CISCO
SECURE

The bridge to possible

Повышение осведомленности и обнаружение угроз в сетях АСУ ТП

Михаил Кадер

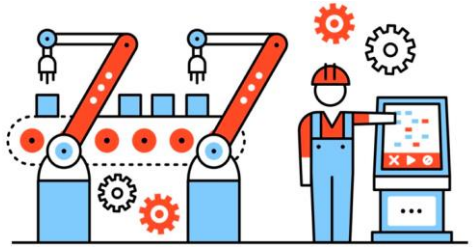
mkader@cisco.com

15.07.2021

Современный мир уже более чем **подключенный**

СЕГОДНЯ
Industrial Control Systems (ICS)

Энергетика, Промышленность, Транспорт, Process Industries



ЗАВТРА
Industrial Internet of Things (IIoT)

Цифровизация повышает возможности для кибератак

68% специалистов по безопасности считают критичными вопросы обеспечения безопасности в IoT

Source: 2018 ZK Research Network Purchase Intention Survey

Недавние нападения на промышленный объекты

2017

A.P. Moller Maersk

Shipping & Logistics

Ransomware: NotPetya

COST: $300 million

2017

Mondelez

Food & Beverage

Ransomware: NotPetya
Attacked twice in a year

COST: $150 million

2018

Saudi Aramco

Oil and Gas

OT-Specific Malware: TRITON

Undisclosed cost

2019

Norsk Hydro

Metals & Mining

Ransomware: LockerGoga

COST: $70 million

2021

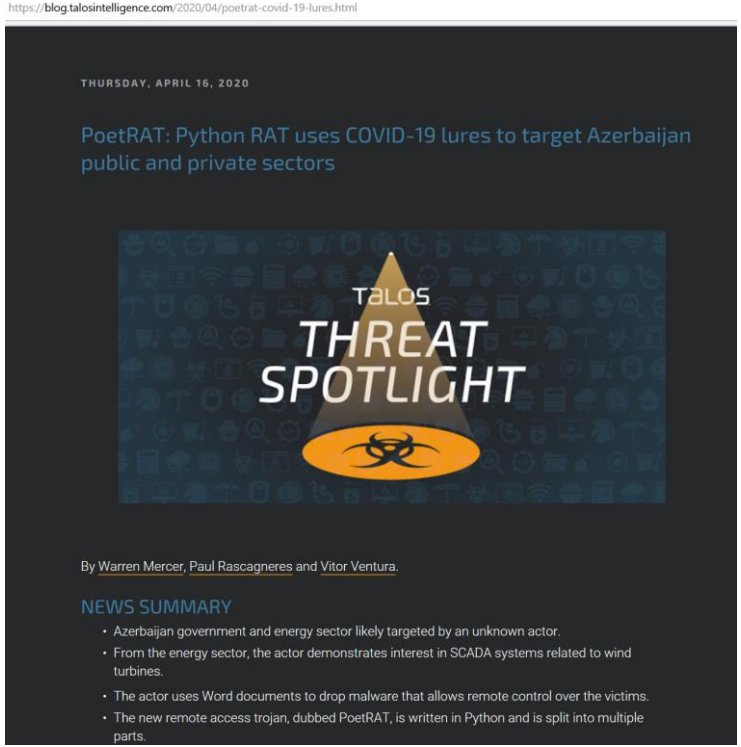
Oldsmar, Florida

Water Utility

TeamViewer Remote Access Breach

PoetRAT:
RAT (remote access trojan) на Python, направленный на системы SCADA

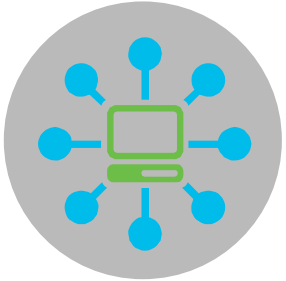
Использование темы COVID-19



https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html

Нельзя защитить то, чего **не знаешь**

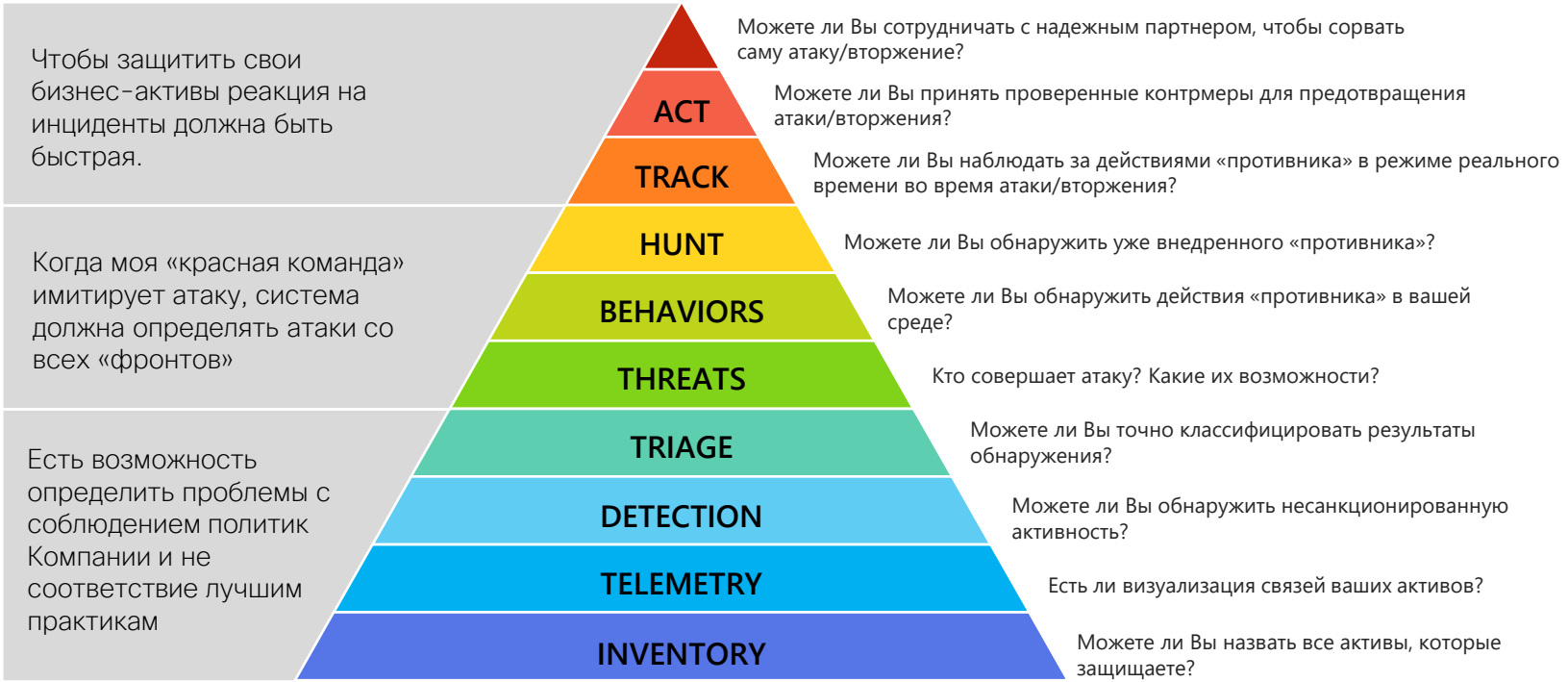
Многие заказчики не имеют полной картиный по установленному оборудованию на OT-сети



Нет четкого понимания, «кто-с кем-как» коммуницирует в OT-сети

Решения по автоматизации внедряются в течении долгого времени и зачастую без четкой политики управления безопасностью

