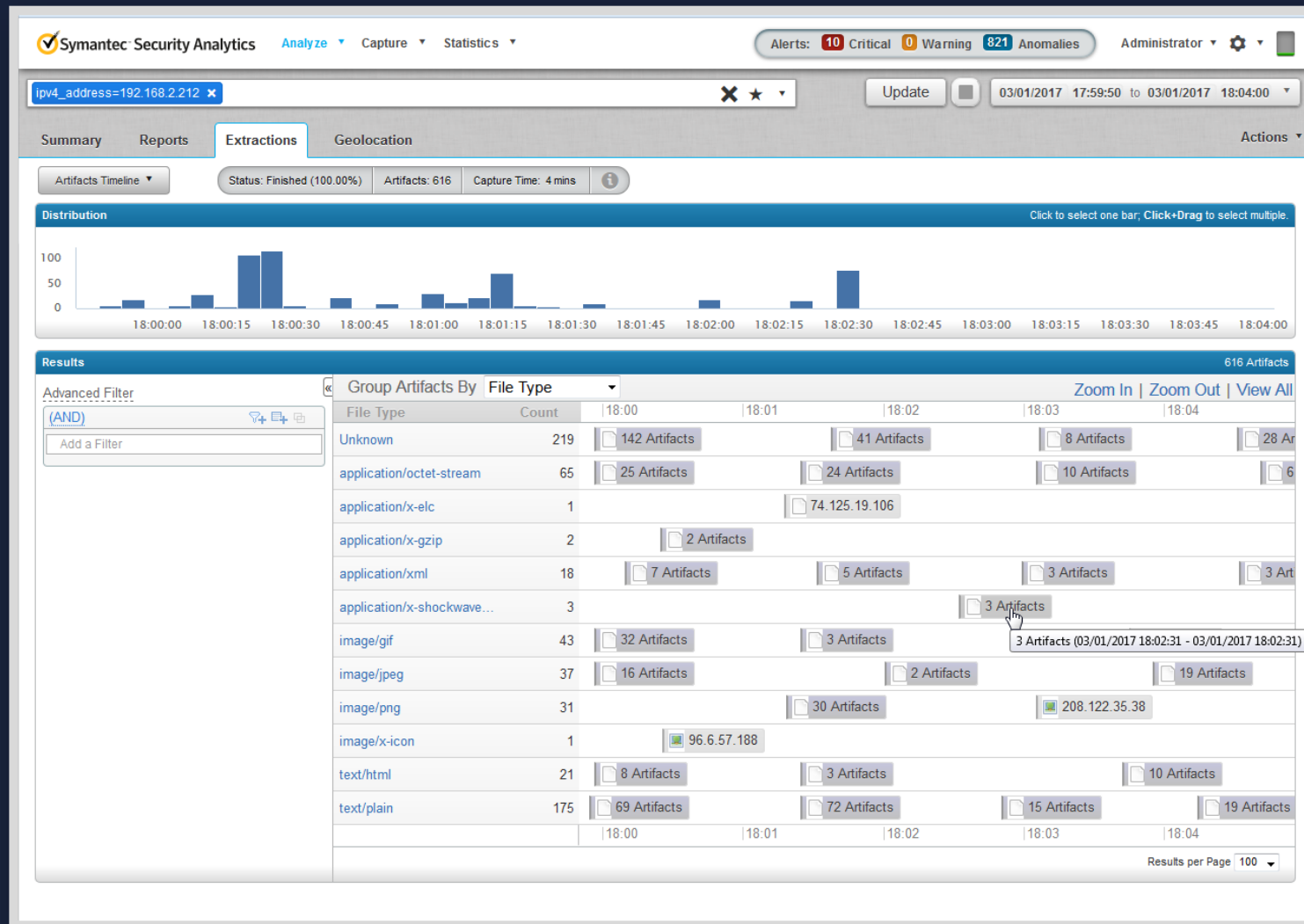
Compare Results Enable Report Comparison Advanced Filter Match All (AND) Add a Filter

HTTP Server	Bytes	Packets	Sessions
bluecoat.com	42.14 MB 5.18%	72.63 K 5.79%	2.49 K 10.64%
tracker	1.21 MB 0.15%	11.19 K 0.89%	1.15 K 4.92%
tcp	9.94 MB 1.22%	16.78 K 1.34%	520 2.22%
default	103.61 MB 12.73%	142.30 K 11.34%	441 1.89%
facebook.com	5.93 MB 0.73%	10.12 K 0.81%	328 1.40%
google.com	3.30 MB 0.41%	5.96 K 0.47%	218 0.93%
ssl	2.99 MB 0.37%	5.38 K 0.43%	203 0.87%
connect.facebook.net/en_us/all.js	3.08 MB 0.38%	5.38 K 0.43%	191 0.82%
yahoo.com	3.47 MB 0.43%	5.69 K 0.45%	160 0.68%
ssl.gstatic.com	3.25 MB 0.40%	5.39 K 0.43%	154 0.66%
s.yimg.com	40.16 MB 4.93%	55.95 K 4.46%	148 0.63%





