Secure OT with CrowdStrike & Rockwell

March 29, 2023

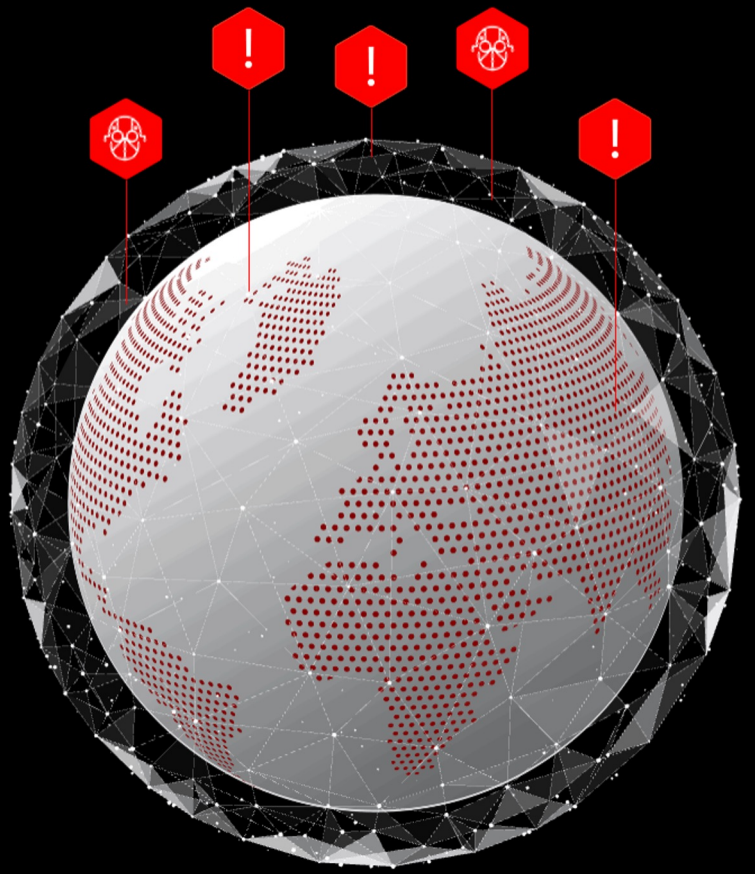
Introduction

Florian Goutaudier
Global OT Specialist

CROWDSTRIKE

We Stop Breaches

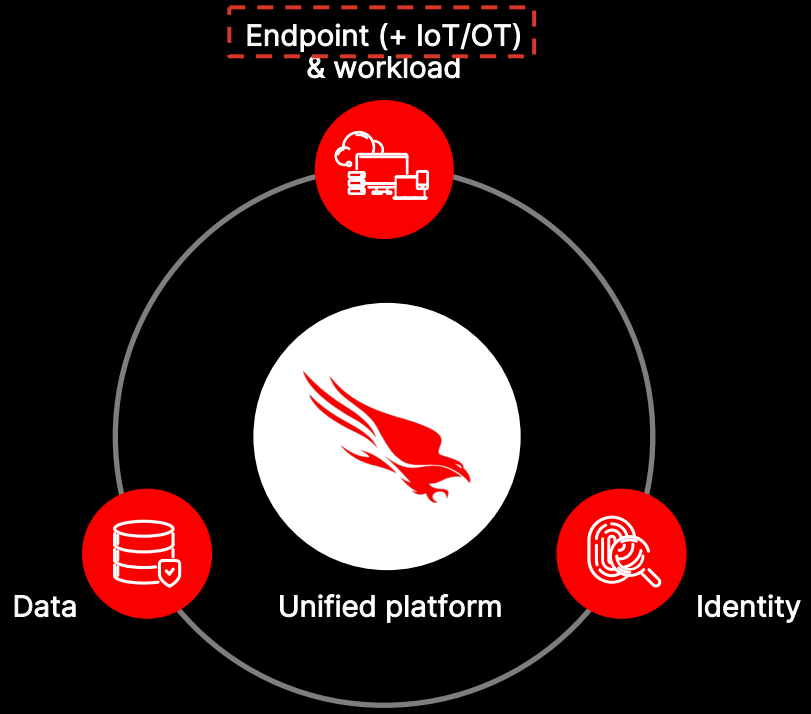
Protection that powers you.



