How to secure Operational Technology environments

…with the new Splunk add-on for OT Security

Ed Albanese
Global Area VP, IoT, Manufacturing, Energy & Retail | Splunk

Young Cho
Manufacturing Solution Strategist | Splunk

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.

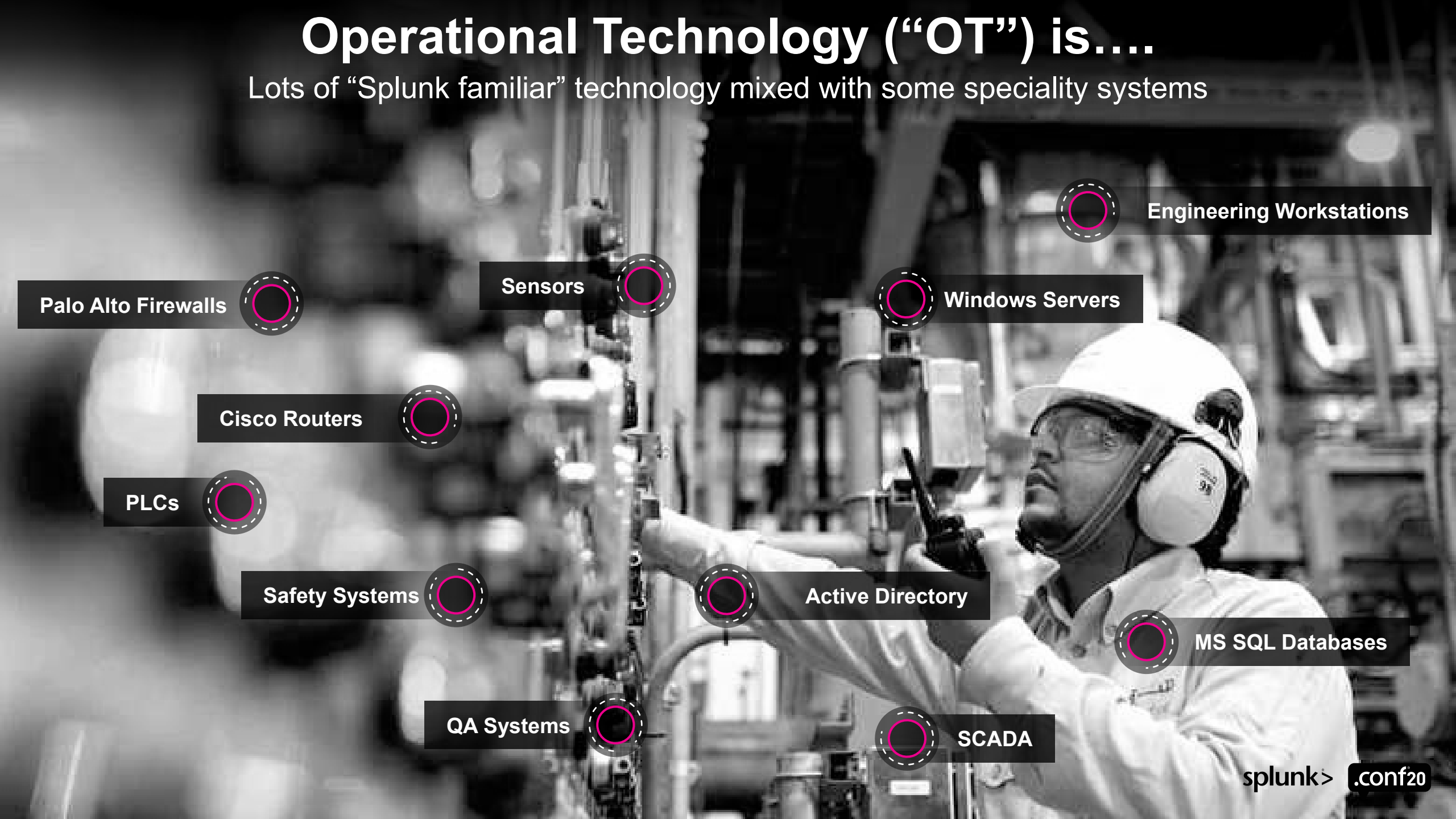
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the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


