Industrial Cyber Security In A Converging IT/OT World

Michael Rothschild
Sr Director, Product Marketing | Indegy

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Critical Infrastructure Is More Than You Think

Operations Technology

PC for Programmable Controller

- Began in 1956
- Resulted in late 60's the PLC

By 2020

1 Billion new middle-class consumers will add

$8T to consumer spending

Increased Demand on Industrial Production

GLOBAL POPULATION TRENDS INCREASE DEMAND FOR

- Manufacturing
- Resources
- Infrastructure

EMERGING MARKET CONSUMERISM

30% More Water

100% More Vehicles

80% More Steel

50% More Energy

RESOURCE PRODUCTIVITY INVESTMENT

$1T Annually

Source: McKinsey

Why Are We Here?

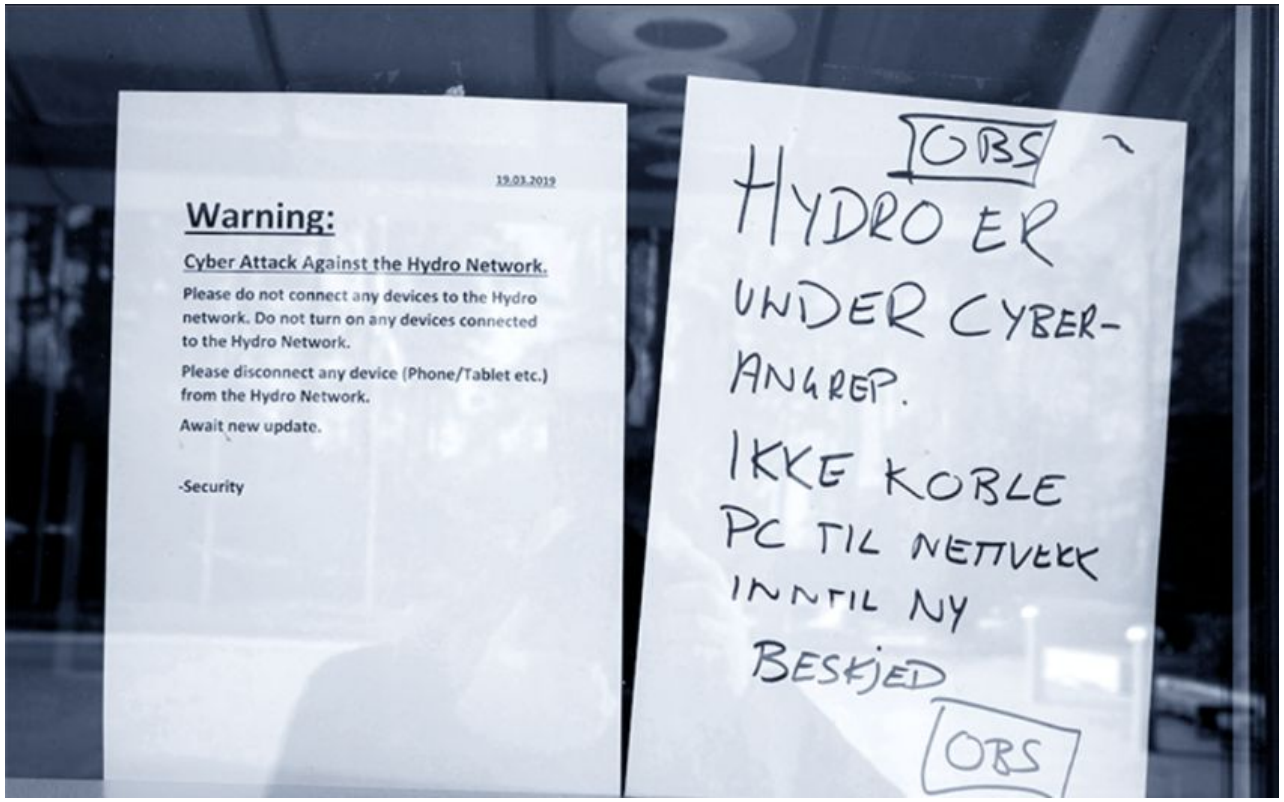
From A Security Perspective

- IT/OT convergence – OT is no longer isolated
- Adoption of IIoT – more devices in more places
- Heterogeneous audience – more people with access credentials
- Increased targeting of OT - an “unsecured” attack surface

