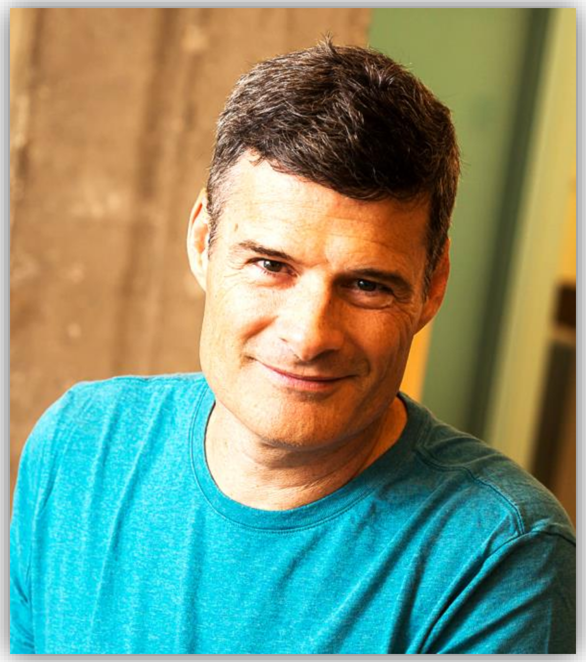
Value of Anomaly and Threat Detection in Industrial Control Systems

Patrick McBride
Chief Marketing Officer, Claroty

About Myself



- **Current:** Chief Marketing Officer, Claroty
- **Past:** Over 25 Years in Cybersecurity

  (All Seats - Customer, Research Analyst, Vendor)

  - iSIGHT Partners
  - Xceedium
  - META Security Group (Security Consultancy)
  - META Group (Gartner)
  - Travelers Insurance

About Claroty - Our Mission

Secure the safety and reliability of industrial control networks that run the world from cyber attacks

Agenda

- ICS Cyber Risk Summary
- Key ICS Cybersecurity Measures
- How can Anomaly Detection Help?
- Case Study: Triton Chemical Plant Attack

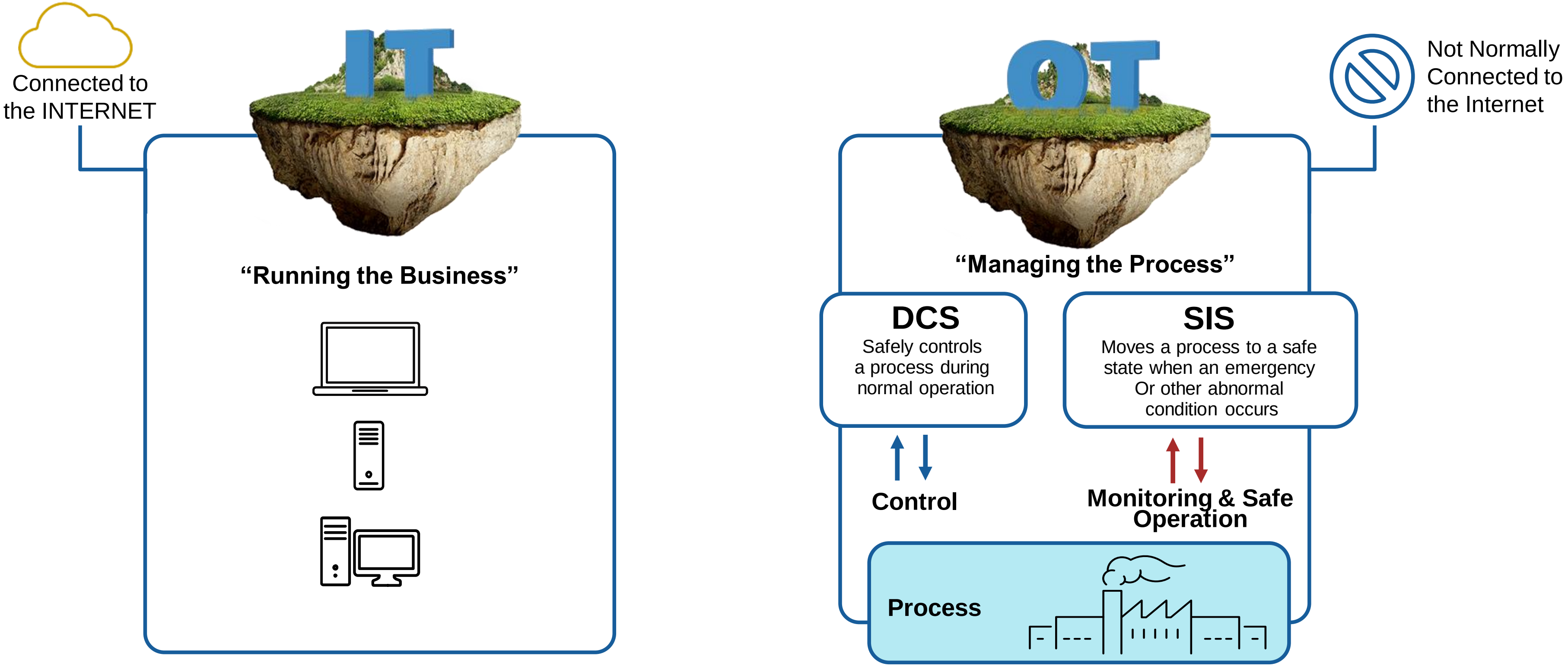
IT

- Designed to be connected
- Updated / replaced regularly
- Designed to be open and collaborative

OT

- Designed to be stand alone
- Lifetime of decades
- Designed to be closed and siloed

An ideal world scenario – “individual islands”



Connected to the INTERNET

“Running the Business”

“Managing the Process”

Not Normally Connected to the Internet

DCS

Safely controls a process during normal operation

SIS

Moves a process to a safe state when an emergency Or other abnormal condition occurs

