Title

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

Presenter

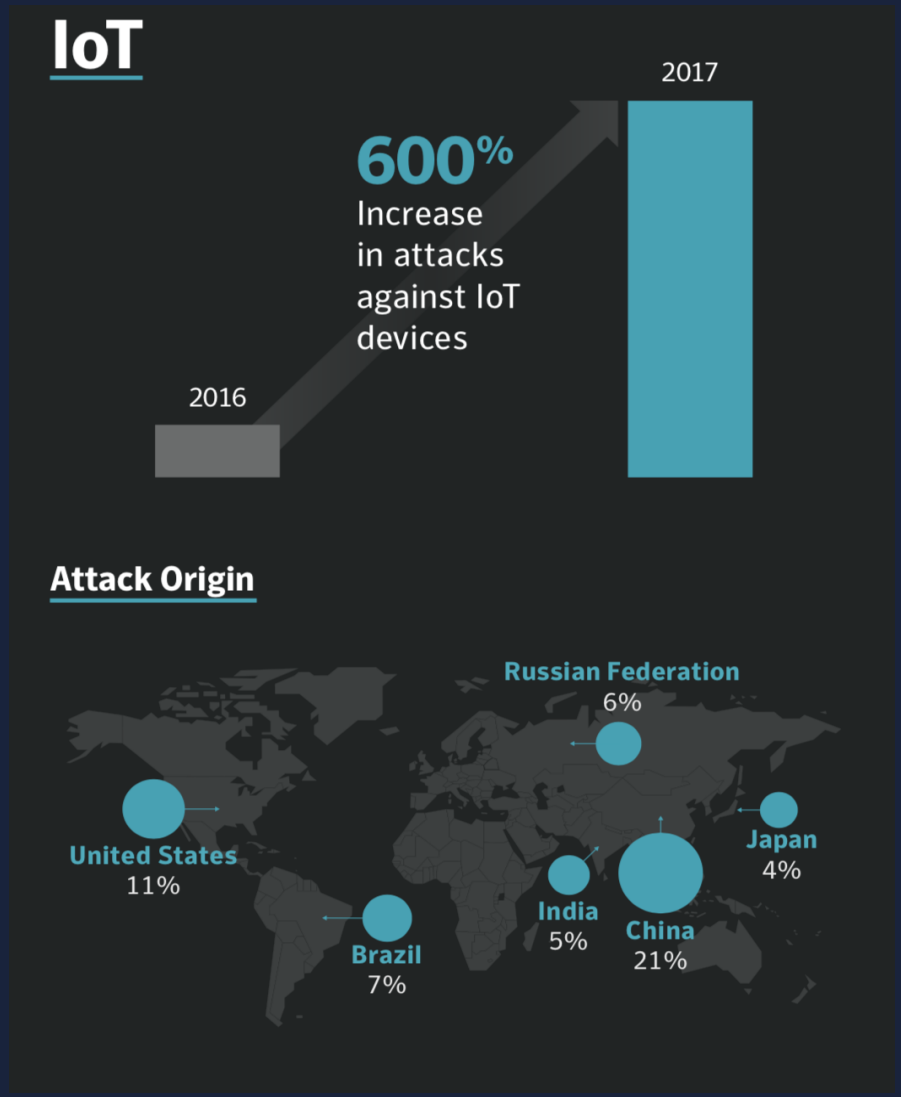
Станислав Бубнов

Date

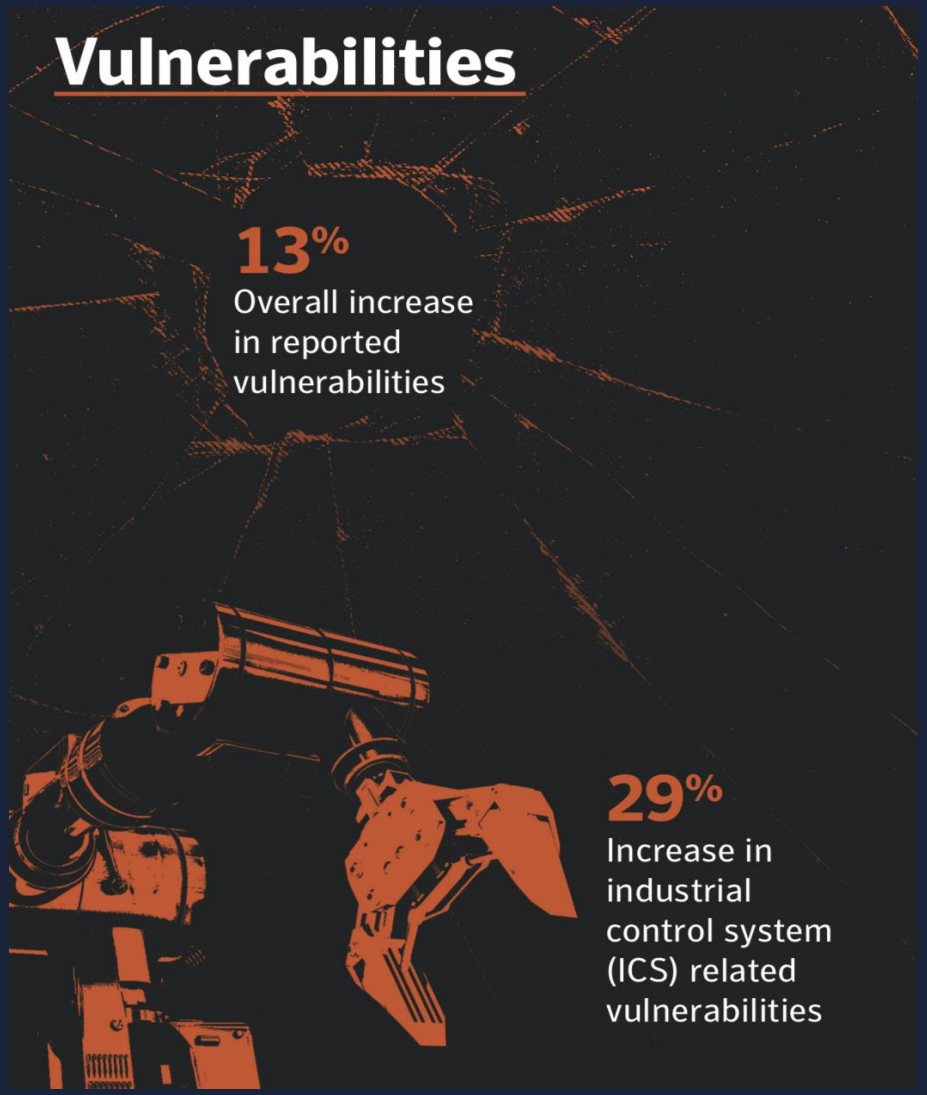
18/10/2018

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



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

Цели

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

ПРИКАРПАТТЯ ОБЛЕНЕРГО

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

- **230,000** Customers lost power[1]
- **30** Substations Disconnected[1]
- **8** Provinces Without Power[1]

Dragonfly 2.0