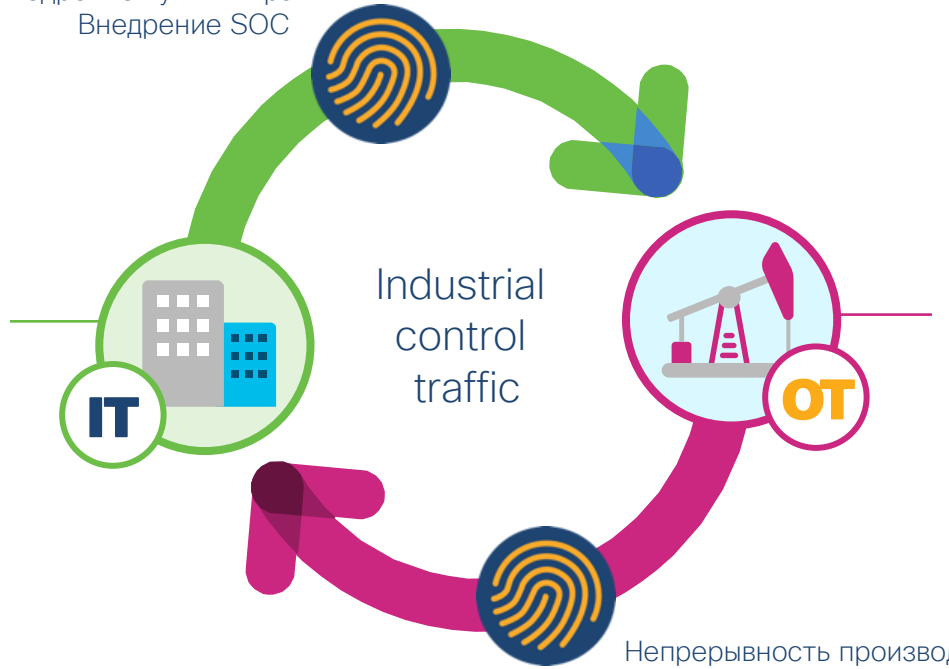
Иерархия потребностей при реагировании на инциденты



Source: https://github.com/swannman/ircapabilitie

Преимущества взаимодействия **IT** и **OT**

Внедрение лучших практик
Внедрение SOC

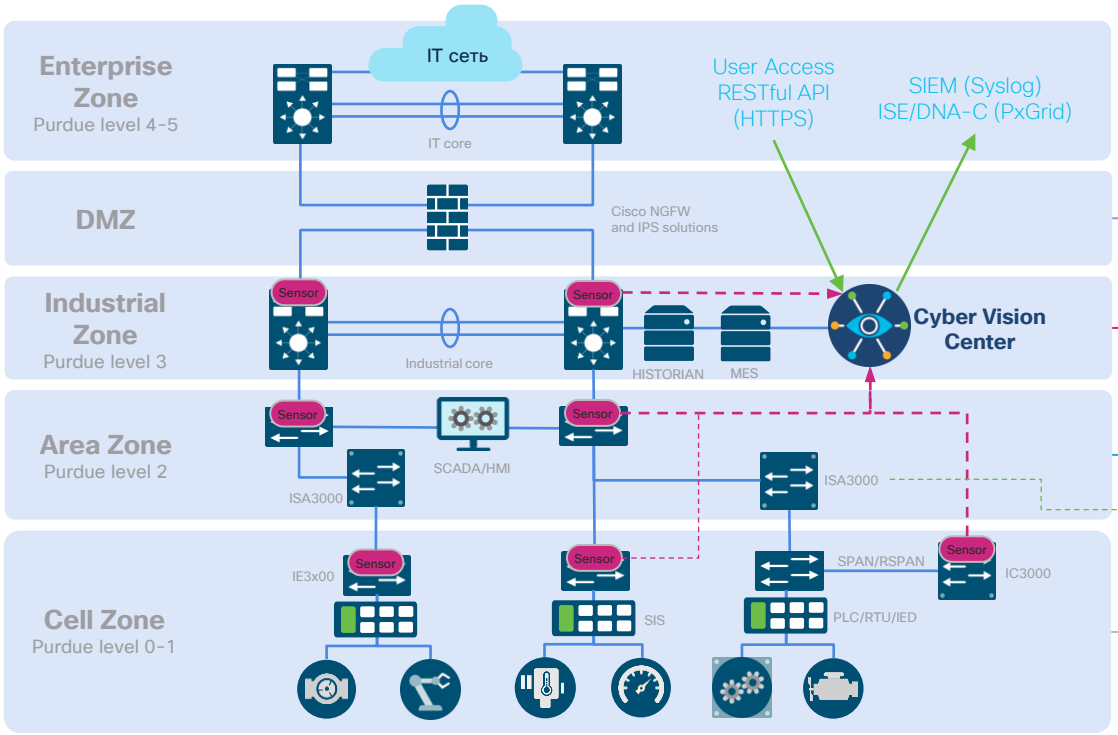


Навыки в кибербезопасности
Сетевые знания
Политики безопасности
Детекция и реакция

Отраслевые знания OT
Знания процессов
Критичные узлы
Конфигурация оборудования

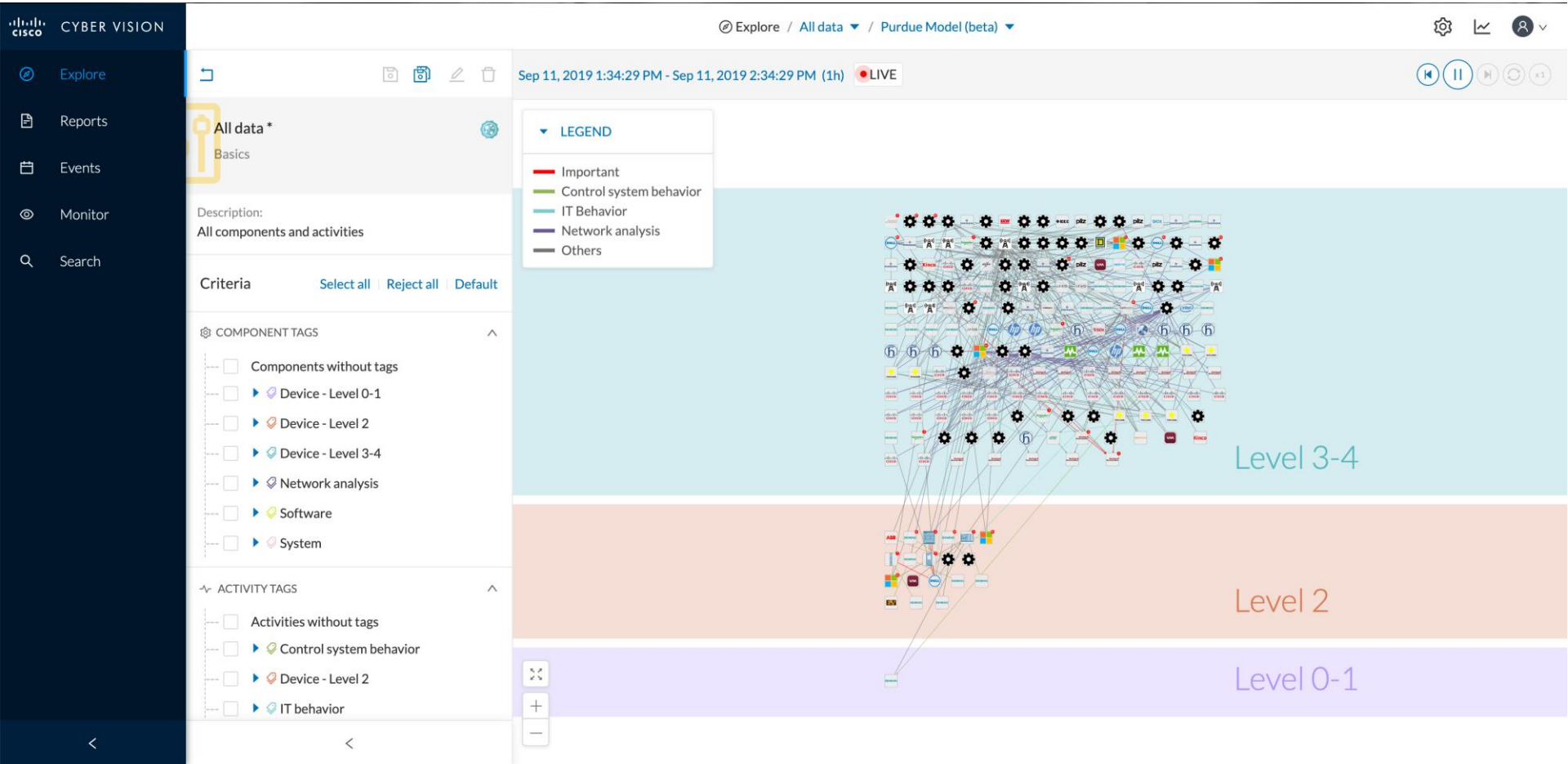
Непрерывность производства
Эталонная модель производственной сети