Ripped From The Headlines

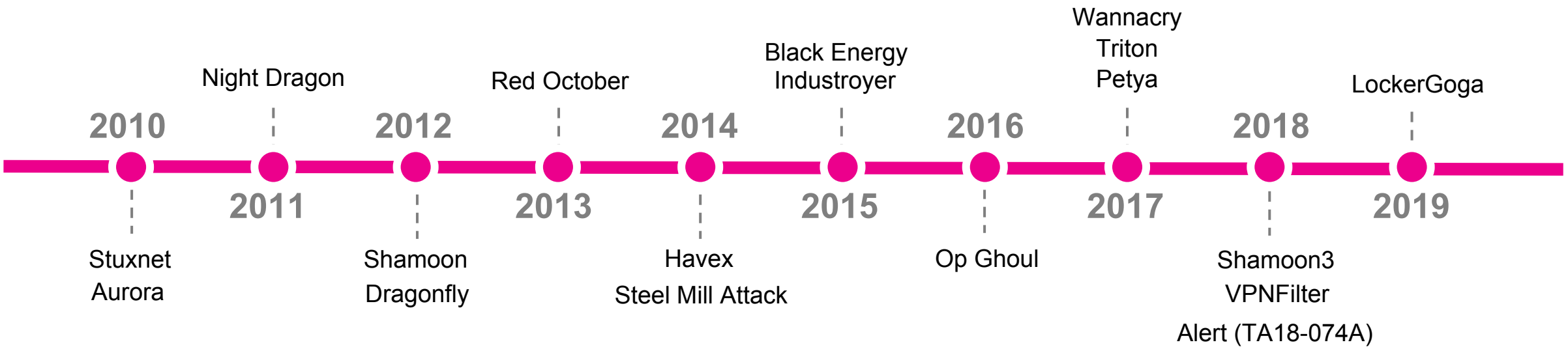
LockerGoga

- First seen in January
- Reemerged in March and took down one of the largest aluminum producers
- Reemerged in April again to take out Hexion and Momentive