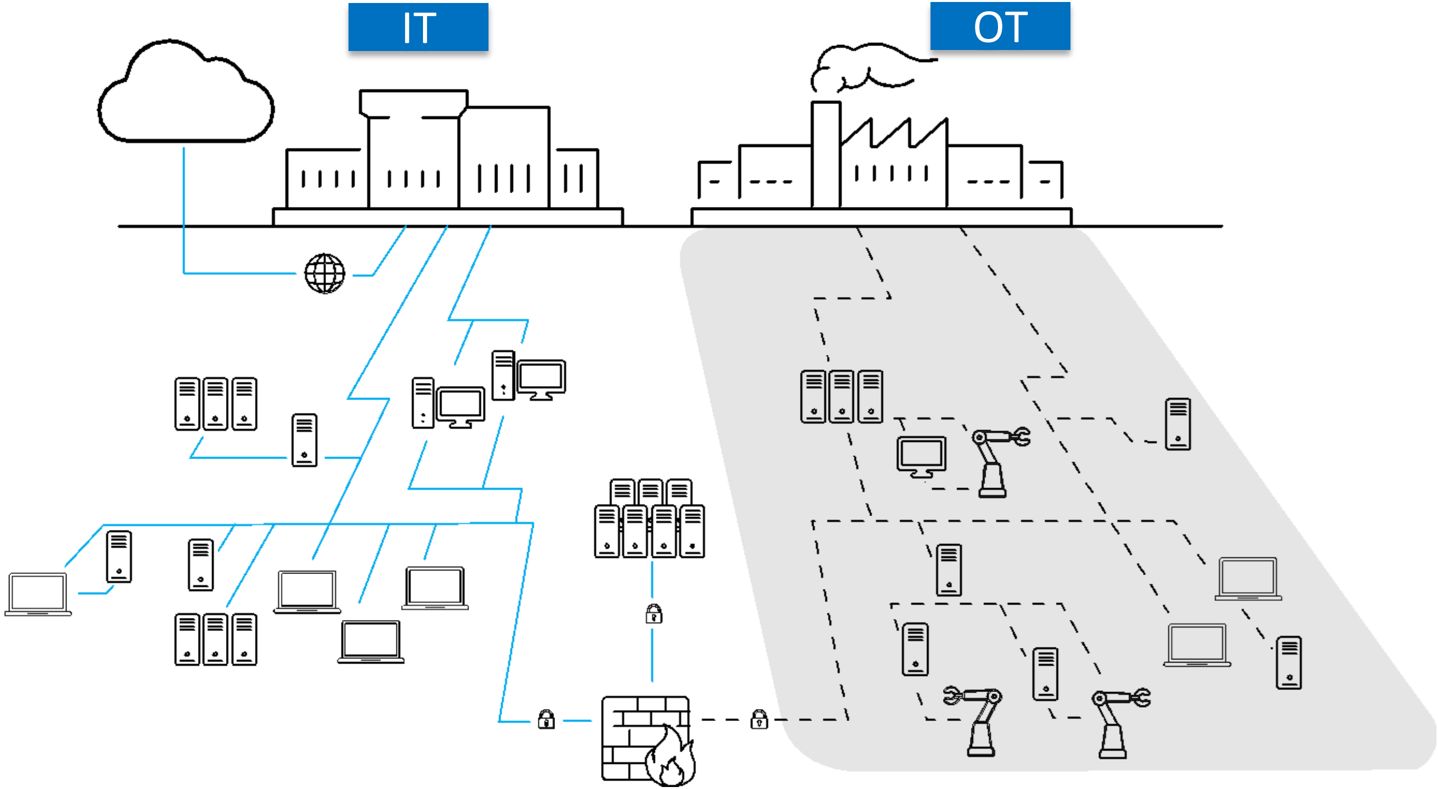
Control

Monitoring & Safe Operation

Process

Meanwhile, in the real world…

- ❑ Remote Maintenance
- ❑ "Shop Floor to Top Floor" KPIs
- ❑ ERP Integration
- ❑ Predictive Analytics



Very Active ICS Threat Landscape Over Last 18 Months

Why Now?

Aggressive Nation State Activity

(Russia, Iran, North Korea)

Repeated Warnings DHS/FBI

(energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors)

“Collateral Damage” Causes Billions in Losses

(WannaCry/NoPetya)

Advanced Safety System Attacks

(Triton/Triss)

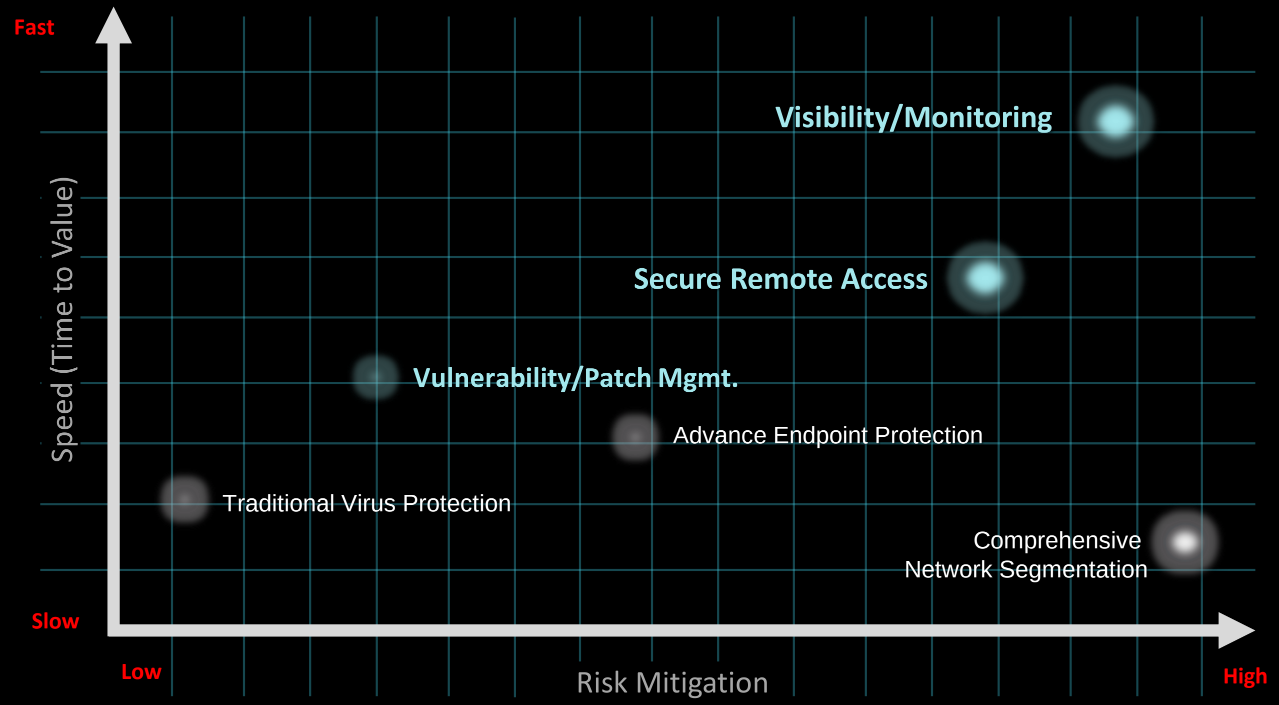
What have we learned?

Threat actors are *actively targeting* ICS/OT systems

&

You don’t have to be the *target* to be a *victim*

Where To Start With ICS Cybersecurity?

