OT Cyber Attacks

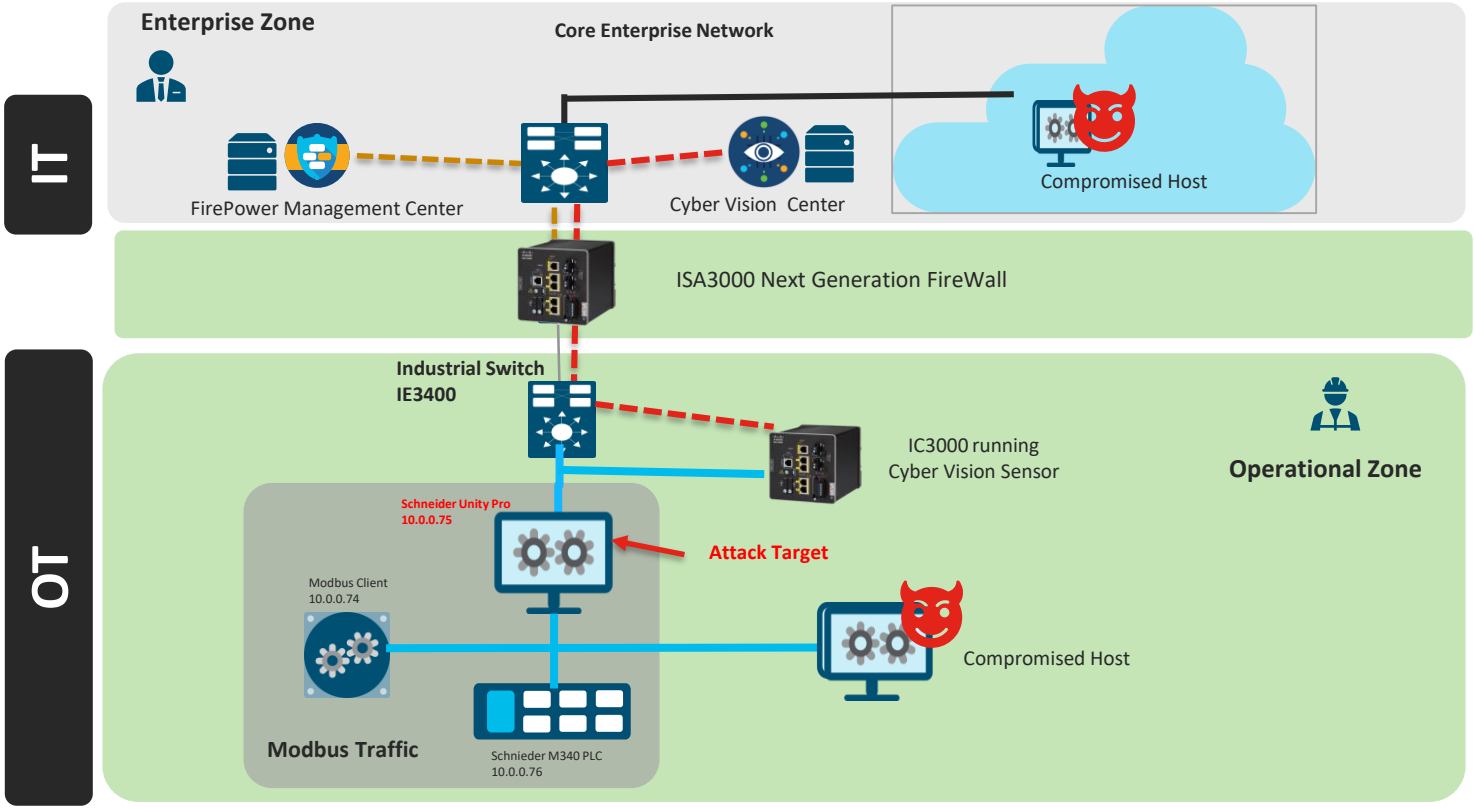
A close look at how it can happen

Steve Matthews and Greg Leonard
Industrial IoT Specialists in EMEAR
November 25, 2020

What you will see today….