A Historical Timeline

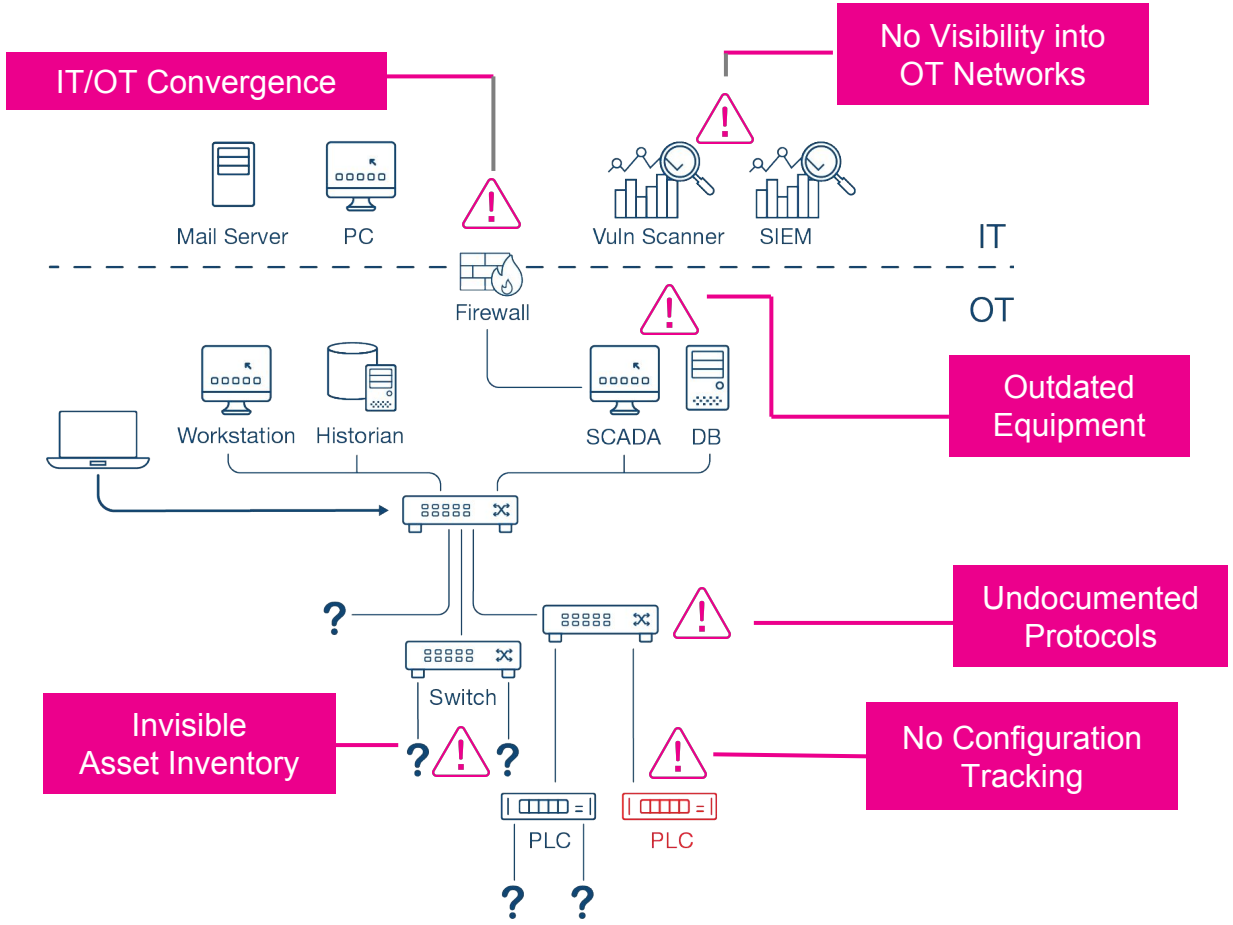
Cyber attacks on critical infrastructure