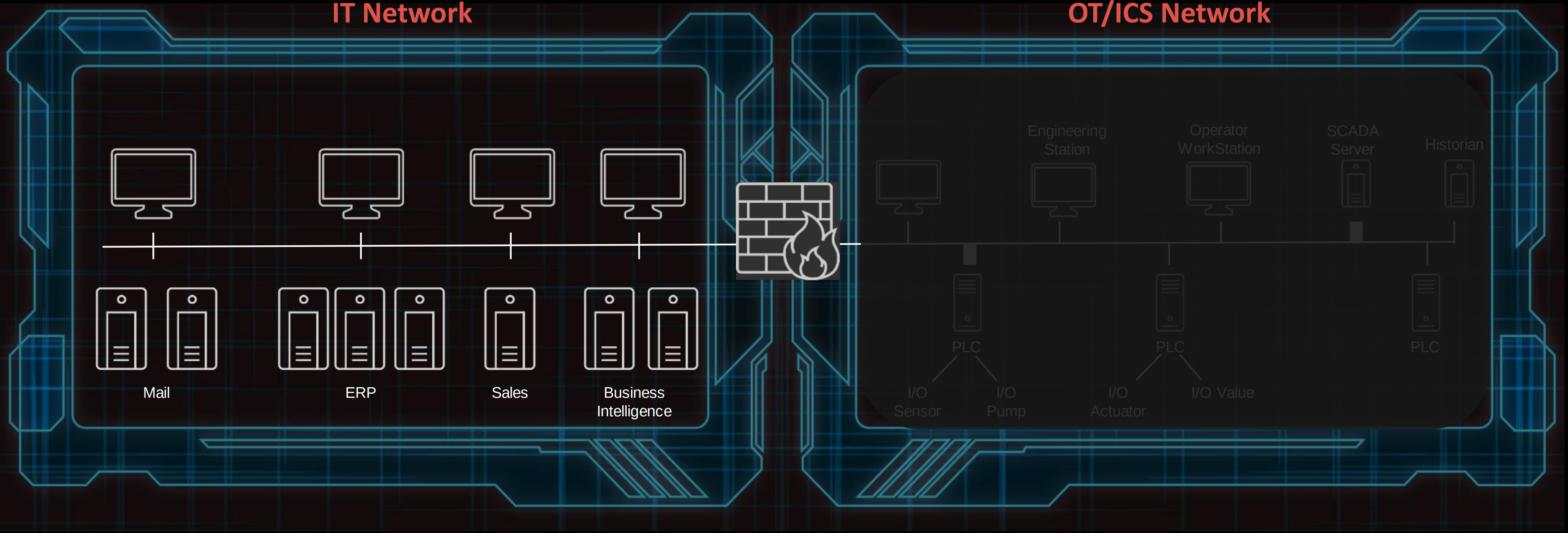


CLAROTY

What can "Anomaly Detection" systems do?

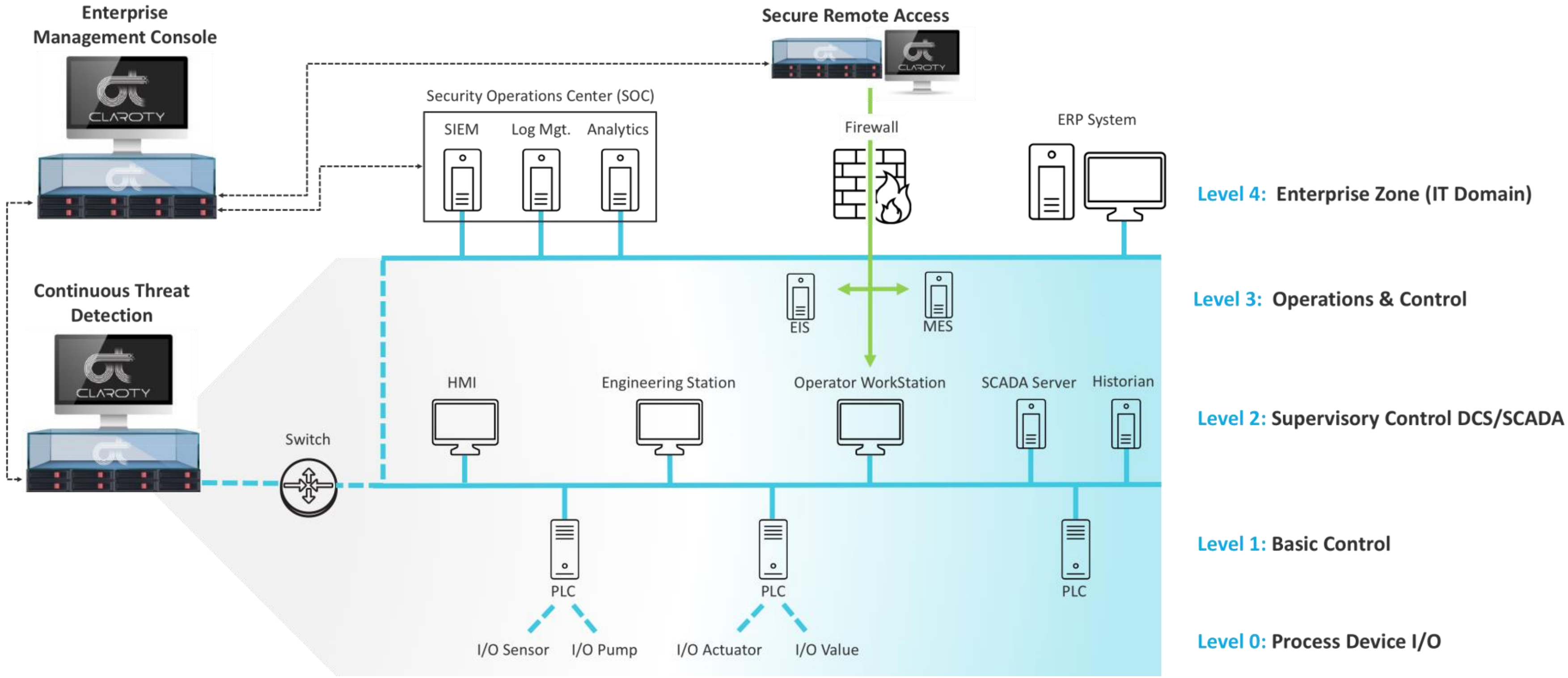
- Provide Visibility into Industrial Networks
- Enhance Asset Management, Compliance, Segmentation
- Provide Threat Detection (malicious and accidental)
- Case Study