# Просмотр артефактов / Извлечение файлов



Визуальное представление сетевых артефактов за период времени

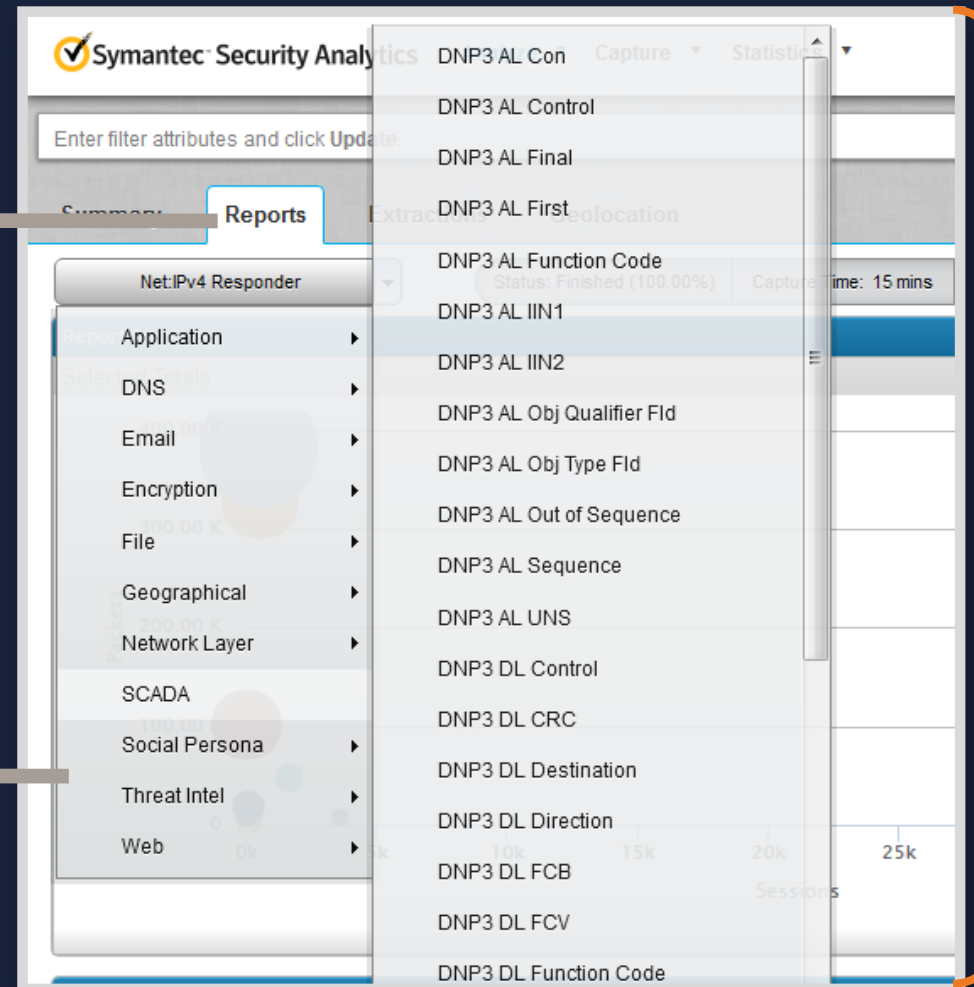
Помогает очень быстро визуализировать последовательность объектов

Существенно улучшает производительность при поиске артефактов

# SCADA Indexed Attributes

Reports  
Tab in  
Platform

SCADA  
анализ



Одни из множества доступных SCADA Атрибутов доступных в Security Analytics

# Анализ угроз в реальном режиме времени



## Intelligence Services

Tap the vast threat data from Symantec Global Intelligence Network to inspect all web, mail and file protocols for malicious activity and files

URL Репутация  
и Категоризация

Репутация  
файла

Другие индикаторы  
компрометации



Content  
Analysis

Подозрительные файлы отправляются  
в Content Analysis (или песочницу) для  
проверки

## Репутационные сервисы для от различных источников



Global  
Intelligence  
Network



Content  
Analysis



PE Scanner  
jSUNPACK  
Geolocation  
More...