Source: Indegy
Activate All Your Senses

Vulnerabilities and Gaps

When Converging IT & OT



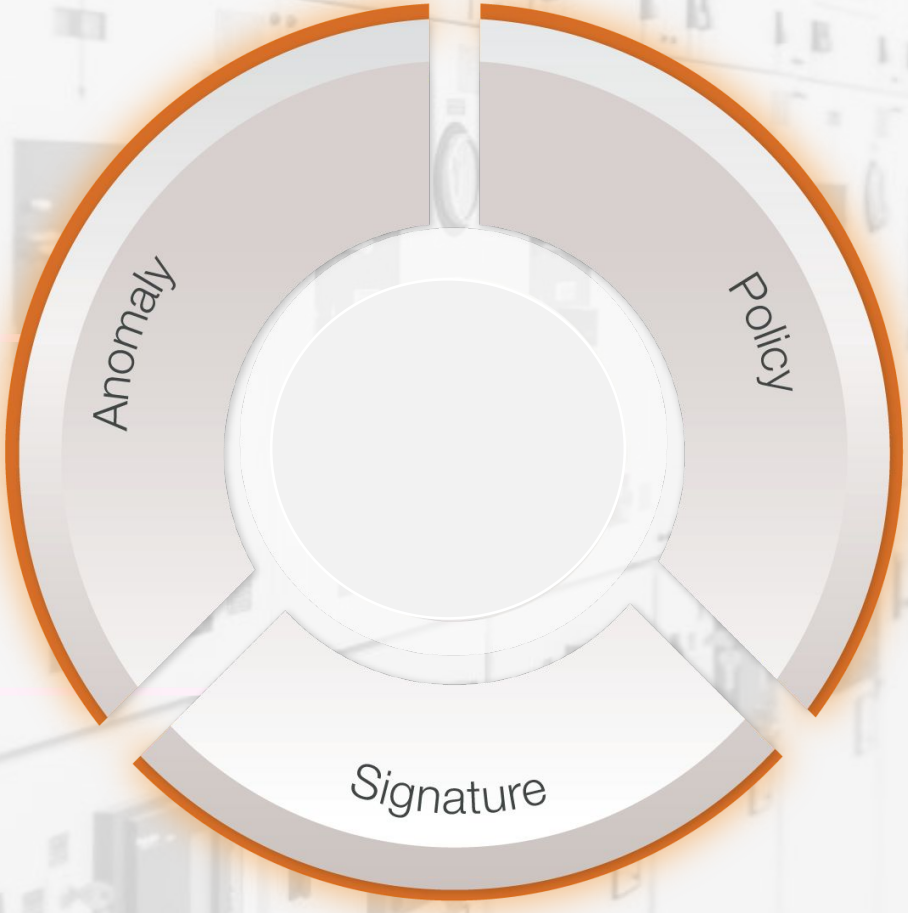
splunk> .conf19

Requirement 1: Threat Detection

Malware | APTs | Ransomware | 3rd Party Access | Insider Threats | Local Access | Rogue Devices | Vuln. Exploits

Multi-Threat Detection Engine

- Machine Learning
- Identifies stealthy, targeted, zero-days



- White and black-listing of activities
- Compliance and internal requirements

- Detection of IT and OT threats and exploitation
- Leverages community knowledge

Requirement 2: Asset Tracking

Typical Asset Scenarios

- Implemented a long time ago
- Recently inherited. And you know there were lots of changes over the years
- No Documentation. Nobody knows anything

Even if there were an accurate list somewhere …

Requirement 2: Asset Tracking

Identify

Assets communicating in the network

Discover

Devices which are not active

Classify

HMI, Historian, Router, PLC, Server, Switch...

Collect

Patch, Hotfix levels, Firmware, Users, PLC backplane

Track

Full configuration change control, including devices

Manufacturer | Classification | Logged User | Firmware Version | Software List | Configuration | Patch level | Operations Data

Taking The Next Step

Beyond The Network

See More – Secure More

- What user was logged in?
- What processes were running?
- “Login attempt” identified, did it work?
- “Code download” identifies, what was the key state at the time?