Why Visibility? You Can't Protect What You Can't See

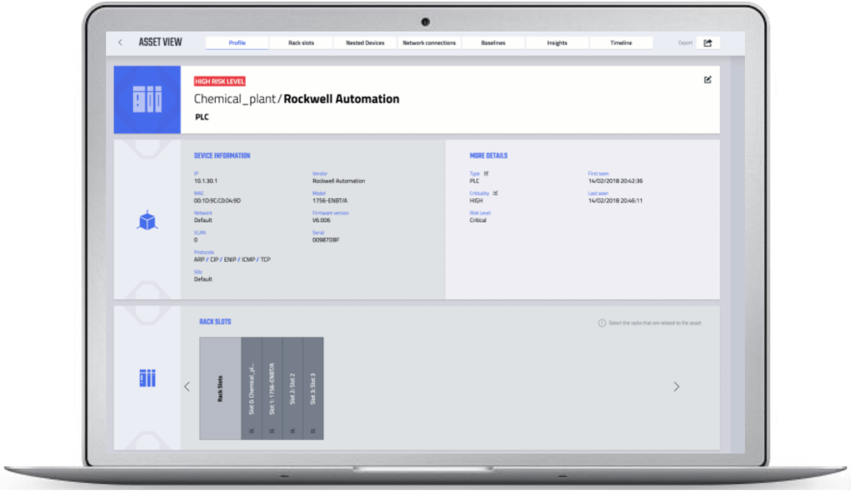


CLAROTY

Visibility - Using Safe/Passive DPI



Automatically Discover Asset Details & Communication Patterns



HIGH RISK LEVEL

Chemical_plant/**Rockwell Automation**

PLC

DEVICE INFORMATION

IP	10.1.30.1
MAC	00:1D:9C:C0:04:9D
Network	Default
VLAN	0
Protocols	ARP / CIP / ENIP / ICMP / TCP
Site	Default
Vendor	Rockwell Automation
Model	1756-ENBT/A
Firmware version	V6.006
Serial	00987DBF

MORE DETAILS

Type	PLC
Criticality	HIGH
Risk Level	Critical
First seen	14/02/2018 20:42:36
Last seen	14/02/2018 20:46:11

RACK SLOTS

Select the racks that are related to the asset

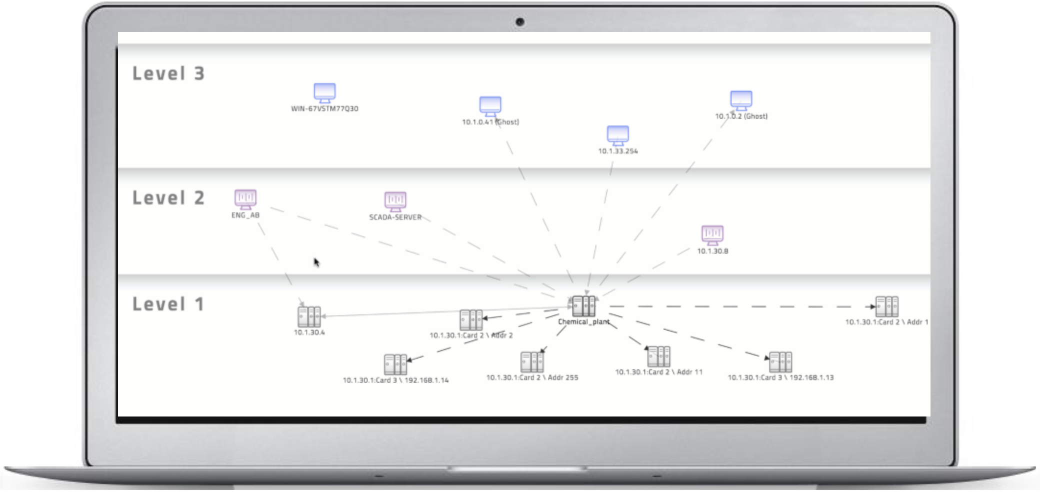
Rack Slots

Slot 0: Chemical_pl...

Slot 1: 1756-ENBT/A

Slot 2: Slot 2

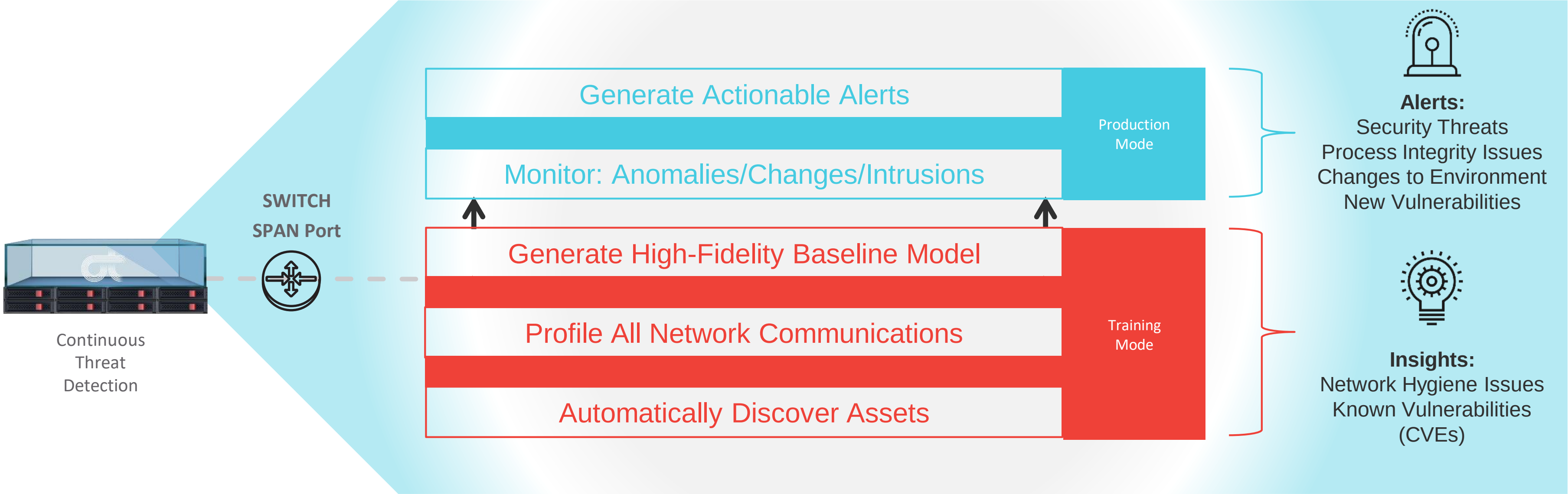
Slot 3: Slot 3


Level 3
WIN-67VSTM77Q30
10.1.0.41 (Ghost)
10.1.33.254
10.1.0.2 (Ghost)
Level 2
ENG_AB
SCADA-SERVER
10.1.30.8
Level 1
10.1.30.4
10.1.30.1:Card 2 \ Addr 2
Chemical_plant
10.1.30.1:Card 2 \ Addr 1
10.1.30.1:Card 3 \ 192.168.1.14
10.1.30.1:Card 2 \ Addr 255
10.1.30.1:Card 2 \ Addr 11
10.1.30.1:Card 3 \ 192.168.1.13

