



Tomorrow's SOC

How Splunk & Dragos Approach Risk Management
and Overcoming the IT/OT Divide

Jose Avila-Gomez
Paul Pelletier
Sam Van Ryder

Tomorrow's SOC Speakers



PANELIST

Jose Avila-Gomez
Senior Industrial
Consultant
Dragos



PANELIST

Paul Pelletier
Director of Security / Public
Sector Field Solutions
Splunk



MODERATOR

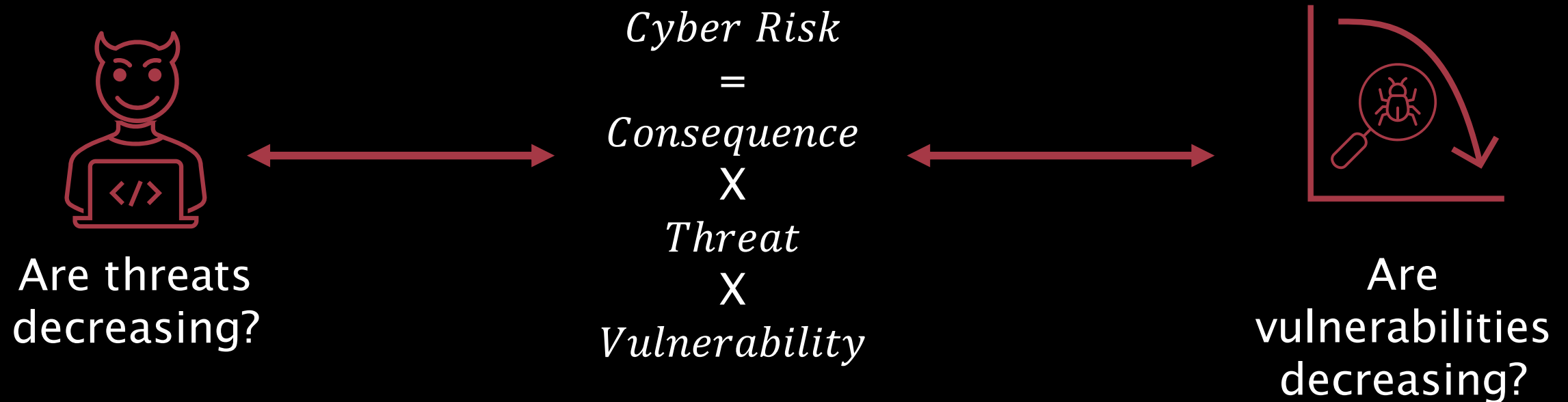
Sam Van Ryder
Director, Strategic
Accounts
Dragos

A woman in a white shirt is looking at a tablet in a server room. The room is filled with computer monitors displaying various data visualizations, including line graphs, bar charts, and world maps. The overall atmosphere is professional and data-driven.

Managing Risk

The “Classic” Cyber Risk Equation

Agnostic to Engineering and Operations



What's Special About Dragos ICRM?

Industrial Cyber Risk Management

$$ICRM = Consequence \times \underbrace{\frac{Threat \times Vulnerability}{Resilience}}_{Susceptibility}$$

Risk not expressed
as probability

Likelihood not an
independent variable

Susceptibility

All Evaluated Per Scenario

$$\frac{\textit{Threat} \times \textit{Vulnerability}}{\textit{Resilience}}$$



Threat

- Based on threat intelligence and research
- Looks at realistic approaches, threat groups, and experience



Vulnerability

- Specific vulnerabilities
- Considers individual device vulnerabilities, and systemic architecture weaknesses

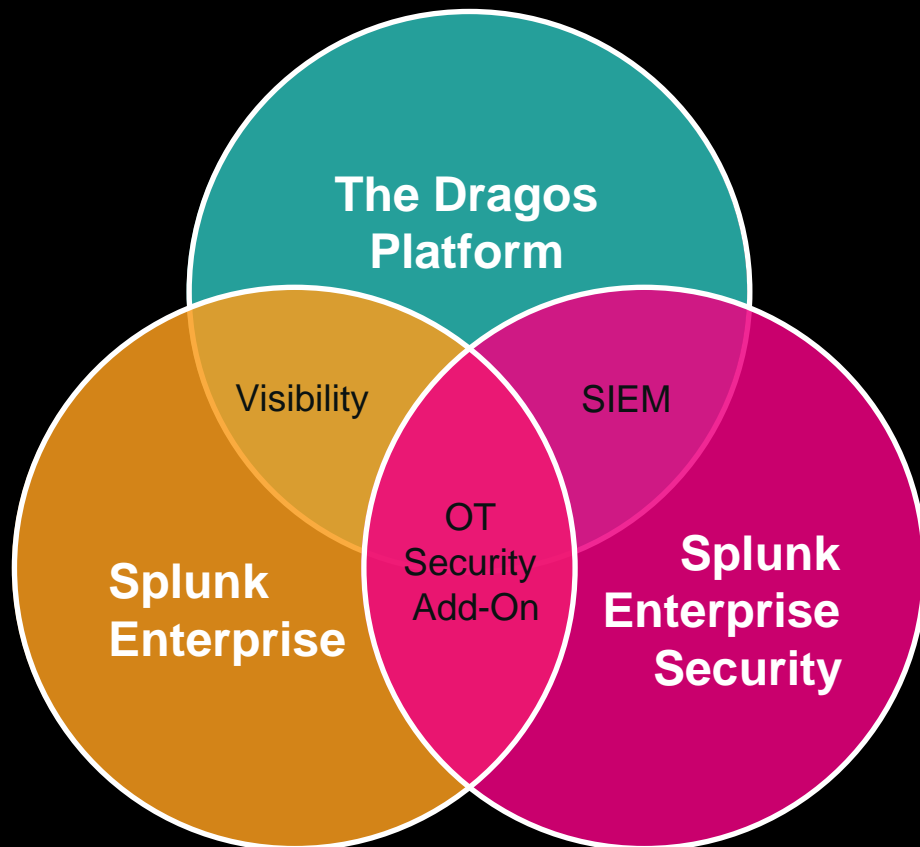


Resilience

- Considers technical, managerial, and procedural countermeasures

Achieving OT Cyber Resilience

“OT Cyber Resilience” is defined as *an organization’s ability to prevent, detect & respond to adverse conditions or malicious compromises of systems that are enabled by digital networks.*



How Splunk approaches risk

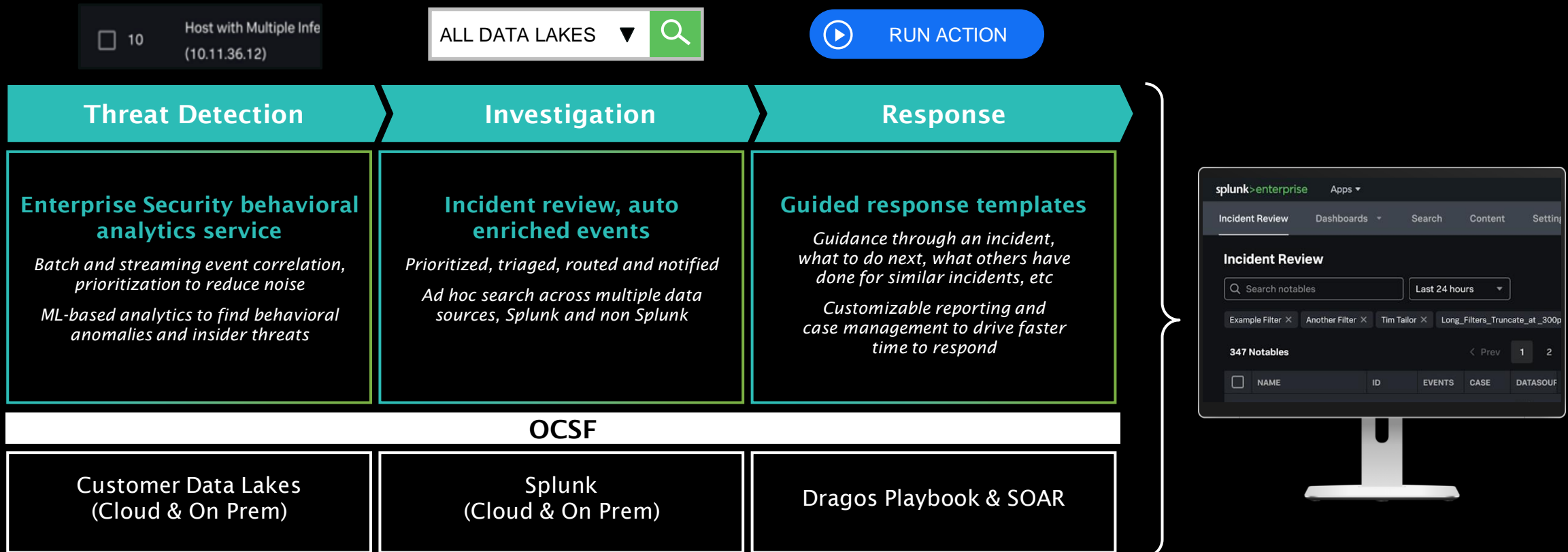
- Risk based analytics
- Consume noise
- Raise the relevant

Resilience

- How do we prevent?
- If not, how do we recover?

Splunk's Direction

End-to-end security operations for a seamless experience across distributed data stores



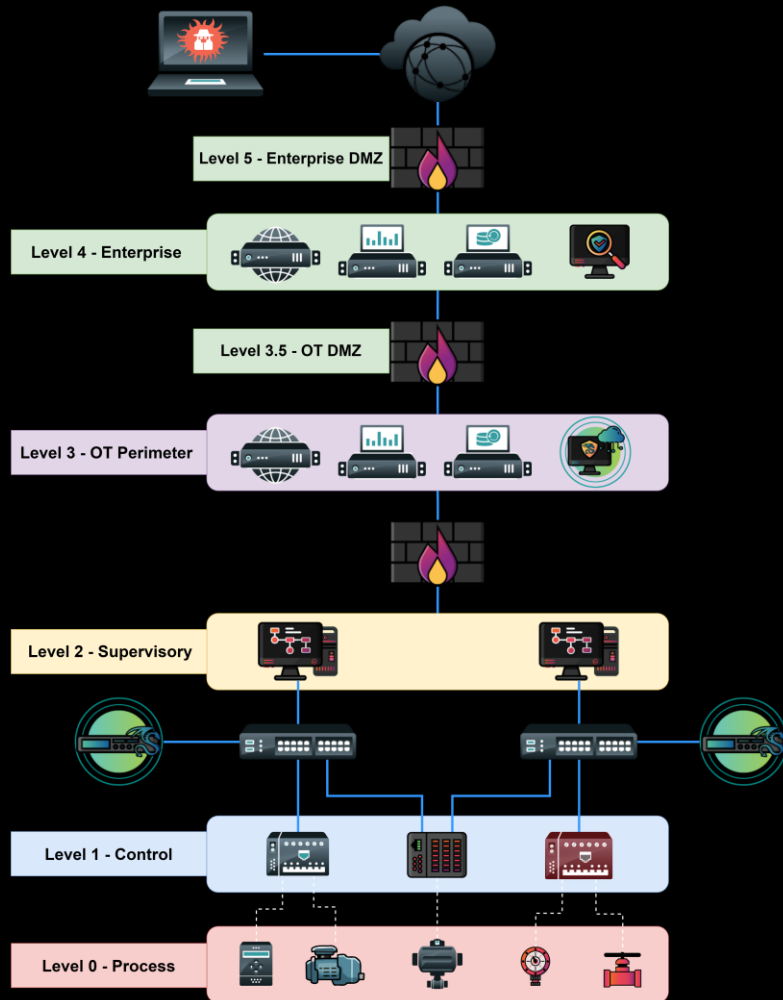
Traditional Notables and RBA Together





Threat Scenario: Remote Access

Threat Scenario: Remote Access



Contributing Events

- IT Event: Contractor/Engineer logged in after hours
- OT Alert: PLC modification without authorization

Justification

In addition to having a strict change-management process, which has not been initiated for this specific change, it's highly abnormal for contractors/engineers to be logging in during off-hours

Challenge

What is the risk?

Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

The screenshot shows the Splunk Playbooks interface. The top navigation bar includes 'JOURNAL', 'NOTIFICATIONS', 'EVIDENCE', and 'PLAYBOOKS'. The left sidebar shows a list of playbooks under the heading 'New RDP Connection Detected', with the first step '1 Collect and note source asset details.' selected and highlighted. The main content area displays the details for this step, including instructions on how to identify the source asset (internal or external) and a list of related QFDS (1). At the bottom, there are navigation buttons: 'PREV', 'SKIP', 'COMPLETE', and 'NEXT'.

Filter Playbook: New RDP Connection Detected
Filter By Status: All

1 Collect and note source asset details.

2 Collect and note destination asset details.

3 Examine the RDP Profile for changes.

4 Determine if access was authorized and expected.

5 Begin incident response procedures.

Collect and note source asset details. [EDIT](#)

Identify the source (client machine) from which the RDP connection originated. If the source was internal, utilize the Asset Explorer app to identify the IP, hostname, system type, administrator(s) responsible for the asset system, and logged on user account at the time of the connection, if available.

If the source was external, investigate its IP address without touching it directly (leverage WHOIS and documentation).

QFDS (1)

RDP

Explores RDP Sessions in the environment, along with their selected protocols, keyboard layouts, client_names, and cookies when available.

[VIEW DATASET >](#)

[PREV](#) [SKIP](#) [COMPLETE](#) [NEXT](#)

Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

JOURNAL

Filter Playbook: New RDP Connection Detected

Filter By Status: All

New RDP Connection Detected

- 1 Collect and note source asset details.
- 2 Collect and note destination asset details.
- 3 Examine the RDP Profile for changes.
- 4 Determine if access was authorized and expected.
- 5 Begin incident response procedures.

ADD PLAYBOOK



OT Asset Investigator

Specify an asset to populate details

Investigating Asset: 173.16.2.95 Time Window: Last 24 hours

Asset Details: 173.16.2.95

Detected Vulnerabilities: 1

Notables: 1

Asset Characteristics		Asset Categorization & Classification	
Field	plc-1	Field	plc-1
ip	173.16.2.95	category	ot controller plc controllogix
nt_host	plc-1	asset_model	controllogix 1756-171/b logix5571
dns		asset_version	32.11
mac	5c:88:16:ee:7c:47	asset_vendor	rockwell automation
asset_id	0112968f	asset_type	PLC
priority	critical	classification	ot
asset_system	area 200		
description	rockwell automation controllogix		
bunit	manufacturing		
owner	mauricio renzi		
site_id	mil_fac		
city	rockford		
country	usa		
location			

Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

JOURNAL

Filter Playbook: New RDP Connection Detected | Filter By Status: All

New RDP Connection Detected

- 1 Collect and note source asset details.
- 2 Collect and note destination asset details.**
- 3 Examine the RDP Profile for changes.
- 4 Determine if access was authorized and expected.
- 5 Begin incident response procedures.

ADD PLAYBOOK

OT Asset Center

Facility/Site: All | System: All | Business Unit: All | Time Period: Last 7 days | Hide Filters

Key OT Asset Indicators

[Edit](#)

TOTAL OT DEVICES # OT Known Devices 127	TOTAL OT ASSETS # Known Assets 327	IT/OT ASSETS DETECTED Last 24 Hours 325	ACTIVE OT DEVICES Last Hour 123 ↘ -1
---	--	---	---

Hardware Assets

Asset	Host	IP	Asset ID	Asset Priority	Vendor	Model	Asset Type	Classification
db1_hm101 172.110.1.108 0d:1e:15:11:fc:cc db1_hm101	db1_hm101	172.110.1.108		medium	hp	z700	HMI	cip:low cip:bca
172.110.1.45 f4:54:33:2f:3e:41 db1_plc01	db1_plc01	172.110.1.45	10346	low	Rockwell Automation	powerflex 70 ec 480v 5.0a	PLC	cip:low cip:pca
172.110.1.53 f4:54:33:7c:6f:a1 db1_plc02	db1_plc02	172.110.1.53	10353	low	Rockwell Automation	powerflex 70 ec 480v 5.0a	PLC	cip:low cip:pca

Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

JOURNAL

Filter Playbook: New RDP Connection Detected | Filter By Status: All

New RDP Connection Detected

- 1 Collect and note source asset details.
- 2 Collect and note destination asset details.
- 3 Examine the RDP Profile for changes.**
- 4 Determine if access was authorized and expected.
- 5 Begin incident response procedures.

ADD PLAYBOOK



Perimeter Investigator

3389 | * | * | *

Port (1) | Device (2) | Destinations (80) | Sources (33)

App	Port	Device	Host	Events	Destination	Host	Events	Source	Host	Events
ms-wbt-server	3389	172.100.1.21 dcc_fw02	172.100.1.21	69	173.16.2.60 roc_plc_30.mfactory.com	173.16.2.60	1	172.100.1.124 dcc_eng02.plea.local	172.100.1.124	1
		172.100.1.20 dcc_fw01	172.100.1.20	20	173.16.2.93 roc_hmi_03.mfactory.com	173.16.2.93	2	10.0.1.5 dceprtr01.copenergy.com	10.0.1.5	2
					10.11.36.28 prod-mfs-005	10.11.36.28	3	10.1.23.100 sched01.copenergy.com	10.1.23.100	3
					10.5.20.160 esxi_test	10.5.20.160	4	172.104.1.104 gcc_hmi02.copgen.ops.local	172.104.1.104	4
					172.100.104.98 dcc_js01.plea.local	172.100.104.98	5	172.110.1.108 db1_hmi01	172.110.1.108	5
					173.16.0.17 dmz_sw_07.mfactory.com	173.16.0.17	6	10.0.0.12 dceprtr02.copenergy.com	10.0.0.12	6
					173.16.1.26 mil_sw_16.mfactory.com	173.16.1.26	7	172.104.1.99 gcc_js02.copgen.ops.local	172.104.1.99	7
					173.16.1.56 mil_plc_16.mfactory.com	173.16.1.56	8	172.100.1.23 dcc_scada01.plea.local	172.100.1.23	8
					173.16.2.70 roc_plc_40.mfactory.com	173.16.2.70	9	172.104.1.11 gcc_plc02	172.104.1.11	9
					192.168.0.7 b4920	192.168.0.7	10	172.104.1.21 gcc_ids01	172.104.1.21	10
					10.1.100.1 aesolutions-pc	10.1.100.1	11	172.104.104.98 gcc_js01.copgen.ops.local	172.104.104.98	11
					10.11.3.6 rockwell-172	10.11.3.6	12	172.110.1.45 db1_plc01	172.110.1.45	12
					10.11.36.1 acme-001	10.11.36.1	13	173.16.2.95 plc-1	173.16.2.95	13
					10.11.36.26 prod-mfs-003	10.11.36.26	14	172.100.1.50 dcc_hmi01.plea.local	172.100.1.50	14
					10.11.36.31 coredev-002	10.11.36.31	15	172.100.1.51 dcc_hmi02.plea.local	172.100.1.51	15

Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

JOURNAL

Filter Playbook: New RDP Connection Detected

Filter By Status: All

New RDP Connection Detected

- 1 Collect and note source asset details.
- 2 Collect and note destination asset details.
- 3 Examine the RDP Profile for changes.
- 4 Determine if access was authorized and expected.**
- 5 Begin incident response procedures.

ADD PLAYBOOK



Remote Access

VPN Sessions					Remote Sessions			
_time	User	Src	Dest	Dom	_time	User	Src	Dest
2022-10-26 10:30:00	bwayne	dbl_plc01	gcc_js01.copgen.ops.local	COPGI	2022-10-27 08:52:05	skyle	gcc_eng02.copgen.ops.local	gcc_his01.copgen.ops.local
2022-10-26 10:30:00	srodgers	dbl_plc01	roc_plc_49.mfactory.com	COPGI	2022-10-27 08:07:10	ckent	gcc_maintence02.copgen.local	gcc_ad01.copgen.ops.local
2022-10-26 12:30:00	bbanner	dwn_plc01	gcc_js01.copgen.ops.local	COPGI	2022-10-27 07:53:08	srodgers	dcc_maintence02.plea.local	gcc_his01.copgen.ops.local
2022-10-26 14:30:00	srodgers	dcc_scada02.plea.local	dcc_js01.plea.local	COPGI	2022-10-27 07:44:44	nramanova	dcc_his01.plea.local	gcc_ad01.copgen.ops.local
2022-10-26 16:30:00	bwayne	dbl_hmi01	gcc_js01.copgen.ops.local	PLEA	2022-10-27 07:18:59	skyle	dbl_hmi01	gcc_js01.copgen.ops.local
2022-10-26 22:30:00	srodgers	exch01.copgenery.com	dcc_js01.plea.local	COPGI	2022-10-27 06:27:40	scada	dcc_sw02	gcc_his01.copgen.ops.local
2022-10-27 00:30:00	srodgers	dwh_plc04	gcc_js02.copgen.ops.local	COPGI	2022-10-27 06:19:21	skyle	dcc_sw02	gcc_ad01.copgen.ops.local
2022-10-27 02:30:00	bbanner	gcc_ad01.copgen.ops.local	gcc_js01.copgen.ops.local	COPGI	2022-10-27 06:04:17	acurry	mil_eng_ws_07.mfactory.com	gcc_js01.copgen.ops.local
2022-10-27 04:30:00	bbatson	dwn_plc02	sck_plc01	COPGI	2022-10-27 06:02:30	acurry	dcc_eng01.plea.local	gcc_his01.copgen.ops.local
2022-10-27 04:30:00	bwayne	dcc_scada01.plea.local	gcc_js01.copgen.ops.local	COPGI	2022-10-27 05:30:41	ckent	mil_desktop_05.mfactory.com	gcc_js01.copgen.ops.local

Threat Scenario: Suspicious Remote Access

Playbooks – Rockwell PLC Keystate Change

JOURNAL NOTIFICATIONS EVIDENCE PLAYBOOKS

Filter Playbook: Rockwell PLC Keystate Change Filter By Status: All

Rockwell PLC Keystate Change

- 1 Collect and note asset details and change time.
- 2 Collect CIP identity information.
- 3 Begin incident response procedures.

ADD PLAYBOOK

Collect and note asset details and change time. EDIT

Within the notification, there is a source asset ID defined. Locate this asset ID in the CIP QFD and verify there are records available for investigations.

Adding a filter for Source Asset:

- Click Add Filter
- Select field "src_asset"
- Select field "is"
- Insert recorded Source Asset ID (note: this is not an IP address)
- Record these destination asset(s), first time seen, and whether there are status codes without correlating service codes

Often keystate changes are part of normal maintenance efforts for tuning programmable logic controllers:

- Multiple keystate changes occurring around the same time window
- the keystates are being changed without correlating commands from the software
- service codes are being sent without correlating keystate changes to the same devices during different windows
- different types of devices

These are all important details that add context to the investigation. Note any other asset IDs initiating keystate changes via service code.

QFDS (1)

CIP

CIP Traffic Summary

VIEW DATASET >

PREV X SKIP COMPLETE NEXT

Threat Scenario: Suspicious Remote Access

Playbooks – Rockwell PLC Keystate Change

JOURNAL

Filter Playbook
Rockwell PLC Keystate Change

Filter By Status
All

Rockwell PLC Keystate Change

- 1 Collect and note asset details and change time.
- 2 Collect CIP identity information.
- 3 Begin incident response procedures.

ADD PLAYBOOK



Risk Events

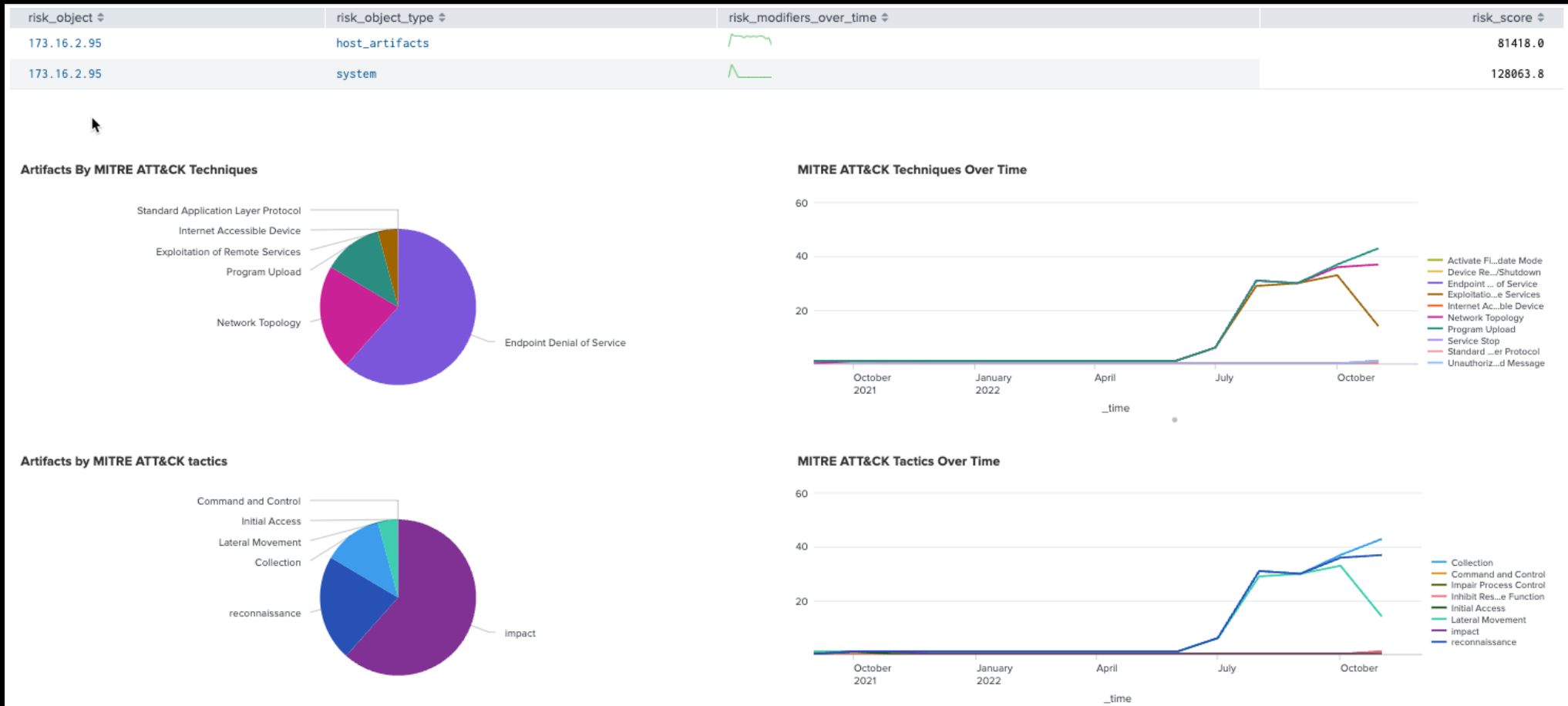
173.16.2.95 Risk Score: 12.1 Event Count: 29

Contributing Risk Events

i	Time	Risk Rule	Risk Score	Annotations	Threat Object
>	Today, 2:45 PM	Program Upload to PLC over CIP	22	T800	--
>	Today, 2:45 PM	Forced Stop of PLC over CIP	22	T881	--
>	Today, 2:45 PM	PLC Write	22	T855	--
>	Today, 2:45 PM	PLC Status Change	22	T816	--
>	Today, 2:45 PM	Program Download to PLC over CIP	22	T845	--
>	Today, 2:35 PM	Program Upload to PLC over CIP	22	T845	--
>	Today, 2:35 PM	WannaCry Connection Attempt	22	T866	--

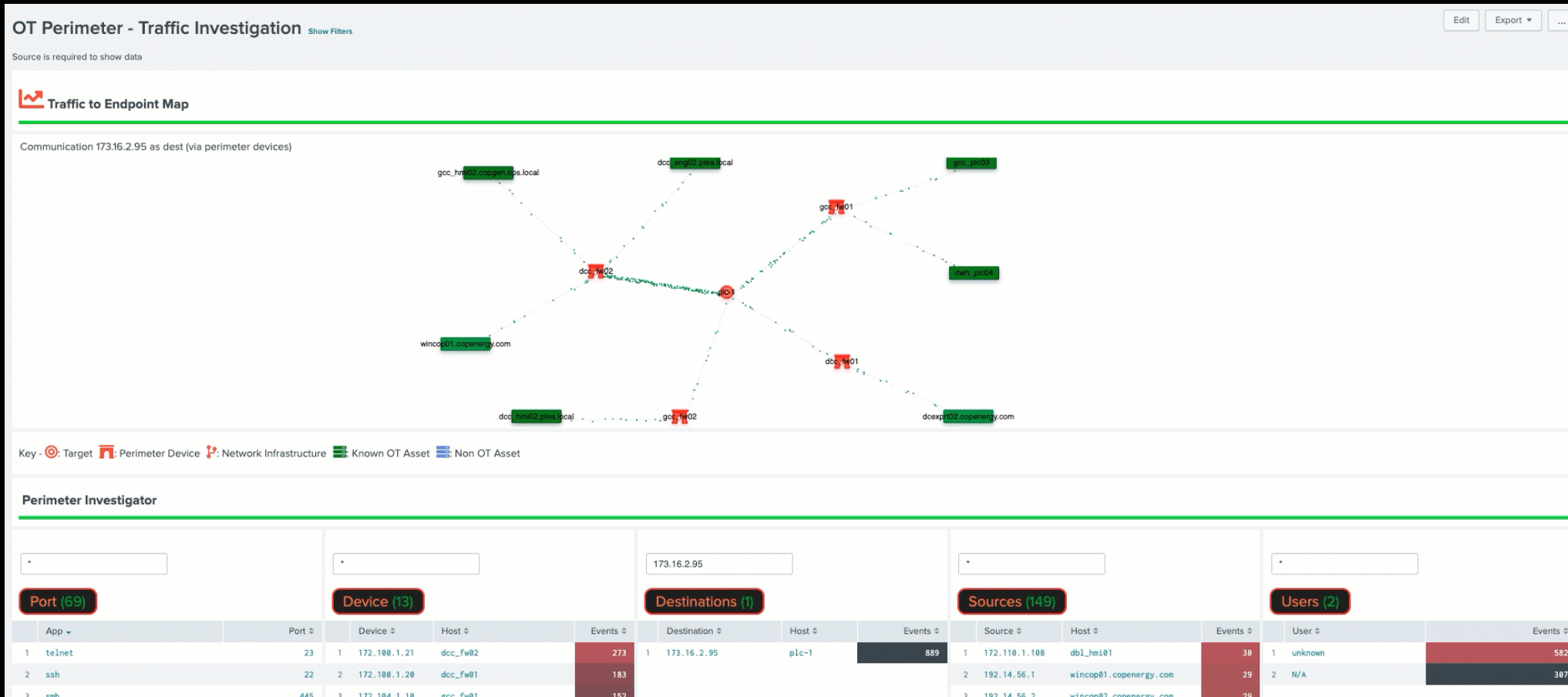
Threat Scenario: Suspicious Remote Access

Rockwell PLC Keystate Change – Risk Workbench



Threat Scenario: Suspicious Remote Access

Rockwell PLC Keystate Change – Real time communication





Tomorrow's SOC

Tomorrow's SOC

Vision of what the future SOC looks like:

SIEM - Incorporation OT (Fusion center)

Visibility across the whole network OT+IT

Security Analytics

Vulnerabilities and Detections

Guidance for response (Playbooks)

Critical Controls for Effective OT Cybersecurity

Tomorrow's SOC

Simplify and Manage Visibility into both IT & OT Environments

SOC (Security Operations Center)

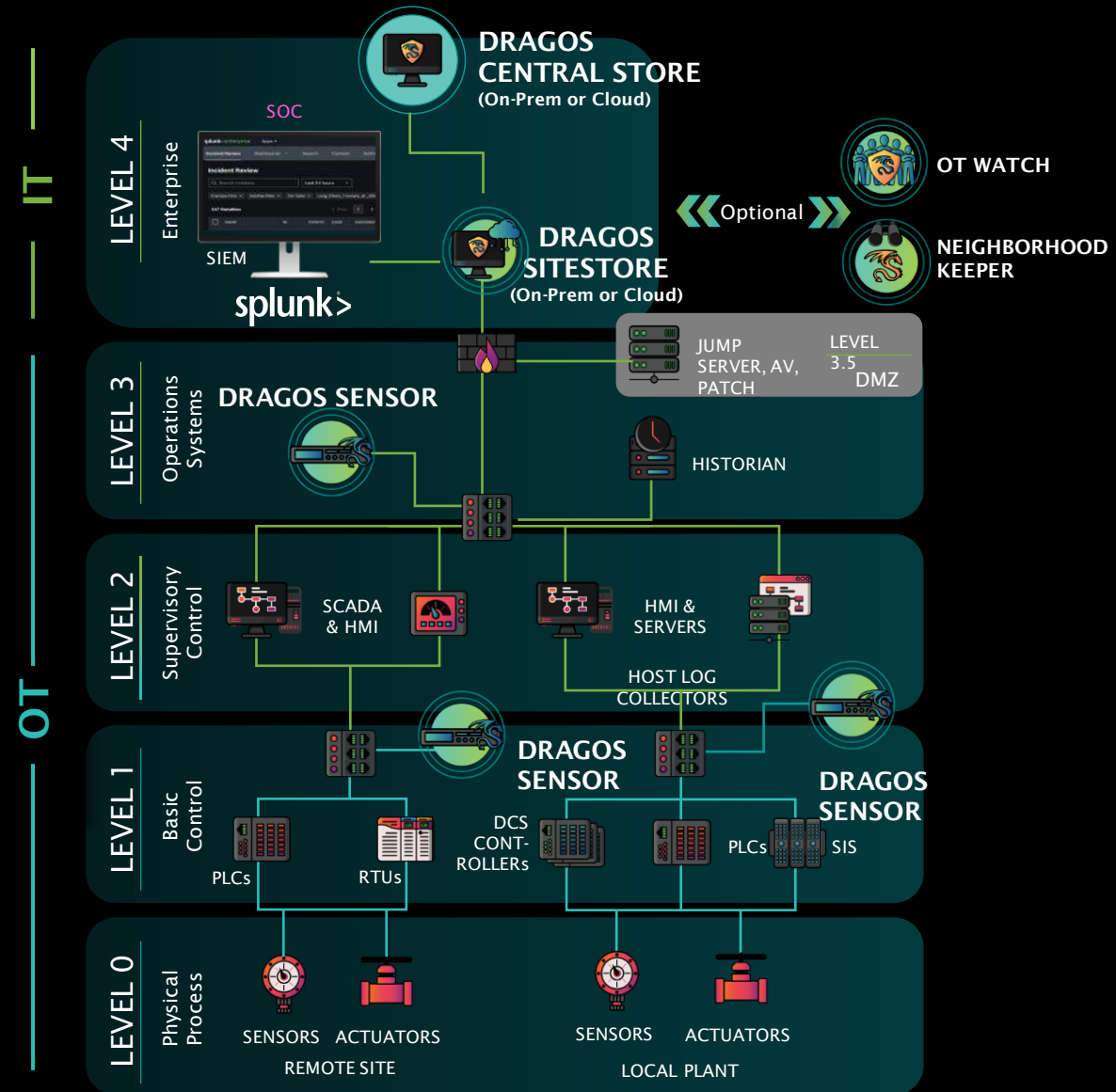
Splunk SIEM

(Security information and event management)

- Risk based alerting
- Advanced Threat Detection
- Embedded threat intelligence
- Rapid response security content

The Dragos Platform

- OT Asset Visibility
- Vulnerability Management
- Threat Detection
- Investigation & Response



Q&A



PANELIST

Jose Avila-Gomez
Senior Industrial
Consultant
Dragos



PANELIST

Paul Pelletier
Director of Security / Public
Sector Field Solutions
Splunk



MODERATOR

Sam Van Ryder
Director, Strategic
Accounts
Dragos

QUESTIONS AND ANSWERS

THANK YOU FOR JOINING US!

DRAGO 

Risk Management:

dragos.com/industrial-cyber-risk-management/

Partner:

dragos.com/partner/splunk/

&

splunk>

Dragos OT Add On:

splunkbase.splunk.com/app/6450