Main IT Security Elements

Firewalls

Asset Management

Intrusion Detection Systems

- Next Gen IDS

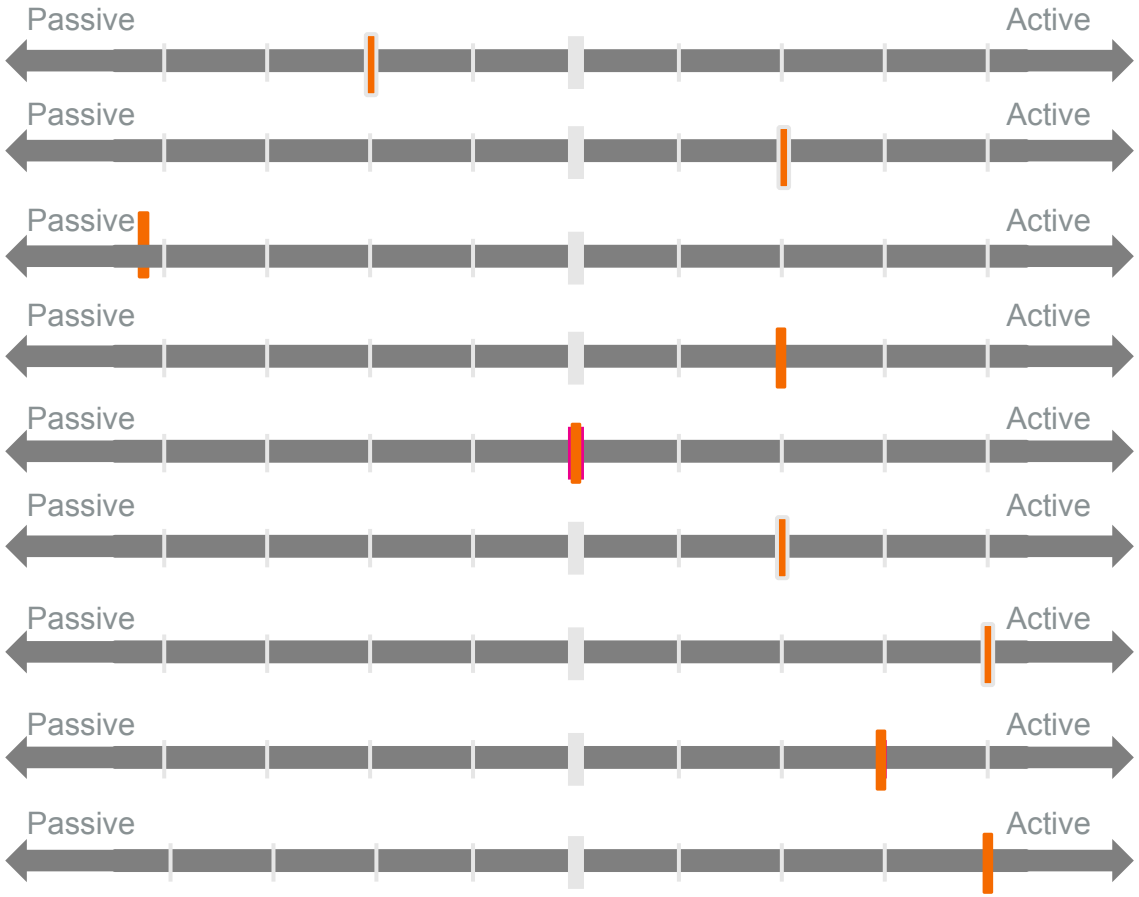
Anti Viruses

- Next Gen AV (EDR)

Vulnerability Management

Deception Technologies

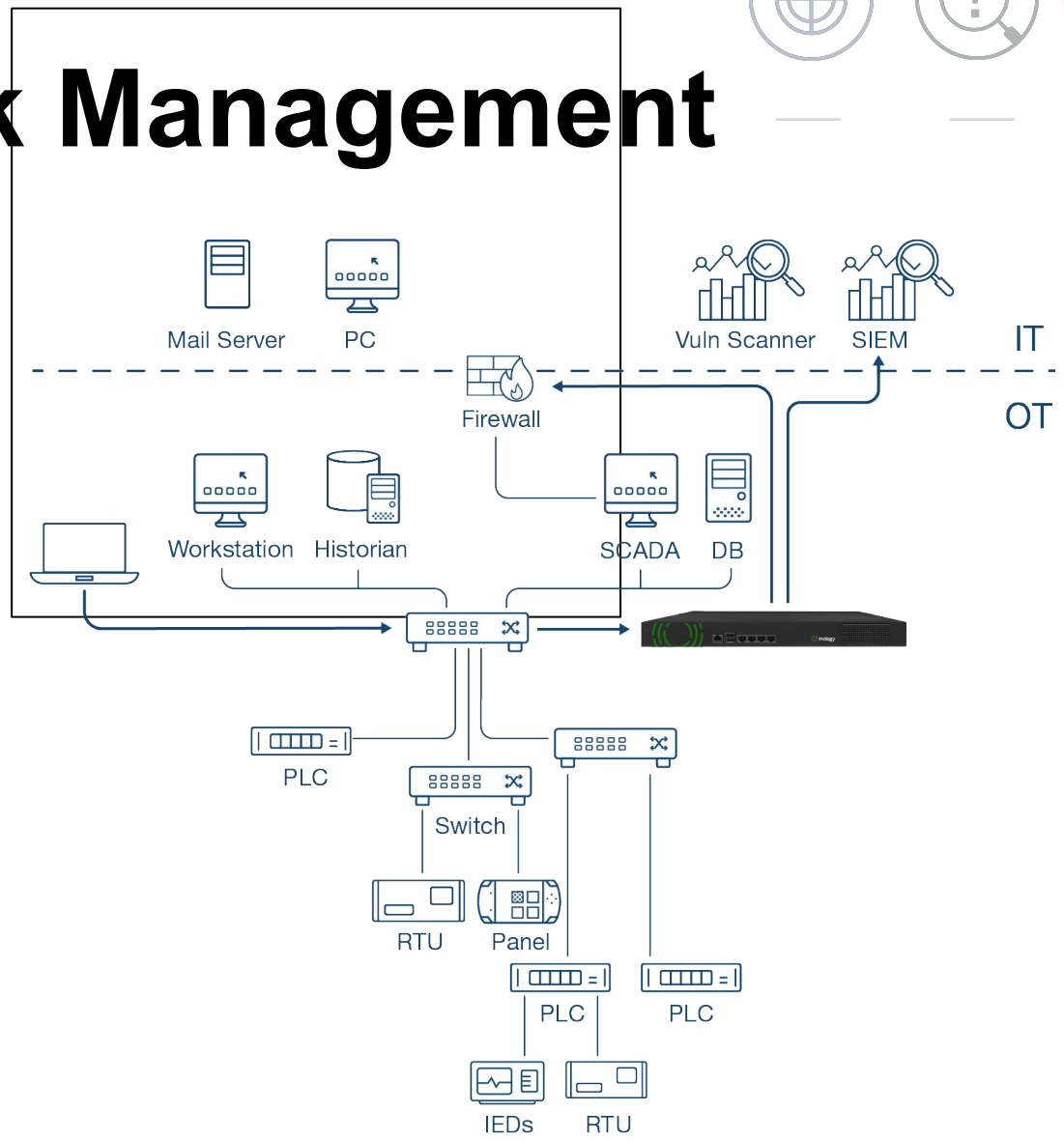
Network Access Control (NAC)