Архитектура - Эталонная модель Пердью

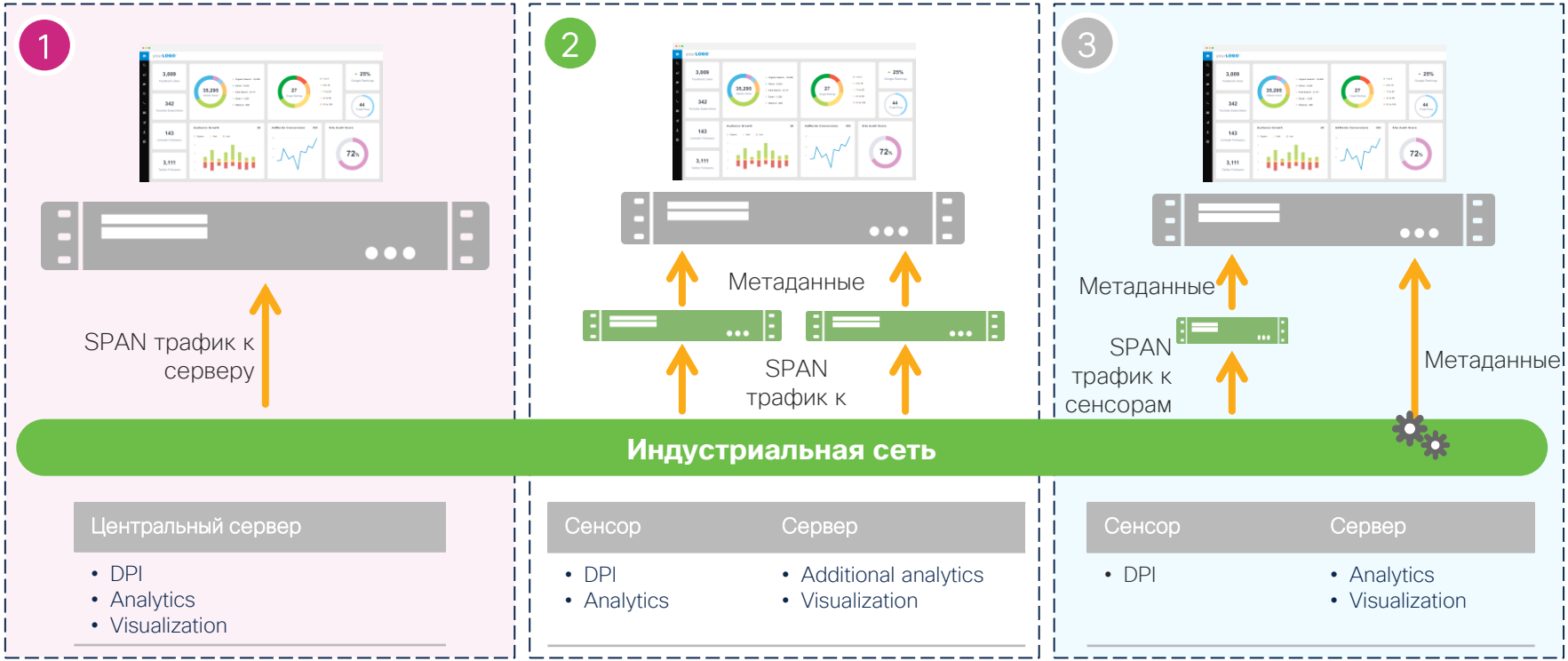


Компоненты Cisco	
Industrial DMZ	• Access control lists (ACLs) • Intrusion detection systems (IDS) and intrusion prevention systems (IPS) • VPN services • Portal and remote desktop services • Application and data mirrors
Industrial zone	• AAA identity services • Network management • Asset inventory • Anomaly detection • Plant-wide services • Traffic enforcement (plant to IDMZ, north/south)
Area zone	• Traffic Enforcement (Cell to Cell, East/West) • QoS Prioritization • SXP • Netflow
Inter-cell (ISA3000)	• Industrial deep packet inspection (DPI) • Stateful firewall and intrusion prevention (IPS) • Hardware bypass
Cell zone	• PoE/PoE+ • Layer 2 NAT • 802.1X • MAC Authentication Bypass (MAB) • Quality of Service marking • Netflow (IE3x00 and IE4000 only) • TrustSec tagging (IE3x00 and IE4000 only) • Edge compute (IE3x00 only)

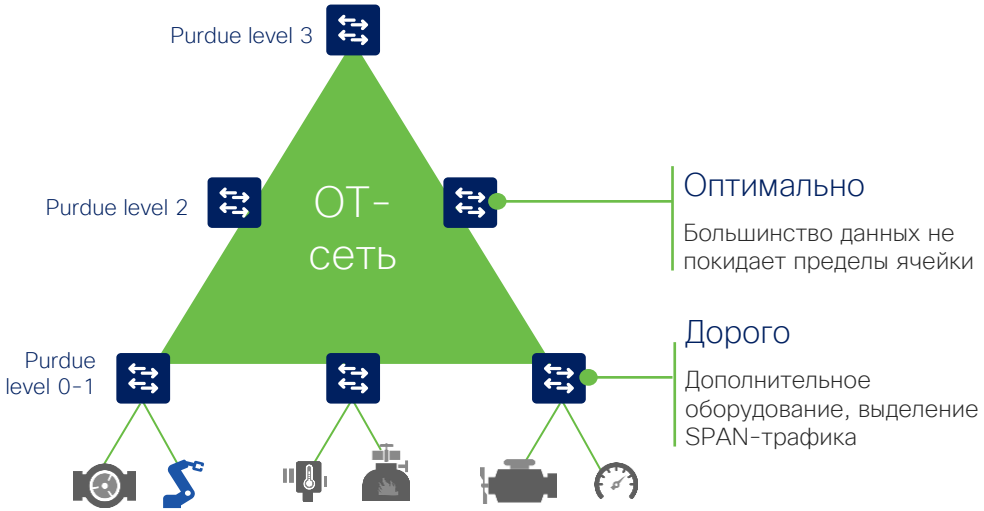
Эталонная модель Пердью в реальности



Типы систем обеспечения безопасности сетей АСУ ТП



Почему важен анализ трафика на сетевом уровне

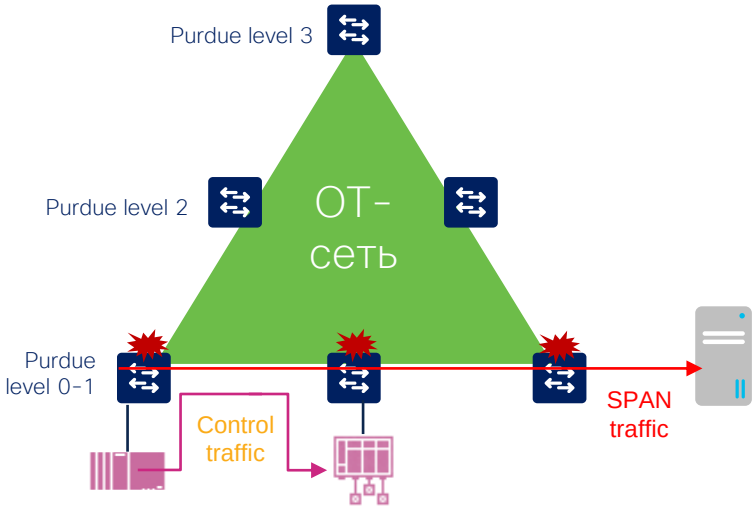


Точка просмотра трафика (DPI) имеет значение

- Зеркалирование трафика на уровне агрегации дает видимость только взаимодействия типа «Север-Юг»
- Зеркалирование трафика на уровне ячейки – дорогое решение

Сенсор на сетевом уровне видит все что подключено к сети

Почему важен анализ трафика на сетевом уровне

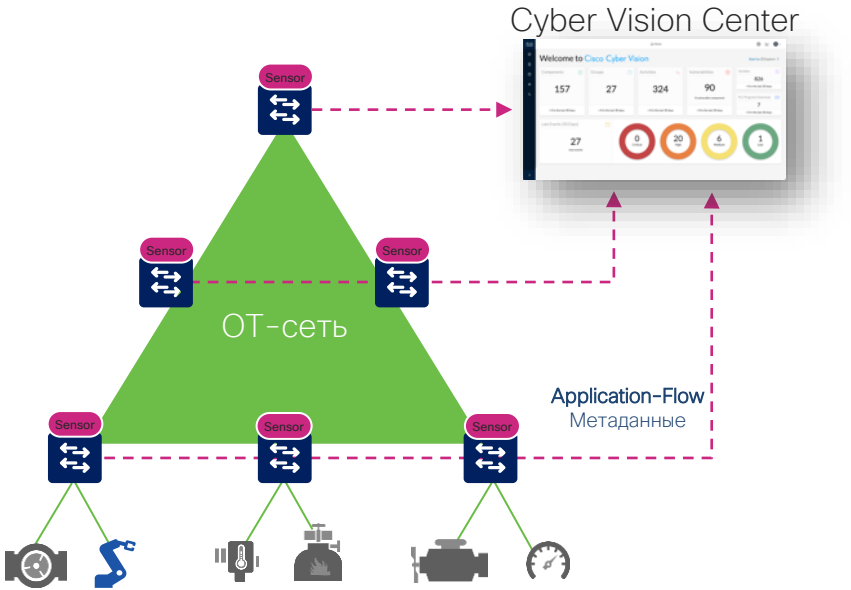


RSPAN увеличивает Jitter

- Блокирование Head-of-line, вызванное трафиком SPAN, отрицательно влияет на чувствительный ко времени цикл управления
- RSPAN в сетях LAN влияет на производительность