Understanding “Extreme Visibility”

Behavior-Based Anomaly/Threat Detection

Safely Detect Known and Unknown Threats

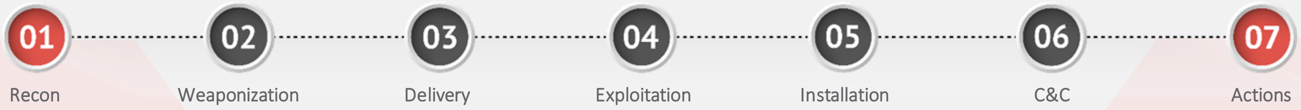


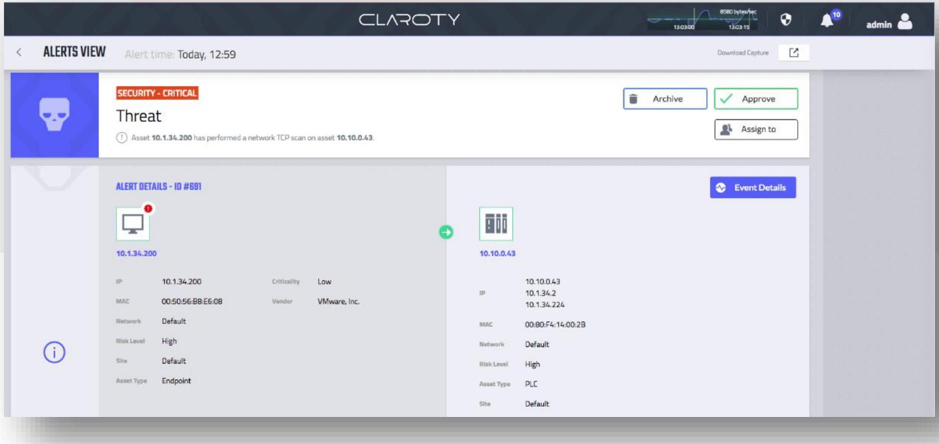
SWITCH
SPAN Port
Continuous Threat Detection
Generate Actionable Alerts
Monitor: Anomalies/Changes/Intrusions
Production Mode
Generate High-Fidelity Baseline Model
Profile All Network Communications
Automatically Discover Assets
Training Mode
Alerts:
Security Threats
Process Integrity Issues
Changes to Environment
New Vulnerabilities
Insights:
Network Hygiene Issues
Known Vulnerabilities (CVEs)

Behavior-Based Anomaly/Threat Detection

Early Warning | Detect Threats Across Cyber Kill Chain

CYBER KILL CHAIN





ALERTS VIEW Alert time: Today, 12:59

SECURITY - CRITICAL

Threat

Asset **10.1.34.200** has performed a network TCP scan on asset **10.10.0.43**.

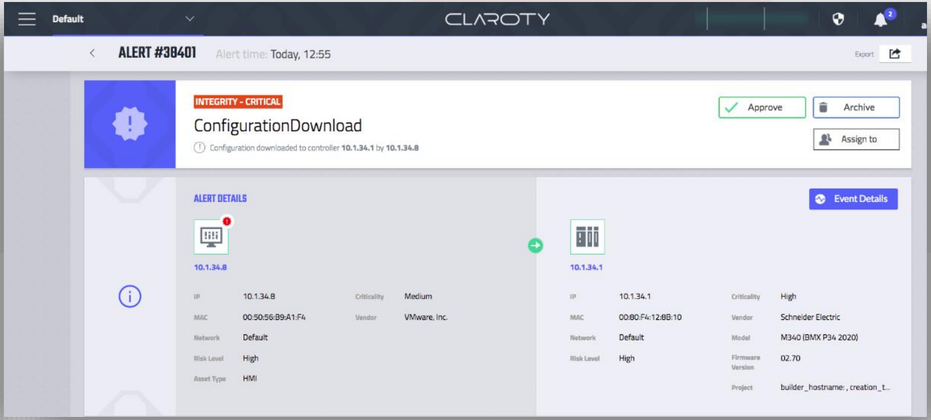
ALERT DETAILS - ID #691

10.1.34.200

IP 10.1.34.200
MAC 00:50:56:BB:E6:08
Network Default
Risk Level High
Site Default
Asset Type Endpoint
Criticality Low
Vendor VMware, Inc.

10.10.0.43

IP 10.10.0.43
10.1.34.2
10.1.34.224
MAC 00:80:F4:14:00:2B
Network Default
Risk Level High
Asset Type PLC
Site Default



ALERT #38401 Alert time: Today, 12:55

INTEGRITY - CRITICAL

ConfigurationDownload

Configuration downloaded to controller **10.1.34.1** by **10.1.34.8**

ALERT DETAILS

10.1.34.8

IP 10.1.34.8
MAC 00:50:56:B9:A1:F4
Network Default
Risk Level High
Asset Type HMI
Criticality Medium
Vendor VMware, Inc.

10.1.34.1

IP 10.1.34.1
MAC 00:80:F4:12:8B:10
Network Default
Risk Level High
Criticality High
Vendor Schneider Electric
Model M340 (BMX P34 2020)
Firmware Version 02.70
Project builder_hostname: , creation_t...

CLAROTY

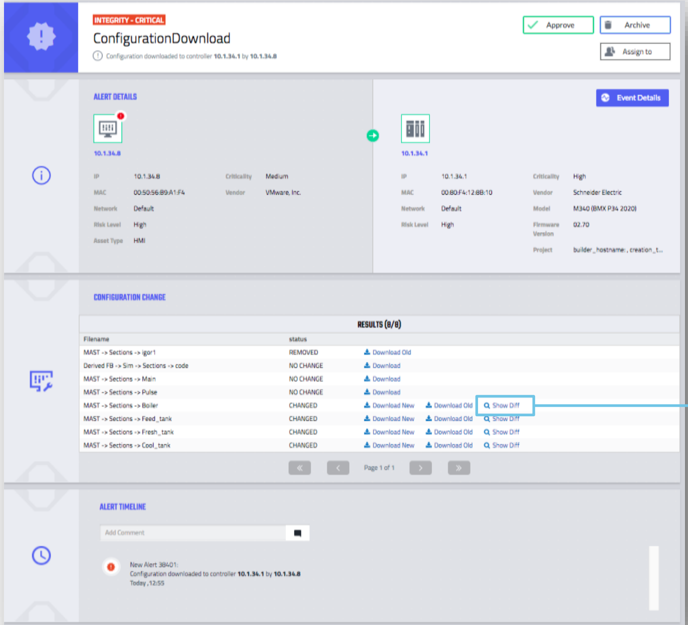
Actionable Alerts

Clear |Consolidated | Context-Rich Alerts = Reduced Time to Remediate

Asset Details

Configuration Changes

Alert Timeline



INTEGRITY - CRITICAL

ConfigurationDownload

Configuration downloaded to controller **10.1.34.1** by **10.1.34.8**

ALERT DETAILS

10.1.34.8

IP 10.1.34.8
MAC 00:50:56:B9:A1:F4
Network Default
Risk Level High
Asset Type HMI
Criticality Medium
Vendor VMware, Inc.