KUKA
splunk>
.conf20


splunk> .conf20

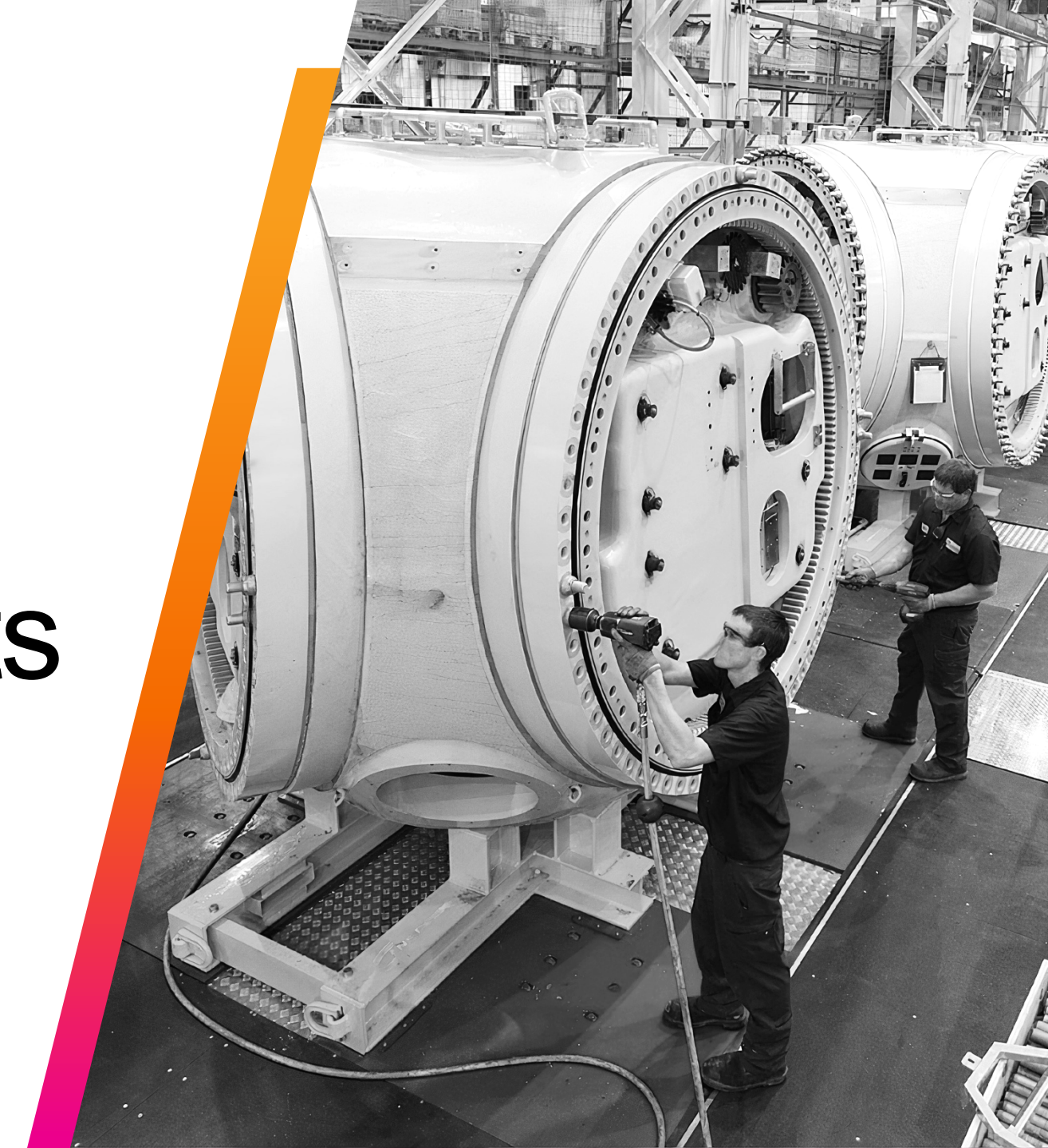
Operational Technology (“OT”) is….

Lots of “Splunk familiar” technology mixed with some speciality systems



splunk> .conf20

Why Splunk in OT environments



splunk> .conf20

“Already by 2018 nearly 60 percent of surveyed organizations had experienced a breach in their industrial control (ICS) or supervisory control and data-acquisition (SCADA) systems.”