Сенсор на уровне сетевого оборудования не влияет на проходящий трафик

Почему важен анализ трафика на сетевом уровне



Мониторинг на уровне сети

- Сенсоры Cyber Vision на уровне сетевого оборудования
- Нет необходимости установки нового оборудования
- Нет влияния на производительность и временные задержки в сети

Простое внедрение
Низкая стоимость владения

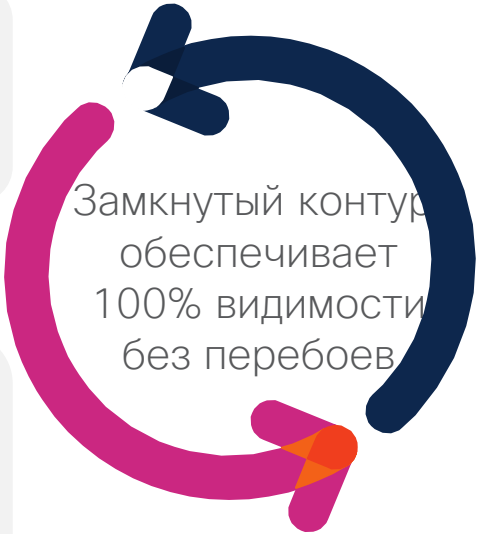
Активный и Пассивный опрос устройств

Пассивный опрос

- Определяет устройства за счет прослушивания трафика
- Нет взаимодействия с производственными устройствами
- Сенсоры на сети получают информацию без SPAN сети

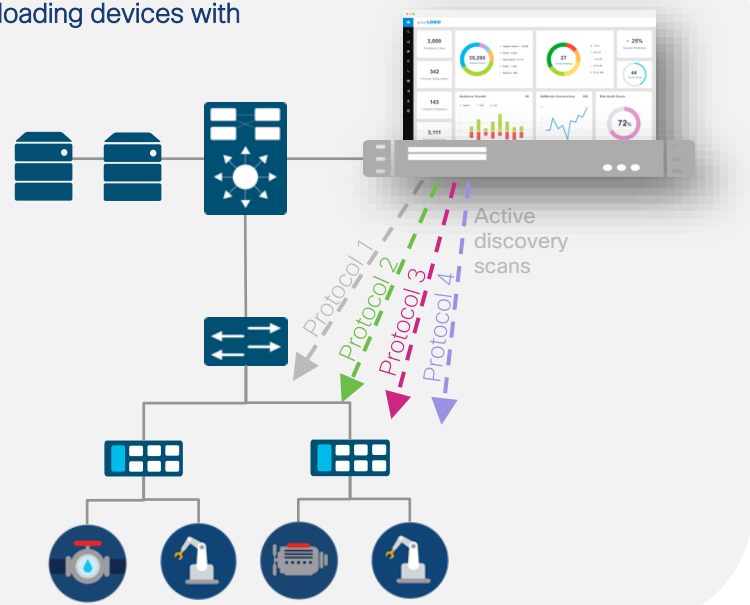
Активный опрос

- Изучает промышленные протоколы взаимодействия за счет пассивного опроса
- Сенсоры отправляют hello запросы для обнаружения устройств
- Получение подробно информации об устройствах

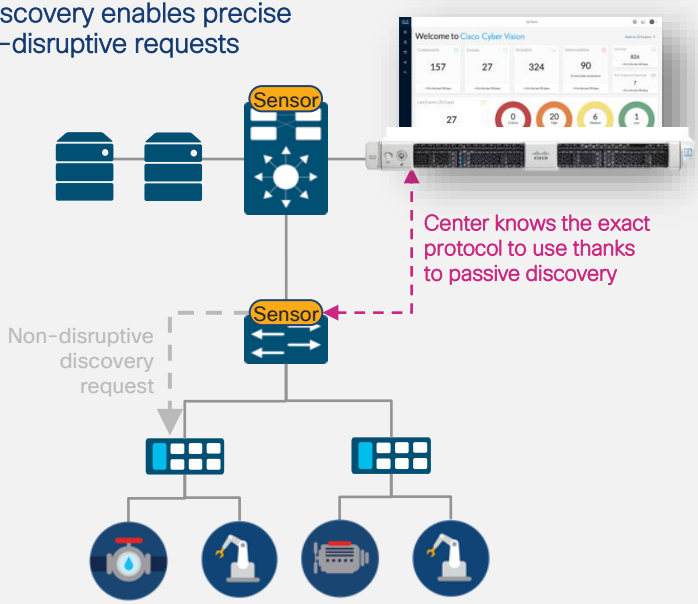


Замкнутый контур делает активное обнаружение безопасным

Basic active discovery solutions scan networks overloading devices with ARP requests



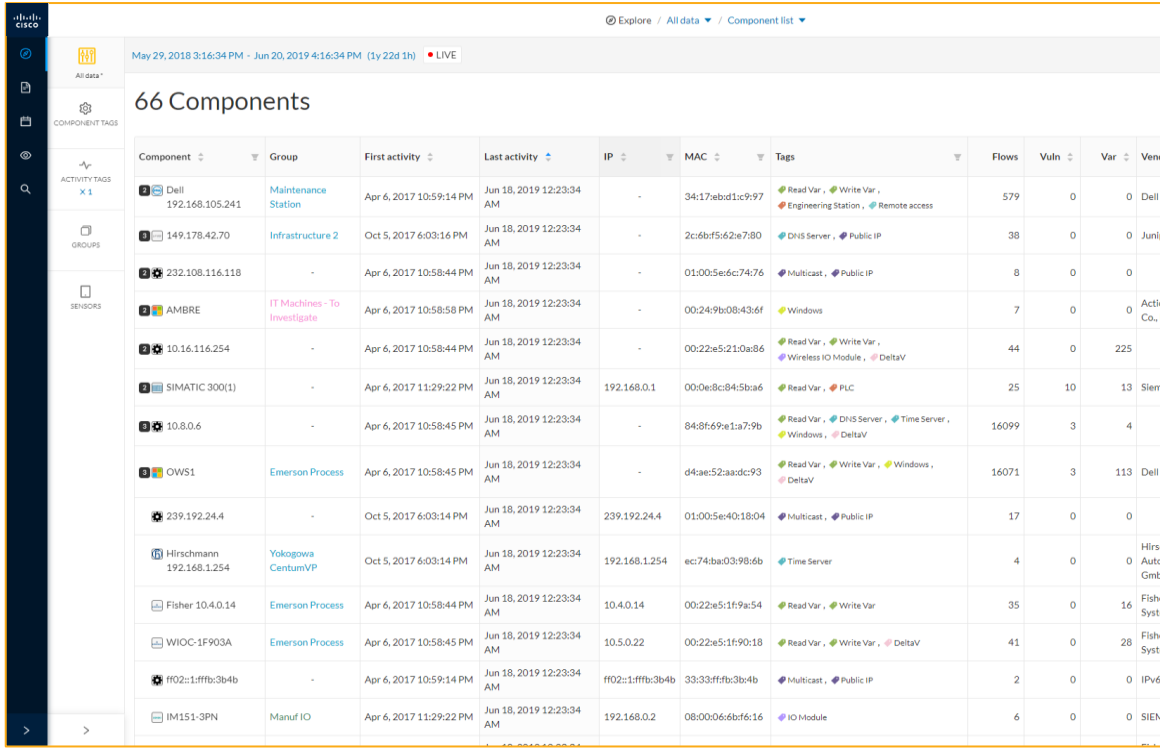
Closed-loop between passive and active discovery enables precise and non-disruptive requests



Контроль участников сети: полная инвентаризация

- Автоматическое определение всего оборудования (IT и OT) внутри сети
- Сбор данных по всему оборудованию
- Группировка участников сети
- Метаданные (тэги) по каждому оборудованию и его взаимодействию с другими участниками сети