# Открытая интеграция: успешное партнёрство

## THREAT INTELLIGENCE

DShield, RIPE NCC, URLVoid, Hunting Malware Like a Pro, mnemonic, VirusTotal, stopforumspam, SORBS, Is It Hacked?, hpHosts, Talos, Built With, Symantec, SPAMHAUS, ANOMALI, DOMAINTOOLS, BFK, twitter, MALWARE DOMAIN LIST, Internet Storm Center, ThreatCrowd, Malc0de.com, Central Ops .net



## PIVOT

splunk, ArcSight, IBM, GUIDANCE SOFTWARE, Radar, paloalto NETWORKS, REVERSING LABS, CounterTack, CISCO SOURCEfire, FireEye, CARBON BLACK ARM YOUR ENDPOINTS, tripwire, ziften

**SECURITY ANALYTICS SUPPORTS BEST-OF-BREED INTEGRATIONS**  
*Work Smarter & Faster – Make Better Decision*

# IBM QRadar™ Integration



Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	De p
<input type="checkbox"/>	3/13/14 5:12:30 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:11:48 PM	10.50.165.17	1852	89.248.166.160	80	tcp_ip	Web.Misc	128 (C)	64 (C)	2	
<input type="checkbox"/>	3/13/14 5:12:25 PM	10.50.165.17	1877	74.125.234.103	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:30 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:25 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	128 (C)	64 (C)	2	
<input type="checkbox"/>	3/13/14 5:12:29 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:24 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:19 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:24 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	236	473	3	
<input type="checkbox"/>	3/13/14 5:12:25 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	
<input type="checkbox"/>	3/13/14 5:12:24 PM	10.50.165.17	1884	184.28.51.55	80	tcp_ip	Web.Misc	64	0	1	

Filter on Destination IP is 89.248.166.160

Filter on Destination IP is not 89.248.166.160

Filter on Source or Destination IP is 89.248.166.160

False Positive

More options...

Plugin options...

Investigate In Security Analytics [Dst IP]

Investigate In Security Analytics [Src & Dst IP]

# ArcSight™ Integration

The screenshot displays the ArcSight Console interface. The main window shows a list of events under the 'Active Channel: 24hr Critical IDS' filter. A context menu is open over the event list, with the 'Blue Coat Security Analytics ...' option highlighted in red. The event list includes columns for Manager Receipt Time, End Time, Name, Attacker Address, Target Address, and Priority.

Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	EXPLOIT-KIT Phoenix exploit kit post-compromise behavior	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:50 PDT	3 Sep 2014 00:46:38 PDT	MALWARE-CNC Win.Trojan.Foreit variant outbound connection	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:45 PDT	3 Sep 2014 00:46:36 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:45 PDT	3 Sep 2014 00:46:36 PDT	EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:36:00 PDT	OS-WINDOWS DCERP NCACN-IP-TCP srvsvc NetPathCanonicalizat...	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:30 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:31 PDT	EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:40 PDT	EXPLOIT-KIT Phoenix exploit kit post-compromise behavior	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:25 PDT	3 Sep 2014 00:38:40 PDT	MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration	192.168.100.130	203.114.112.156	7
2 Sep 2014 21:51:18 PDT	2 Sep 2014 22:29:55 PDT	EXPLOIT-KIT Blackholev2 exploit kit url structure detected	192.168.100.130	203.114.112.156	7

# Splunk™ Integration



splunk> App: Blue Coat Security Analytics App For Splunk

Blue Coat Security Analytics For Splunk Dashboard Views Threat Views Search

New Search

index=estreamer sourcetype=estreamer]

71,951 of 71,951 events matched

Events (71,951) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Oct 22, 2014

List Format 50 Per Page

< Hide Fields	All Fields	i	Time	Event
		>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IMPACT event_sec=1428431733 event_id=132455 sensor=172.21.0.1 host = blackhole   source = eStreamer   sourcetype = eStreamer
Selected Fields		>	4/7/15 11:35:33.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1428431733 event_usec=917257 sensor=8.1.100.1 c="A Network Trojan was Detected" ids_policy="Initial Passive" 0-0000-0000-000000000000 sec_0 host = blackhole   source = eStreamer
a host 1		>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IM host = blackhole   source = eStreamer
a source 1		>	4/7/15 11:35:33.000 AM	rec_type=9 rec_type_simple=IM host = blackhole   source = eStreamer
a sourcetype 1		>	4/7/15 11:35:33.000 AM	rec_type=400 rec_type_simple=c="A Network Trojan was Detected" ids_policy="Initial Passive" 0-0000-0000-000000000000 sec_0 host = blackhole   source = eStreamer
Interesting Fields				
# app_proto 1				
# blocked 2				
a class 13				
a class_desc 13				
# client_app 1				
# connection_id 1				
# connection_sec 1				
# date_hour 24				
# date_mday 31				
# date_minute 60				
# date_month 7				

Event Actions

- Build Event Type
- Extract Fields
- Analyze IPs with Security Analytics
- Show Source

# Доступные конфигурации

- До 2-х полок могут быть подключены напрямую.
- 3-5 полок можно подключить 10G-HD портом при подключении к коммутаторам Brocade 6500 серии.

300TB



600TB



1.5PB 







# Спасибо

## Internet of Things