McKinsey & Company, April 2019, “Critical infrastructure companies and the global cybersecurity threat”

Most Common Approach

Step 1.

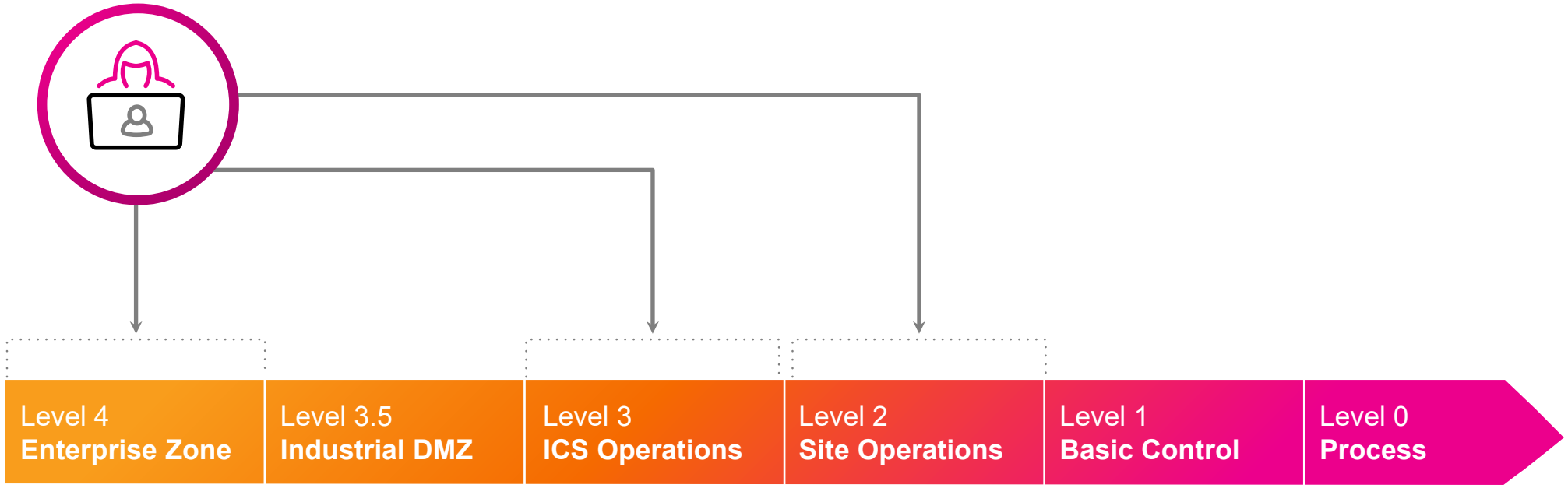
Corporate SIEM

Step 2.

OT-Specific Solution

“Corporate Tech” is typically the attack vector against OT

Same technology typically found in IT environments located in Level 4, 3 or 2



It's **almost always** corporate tech….

OT attacks are generally initiated at the OS, DB, networking, email or similar

Dec 2016

Industroyer malware disabled a substation in the Ukraine. Phishing attack. Gained access to Engr Workstation.

Aug 2017

TRISIS attack shuts down an oil refinery in Saudi Arabia. RDP traffic through DMZ firewall to Engr Workstation.

Jul 2019

Chinese hackers conducted a spear-phishing campaign against employees of 20 U.S. utility companies.

