Building Resilience with OT Security

FH JOANNEUM, Kapfenberg
Feb 25, 2025

splunk>
a CISCO company

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or 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 or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

splunk>
a cisco company

Agenda

1. Market Trends & Best Practices
2. How Splunk Adds Value
3. Customer Stories

splunk>

What's on the Industry's Mind?

Why is NIS2* so Important for OT Security?

- EU-wide legislation to boost the overall level of cybersecurity
- Start: 18 October 2024
- Strict incidence reporting mandate (24h)
- Personal liability of C-level
- Huge penalties up to €10M

Need for unified visibility across IT and OT environments

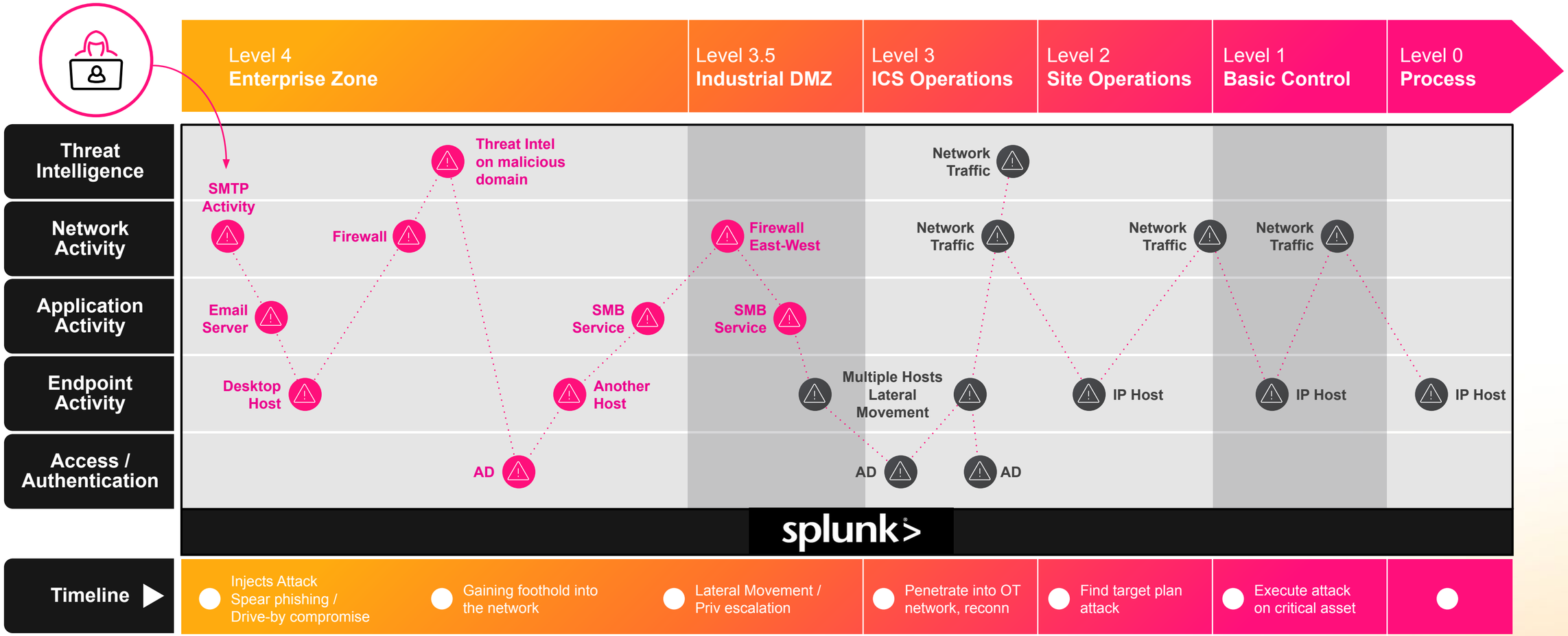
*NIS2 Directive: Network and Information Security Directive