Cyber Attacks on the Energy Sector

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

- **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 `.*`

Компрометация внутренних систем

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

2 `wannacry`

Переход к операционным технологиям

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

3

Доступ к PLC

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

4 `triton` `stuxnet` `industroyer`

Выгода

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

ICSP, CSP

CSP

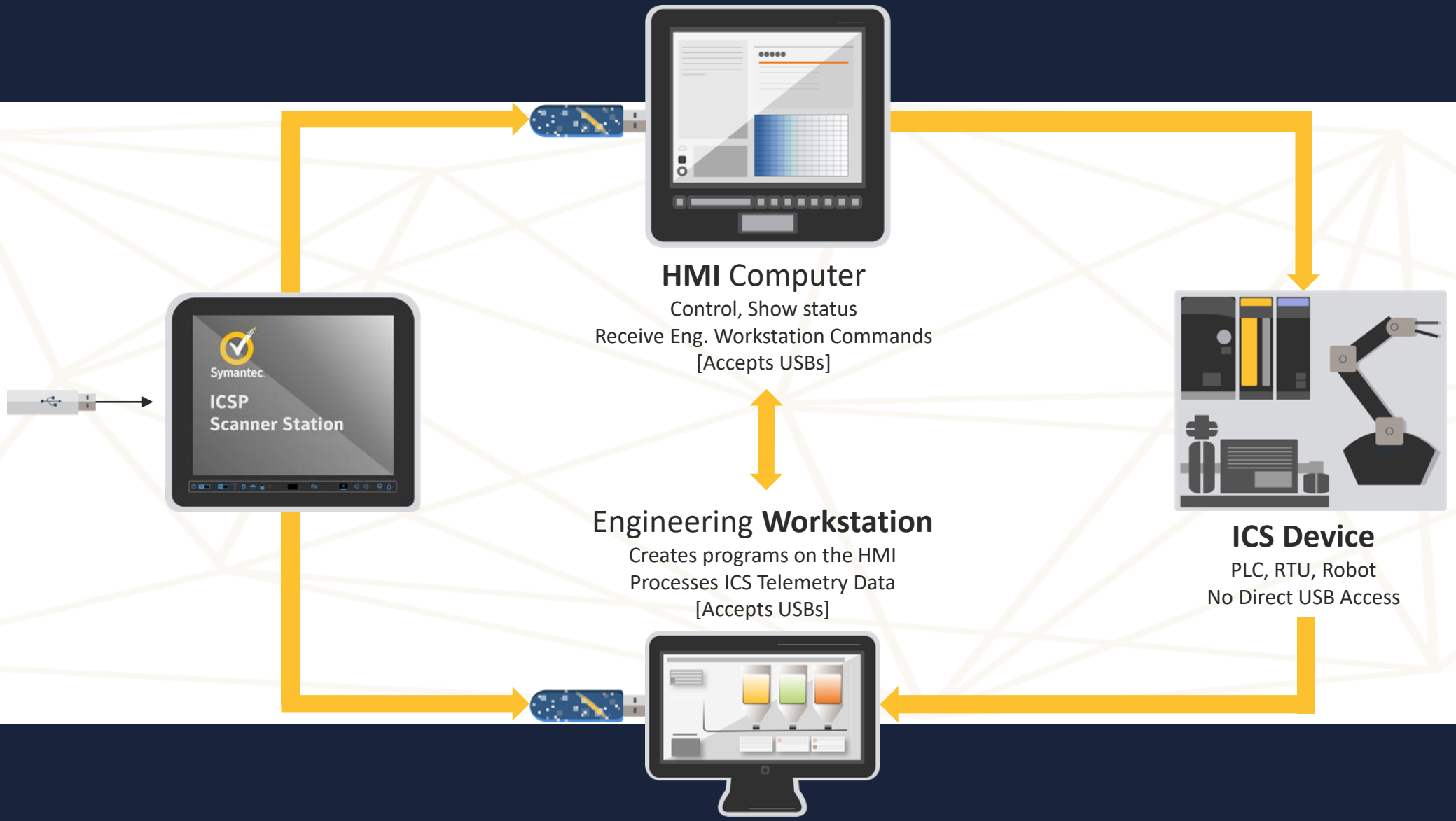
a trusted strategy.