Oct 2019

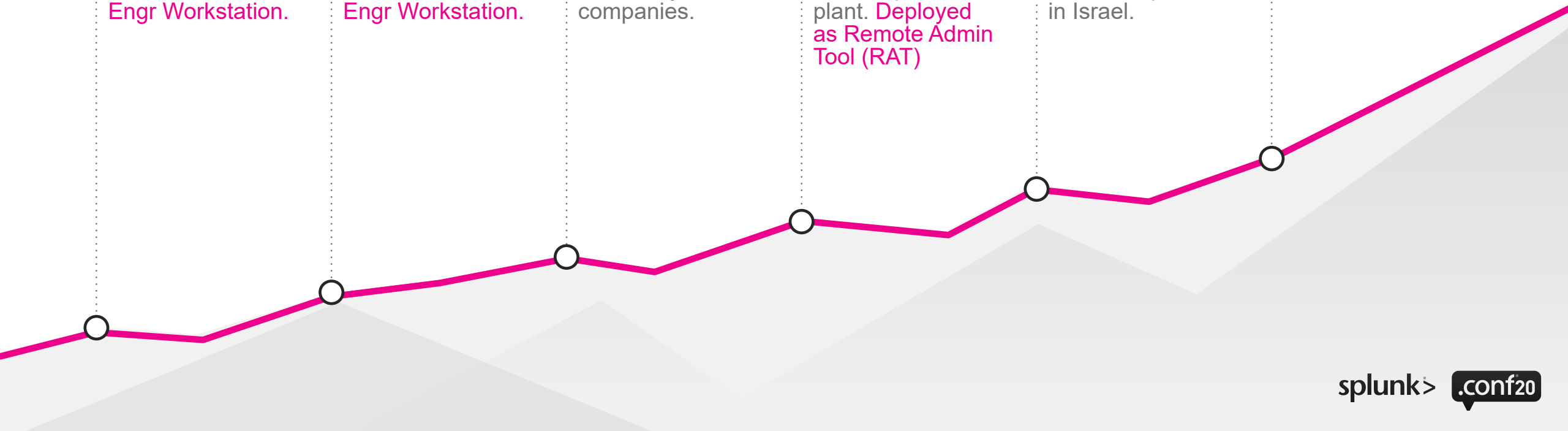
India announced that North Korean malware had been identified in the networks of a nuclear power plant. Deployed as Remote Admin Tool (RAT)

Apr 2020

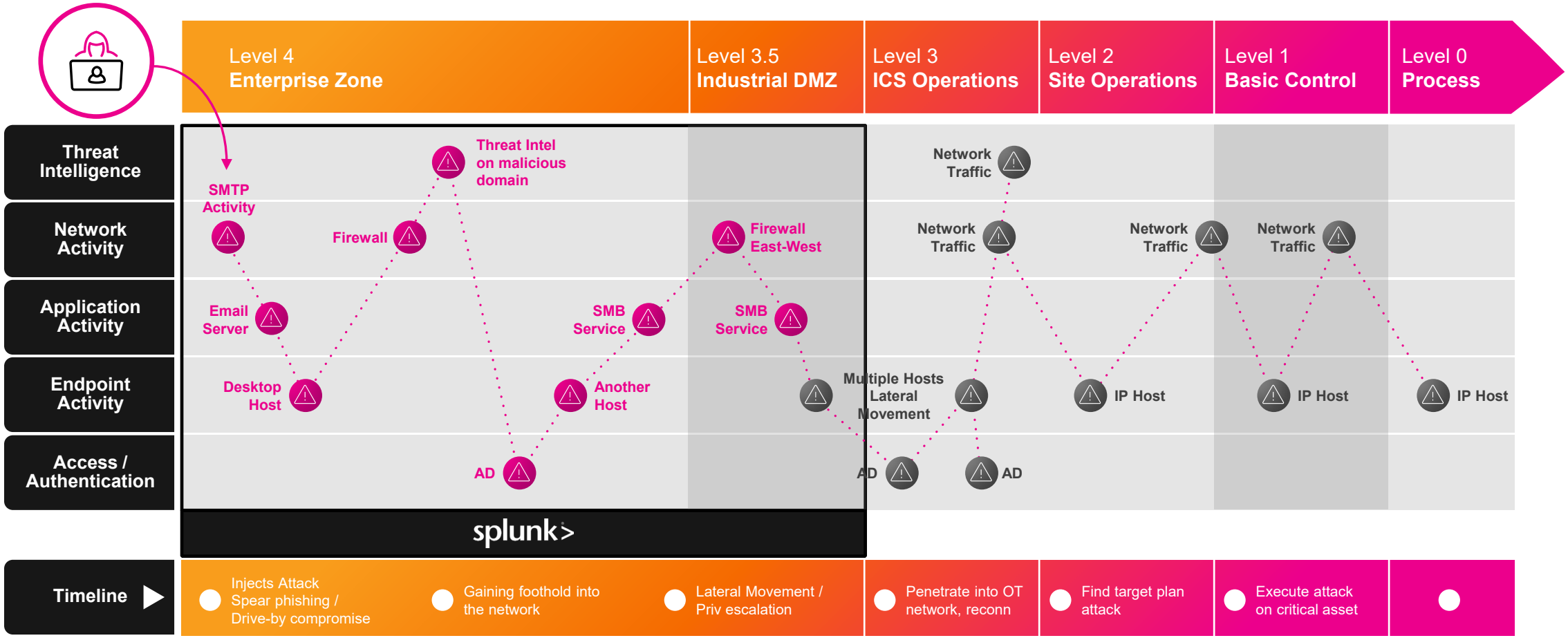
Suspected Iranian hackers unsuccessfully targeted control systems of water treatment plants in Israel.