1. A cyber attack of an OT workstation for SCADA system
   - Witness how to discover vulnerabilities and exploit them
2. How an OT Cyber Security tool called Cyber Vision will capture such an attack
   - What attack events look like
3. How a Next Generation Firewall called Cisco Firepower Threat Defense recognises and stops the attack in its tracks

Lab Demo Setup



IoT Networking + Security Portfolio

https://www.cisco.com/go/iot

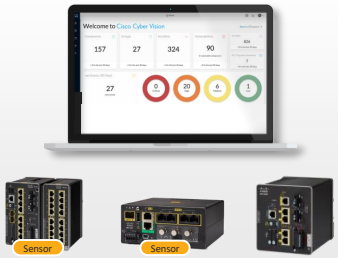
Industrial Switching
1K, 2K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS, ESS

Industrial Routing
IR8XX, IR1101, CGR1120, CGR1240, CGR2010

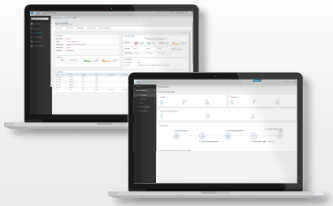
Embedded IoT
ESS, ESR, ESW, Resilient Mesh

Industrial Wireless
Fluidmesh, IW6300, IW3702, IR5XX, IXM Gateway

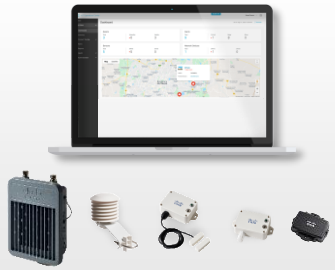
Industrial Security
ISA 3000, Cyber Vision



Edge Intelligence
IOx



Full-stack as a Service
Industrial Asset Vision



Management & Automation
Field Network Director, Industrial Network Director, IoT Operations Center

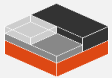
Cisco Cyber Vision **portfolio**

Cyber Vision Center

Hardware Appliance
CV-CNTR-S5

Intel 2.3GHz (16 Core) CPU, 32GB RAM
x2 800GB SSD RAID-1 or x4 800GB SSD RAID-10

Software Appliance
CV-CNTR-ESXI



VMWare ESXi 6.x+
OVA

Minimum requirements
CPU: Intel Xeon, 4 cores
RAM: 8GB
Storage: 50GB
SSD highly recommended
Network: 2 network interfaces