Обеспечение защиты элементов индустриальной сети

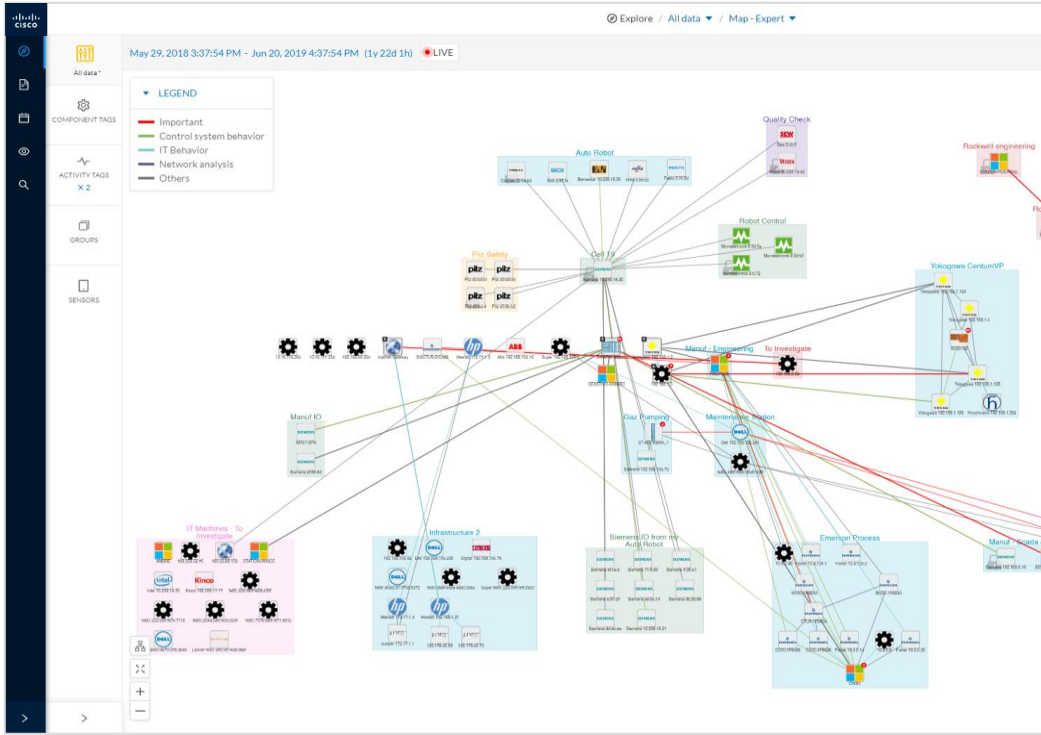


Component	Group	First activity	Last activity	IP	MAC	Tags	Flows	Vuln	Var
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	-	34:17:eb:d1:c9:97	Read Var, Write Var, Engineering Station, Remote access	579	0	0
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23:34 AM	-	2c:6b:f5:62:e7:80	DNS Server, Public IP	38	0	0
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	01:00:5e:6c:74:76	Multicast, Public IP	8	0	0
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23:34 AM	-	00:24:9b:08:43:6f	Windows	7	0	0
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	-	00:22:e5:21:0a:86	Read Var, Write Var, Wireless IO Module, DeltaV	44	0	225
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.1	00:0e:8c:84:5b:a6	Read Var, PLC	25	10	13
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	84:8f:69:e1:a7:9b	Read Var, DNS Server, Time Server, Windows, DeltaV	16099	3	4
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	-	d4:ae:52:aa:dc:93	Read Var, Write Var, Windows, DeltaV	16071	3	113
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	239.192.24.4	01:00:5e:40:18:04	Multicast, Public IP	17	0	0
Hirschmann 192.168.1.254	Yokogowa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM	192.168.1.254	ec:74:ba:03:98:6b	Time Server	4	0	0
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM	10.4.0.14	00:22:e5:1f:9a:54	Read Var, Write Var	35	0	16
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM	10.5.0.22	00:22:e5:1f:90:18	Read Var, Write Var, DeltaV	41	0	28
ff02::1:fffb:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM	ff02::1:fffb:3b4b	33:33:ff:fb:3b:4b	Multicast, Public IP	2	0	0
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM	192.168.0.2	08:00:06:6b:f6:16	IO Module	6	0	0

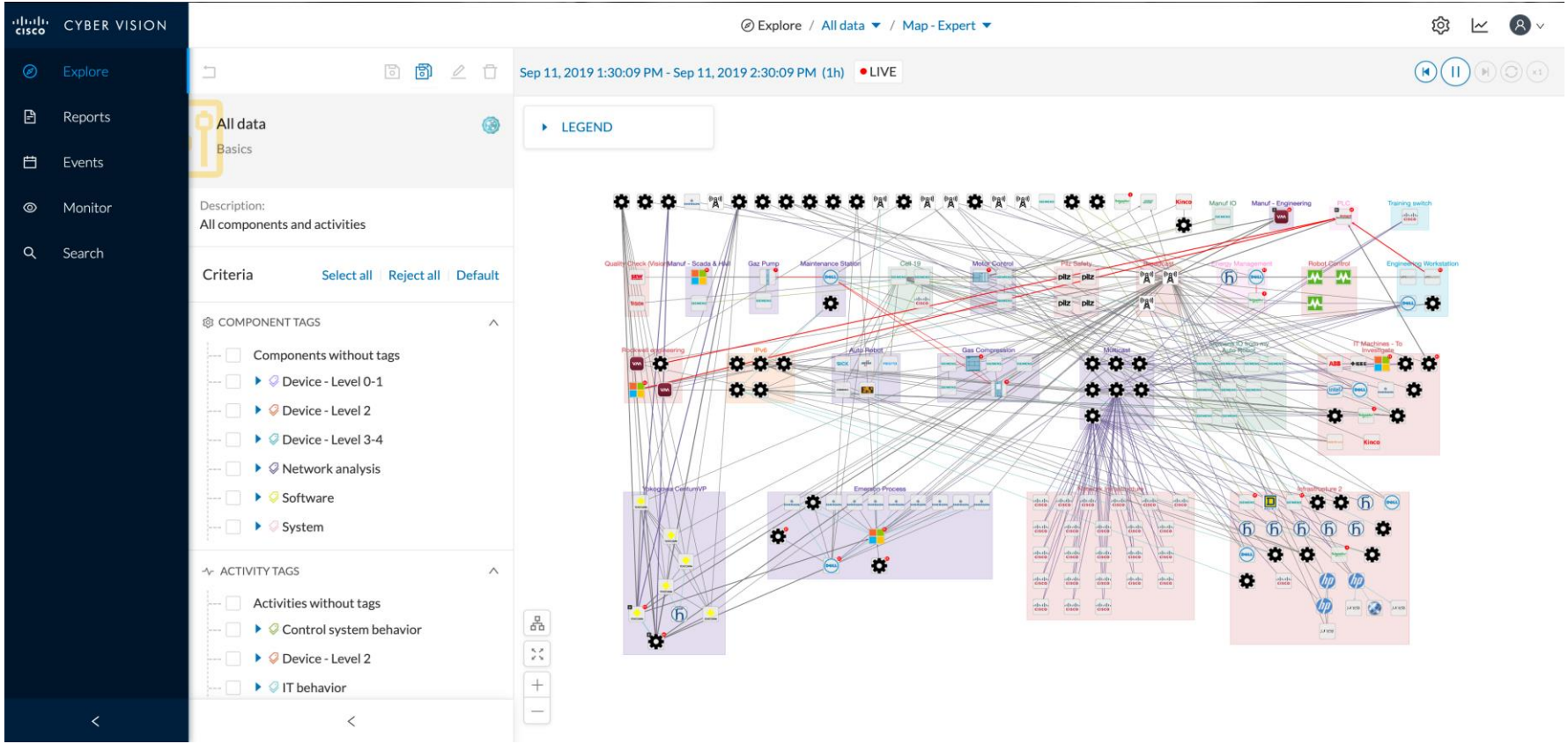
Контроль взаимодействий

- Определения всех связей и взаимодействий между участниками сети
- Детекция не нужных коммуникаций
- Установка тэгов на все коммуникации для упращения анализа
- Режим онлайн и просмотр записи