May 2020

Russian hacking group compromised the networks of energy companies in Germany by exploiting IT supply chains.

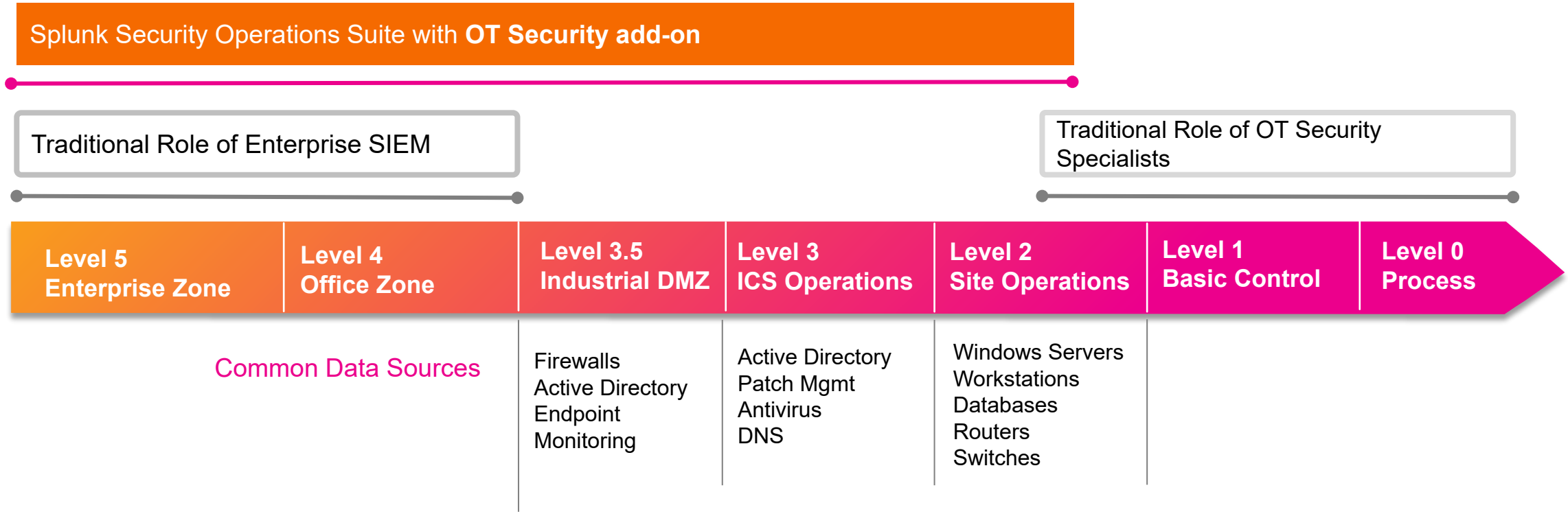


Visibility Across Zones Is Essential



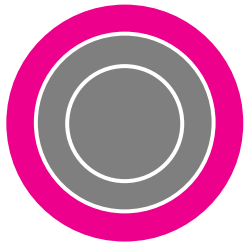
splunk> .conf20

Bridging the Gap Between Corporate SIEM and OT-network Monitoring Tools



Coverage Options: Basic, Better, Best

OT Security focus needs to start with monitoring corporate tech



Level 1

Splunk Corporate + OT Network Perimeter

- Splunk for perimeter firewall monitoring of all OT locations

Level 2

Splunk Corporate + OT Network Perimeter + Levels 2/3

- Splunk for perimeter firewall monitoring of all OT locations
- Splunk deployed in Levels 2 & 3 of every OT environment