Cyber Vision Sensors

Hardware-Sensor
Dedicated hardware sensor

IC3000 Industrial Compute

Network-Sensors
Software built into Cisco's industrial network equipment

Cyber Vision 3.1

IE 3400 Switch

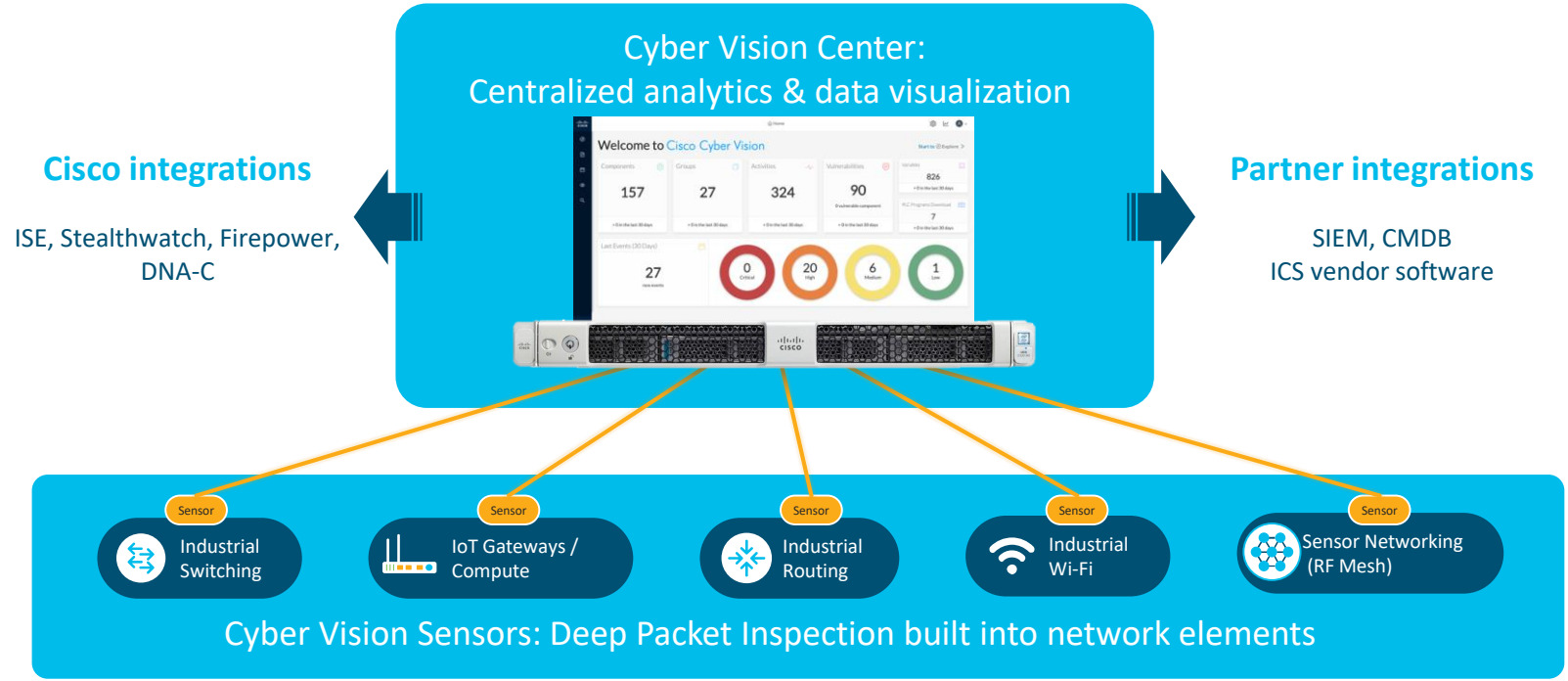
IE 3400H Switch

IR 1101 Gateway

Catalyst 9300

Two tier **edge monitoring** architecture

Industrial cybersecurity that can be deployed at scale



Cisco Cyber Vision

Asset Inventory & Security Platform for the Industrial IOT

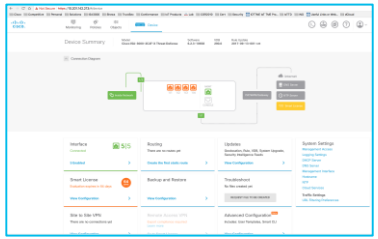
ICS Visibility
Asset Inventory
Communication Patterns
Device Vulnerability

Operational Insights
Identify configuration changes
Record control system events
relevant to the integrity of the system

Threat Detection
Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

Cisco Cyber Vision helps companies protect
their industrial control systems against cyber risks

ISA 3000 – Platform Summary



Cisco Industrial Security Appliance 3000

- Services include Firewall, VPN and IPS, DHCP, NAT, and others
- Supports Industrial Protocols / Application detection and DPI
- Ruggedized hardware with DIN Rail mounting
- Thermals: -40 C to +60 C (continuous operation)
- Hazloc with nA protection
- Industrial, Utility, Marine, Railway Compliance support

Firewall Software:

- Next Gen Firepower Threat Defence with IPS
- ASA + Firepower IPS Module

Management :

- For FTD: Firepower Device Manager and/or Firepower Mgmt Center
- For ASA: ASDM + FMC (Firepower Management Center)

ISA3000 Industrial Protocol Support

Protocol/Application Detector

BACNet
COSEM
COTP
DNP3
Emission control protocol
Fujitsu device control
GOOSE
GSE
IEC-60870-5-104
ISO MMS
Modbus
OPC-UA
Q931
SRC
TPKT
CIP
Honeywell Control Station/NIF Server
Honeywell Experion DSA Server Monitor

Deep Packet Inspection

Options to inspect header, payload to filter based on functions, commands and data

Modbus
DNP3
CIP
IEC-60870-5-104
IEC-61850-MMS
Siemens S7+

e.g., detect Modbus read coils, write single coil etc.


CISCO