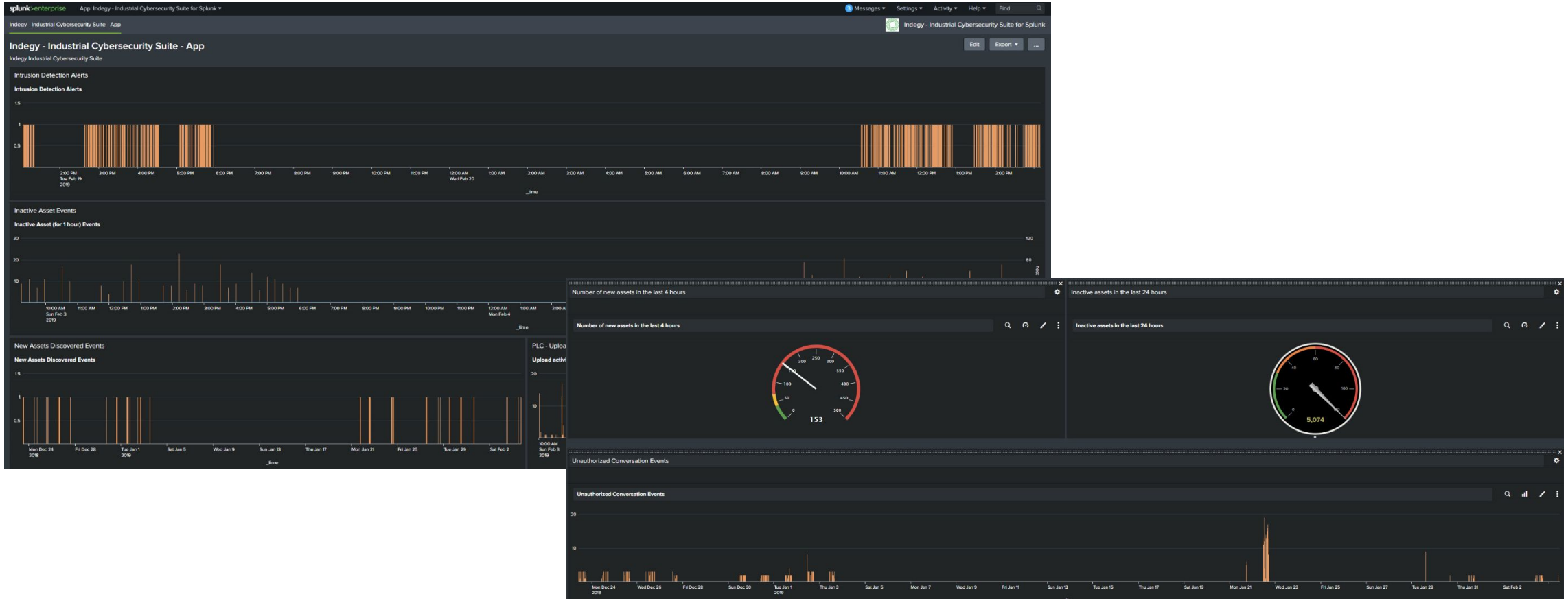
Requirement 3: Risk Management

The Ecosystem of Trust

- Visibility across both IT and OT environments
- Deep situational awareness
- Compliance with regulatory requirements
- Higher responsiveness when incidents occur
- Proactive maintenance