Level 3

Splunk Corporate + OT Network Perimeter + Levels 2/3 + OT Solution(s)

- Splunk for perimeter firewall monitoring of all OT locations
- Splunk deployed in Levels 2 & 3 of every OT environment
- Asset discovery + inventory
- OT threat detection
- Combined IT/OT SOC with centers of excellence

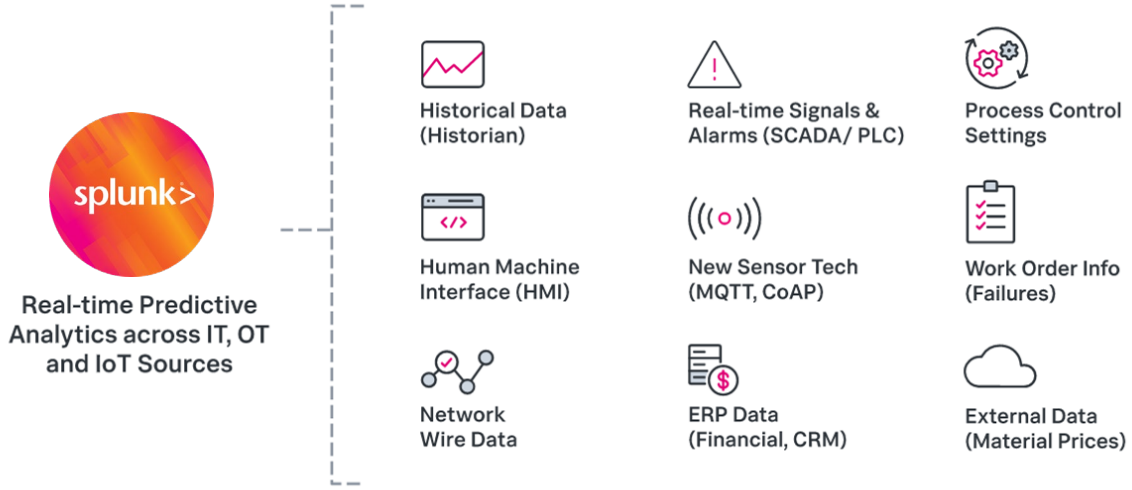
Splunk Add-on for OT Security

splunk> .conf20

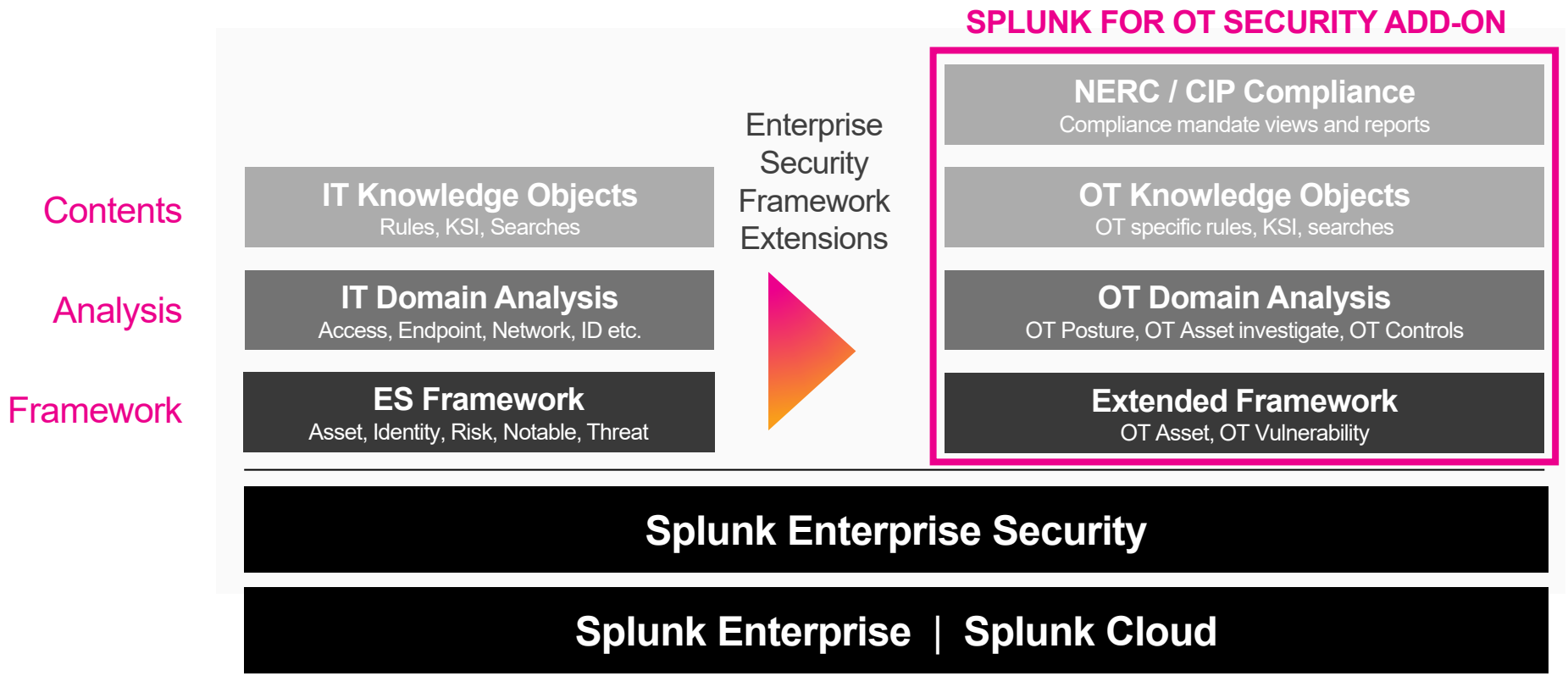
Splunk for OT Security Domain Add-On

Three focus areas

- Expanded ability to ingest, monitor OT Assets
- Improved OT Vulnerability Management including support for Mitre ICS ATT&CK
- Interfaces and reports to support NERC CIP audit and compliance



OT Security Solution - Included Components



OT Data Source Integrations

A wide variety of sources integrate to Splunk's common information model

splunk>

- Logs (OS, App, etc.)
- CVEs
- Network Traffic
- Asset Inventory
- Notables
- Patch Management
- Endpoint activity

MITRE ATT&CK™ framework for ICS

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command/Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Eng. Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating System	Serial Connection Enumeration		Monitor Progress State		Denial of Service	Program Download	Loss of Safety
Spear-phishing Attachment	Scripting					Point and Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Setting	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Informtion
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

splunk> .conf20

NERC CIP reporting

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009	CIP-010	CIP-011	CIP-012	CIP-013