CROWDSTRIKE

We Pioneered a New Approach for Modern Security:

Unified protection across endpoint, workload, identity, and data



CROWDSTRIKE

Organizations around the world are struggling to address IoT/OT security risks

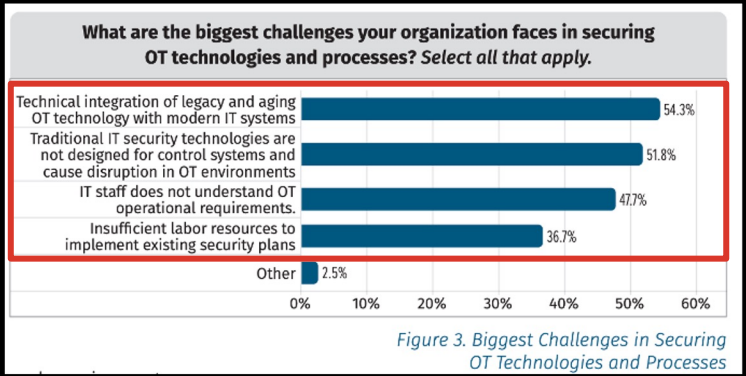


Figure 3. Biggest Challenges in Securing OT Technologies and Processes

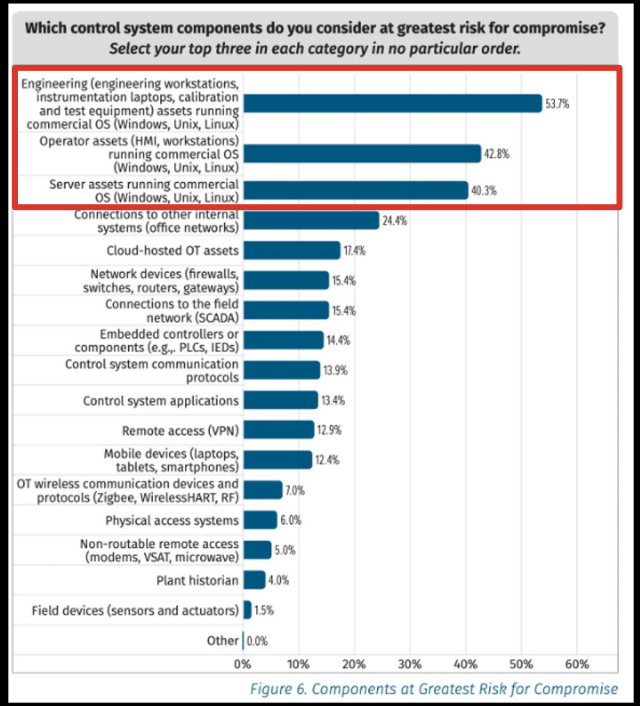


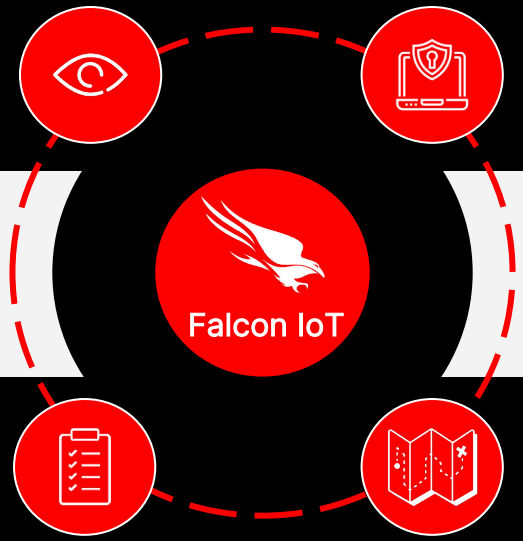
Figure 6. Components at Greatest Risk for Compromise

CROWDSTRIKE

Crowdstrike is uniquely positioned to solve the most pressing IoT/OT security challenges