10.1.34.1

IP 10.1.34.1
MAC 00:80:F4:12:8B:10
Network Default
Risk Level High
Criticality High
Vendor Schneider Electric
Model M340 (BMX P34 2020)
Firmware Version 02.70
Project builder_hostname: , creation_t...

CONFIGURATION CHANGE

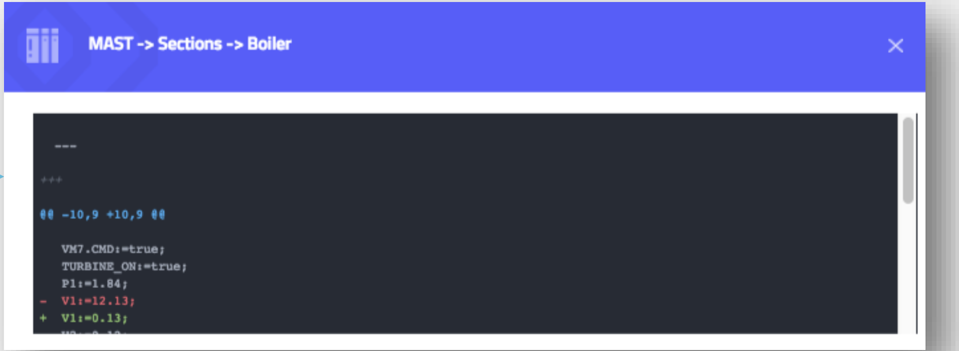
RESULTS (8/8)

Filename	status			
MAST -> Sections -> igor1	REMOVED	Download Old		
Derived FB -> Sim -> Sections -> code	NO CHANGE	Download		
MAST -> Sections -> Main	NO CHANGE	Download		
MAST -> Sections -> Pulse	NO CHANGE	Download		
MAST -> Sections -> Boiler	CHANGED	Download New	Download Old	Show Diff
MAST -> Sections -> Feed_tank	CHANGED	Download New	Download Old	Show Diff
MAST -> Sections -> Fresh_tank	CHANGED	Download New	Download Old	Show Diff
MAST -> Sections -> Cool_tank	CHANGED	Download New	Download Old	Show Diff

ALERT TIMELINE

New Alert 38401:
Configuration downloaded to controller **10.1.34.1** by **10.1.34.8**
Today ,12:55

Actual PLC Code Diffs!

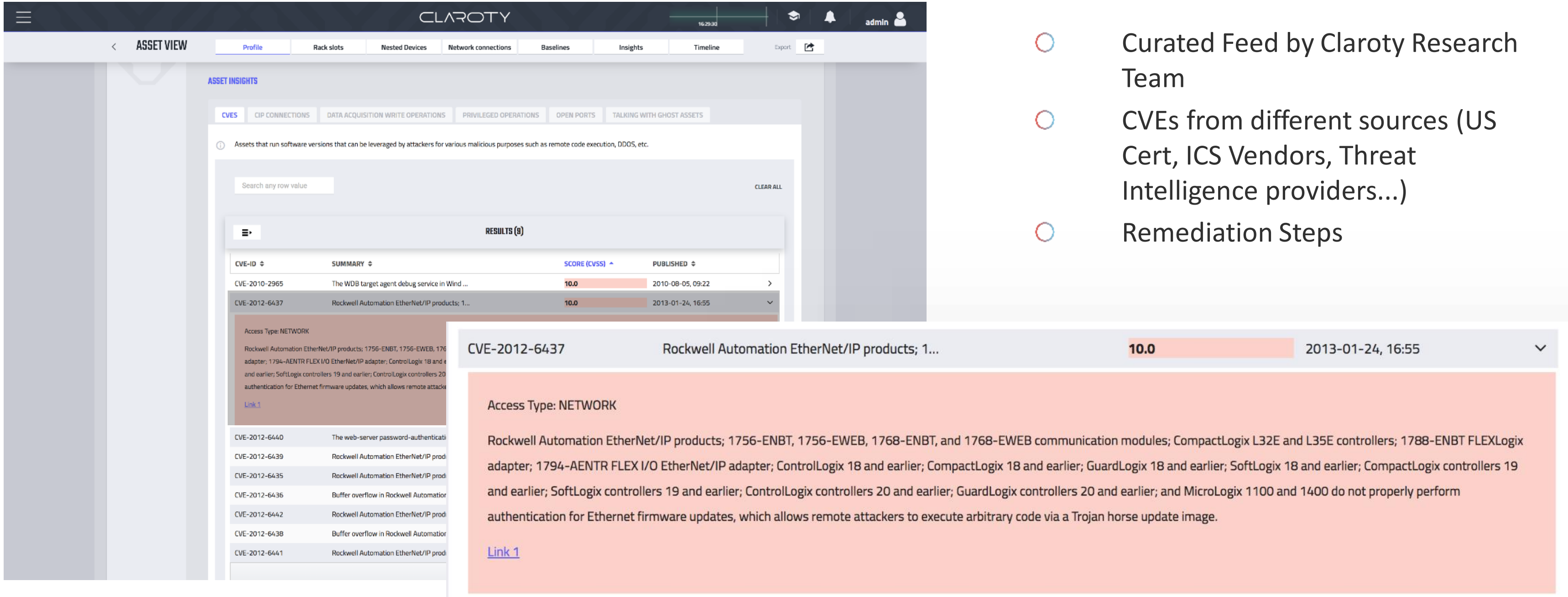


MAST -> Sections -> Boiler

```
 ---
+++
@@ -10,9 +10,9 @@
   VM7.CMD:=true;
   TURBINE_ON:=true;
   P1:=1.84;
-  V1:=12.13;
+  V1:=0.13;
```

Continuous Vulnerability Monitoring

Pinpoint Matching of CVEs with ICS Assets



Assets that run software versions that can be leveraged by attackers for various malicious purposes such as remote code execution, DDOS, etc.

CVE-ID	SUMMARY	SCORE (CVSS)	PUBLISHED
CVE-2010-2965	The WDB target agent debug service in Wind ...	10.0	2010-08-05, 09:22
CVE-2012-6437	Rockwell Automation EtherNet/IP products; 1...	10.0	2013-01-24, 16:55
CVE-2012-6440	The web-server password-authenticati		
CVE-2012-6439	Rockwell Automation EtherNet/IP prod		
CVE-2012-6435	Rockwell Automation EtherNet/IP prod		
CVE-2012-6436	Buffer overflow in Rockwell Automation		
CVE-2012-6442	Rockwell Automation EtherNet/IP prod		
CVE-2012-6438	Buffer overflow in Rockwell Automation		
CVE-2012-6441	Rockwell Automation EtherNet/IP prod		

CVE-2012-6437 Rockwell Automation EtherNet/IP products; 1... 10.0 2013-01-24, 16:55

Access Type: NETWORK

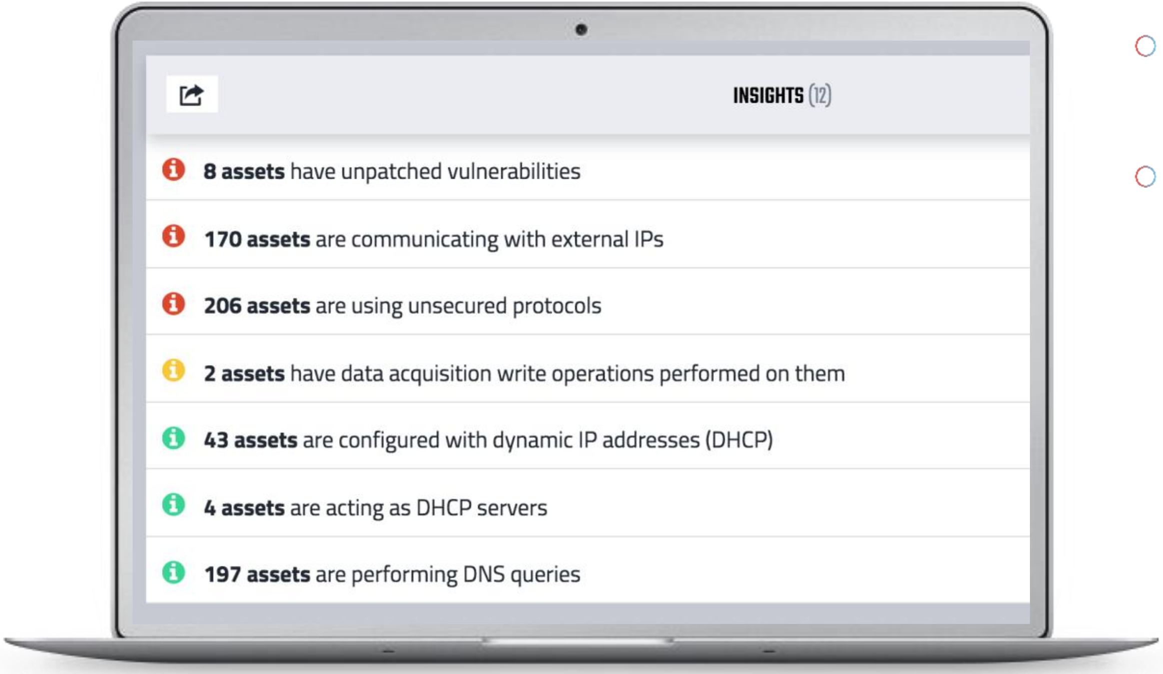
Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.

Link 1

- ○ Curated Feed by Claroty Research Team
- ○ CVEs from different sources (US Cert, ICS Vendors, Threat Intelligence providers...)
- ○ Remediation Steps

Continuous Vulnerability Monitoring

Network Hygiene Issues



INSIGHTS (12)

- 8 assets have unpatched vulnerabilities
- 170 assets are communicating with external IPs
- 206 assets are using unsecured protocols
- 2 assets have data acquisition write operations performed on them
- 43 assets are configured with dynamic IP addresses (DHCP)
- 4 assets are acting as DHCP servers
- 197 assets are performing DNS queries

○ Real-Time detection of network configuration issues

○ “Network Hygiene” weaknesses that can leave industrial networks exposed

Case Study: Triton (aka TriSis/HatMan)

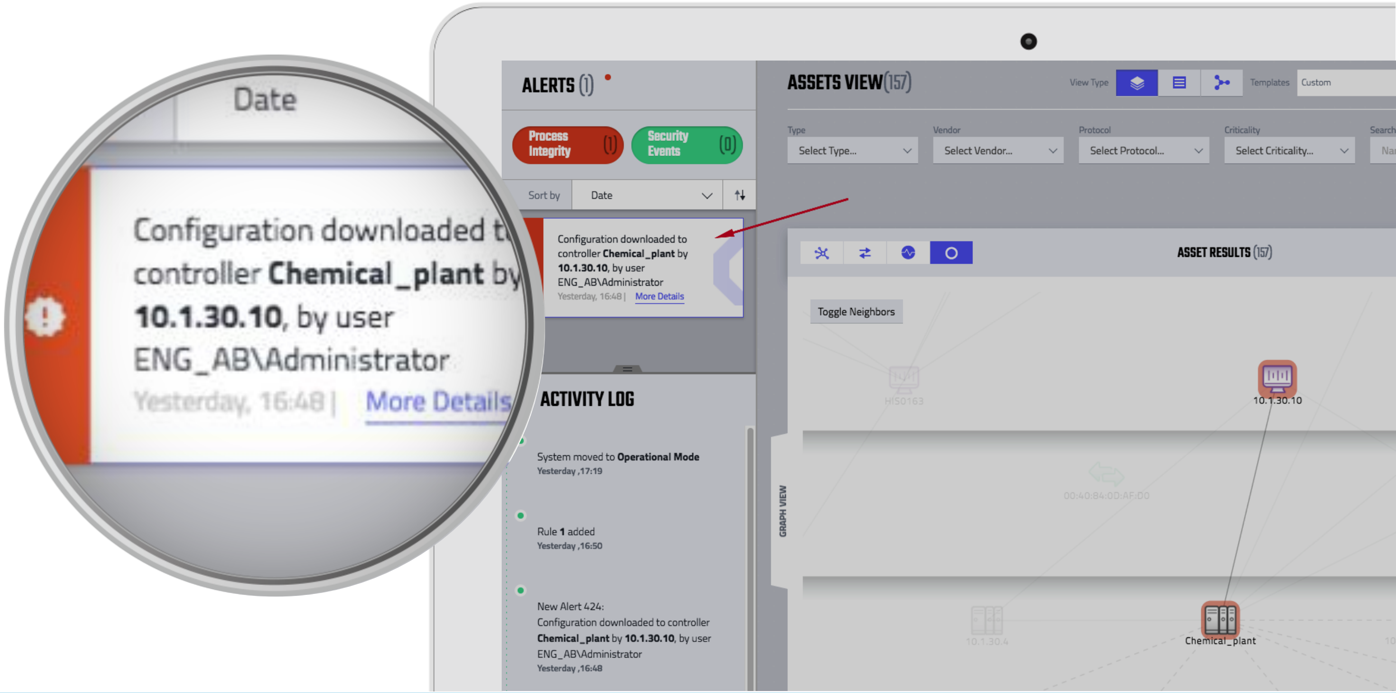
The Basics

- Malware designed to install a Remote Access Trojan (RAT) that allow read/write/execute over SIS in run/remote mode
- Memory-based attack, No payload
- “Very well written”, very few bugs
- 0-day for privilege elevation to read/write the firmware memory