BES Cyber System Identification and Categorization	**Security Management Controls**	**Training and Personnel Security**	**Electronic Security Perimeter**	**Physical Security of BES Cyber Systems**	**Systems Security Management**	**Incident Reporting and Response Planning**	**Recovery Plans for BES Cyber Systems**	**Configuration Change Management and Vulnerability Assessments**	**Information Protection**	**Control Center Communication Network**	**Supply Chain Risk Management**
BES Cyber System Identification	Cyber Security policy for High/Medium Systems	Awareness	Electronic Security Perimeter	Physical Security Plan	Ports and Services	Cyber Security Incident Response Plan	Recovery Plan Specifications	Configuration Change Management	Information Protection	Physical and Logical Risk Mitigation for Data	Risk Management Plan
Regular Approval	Cyber Security Policy for Low Systems	Training	Interactive Remote Access Management	Visitor Control Program	Security Patch Management	Cyber Security Incident Response PLAN Implementation and Testing	Recovery Plan Implementation and Testing	Configuration Monitoring	BES Cyber Asset Reuse and Disposal	Proof of Implementation	Proof of Implementation
	Identification of Senior Manager	Personal Risk assessment Program		Physical Access Control System	Malicious Code Prevention	Cyber Security Incident Response Plan Review, Update, Communication	Recovery Plan Review, Update, and Communication	Vulnerability Assessments			CIP Senior Manager Approval
	Delegation of Authority	Access Management Program		Maintenance and Testing Program	Security Event Monitoring			Transient Cyber Assets and Removable Media			
		Access Revocation Program			System Access Controls						

Get Started Now

Download Splunk for OT Security

splunkbase.com

Learn more at Splunk.com

splunk.com/ot-security

splunk> .conf20

Thank You

Please provide feedback via the

SESSION SURVEY