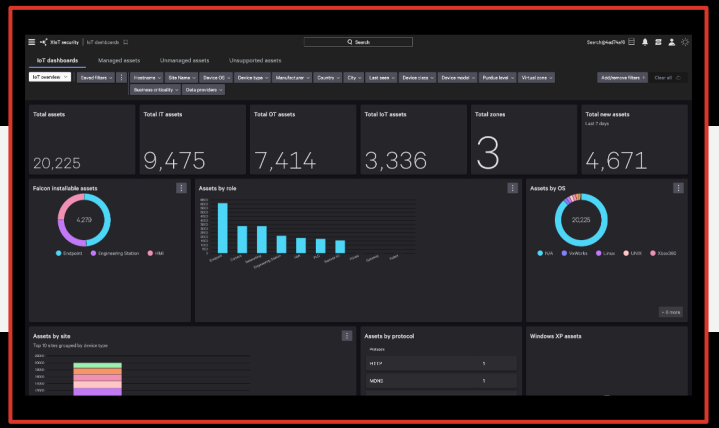
Complete visibility in *10 mins or less*

Extend industry-leading EDR/XDR to IoT/OT



ICS vendor certified

Asset relationship mapping



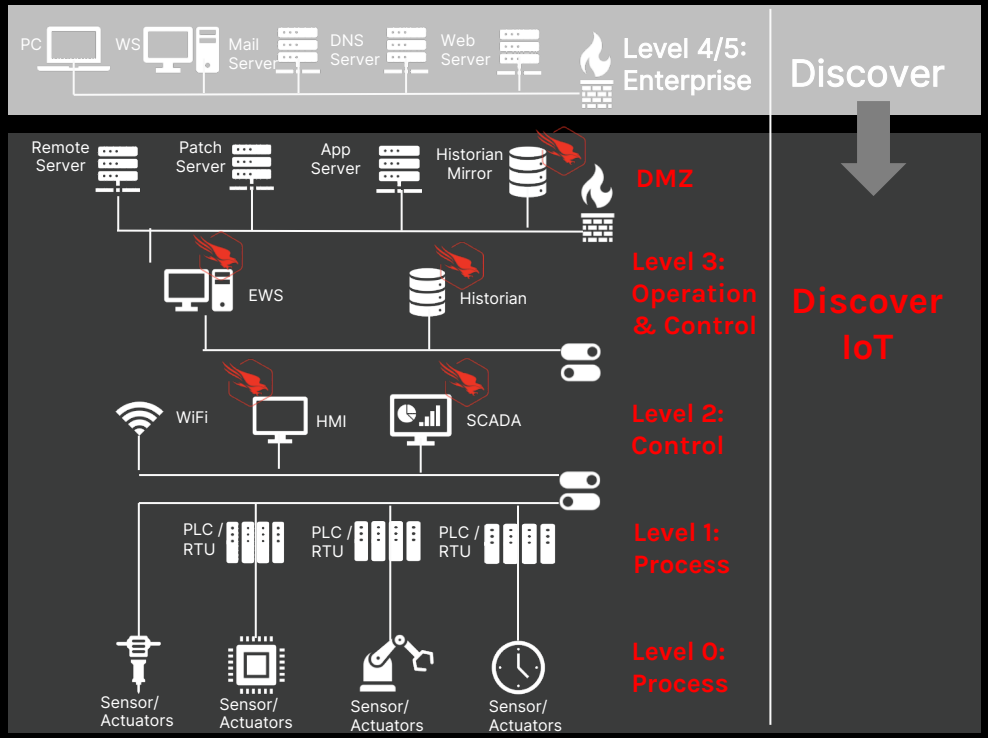
Comprehensive, simplified visibility

Leave no endpoint unprotected

Accelerate OT Digital Transformation

CROWDSTRIKE

Falcon Discover for IoT

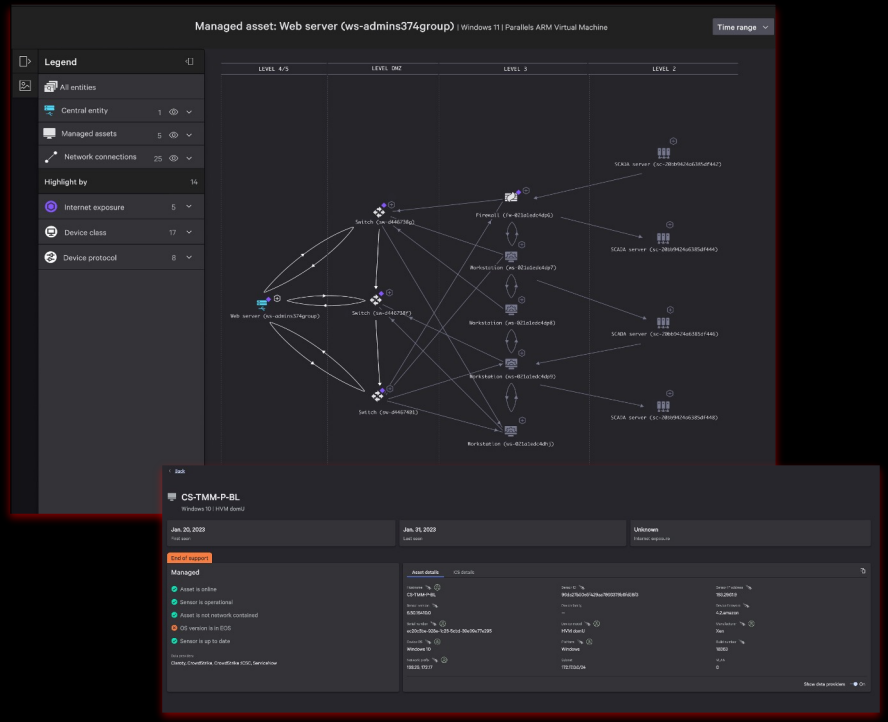


Purdue Model for ICS Security

- Complete asset visibility in *10 minutes or less*
- Zero infrastructure to deploy, no network configuration changes
- Asset relationship mapping to speed threat investigation and response
- ICS application inventory

CROWDSTRIKE

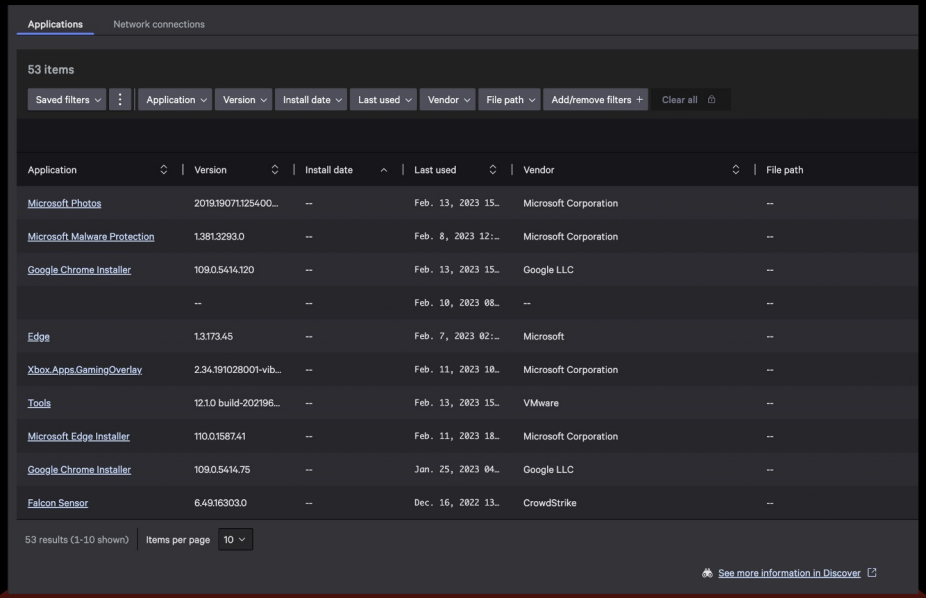
Speed investigation & response with Asset Graph



- Identify assets converging IT-OT
- Quickly determine related network connections and risky internet exposure
- Find assets with vulnerable OS or firmware
- Analyze assets and their relationships by Purdue level