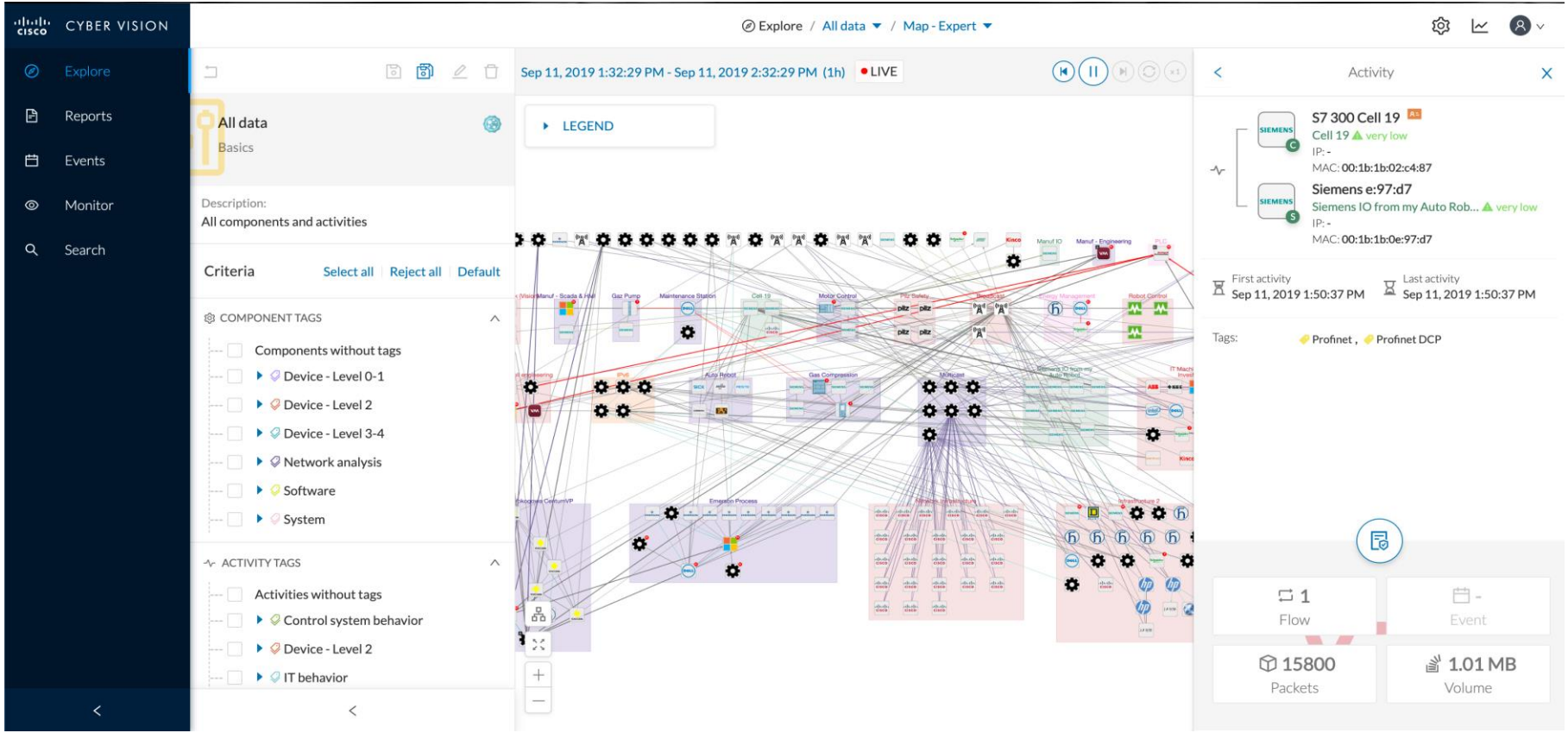
Инструмент сегментации и защиты сети



Map Expert



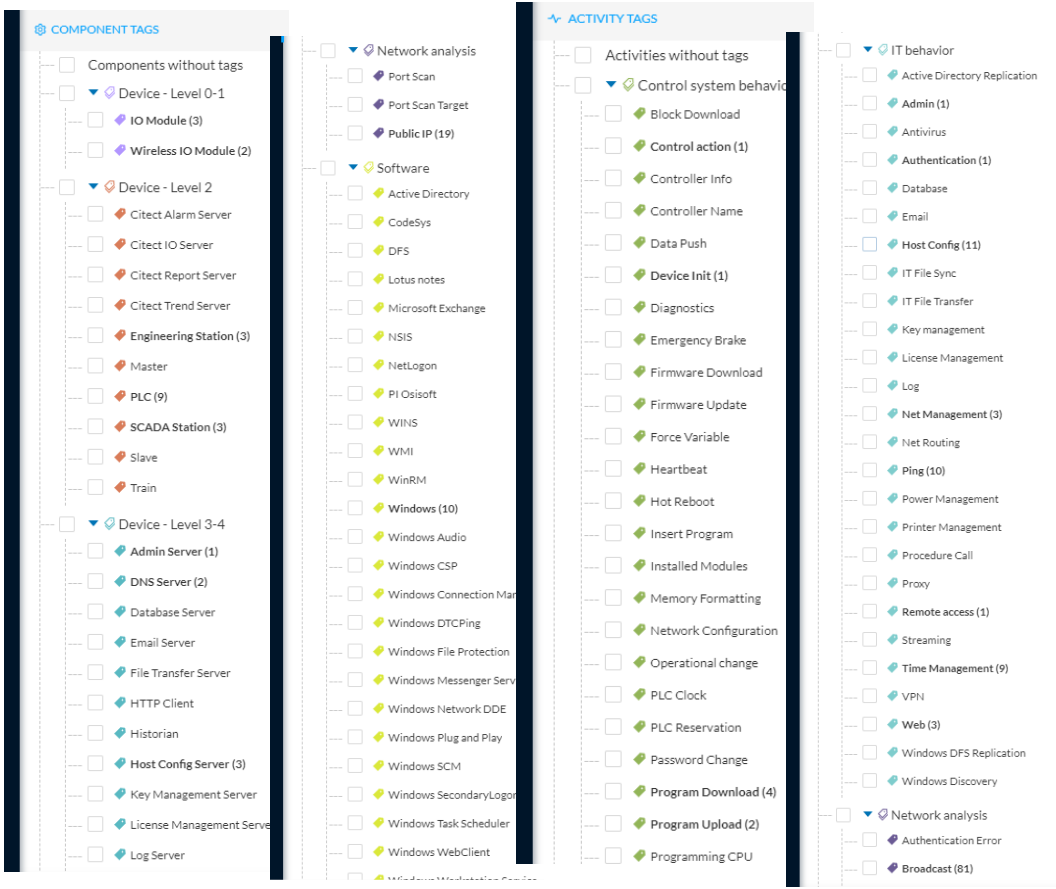
Map Expert



Метаданные для аналитики

- Характеристики устройства и его взаимодействия транслируются в тэги для облегченного анализа и контроля пользователем
- Общий язык, нет привязки к вендорам
- Не нужно быть экспертом в протоколах для понимания картины работы сети
- Автоматическая привязка к информации по устройству и его активности
- Новые тэги можно добавить и через RESTful API

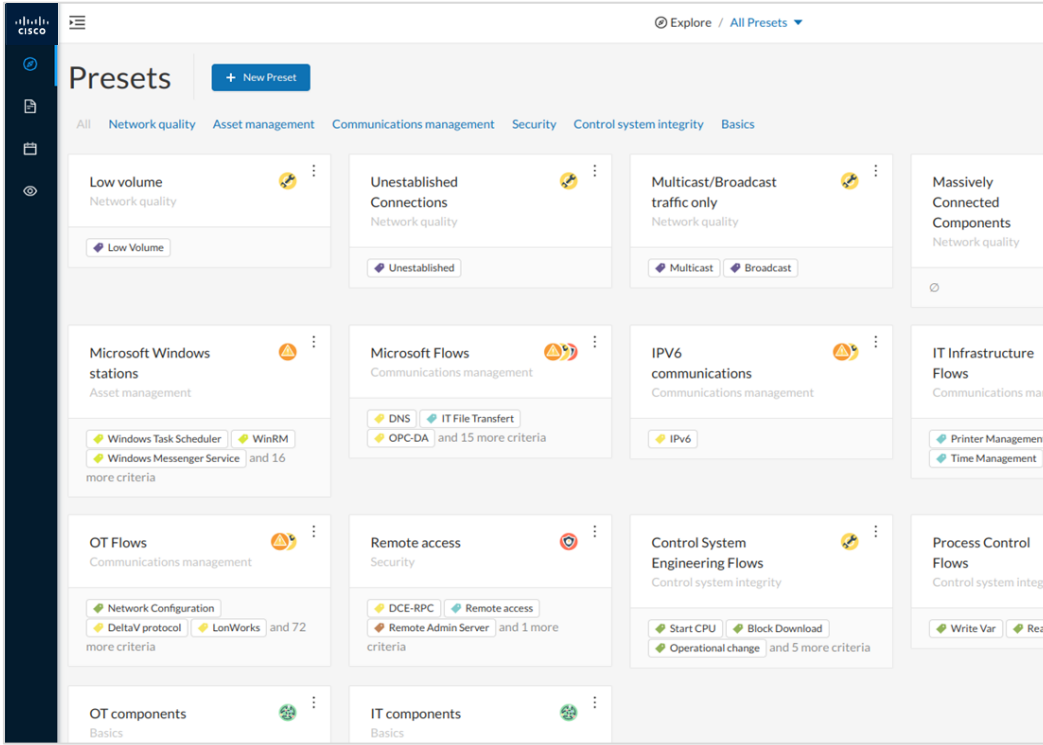
Увидеть активы и их взаимодействие в унифицированном формате