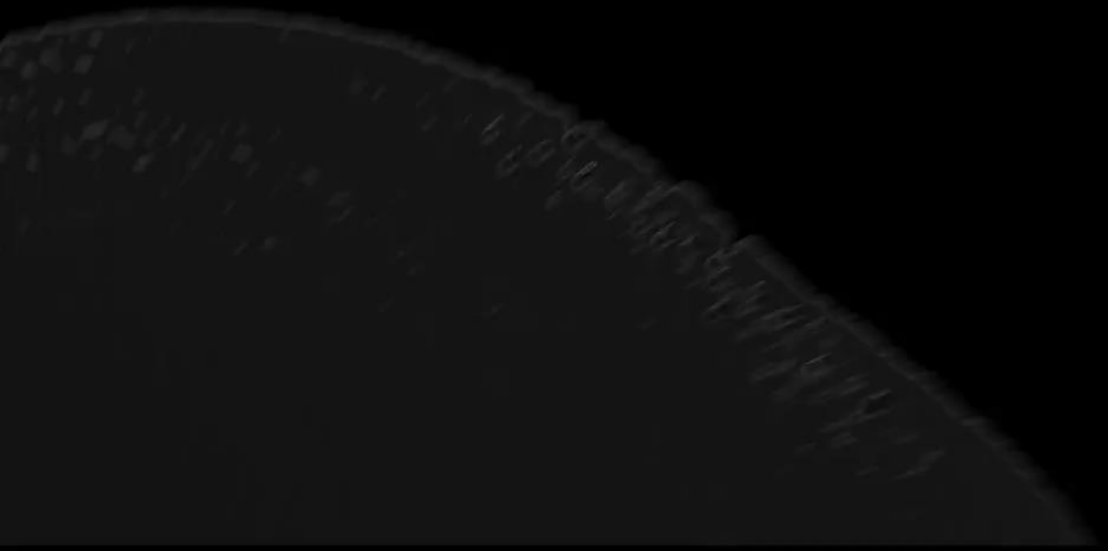
USB Scanning

Section

ICSP (Sheepdip)

Industrial Control System Protection (ICSP)





Лучшее USB сканирование на наличие вредоноса – Powered by Symantec STAR

Машинное обучение	Репутация	Сигнатуры	Эмуляция
• Определение без сигнатур • Высочайшая эффектность модели, наученной 7 триллионами точек измерения • Атрибуты, анализ поведения, машинное обучение • Постоянное обучение	• 200M+ рабочих мест для оценки репутации файлов • “Мудрость толпы”	• Легкие сигнатуры • Продвинутые сигнатурные техники проверки (не только проверка по хэш)	• Эмуляция X86 • Эмуляция java script • Эмуляция VBS/VBA • Unrar/UnZip • PE/Non-PE

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

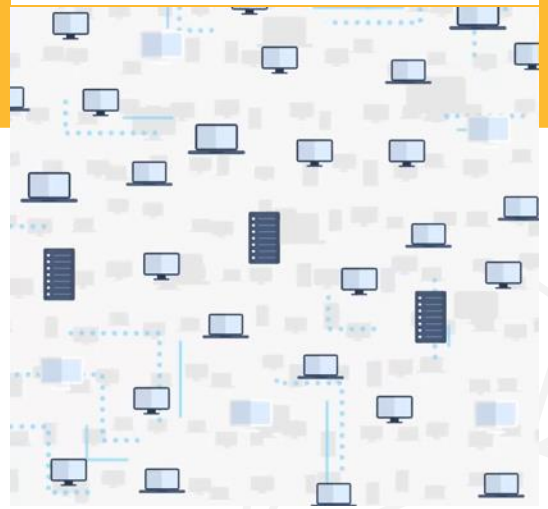
Лучшая в мире защита критичных систем

авто-изоляция

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

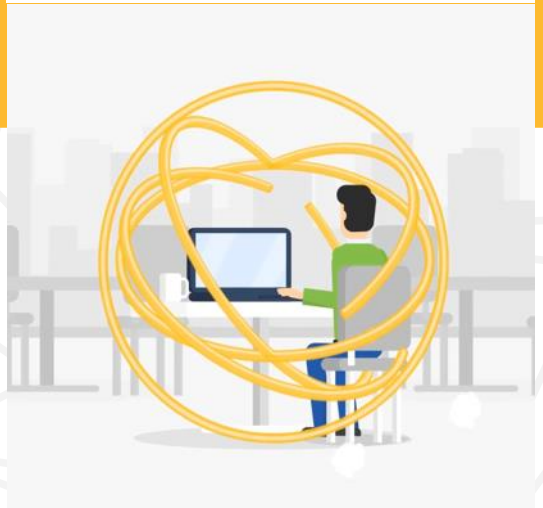
широкая совместимость

- 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, пользователях 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