CROWDSTRIKE

Get control of apps in ICS networks



Identify apps on xIoT assets

Allow/block specific apps

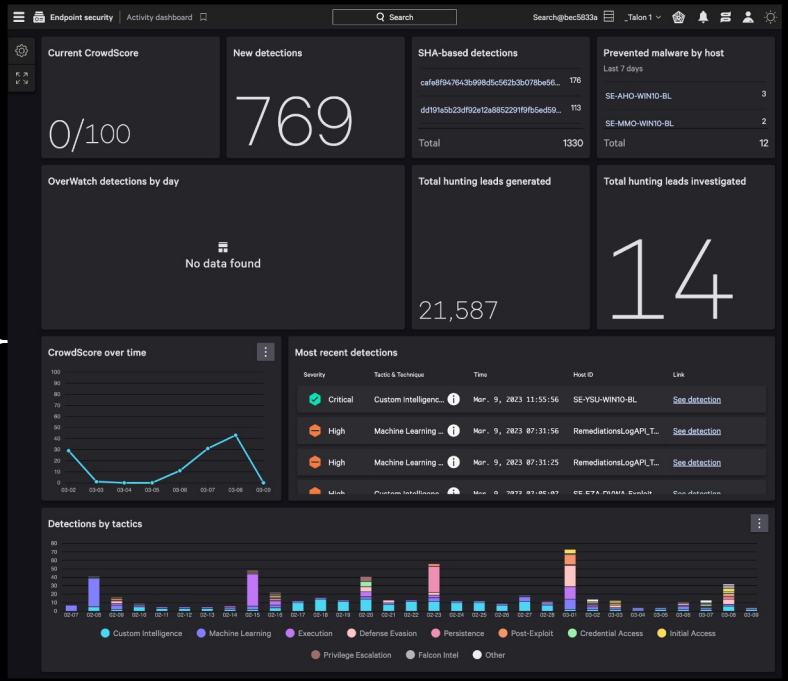
Track changes made to apps

CROWDSTRIKE

Falcon Insight for IoT

Extend industry-leading EDR/XDR to xIoT

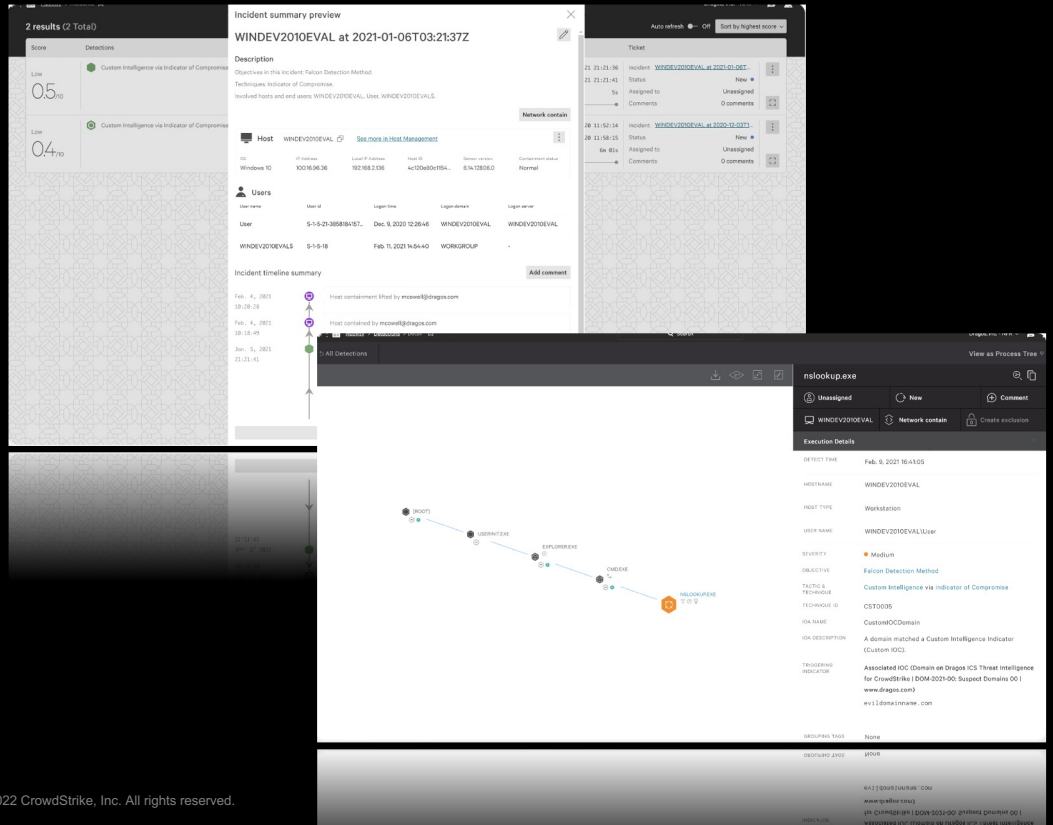
- Complete protection of xIoT assets
- ICS-aware asset and threat context
- ICS-safe policy recommendations
- OT-specific threat detections
- Rigorous ICS vendor testing and certification



CROWDSTRIKE

Detect advanced xIoT threats

AI-powered, ICS-specific threat detection



Common schema allows xIoT detections across Falcon & 3rd-party domains

Simple search without specialized query language (IoCs, artifacts)

Explore relationships & potentially impacted systems/users to find other leads

Create custom detection - assign search frequency, severity, notification

Detect changes made to xIoT apps and project files

CROWDSTRIKE

CROWDSTRIKE

TLP AMBER

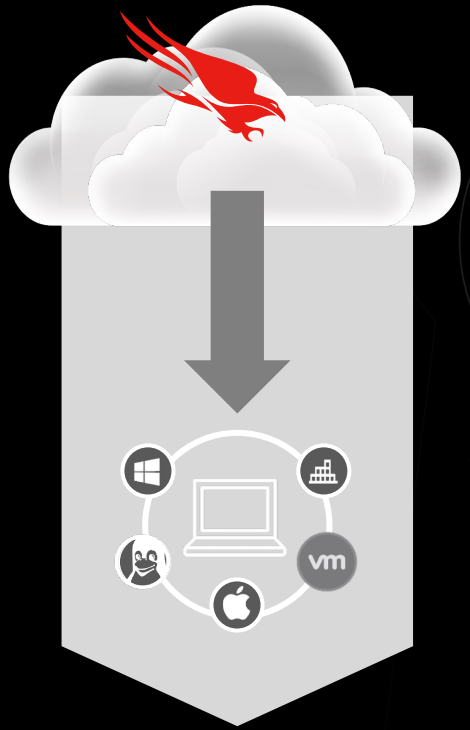
EDR FOR ICS ENVIRONMENTS
FEATURES AND CAPABILITIES

EDR/EPP optimized for ICS

- Next-generation Antivirus
- Security events for File/Process/Registry/Network
- Real-time response
- Complete visibility, context and attribution
- Anomaly & Threat detections
- ICS safe/tested and recommended prevention policies

ICS COLLECTOR

- Asset Inventory collection
- Subnet entities collection
- ICS Protocol Querying
- ICS firmware visibility
- Legacy device detection
- Vulnerability context collection
- Detections context collection
- Run on-demand/always
- Controlled through Falcon agent



ICS Application visibility

- Project file visibility
- Application discovery
- ICS application repository
- Optional: ICS application safeguard**

OT DETECTIONS

- File/Process/Registry/Network for HMI, EWS, Historian
- IOCs and IOAs for OT Ransomware*
- PLC specific detections

CERTIFIED

- Certified with popular ICS automation vendors
- Compatible and safety testing
- No infrastructure to deploy
- Scalable

** safeguard requires file integrity monitoring

* Can also load specialized IOCs and IOAs from Dragos/Claroty

Rockwell & CrowdStrike

- Falcon Sensor validate for use on RA HMIs
- RA now a certified CrowdStrike reseller
- Teams collaborating to bring every greater security to OT

CROWDSTRIKE

CROWDSTRIKE

TLP AMBER

CERTIFICATION DOCUMENT, DISCOVER IOT ENHANCEMENTS AND REFERENCE ARCH UPDATE

Falcon Discover IoT

SETUP, USE CASES, FAQ

Rockwell Automation

Testing Types – Rockwell Validation of the Falcon Agent

Testing Types	Details
General Compatibility	Evaluate how well software functions in a particular hardware/software environment
Compatibility vs Falcon Modules	Evaluate how well software functions according to the modules that have been enabled (Insight, Prevent, Discover, Spotlight, Device Control, Identity Protection, Falcon Discover for IoT with ICS collector running…)
Compatibility vs Falcon sensor version	Evaluate how well software functions according to running sensor version (oldest -> latest)
Compatibility vs Prevention policy type	Evaluate same as above with several prevention policy types (detection mode only vs basic prevention)
Burn-in	identify defects in software that may not become apparent until the software has been running for an extended period of time
OEM Functional	Evaluate the functionality of software and hardware developed by the OEM
Deployment	Evaluate the CS ability to support specific deployment criteria for the OEM environment. (proxy, reboot suppression) – see details

CROWDSTRIKE


Thank you!
Q&A