IT.Integrator | cisco Partner

Cisco Cyber Vision: наскрізний моніторинг і безпека індустріальних мереж

Михайло Скуратівський
IT Інтегратор

IT.Integrator | cisco Partner

Драйвери ринку кібербезпеки в Україні

Критична інфраструктура

Постанова КМУ №518
Наказ Міністерства енергетики України №417
(дослівний переклад NIST Cybersecurity Framework)

«…Функції кібербезпеки узгоджені з чинними підходами щодо управління ризиками кібербезпеки та допомагають продемонструвати ефективність інвестицій в кібербезпеку…»

Постанова КМУ №518 від 19.06.2019 «Загальні вимоги до кіберзахисту ОКІ»

Постанова КМУ №257 від 24.03.2023 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»

Державні установи

Закони України та підзаконні акти і низка НД ТЗІ
Міжнародні стандарти, зокрема ISO 2700x

IT.Integrator | cisco Partner

Об’єднання двох світів: IT & OT

IT та OT стають більше взаємозалежними по захисту промислових мереж від кіберзагроз

IT.Integrator | cisco Partner

Cisco визнана лідером у сфері безпеки IoT/OT

За даними Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, 4 квартал 2021 року, компанія Cisco була визнана лідером у сфері кібербезпеки IoT/OT.

FORRESTER®
WAVE LEADER 2021
Industrial Control Systems (ICS) Security Solutions

Це рішення, забезпечує надійну безпеку в складних умовах, включаючи операційні технології (OT), промислові системи управління (ICS) і кіберфізичні системи (CPS)

IT.Integrator | cisco Partner

Cisco Cyber Vision

Платформа “видимості” (visibility) & безпеки для промислового Інтернету речей

“Видимість” активів (Visibility)

Інвентаризація активів
Виявлення патернів комунікаційних активностей

Відображення поточного стану кіберзагроз (Security Posture)

Ідентифікація вразливостей пристроїв
Скоринг ризиків

Операційна аналітика (Operational Insights)

Відстеження модифікацій процесу/пристрою
Запис подій системи контролю

Контекст і аналітика стають фундаментальними елементами по захисту мереж ОТ

IT.Integrator | cisco Partner

Традиційний підхід по впровадженню “видимості” в ОТ

Типові промислові рішення для “видимості” та виявлення вразливостей вимагають SPAN рішень (дзеркалювання трафіку)

Додаткові комутатори
для збору SPAN трафіку

Додаткові витрати на СКС
для збору SPAN трафіку

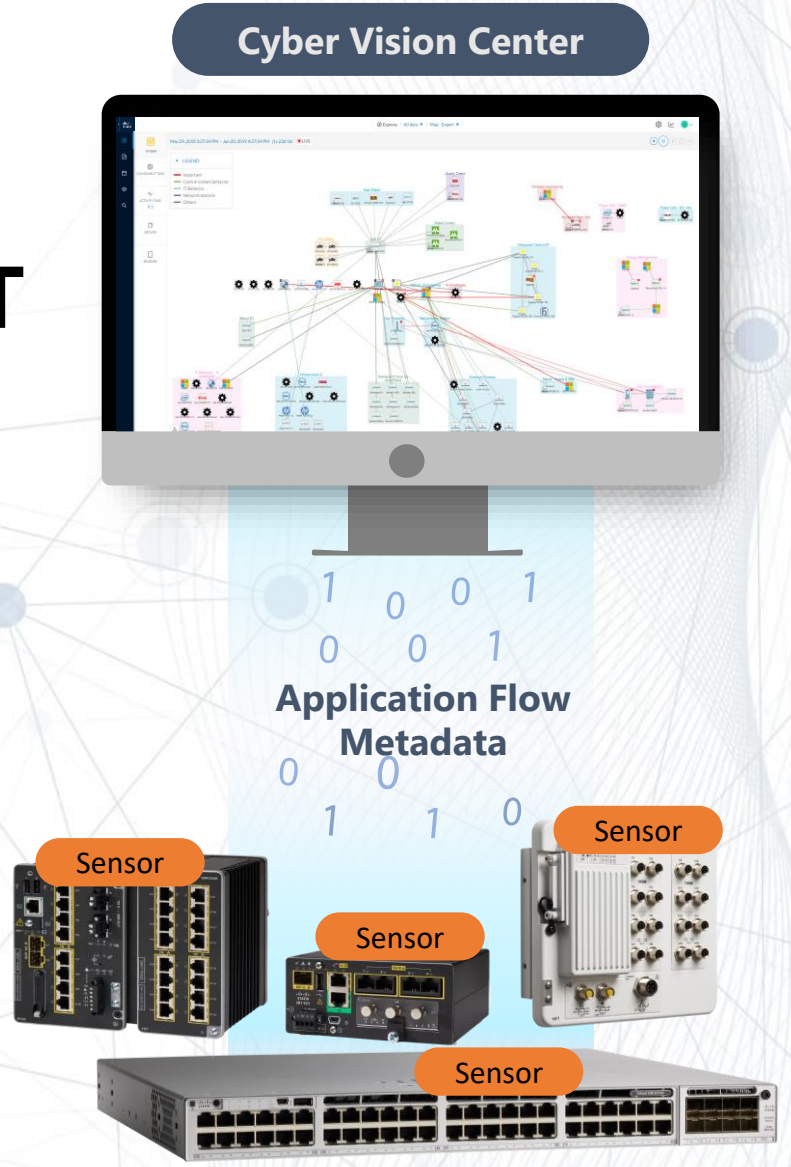
Експоненціальне збільшення трафіку
за рахунок навантаження SPAN трафіком