S4 2018: Paul Forney (Schneider Electric) Testimonial

Out-of-the-box reporting

Actionable real-time alerts and intelligence



Configuration downloaded to controller **Chemical_plant** by **10.1.30.10**, by user ENG_AB\Administrator

Yesterday, 16:48 | More Details

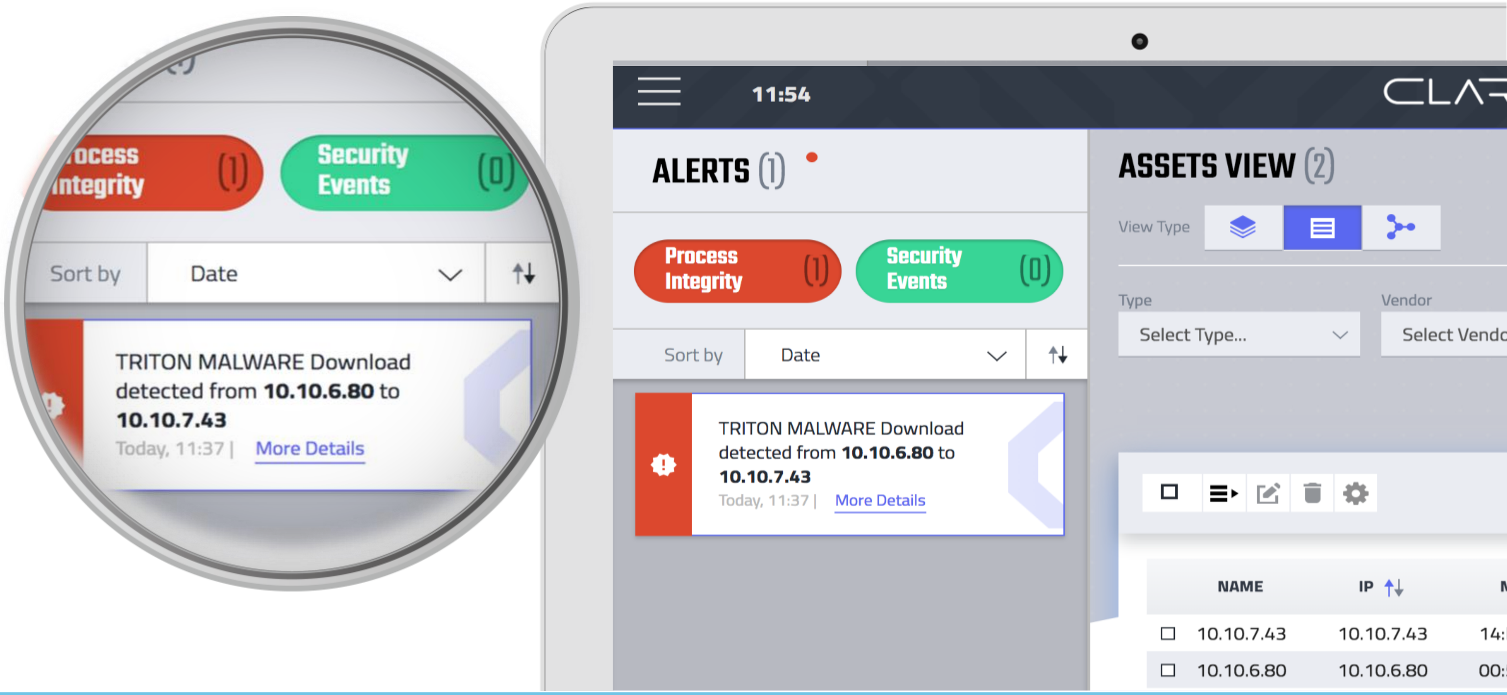
ACTIVITY LOG

System moved to **Operational Mode**
Yesterday ,17:19

Rule **1** added
Yesterday ,16:50

New Alert 424:
Configuration downloaded to controller **Chemical_plant** by **10.1.30.10**, by user ENG_AB\Administrator
Yesterday ,16:48

Modified reporting



TRITON MALWARE Download detected from **10.10.6.80** to **10.10.7.43**

Today, 11:37 | More Details

TRITON MALWARE Download detected from **10.10.6.80** to **10.10.7.43**

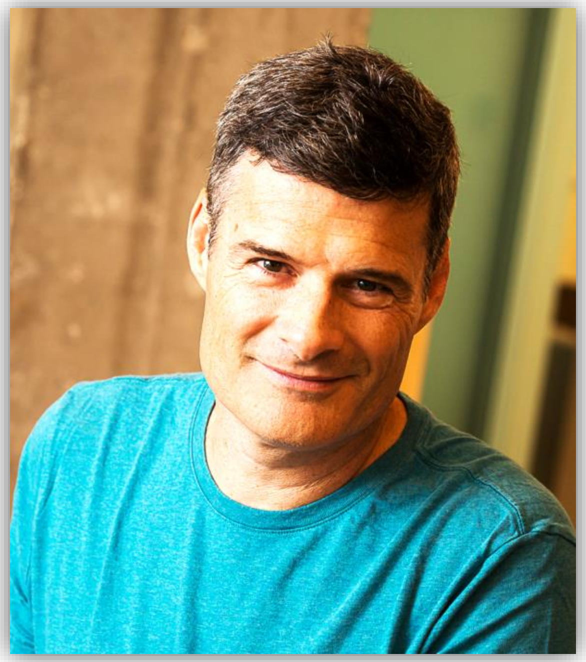
Today, 11:37 | More Details

	NAME	IP	
□	10.10.7.43	10.10.7.43	14:
□	10.10.6.80	10.10.6.80	00:

What can "Anomaly Detection" systems do?

- Provide Visibility into Industrial Networks
- Enhance Asset Management, Compliance, Segmentation
- Provide Threat Detection (malicious and accidental)
- Case Study

Thank You!



Questions/Comments?
patrick.m@claroty.com