Indegy App On Splunkbase



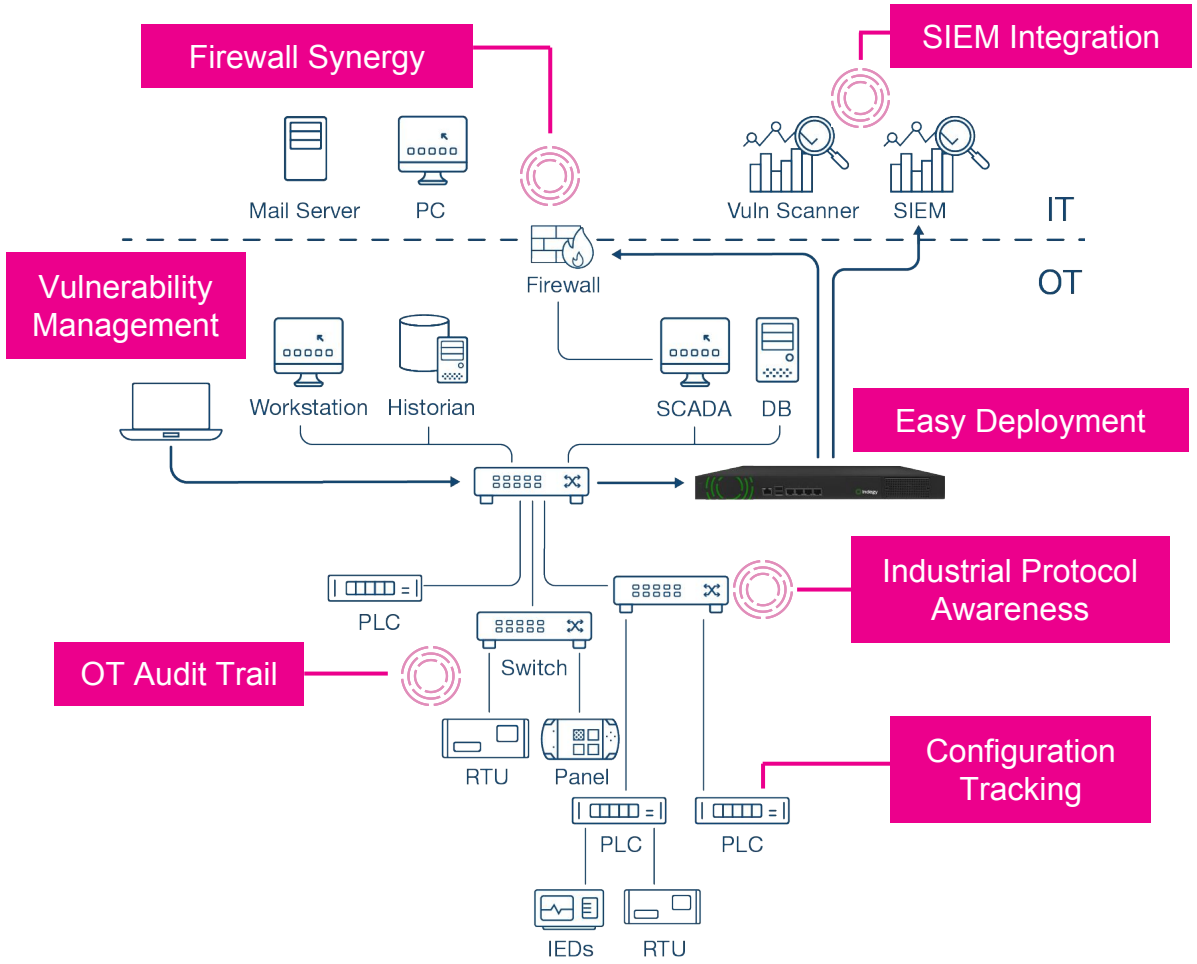
Securing Your OT Environment

Implementing These Three Areas Secures Your OT Environment From The Latest Threats