Сукупна вартість володіння (TCO) на основі SPAN є не вигідною в довгостроковій перспективі

IT.Integrator | cisco Partner

Сучасний підхід Cisco Cyber Vision по впровадженню “видимості” в ОТ

Промислові комутатори та шлюзи Cisco “бачать” усе, що до них під’єднано, для комплексного моніторингу кіберзагрор, та відповідної реакції на них.



Глибока перевірка пакетів (DPI) та активне виявлення (Active Discovery) активів вбудовані у вашу мережеву інфраструктуру

IT.Integrator | cisco Partner

Функціональна роль сенсора Cyber Vision, як ключового елементу “видимості” OT мережі

Збирає трафік промислової мережі

Captures industrial network flows (passive) and queries devices (active). Stores data locally in case the Center is not accessible

Розбирає промислові протоколи (DPI)

Understands most OT and IT communication protocols to analyze packet payloads and extract meaningful information

Надсилає метадані до Cyber Vision Center

Sends metadata to the Center for storage, analysis and visualization. This only adds 3 to 5% extra traffic to the network

IT.Integrator | cisco Partner

Що це дає для IT: підвищення безпекі IT/OT

Сегментація OT мереж

Знайте свої активи OT, щоб впроваджувати політики доступу, не перериваючи виробництво

Конвергентні операції безпеки

Отримуйте контекст OT і події в SOC, щоб створювати та застосовувати правильні політики безпеки

Зменшіть поверхню атаки

Визначення ризиків для коригувальних дій та впровадження найкращих практик

Стимулюйте співпрацю між IT та OT

Поділіться спільним розумінням ситуації, щоб разом будувати політики безпеки

Використовуйте існуючу мережу Cisco, для збільшення “видимості” OT і захисту всього підприємства

IT.Integrator | cisco Partner

Що це дає для OT: підвищення ефективності виробництва

Підвищення продуктивності мережі

Виявлення проблем з конфігурацією мережі, непотрібного трафіку та старих пристроїв

Скорочення часу простою

Виявляйте проблеми з пристроєм і конфігурацією, перш ніж вони порушать виробництво

Швидший пошук і усунення проблем

Записуйте всі події OT для аналізу першопричин, коли компоненти АСУ ТП мають проблеми

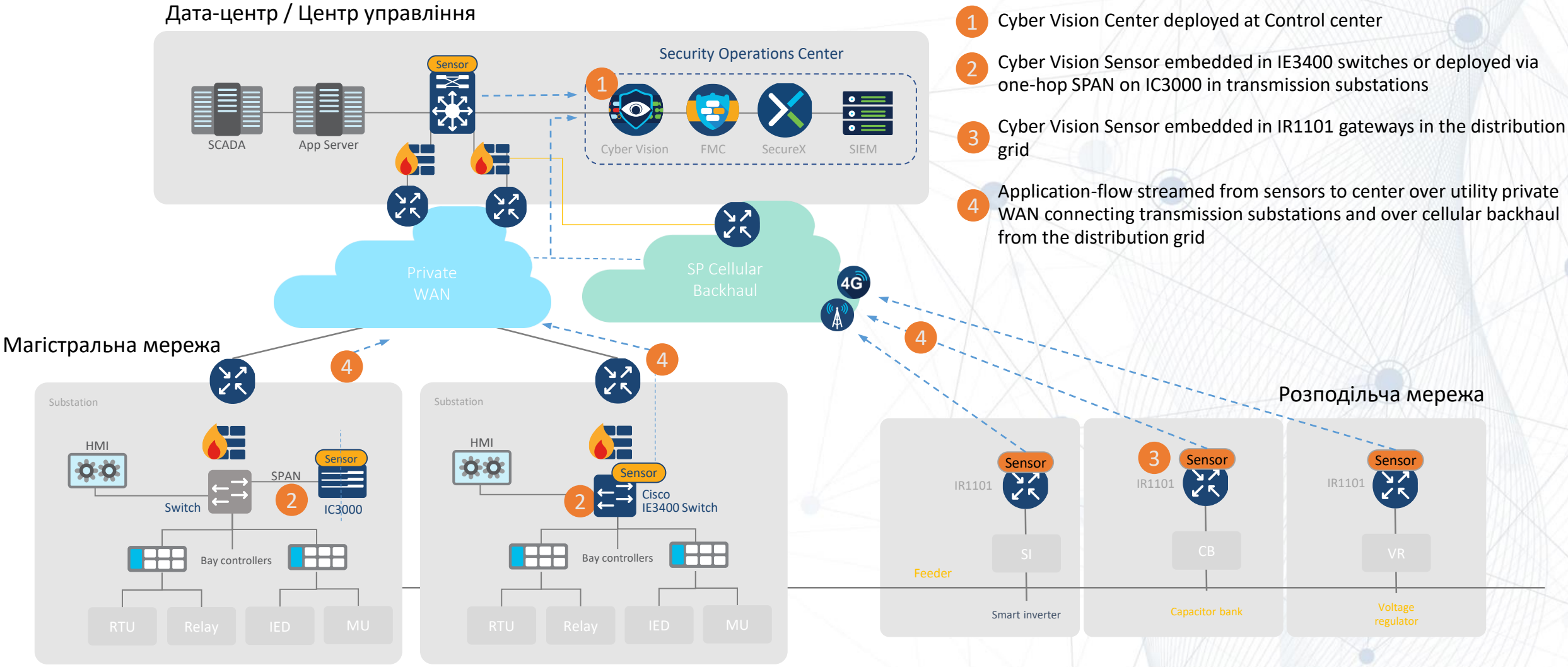
Моніторинг діяльності підрядників

Відстежуйте сеанси віддаленого доступу та всі зміни, внесені постачальниками до вашої АСУ ТП

Промислова мережа Cisco забезпечує всебічну “видимість” для підвищення операційної ефективності

IT.Integrator | cisco Partner

Архітектура OT/IT безпеки в енергетичних компаніях



1. Cyber Vision Center deployed at Control center
2. Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in transmission substations
3. Cyber Vision Sensor embedded in IR1101 gateways in the distribution grid
4. Application-flow streamed from sensors to center over utility private WAN connecting transmission substations and over cellular backhaul from the distribution grid

IT.Integrator | cisco Partner

Демо: “Видимість” активів

Cisco Cyber Vision

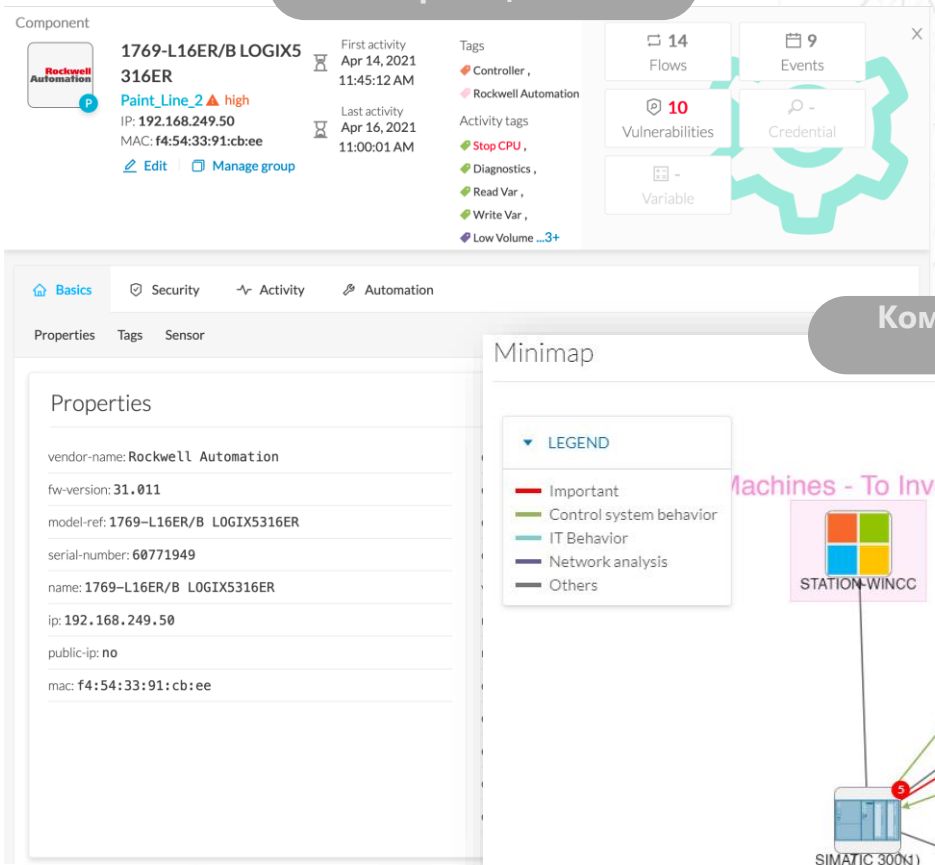
Інвентаризація активів

Комплексна актуальна інвентаризація всіх активів у вашому оточенні

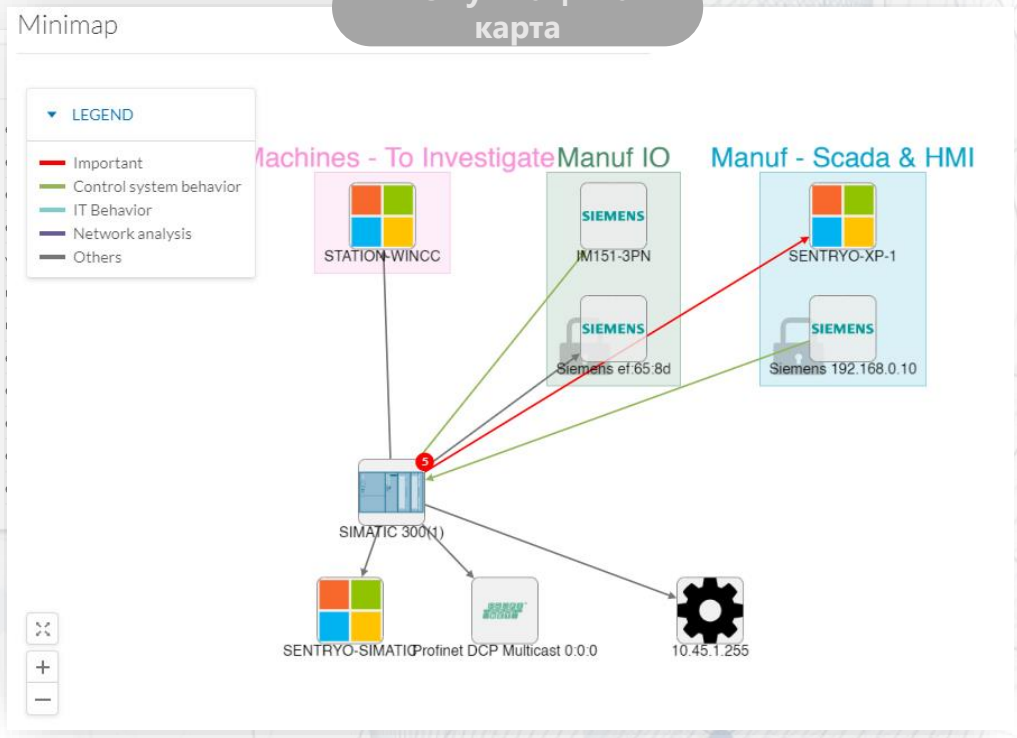
Коммунікаційні патерни

Динамічна карта зв'язку з детальними інформаційнійними потоками на прикладному (application) рівні

Інвентаризація активів



Комунікаційна карта



IT.Integrator | cisco Partner

Демо: Відображення поточного стану кіберзагроз

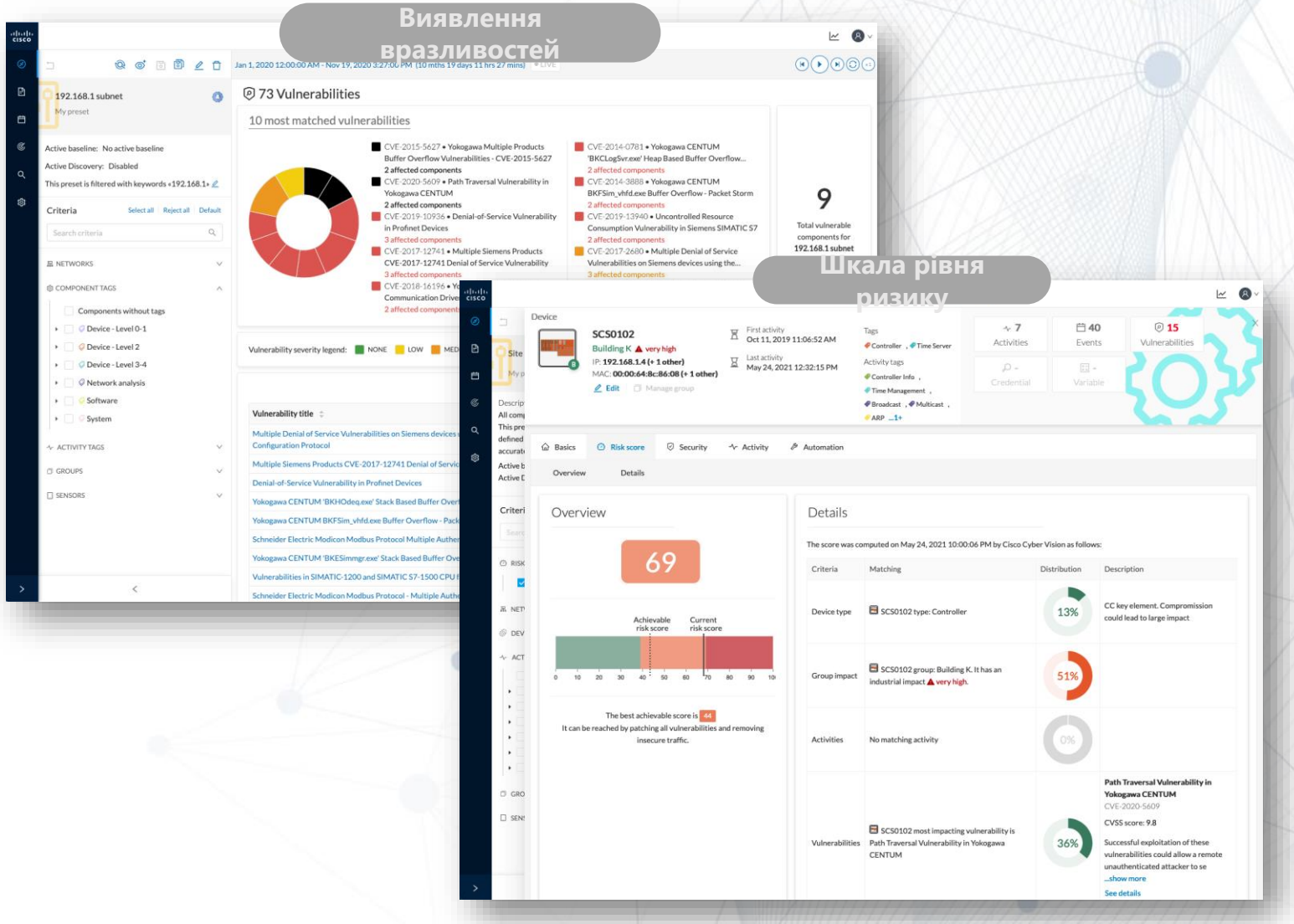
Cisco Cyber Vision

Виявлення вразливостей

Визначте відомі вразливості активів, щоб ви могли виправити їх до того, як вони будуть використані

Скоринг ризиків

Оцінка ризиків з активами на основі їх впливу та ймовірності, щоб допомогти вам покращити відповідність вимогам кібербезпеки



IT.Integrator | cisco Partner

Демо: Операційна аналітика

Cisco Cyber Vision

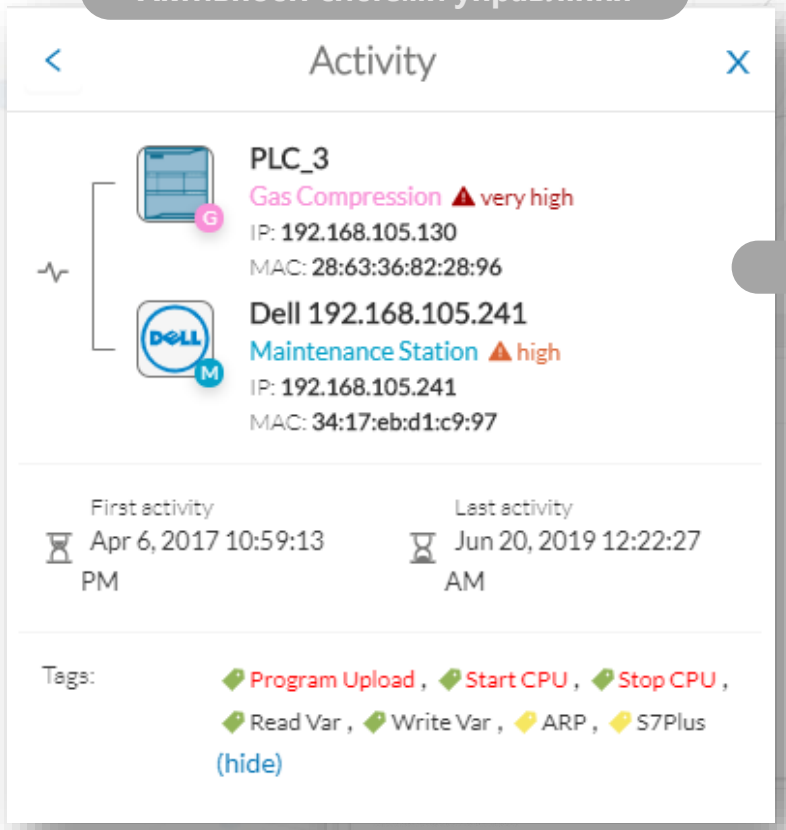
Активності системи управління

Відстежування процесів модифікації
Виявлення змін у конфігурації
Запис подій системи контролю

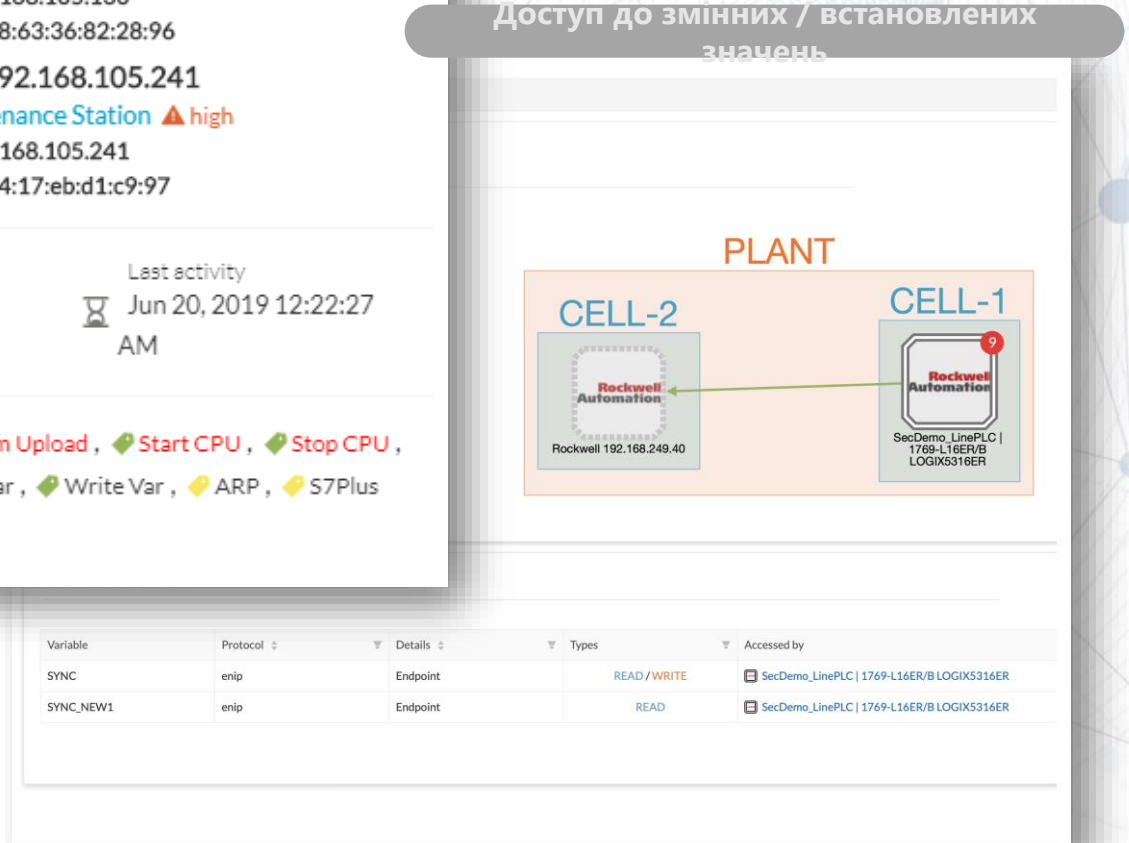
Доступ до змінних / встановлених значень

Відстеження, до яких - змінних даних, об'єктів та встановлених значень звертаються або змінюють

Активності системи управління



Доступ до змінних / встановлених значень



IT.Integrator | cisco Partner

Приклад застосування

Велика енергетична компанія в EMEA+UA

Бізнес-драйвери
- 1000 підстанцій для моніторингу та безпеки
- Обмежений простір для встановлення обладнання на підстанціях
- Підтримка стандарту IEC-61850 (MMS/GOOSE)
- Потрібна інтеграція з міжмережевими екранами

Рішення
- На кожній підстанції встановлено по одному датчику Cyber Vision
- Один центр Cyber Vision Center в диспетчерській
- Інтеграція з IBM QRadar (SIEM)
- Інтеграція з міжмережевими екранами Cisco FTD і Fortinet

Результати
- Розгортання першої черги включає 52 підстанції
- Cyber Vision, інтегрована в SOC
- Добре адаптована периферійна архітектура рішення для обмеженого простору для встановлення обладнання на підстанції і нижчі витрати на обладнання

IT.Integrator | cisco Partner

Cisco Cyber Vision портфоліо

Cyber Vision Center

Hardware Appliance
UCS based servers with Hardware RAID

CV-CNTR-M5S5
- 16 core CPU
- 64 GB RAM
- 800GB drives

CV-CNTR-M5S3
- 10 core CPU
- 32 GB RAM
- 480GB drives

Software Appliance
Virtual Machines

VMWare ESXi OVA

HyperV VHD

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Amazon Web Services

Microsoft Azure

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Cyber Vision Sensors

Catalyst IE3300 and IE3400 Switches

Catalyst IE3400HD IP67 Switch

Catalyst IR1101 LTE/5G Gateway

Catalyst IR8300 Multiservice Router

Catalyst IE9300 Rugged* Aggregation Switches

Catalyst 9300/9400

Network-Sensors
Deep Packet Inspection built into network-elements eliminating the need for SPAN

IC3000 Industrial Compute

Hardware-Sensor
DPI via SPAN to support brownfield

IT.Integrator | cisco Partner

Cyber Vision розширює IT-безпеку на OT

Cyber Vision Center
OT Application Flow Analysis

OT CONTEXT

OT CONTEXT

Cisco Secure Firewall
Traffic Filtering

Cisco ISE
Access Control
Policy-based Segmentation

VISIBILITY

Cyber Vision Sensors

Глибока перевірка пакетів, вбудована у вашу промислову мережу Cisco

Cisco Secure Analytics
NetFlow analysis

Cisco SecureX
Correlate Threat Intelligence
Orchestrate Remediation

Найширше рішення для безпеки OT на ринку • На базі Talos Threat Intelligence

IT.Integrator | cisco Partner

Cisco прагне привнести свою експертизу, досвід і простоту використання у сферу промислової безпеки

Cisco Industrial Networks

Підключайте будь-що будь-де

Cisco Security

Комплексна кібербезпека IT/OT

Cisco Validated Designs

Сучасний архітектурний дизайн

Cisco Customer Services

Клієнтська підтримка для розгортання рішень промислової безпеки

Усі вони працюють разом для успішного розгортання промислової безпеки

IT.Integrator | cisco Partner

Дякую за увагу!