Использование пресетов

- Фильтры для просмотра нужных групп или типов данных на основании тэгов
- Разбор большого объема данных
- Переиспользование пресетов другими пользователями
- Предопределенные пресеты внутри системы, возможность создавать свои

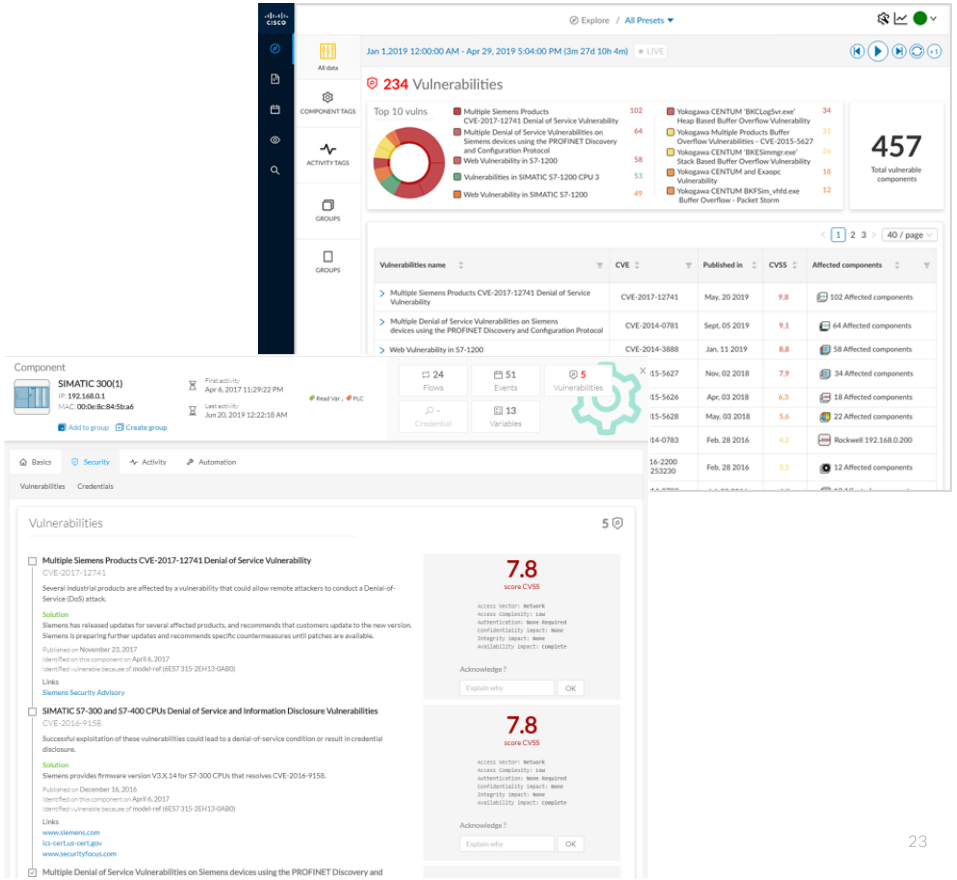
Фокус на то, что важно



Контроль уязвимостей участников сети

- Автоматический контроль программных и аппаратных уязвимостей
- Детальная информация по каждой уязвимости
- Встроенная база данных, пополняется Cisco Research Teams

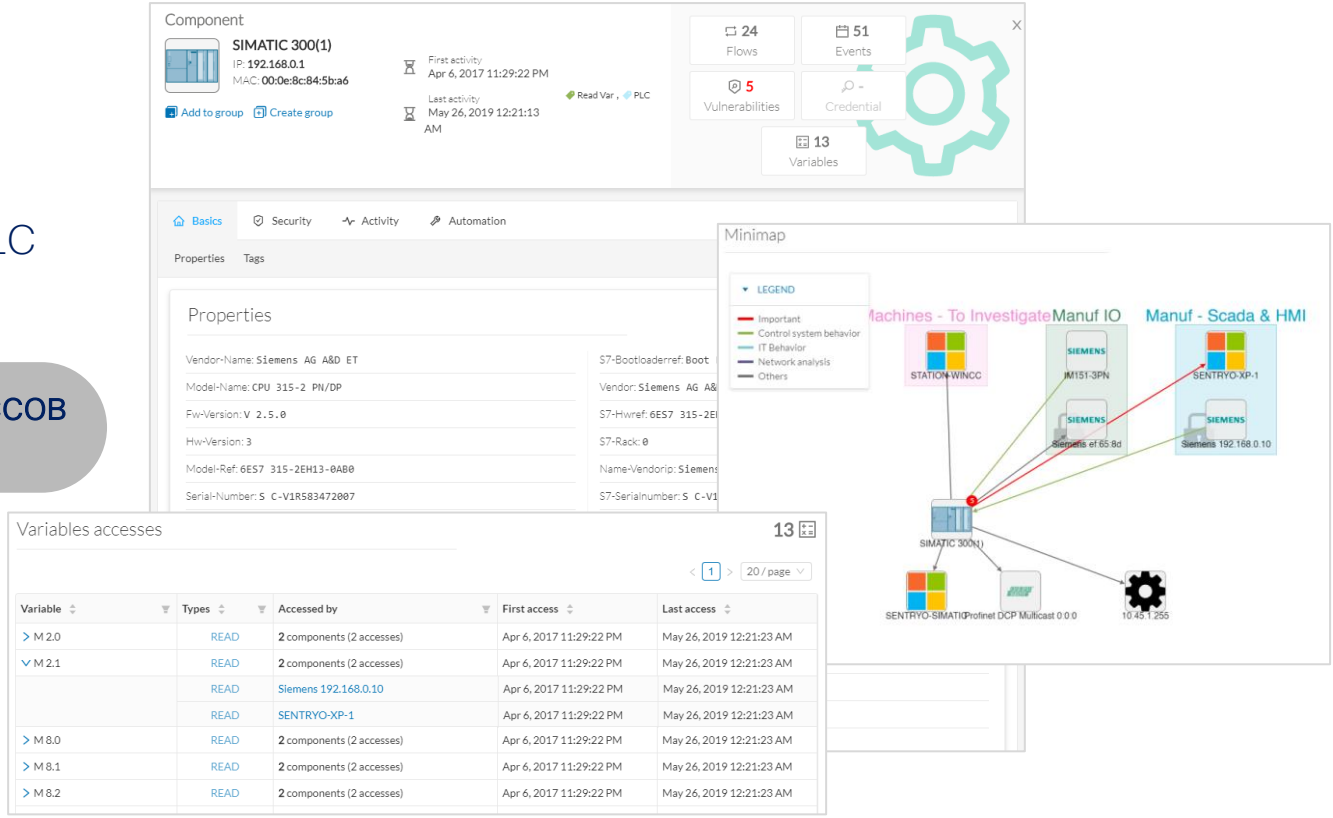
Использование лучших практик обеспечения безопасности



Детальная информация по каждому устройству

- Свойства устройств
- Карта взаимодействия
- Изменение программ PLC
- Переменные

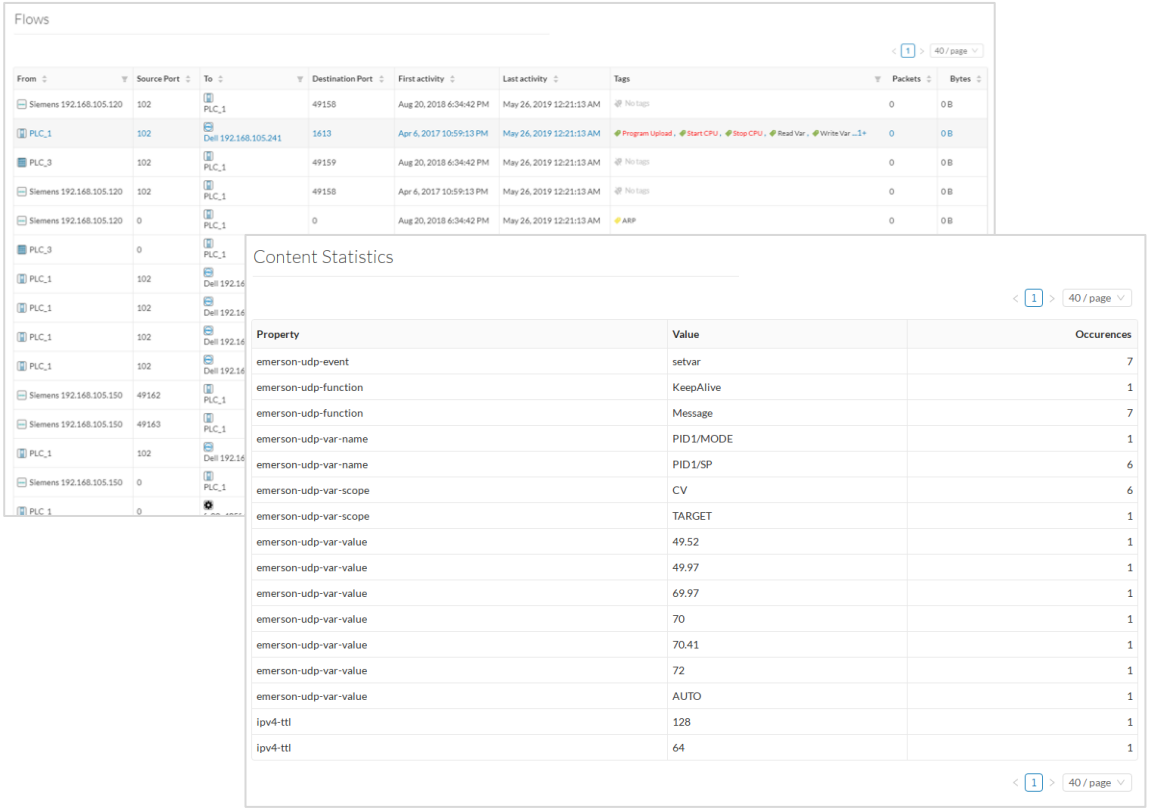
Мониторинг всех процессов и параметров



Разбор инцидентов

- Доступ к полной истории взаимодействия устройства в сети
- Детальные свойства и статистика по каждому потоку данных
- Режим онлайн или исторический анализ по времени

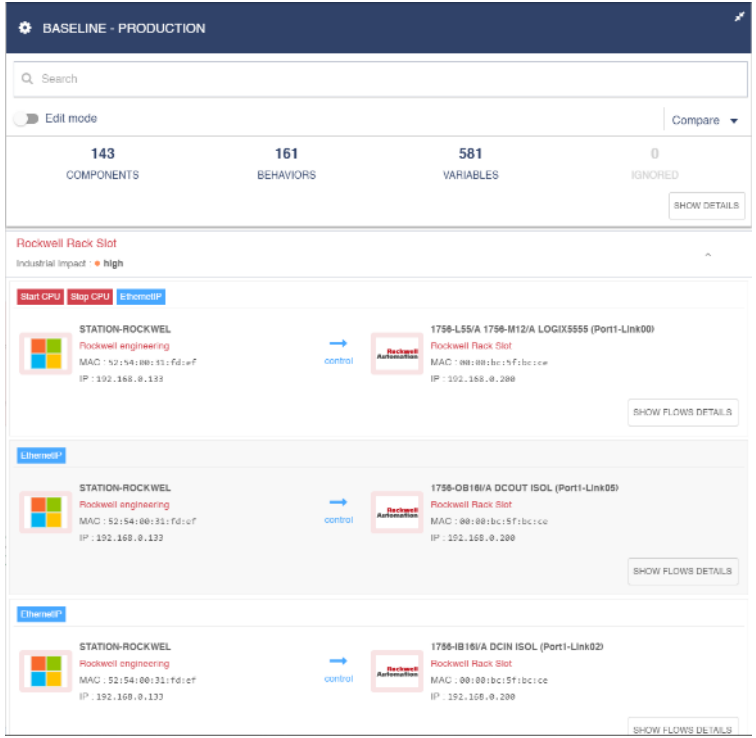
Протоколирование взаимодействия



Обнаружение аномалий

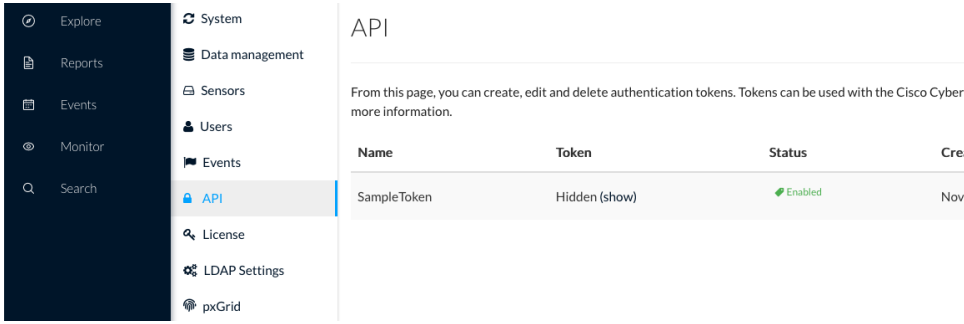
- Создание эталонной модели участников сети и их взаимодействия
- Отклонение от эталонной модели – автоматическая тревога
- Импорт правил атак для детекции злонамеренного поведения
- Улучшение безопасности через обучение модели обнаружения угроз

Обнаружение атак и аномального поведения



Интеграция через **RESTful API**

- Использование внешних приложений для автоматизации функций безопасности
- Изменение тэгов, пресетов и групп
- Кастомизированные сценарии обнаружения



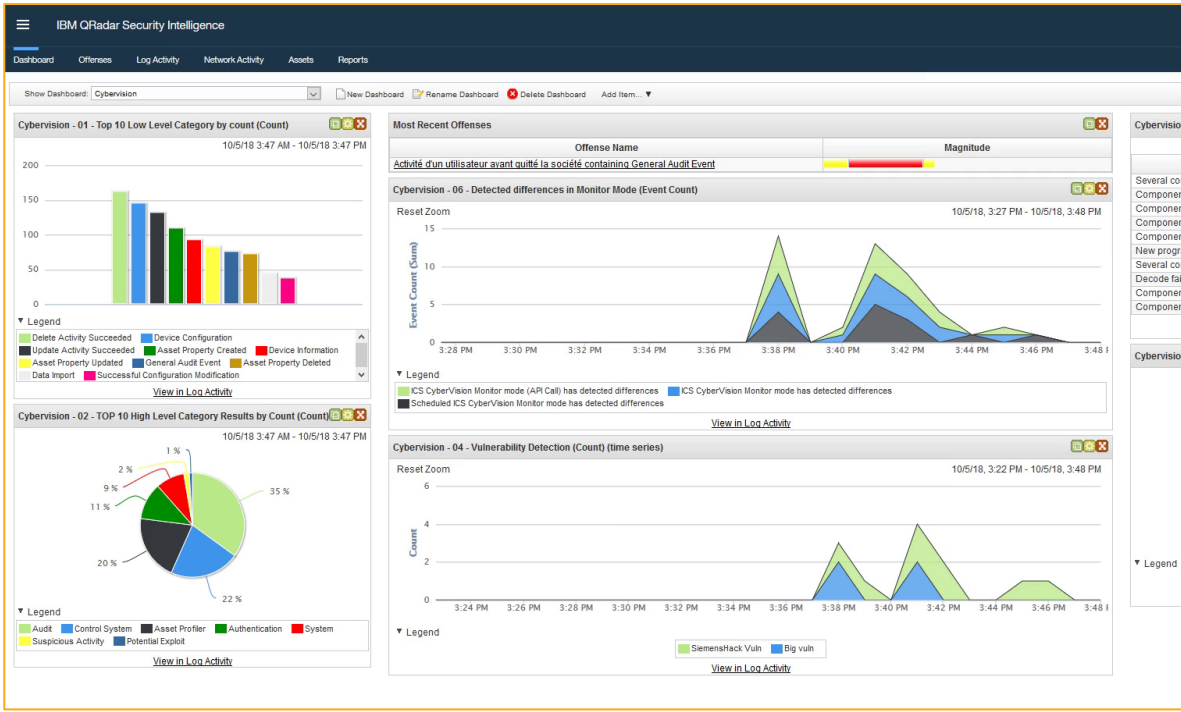
Интеграция данных
в любые внешние приложения

Интеграция с IBM QRadar

Универсальное управление IT/OT безопасностью в SIEM

Визуализация

Syslog




cisco
SECURE