Threat Detection

Asset Tracking

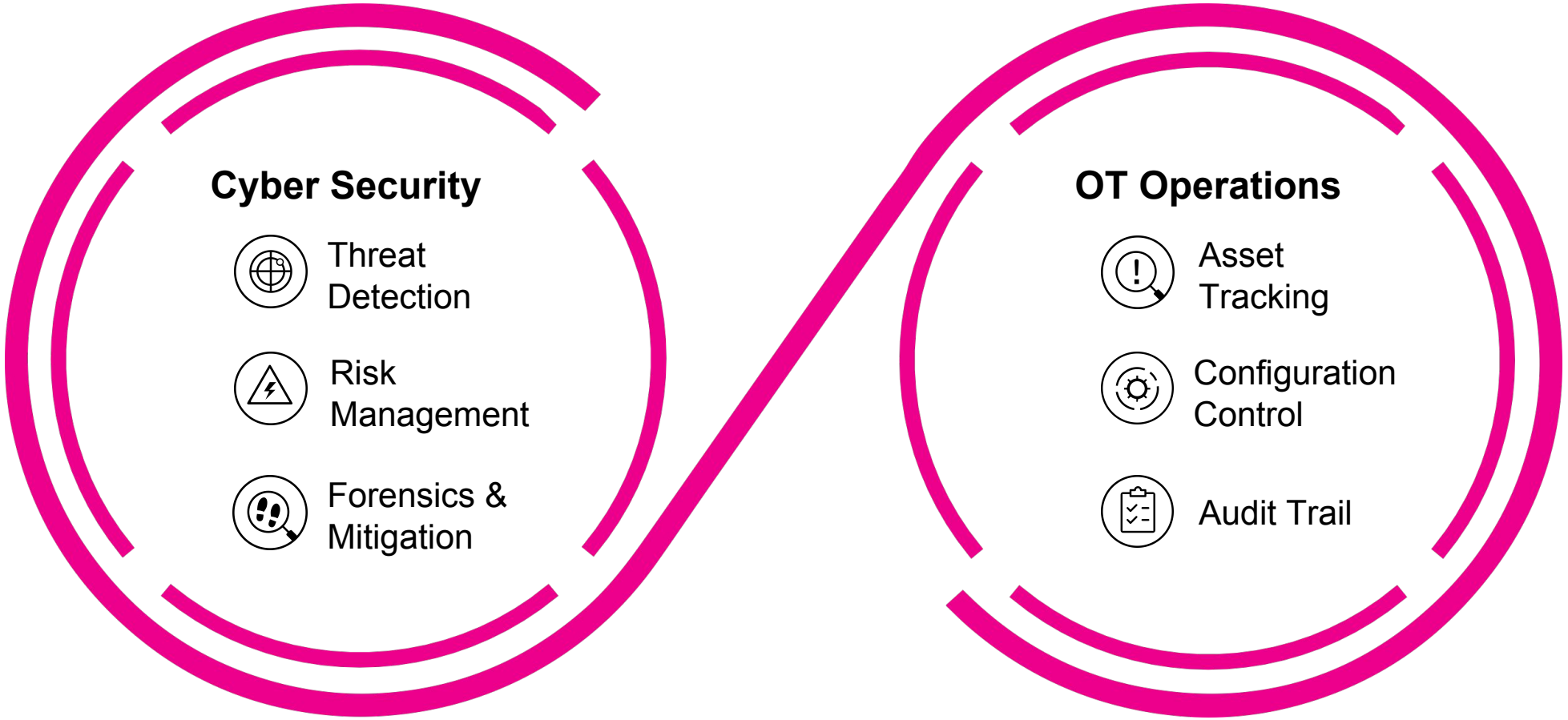
Risk Management



splunk> .conf19

Security and Operations

Hand in Hand



.conf19

splunk>

Indegy

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION