DRAGOS splunk>

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

DRAGOS

splunk>

Managing Risk

The “Classic” Cyber Risk Equation

Agnostic to Engineering and Operations

Are threats decreasing?

$$Cyber\ Risk = Consequence \times Threat \times Vulnerability$$

Are vulnerabilities decreasing?

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

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

Threat

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

Vulnerability

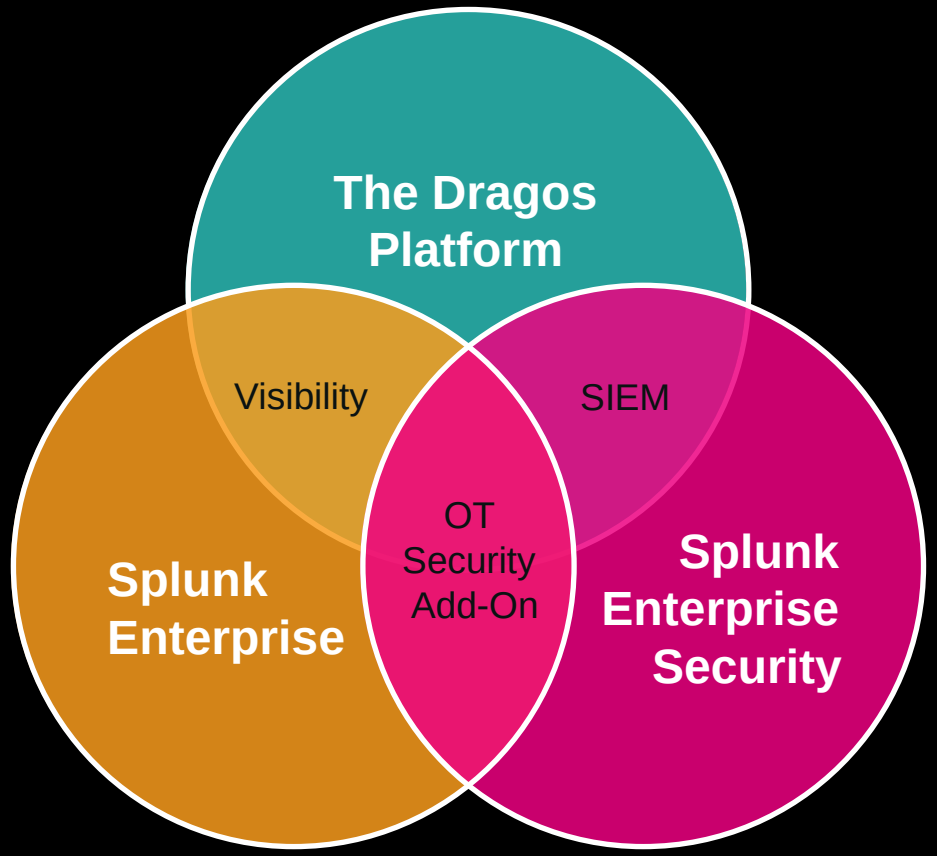
- Specific vulnerabilities
- Considers individual device vulnerabilities, and systemic architecture weaknesses

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

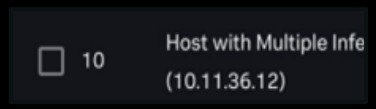
- Risk based analytics
- Consume noise
- Raise the relevant

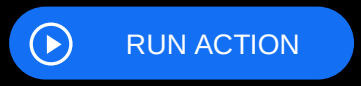
Resilience

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

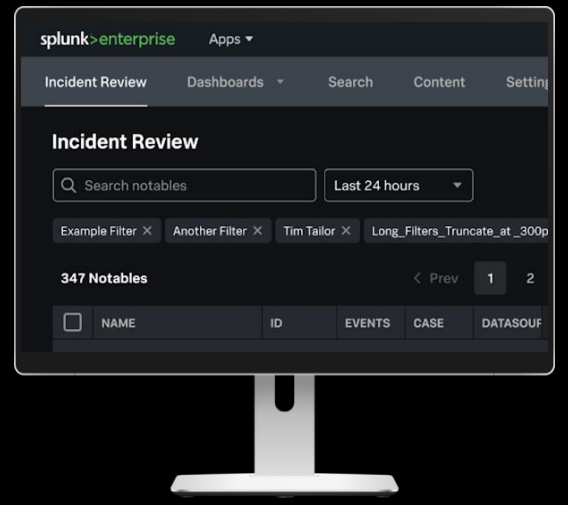
Splunk's Direction

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





Threat Detection	Investigation	Response
Enterprise Security behavioral analytics service *Batch and streaming event correlation, prioritization to reduce noise* *ML-based analytics to find behavioral anomalies and insider threats*	**Incident review, auto enriched events** *Prioritized, triaged, routed and notified* *Ad hoc search across multiple data sources, Splunk and non Splunk*	**Guided response templates** *Guidance through an incident, what to do next, what others have done for similar incidents, etc* *Customizable reporting and case management to drive faster time to respond*
OCSF		
Customer Data Lakes (Cloud & On Prem)	Splunk (Cloud & On Prem)	Dragos Playbook & SOAR



Traditional Notables and RBA Together

Traditional Notables

Realm of Known

- High Fidelity
- Low Volume
- Actionable
- i.e. Ransomware signature

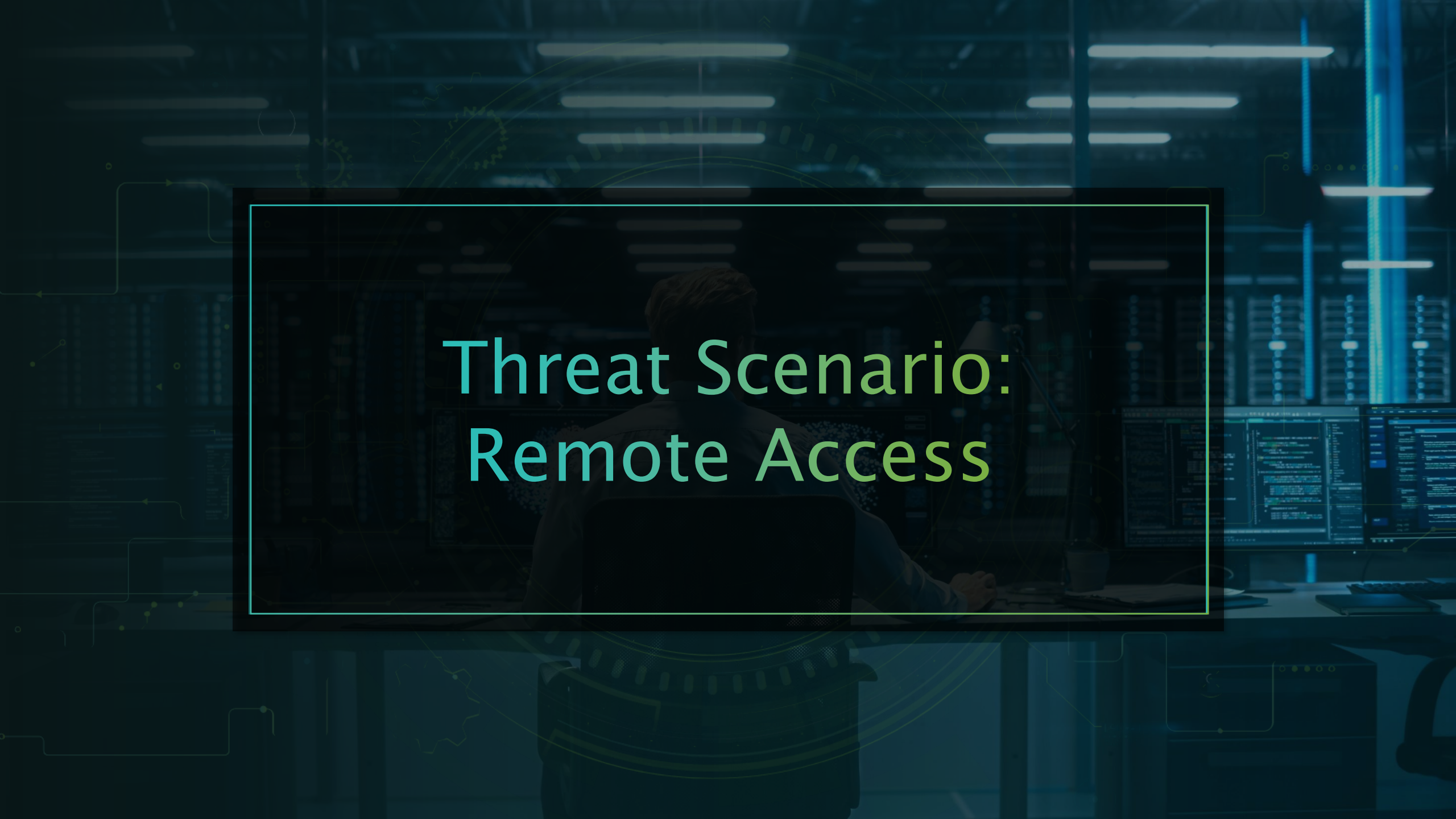
Point-in-time

Risk Based Alerting

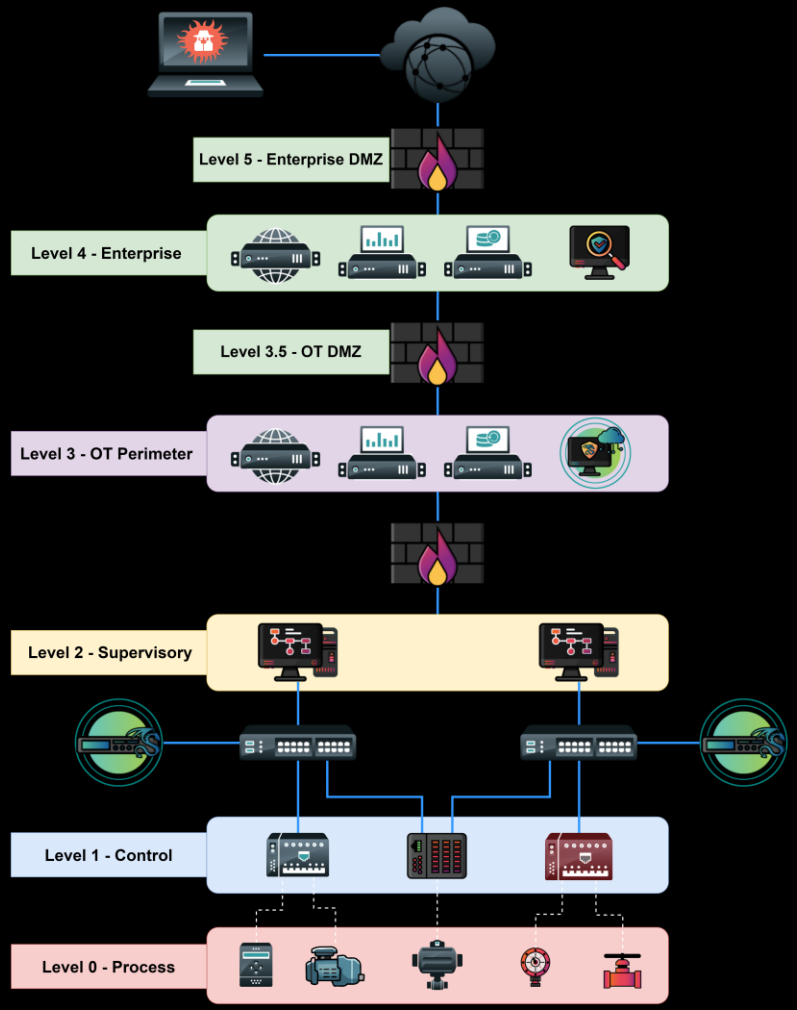
Realm of Unknown

- Risky behavior detection
- Risk Scoring
- Alignment to Security Frameworks
- Reduce False Positives

Period-of-time


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

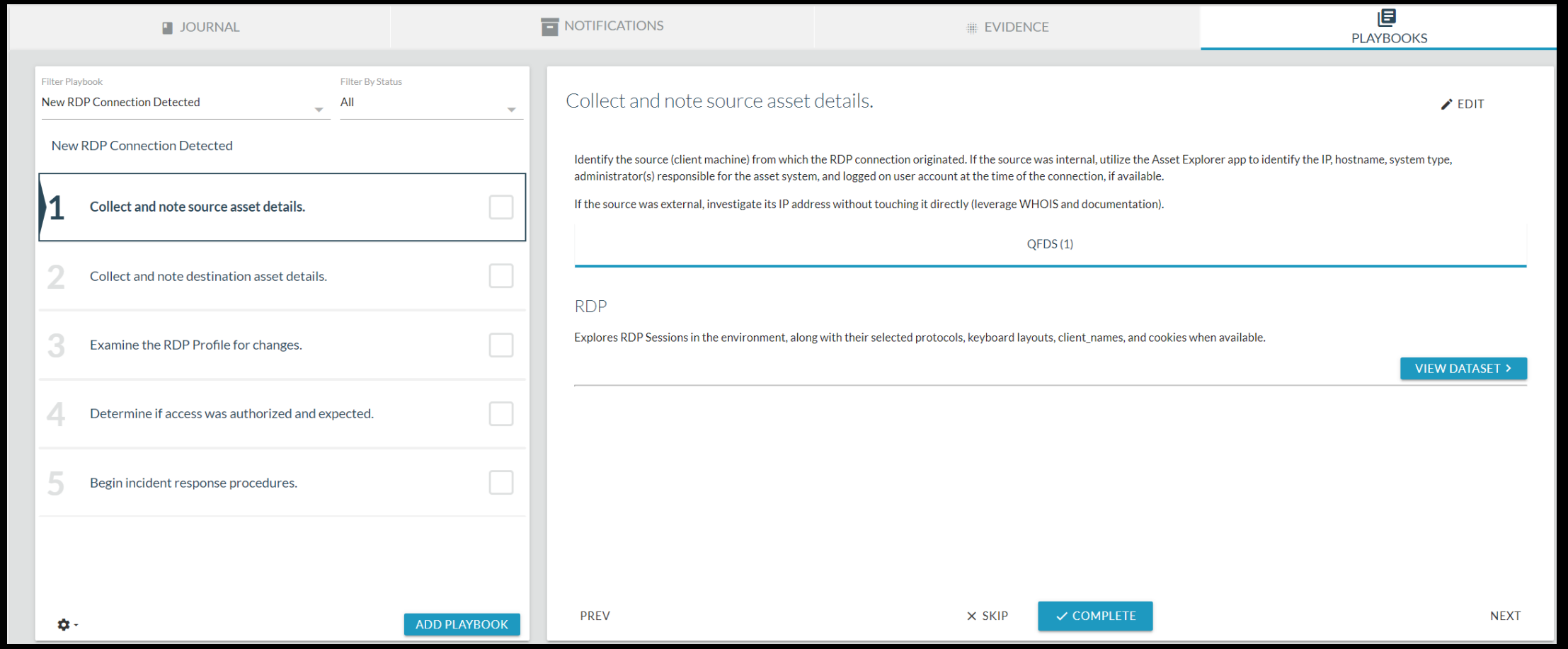
In addition to having a strict change-management process, which has not been initiated for this specific change, it's highly abnormal for contractors/engineers to be logging in during off-hours

Challenge

What is the risk?

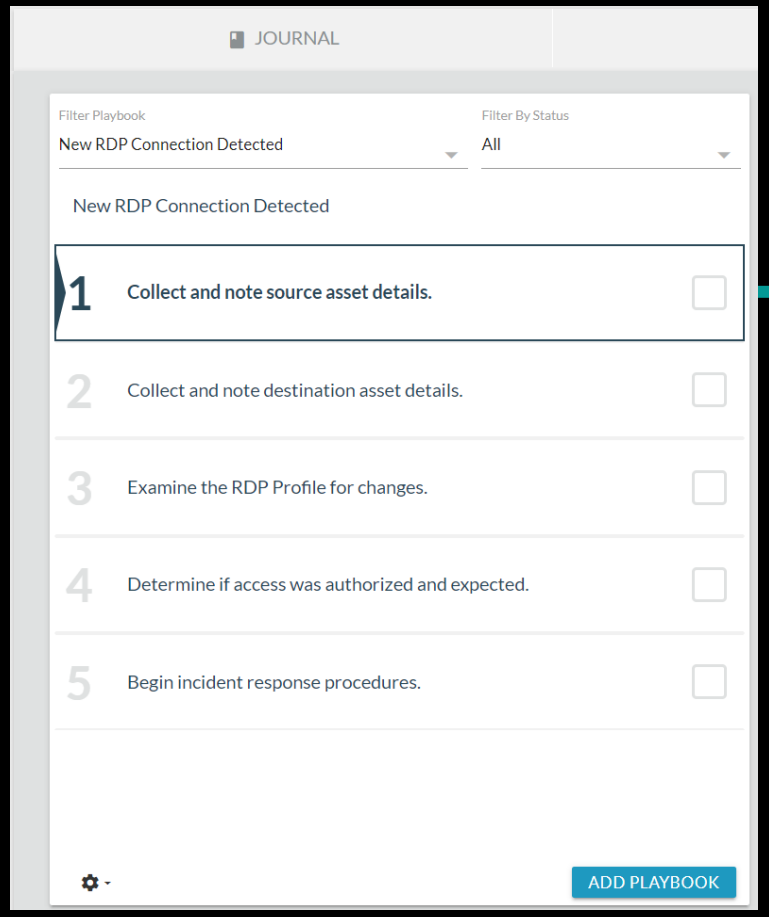
Threat Scenario: Remote Access

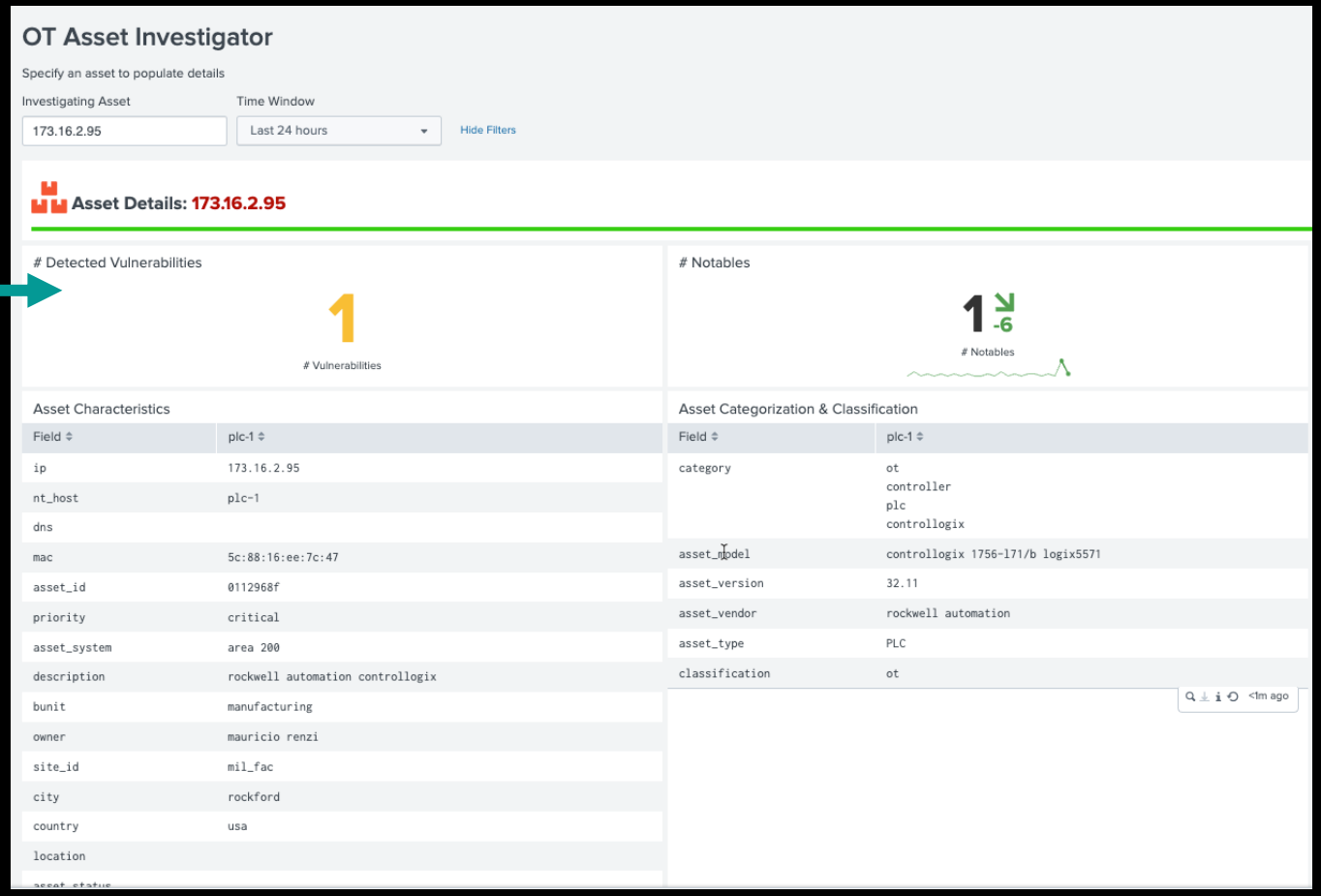
Playbooks – New RDP Connection Detected



Threat Scenario: Remote Access

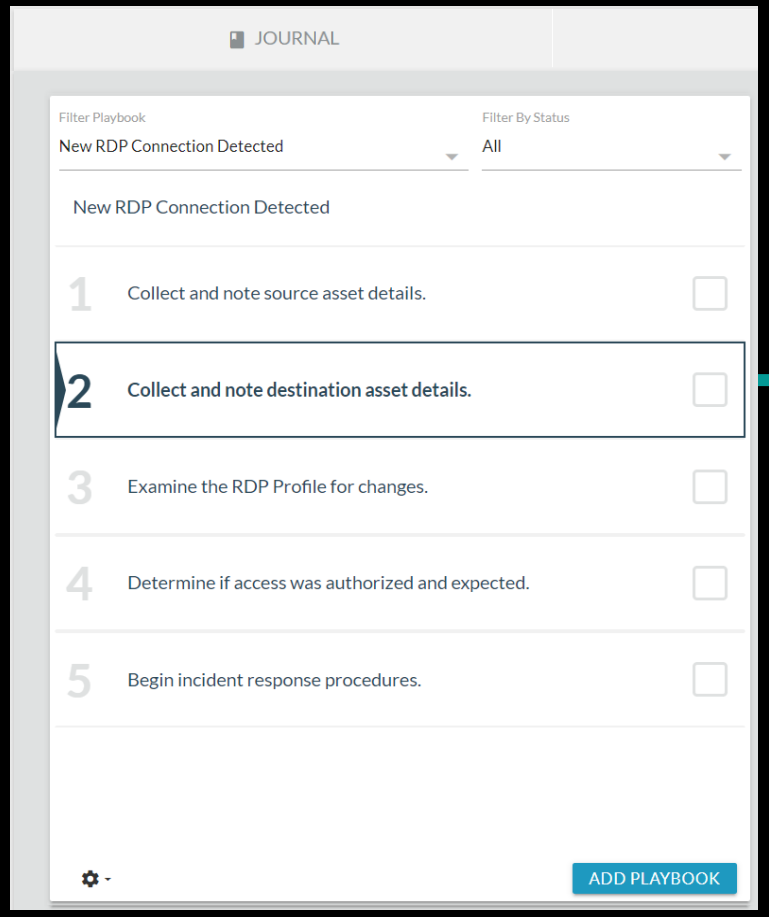
Playbooks – New RDP Connection Detected

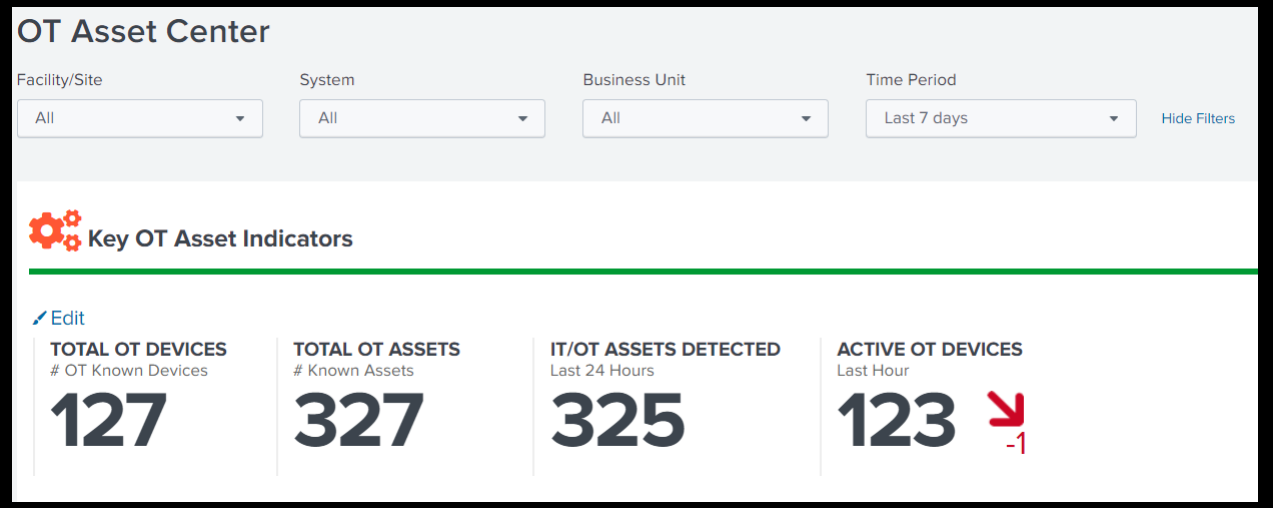


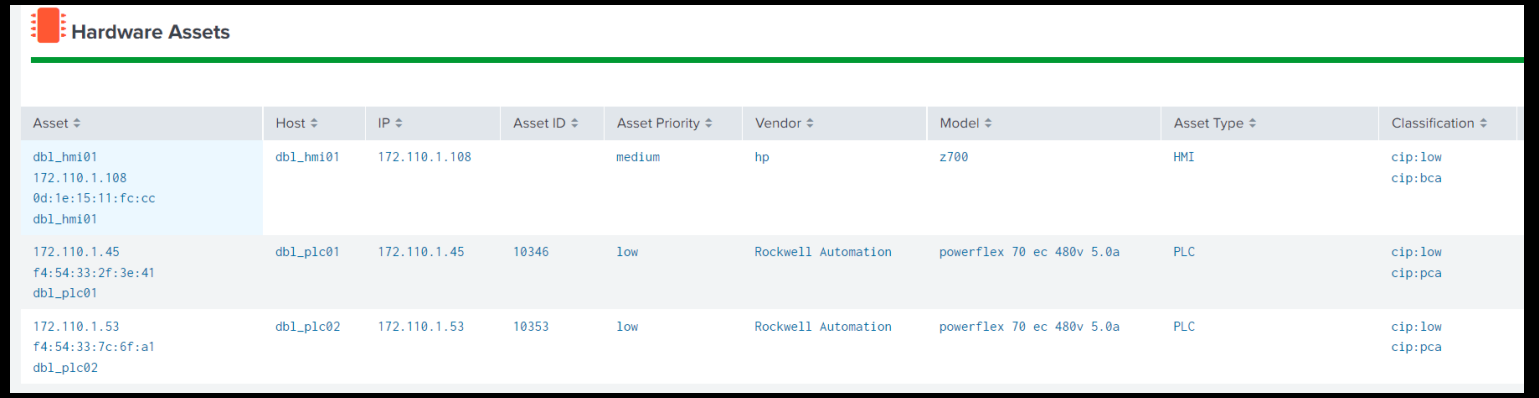


Threat Scenario: Remote Access

Playbooks – New RDP Connection Detected

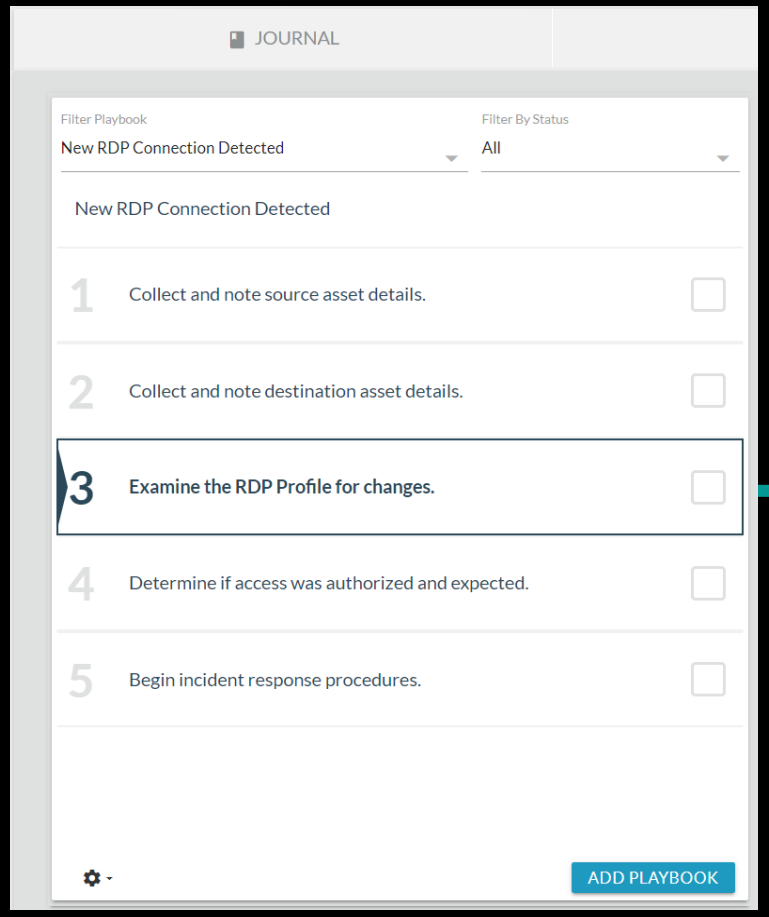


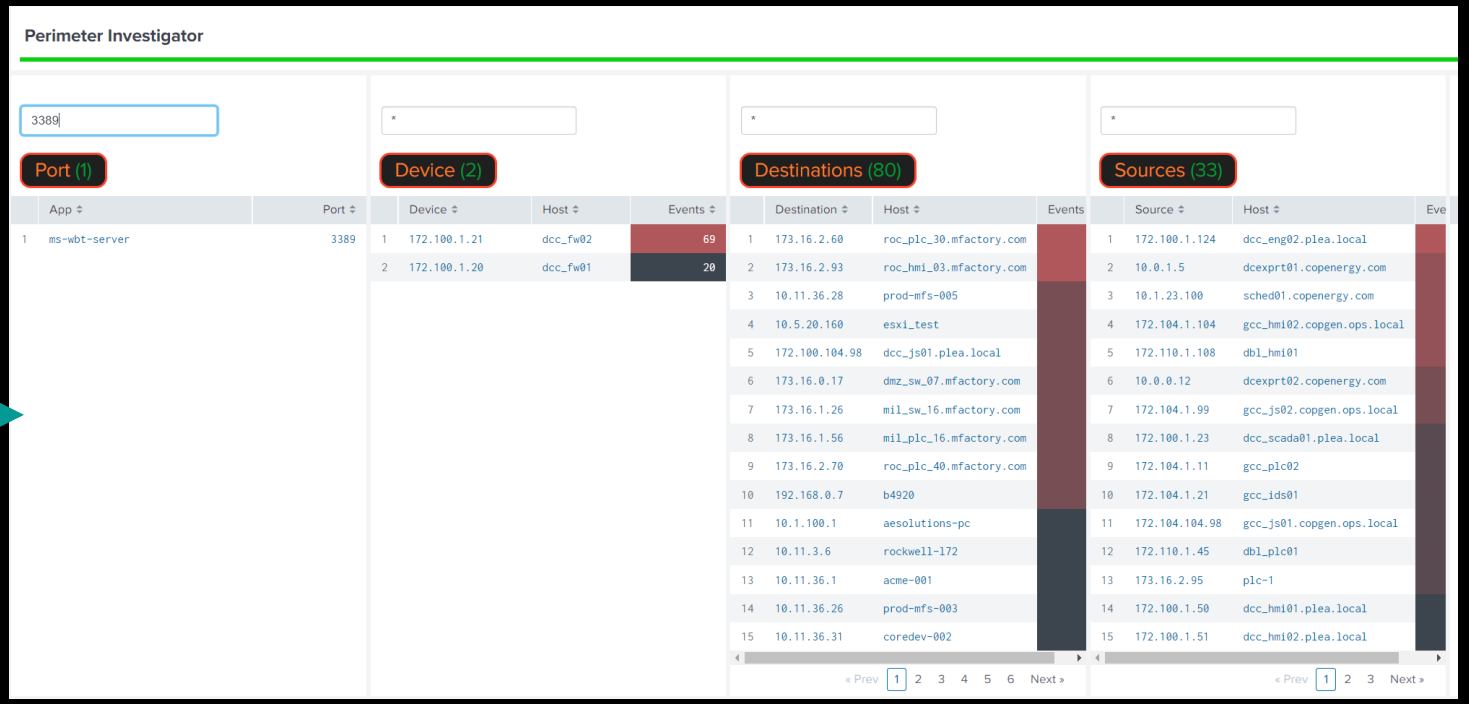




Threat Scenario: Remote Access

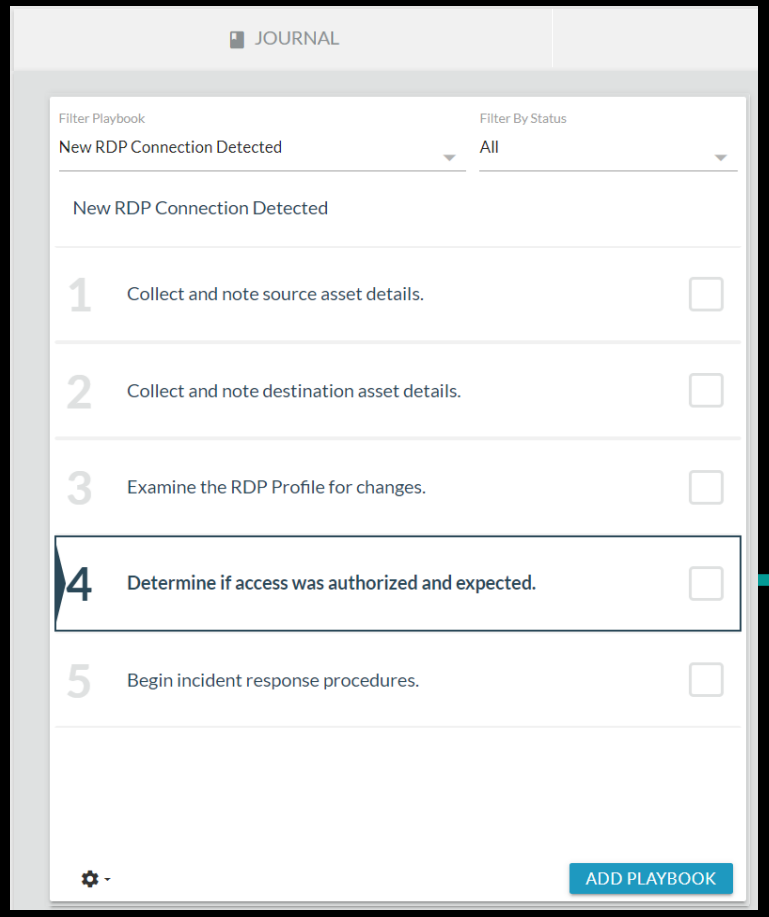
Playbooks – New RDP Connection Detected

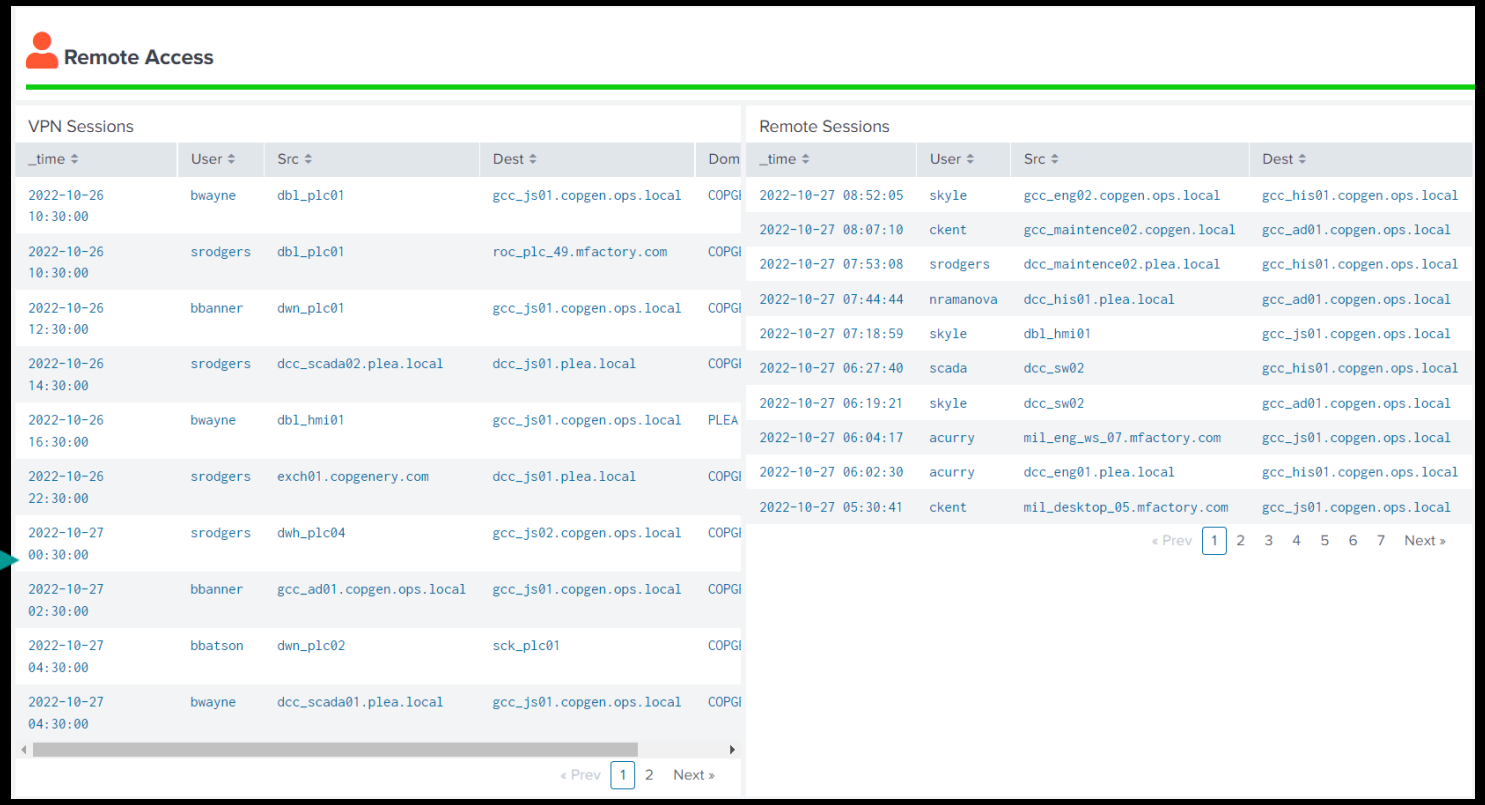




Threat Scenario: Remote Access

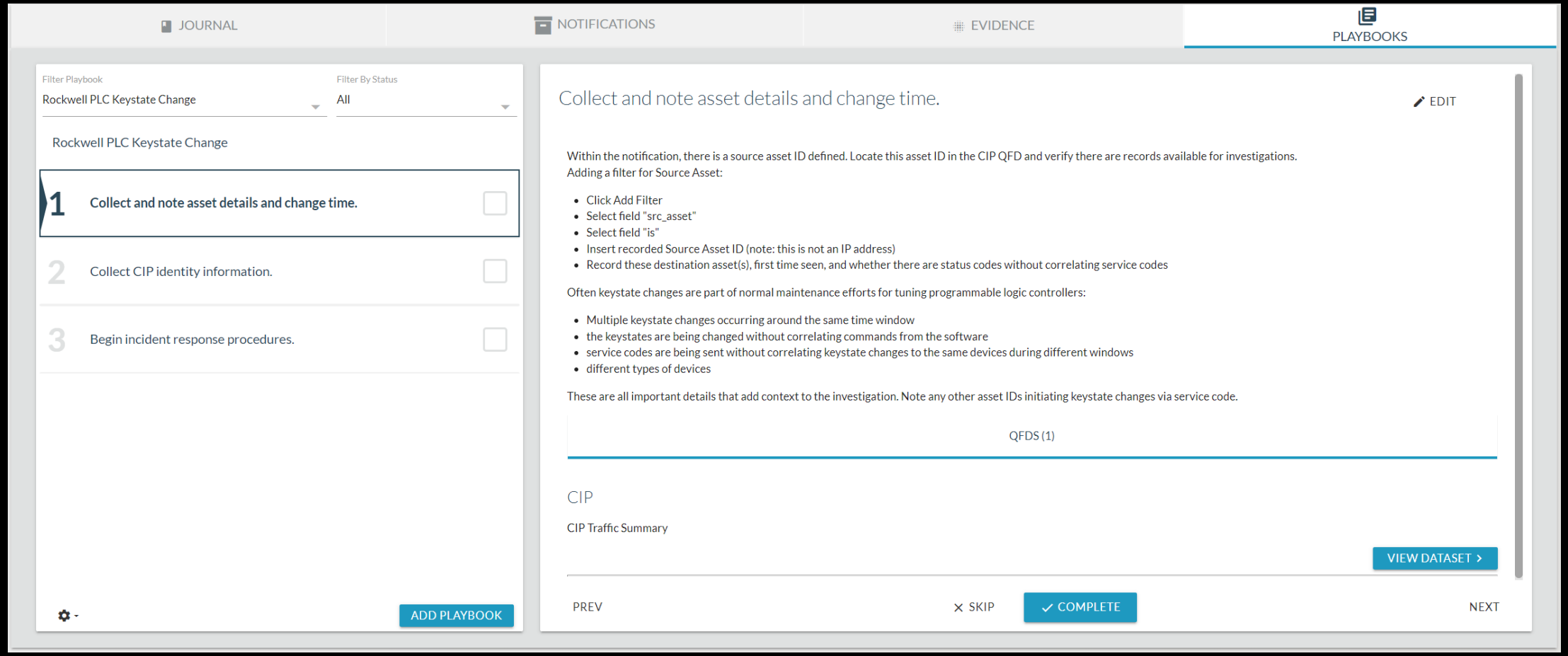
Playbooks – New RDP Connection Detected





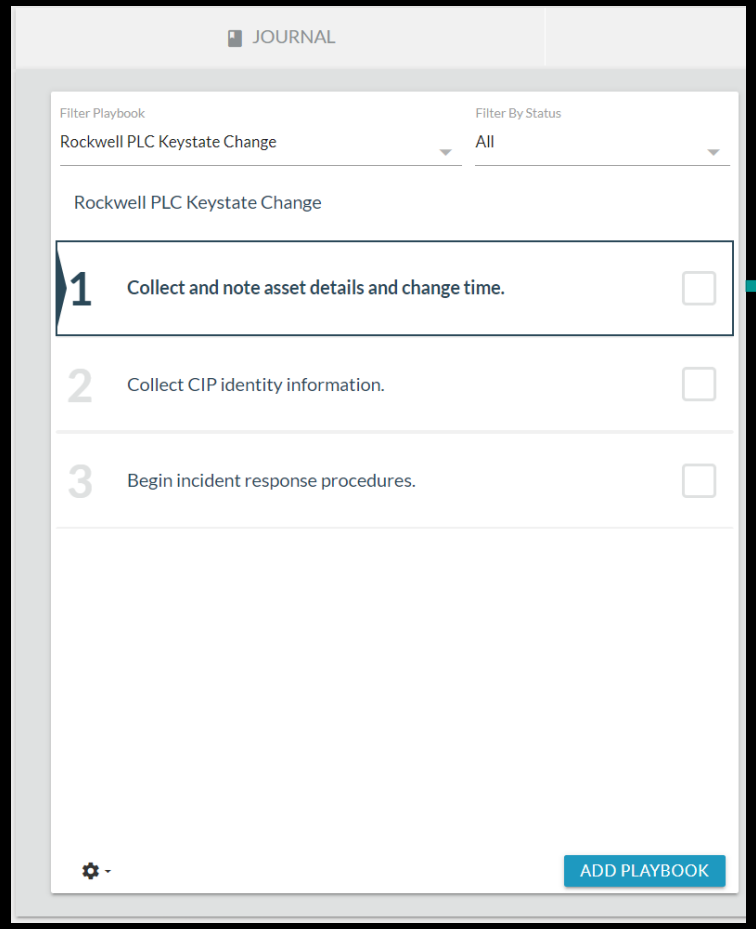
Threat Scenario: Suspicious Remote Access

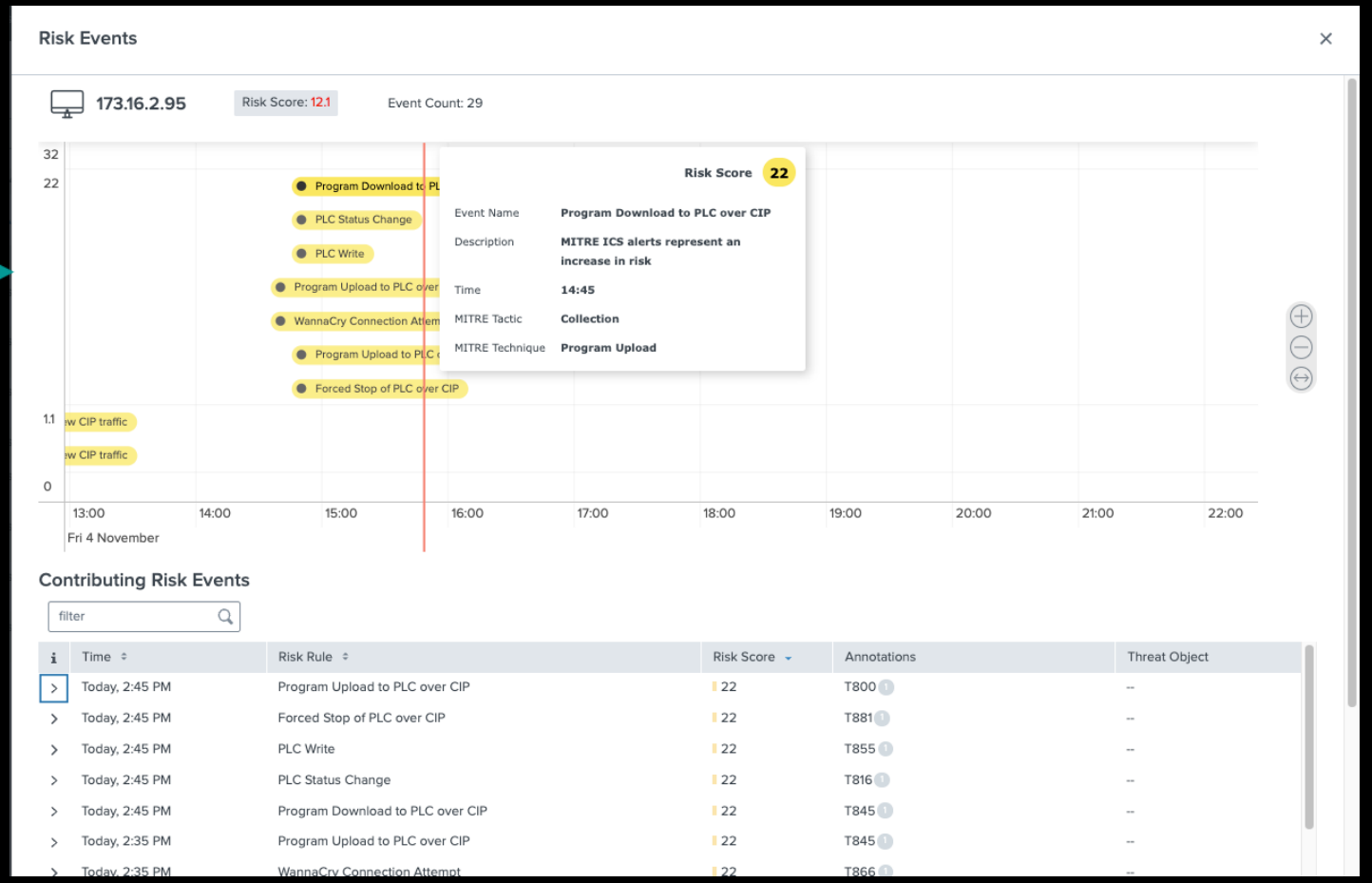
Playbooks – Rockwell PLC Keystate Change



Threat Scenario: Suspicious Remote Access

Playbooks – Rockwell PLC Keystate Change



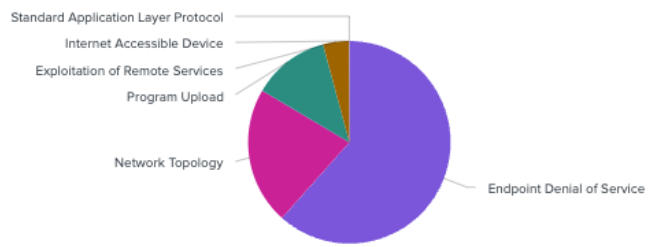


Threat Scenario: Suspicious Remote Access

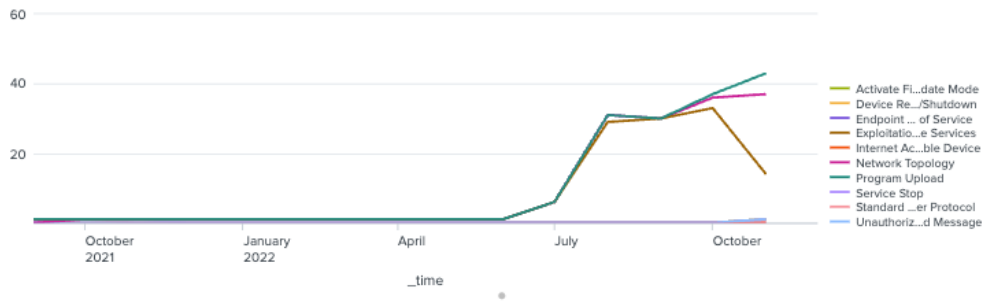
Rockwell PLC Keystate Change – Risk Workbench

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
173.16.2.95	host_artifacts		81418.0
173.16.2.95	system		128063.8

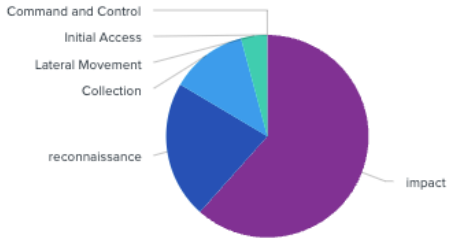
Artifacts By MITRE ATT&CK Techniques



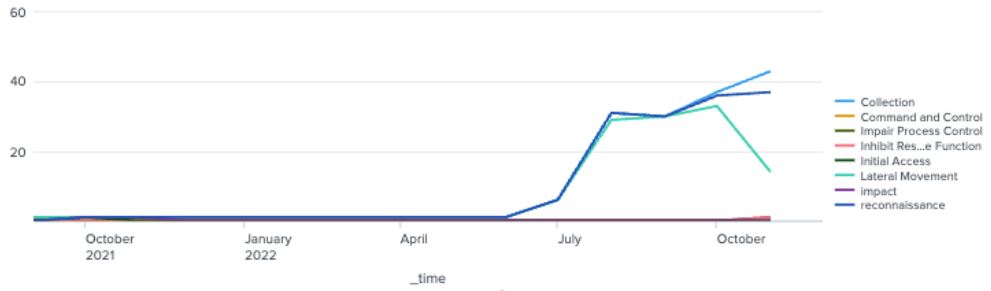
MITRE ATT&CK Techniques Over Time



Artifacts by MITRE ATT&CK tactics

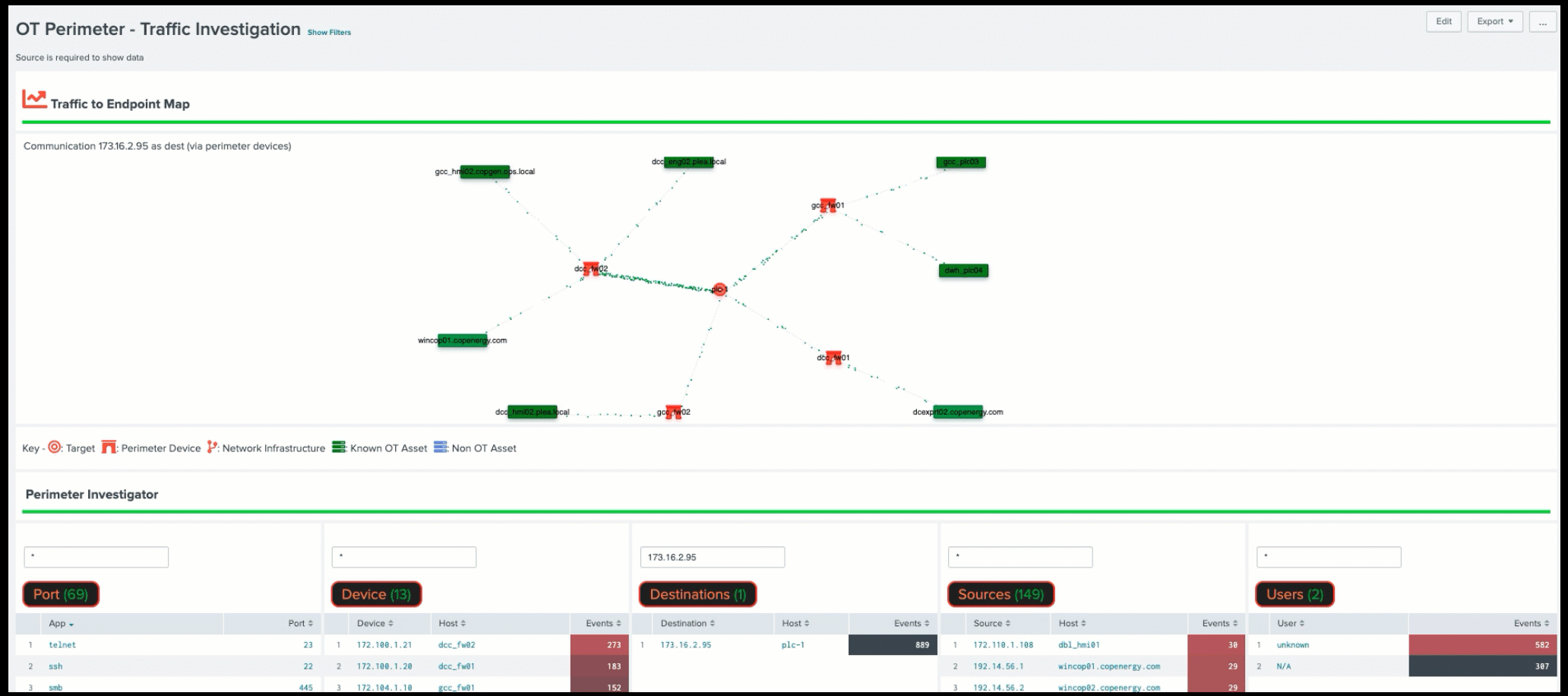


MITRE ATT&CK Tactics Over Time



Threat Scenario: Suspicious Remote Access

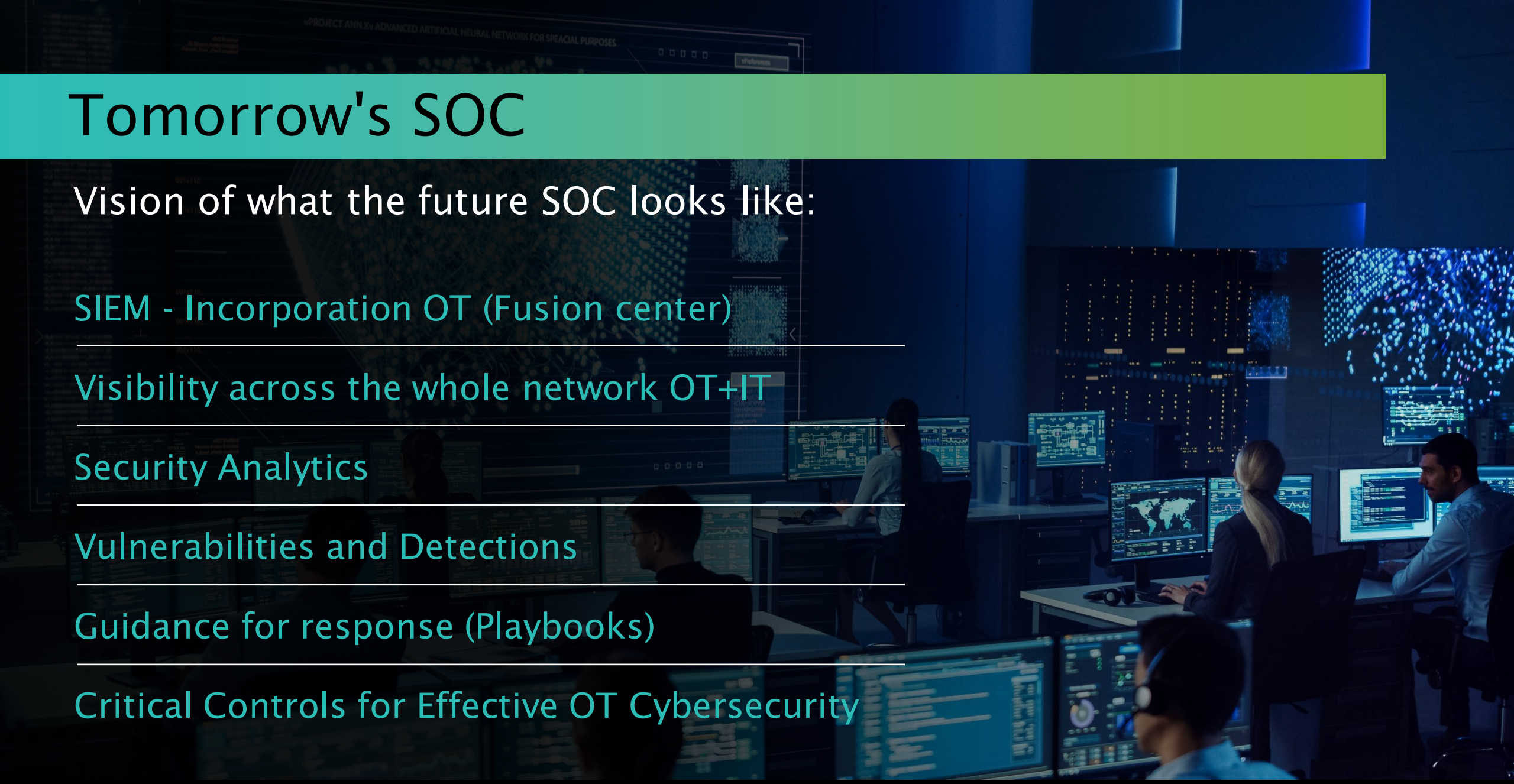
Rockwell PLC Keystate Change – Real time communication




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

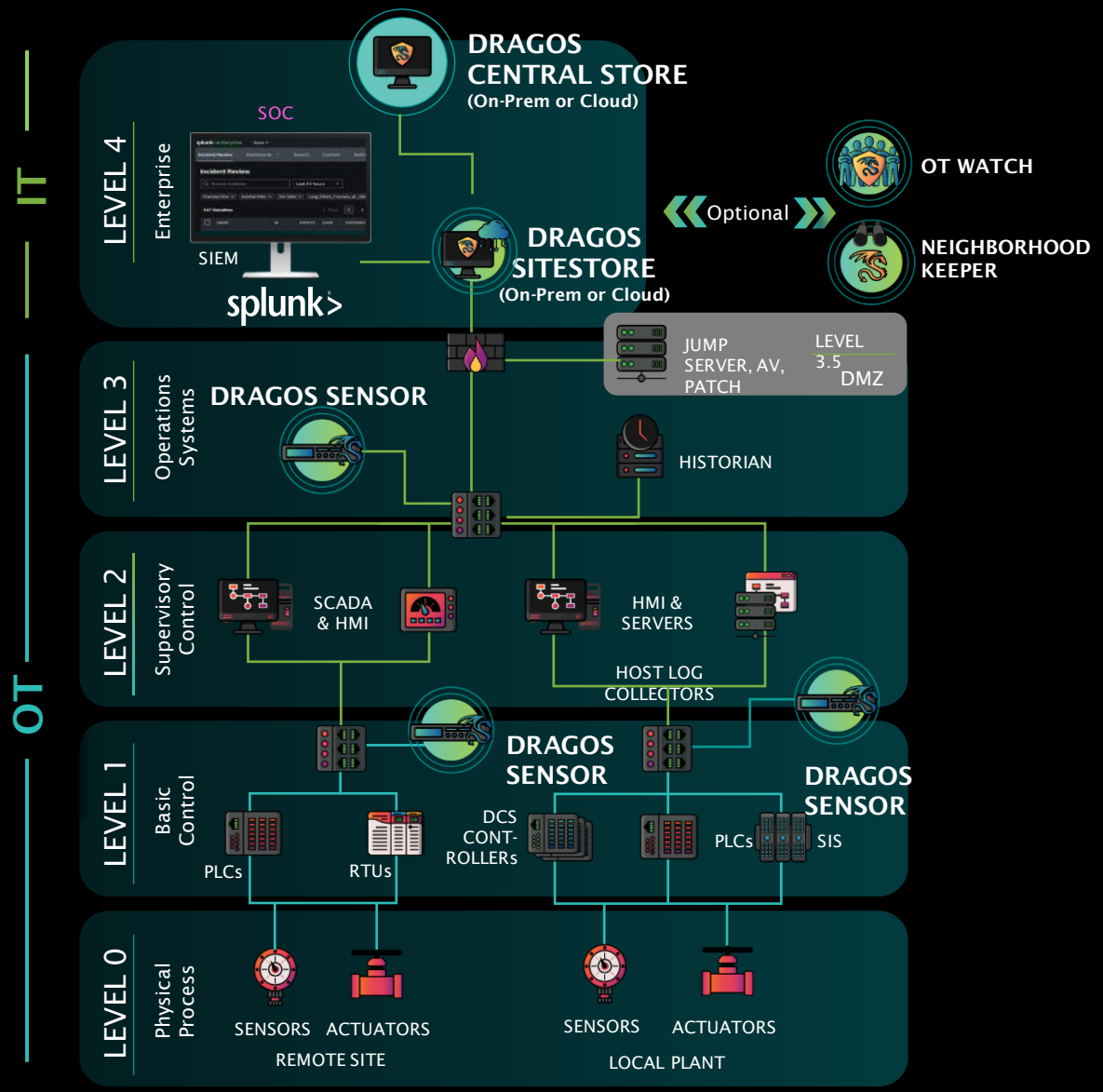
SOC (Security Operations Center)

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!

DRAGOS

Risk Management:
dragos.com/industrial-cyber-risk-management/

Partner:
dragos.com/partner/splunk/

&

splunk>

Dragos OT Add On:

splunkbase.splunk.com/app/6450