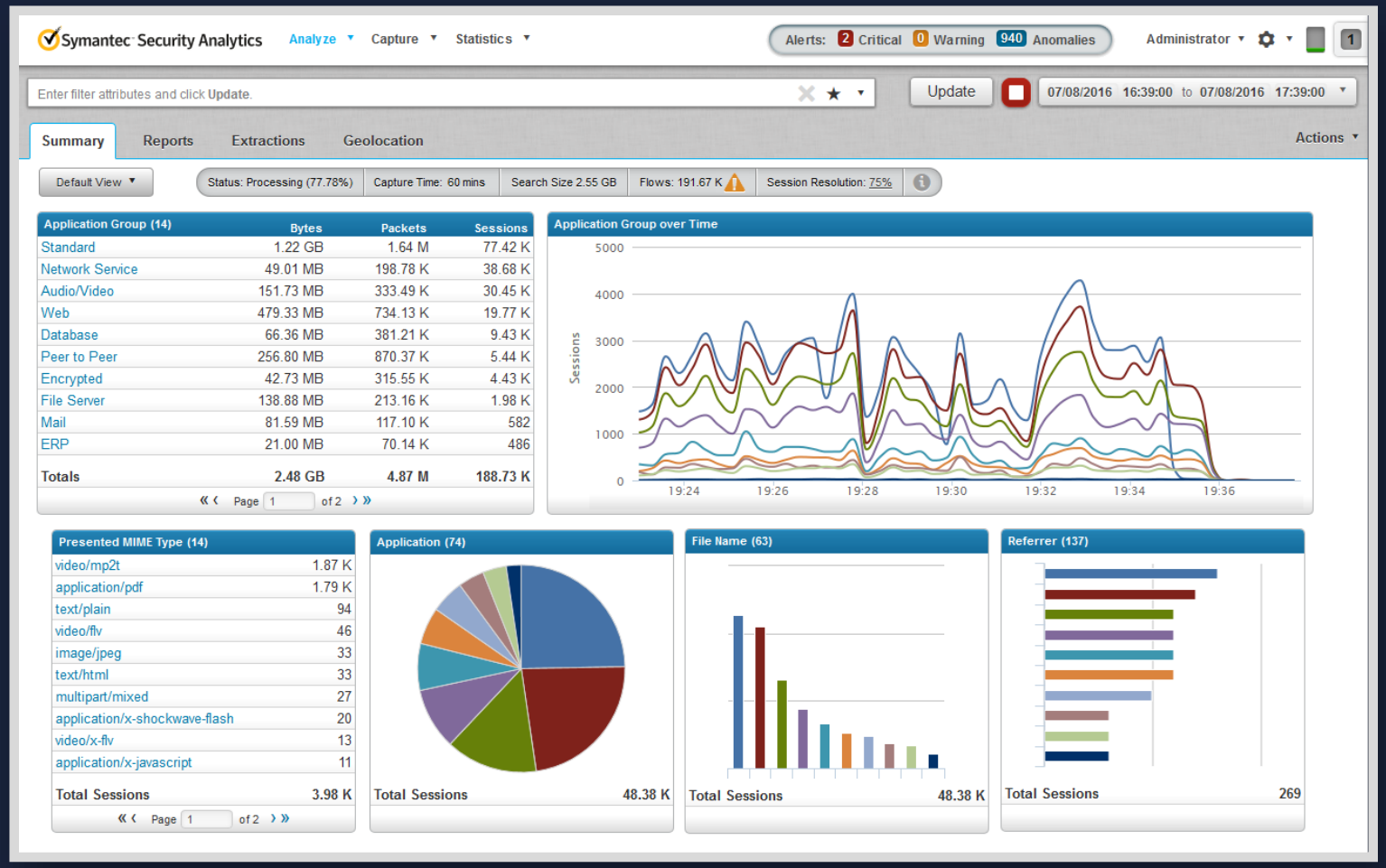
Определяем источник

- 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 методи

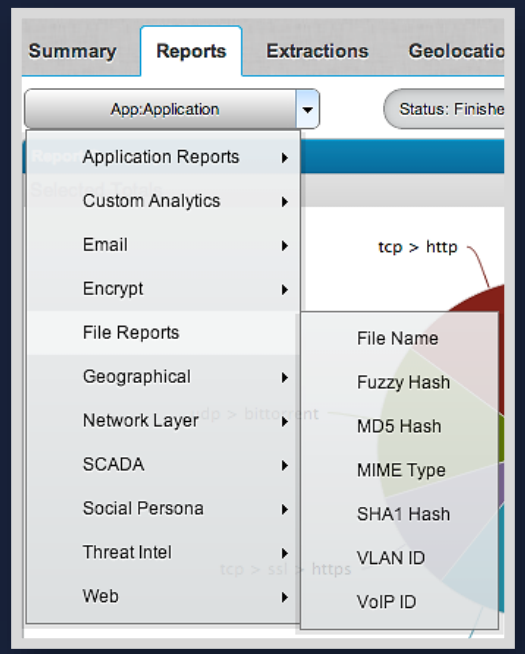
Pivot Into Security Analytics

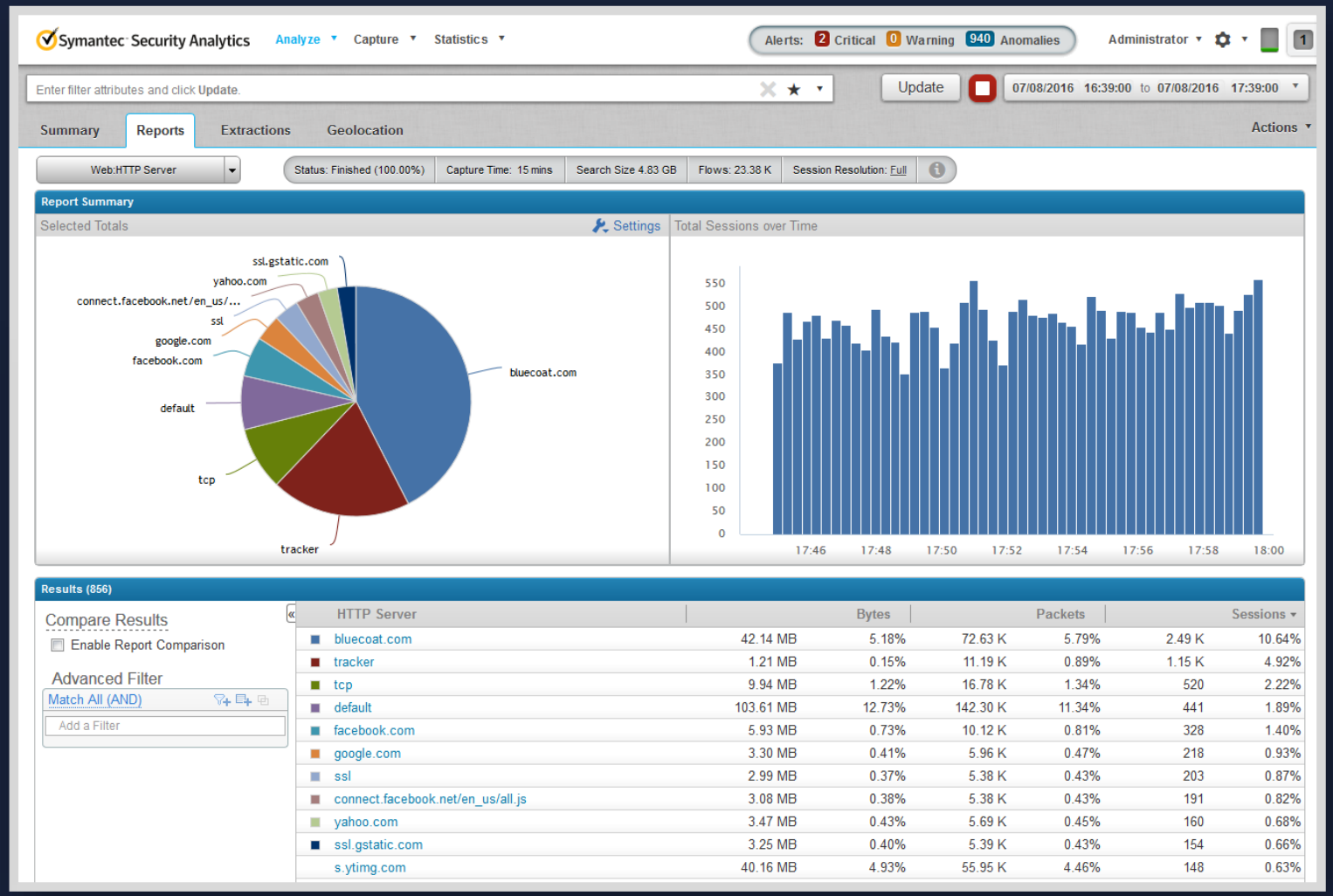


- Глубокий анализ каждого сетевого события
- Начало расследования с деталей алерта (IP / timeframe)
- Интерфейс может быстро сузить или расширить рамки поиска по времени или другим критериям
- Интерактивные отчёты по метаданным Уровней 2-7

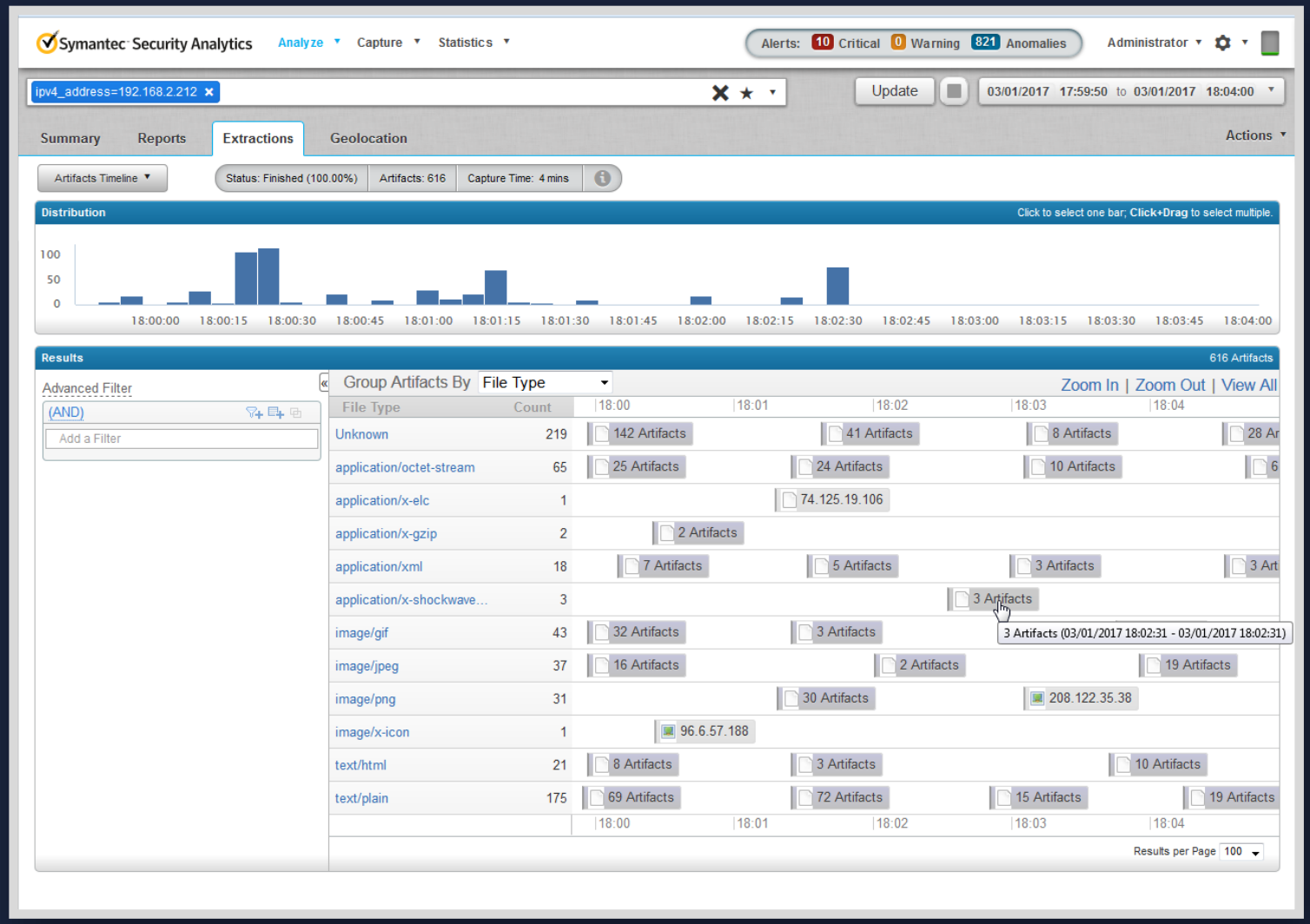
Обзор / Анализ отчетов

Множество настраиваемых отчётов для мгновенного отображения деталей по каждому событию





Просмотр артефактов / Извлечение файлов



Визуальное представление сетевых артефактов за период времени

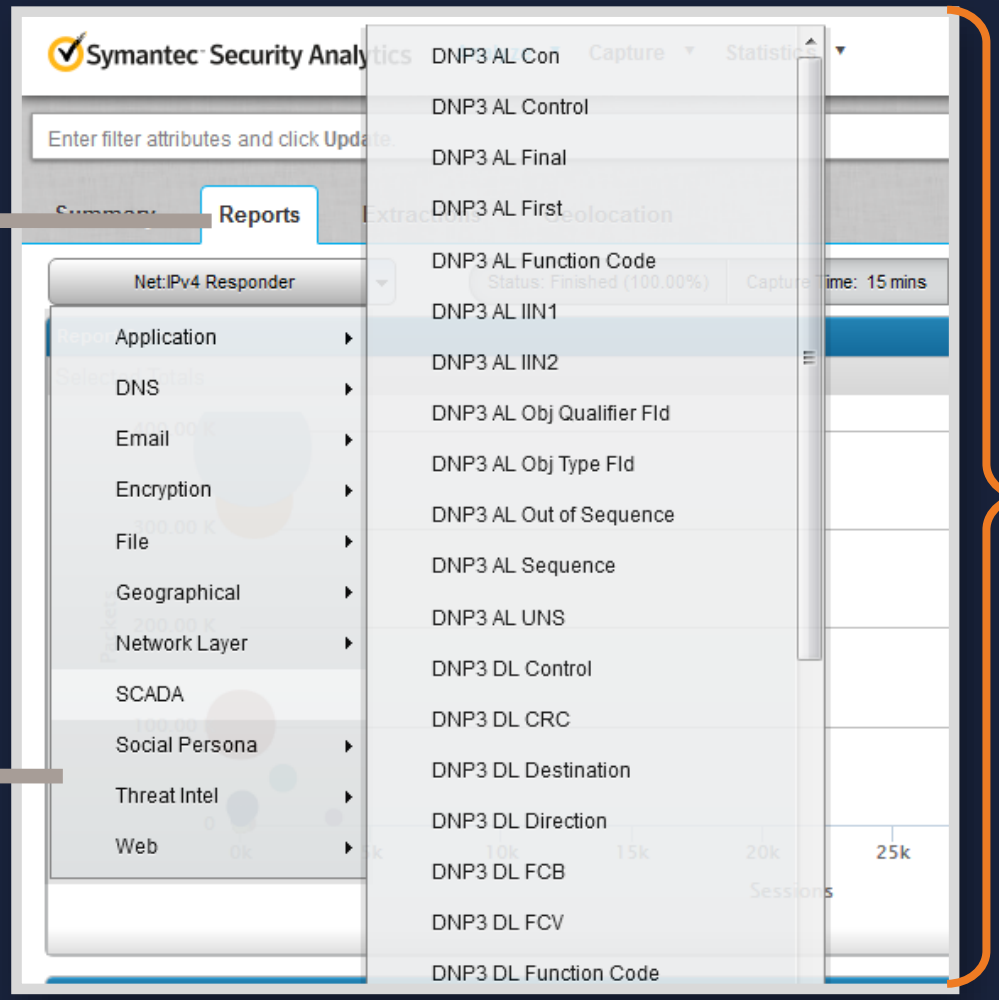
Помогает очень быстро визуализировать последовательность объектов

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 режим времени

Intelligence Services

Tap the vast threat data from Symantec Global Intelligence Network to inspects 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
- FireEye
- lastline
- VIRUS TOTAL
- ClamAV
- yara
- robtex
- Google Safe Search
- SORBS
- SANS
- cuckoo

PE Scanner
jSUNPACK
Geolocation
More…

Открытая интеграция: успешное партнёрство

THREAT INTELLIGENCE

DShield, RIPE NCC, URLVoid, mnemonic, VirusTotal, Hunting Malware Like a Sir, stopforumspam, SORBS, Is It Hacked?, hpHosts, Talos, built with, Symantec, SPAMHAUS, ANOMALI, DOMAINTOOLS, BFK, twitter, MALWARE DOMAIN LIST, Internet Storm Center, ThreatCrowd, Malc0de.com, CentralOps.net Advanced online Internet utilities

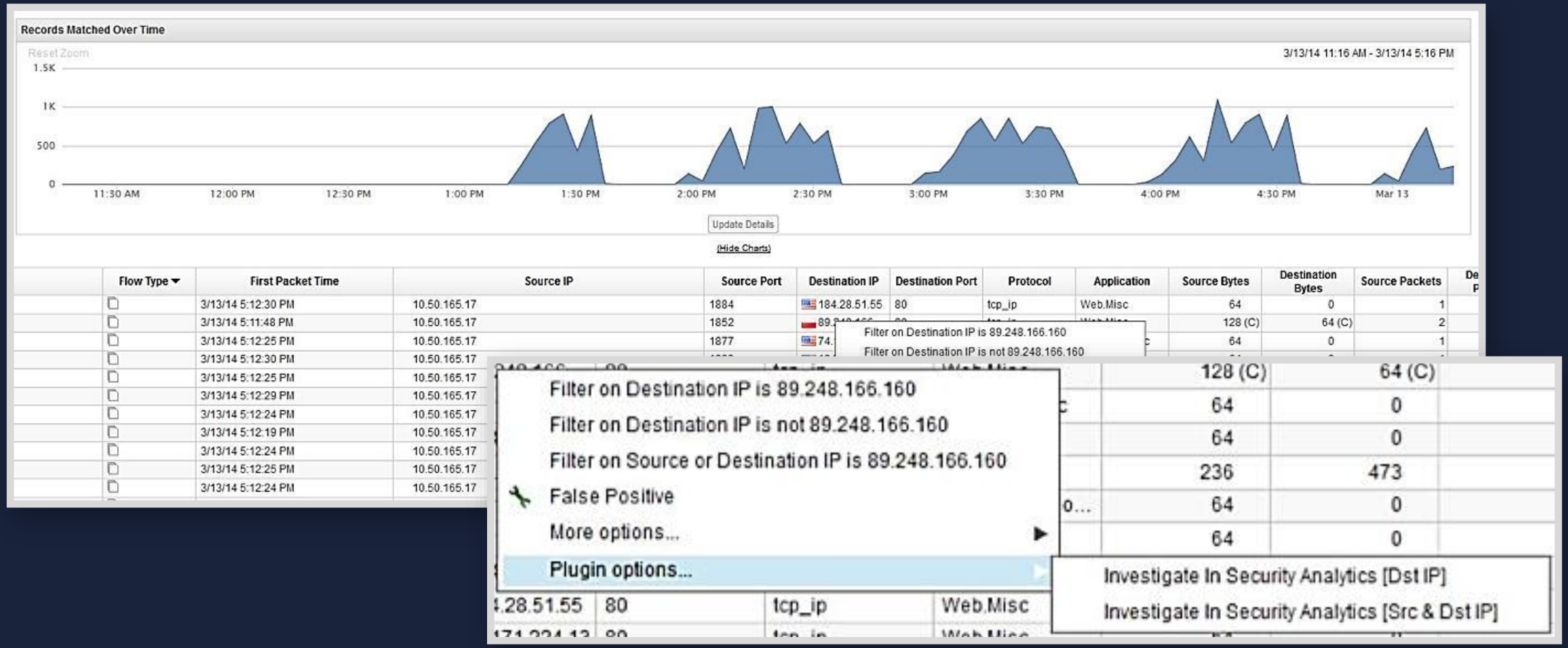
PIVOT

splunk>, ArcSight, IBM QRadar, GUIDANCE SOFTWARE, REVERSINGLABS, paloalto NETWORKS, CounterTack, CISCO SOURCEfire, FireEye, CARBON BLACK ARM YOUR ENDPOINTS, tripwire, ziften

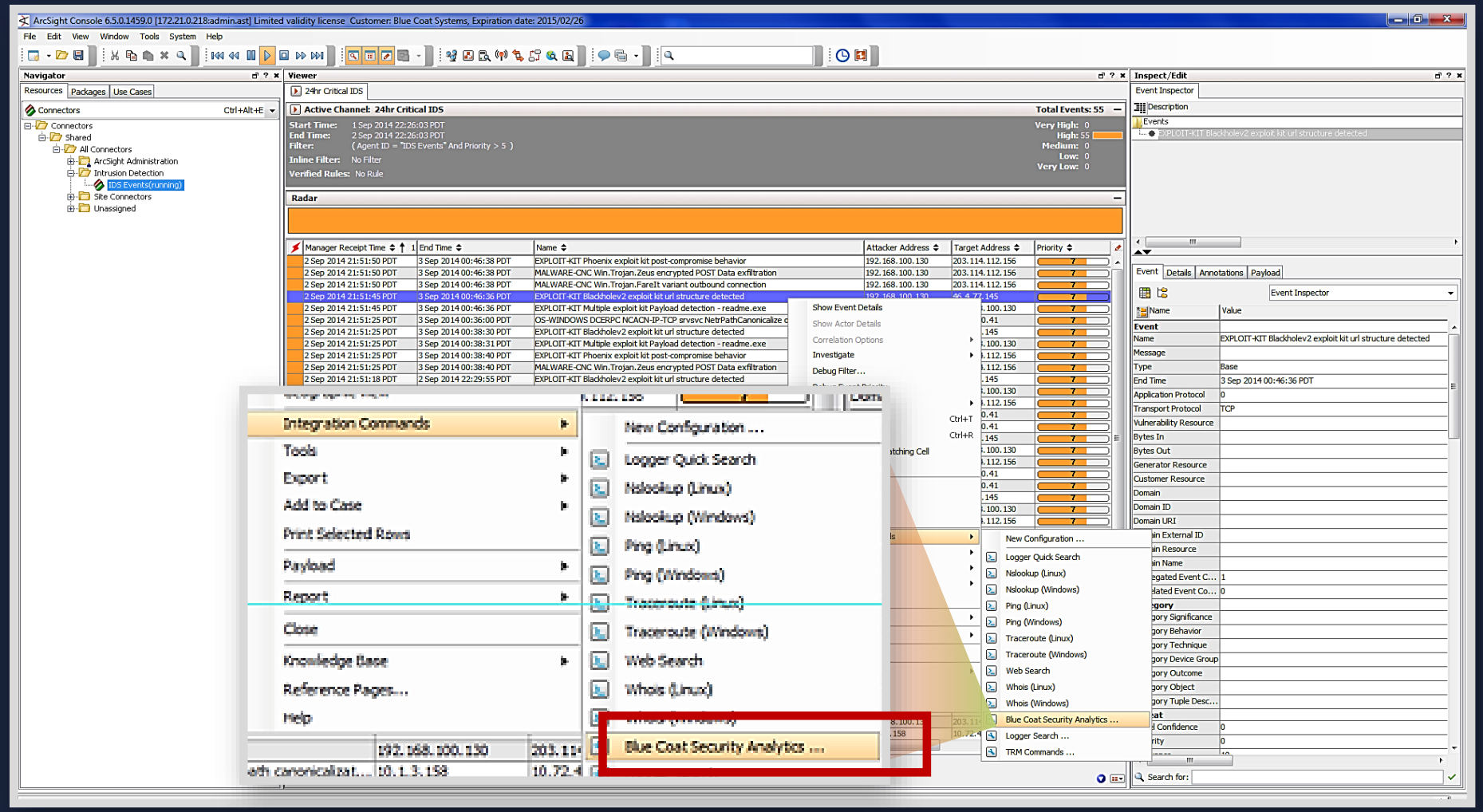
SECURITY ANALYTICS SUPPORTS BEST-OF-BREED INTEGRATIONS

Work Smarter & Faster – Make Better Decision

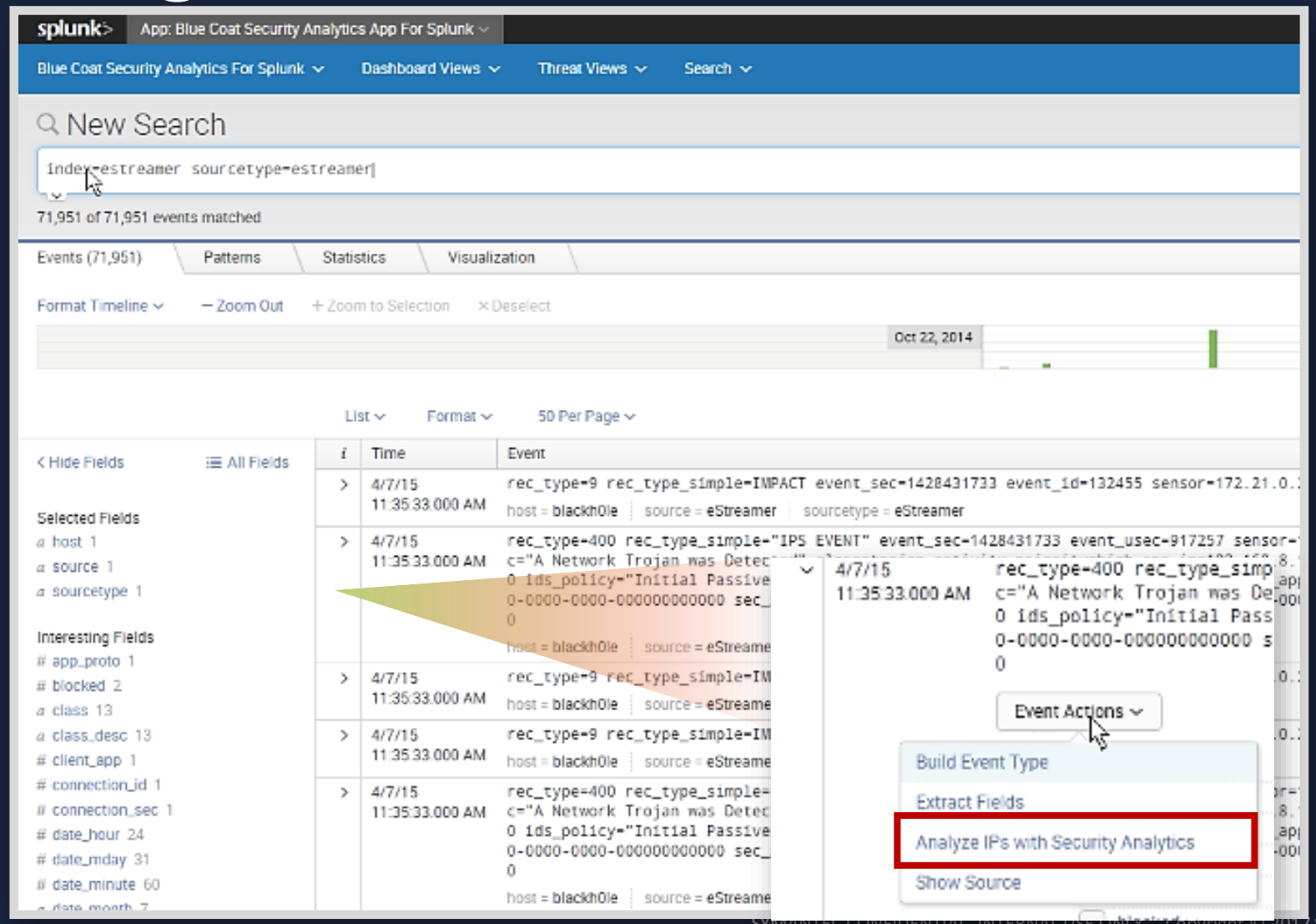
IBM QRadar™ Integration



ArcSight™ Integration



Splunk™ Integration



splunk>

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