Best Practices

IT / OT SOC: VISIBILITY ACROSS IT AND OT

splunk> turn data into doing

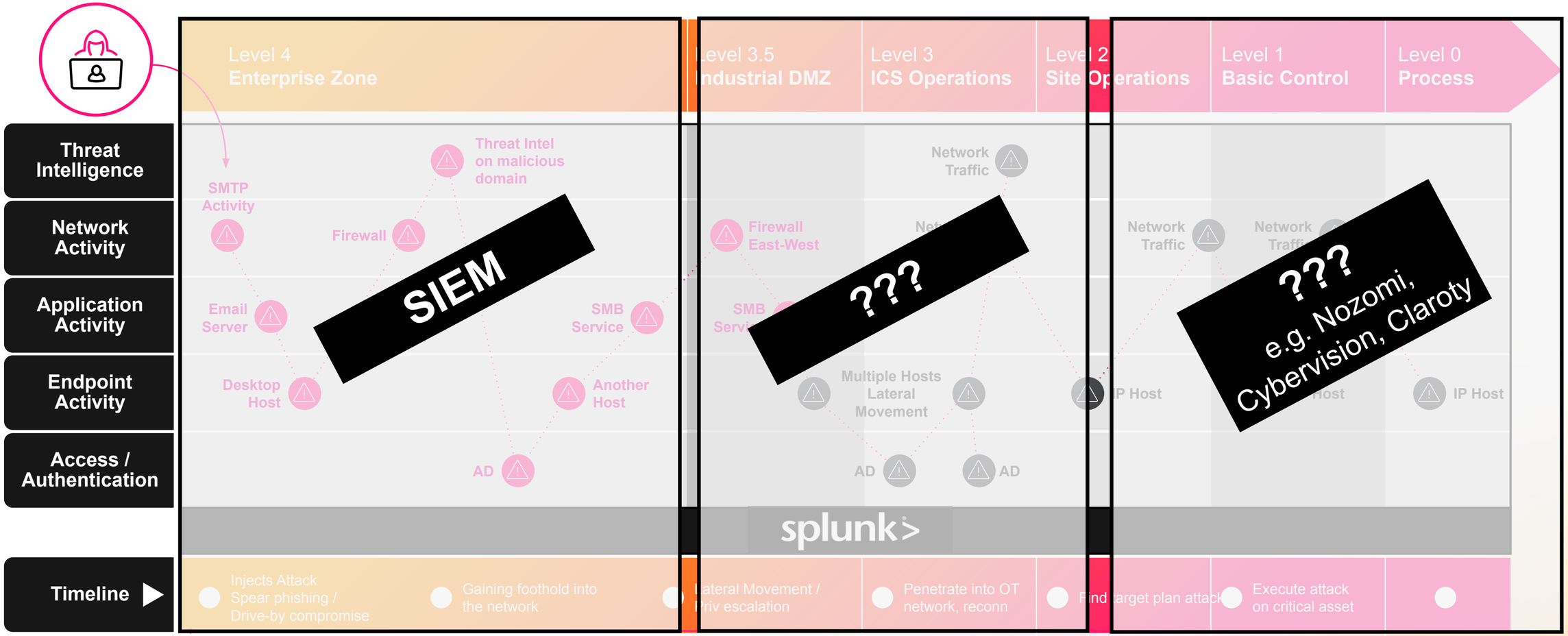
During a Cyberattack Visibility Across Zones is Essential



140 days, median days before detection

Imagine...

Where is your blind spot? 100% centralized visibility or working in silos?



Do You Know Whether You Have Been Hacked?

Worse than being hacked is not knowing you have been hacked

Where is your weakest spot in your processes and production?
You know best!

Known Knowns Things we are aware of and understand.	**Known Unknowns** Things we are aware of but don't understand.
Unknown Knowns Things we understand but are not aware of.	**Unknown Unknowns** Things we are neither aware of nor understand.

Highest risk to your environment

Best Practices

FALSE ALERTS

splunk> turn data into doing

Fighting False Alerts the Smart Way

- False alerts are a key challenge in OT environments:
  2,000 - 10,000 false alerts / day
- Noisy SOC leads to burnout and missing of key notables
- Solution: **Risk Based Alerting**

How Splunk Adds Value

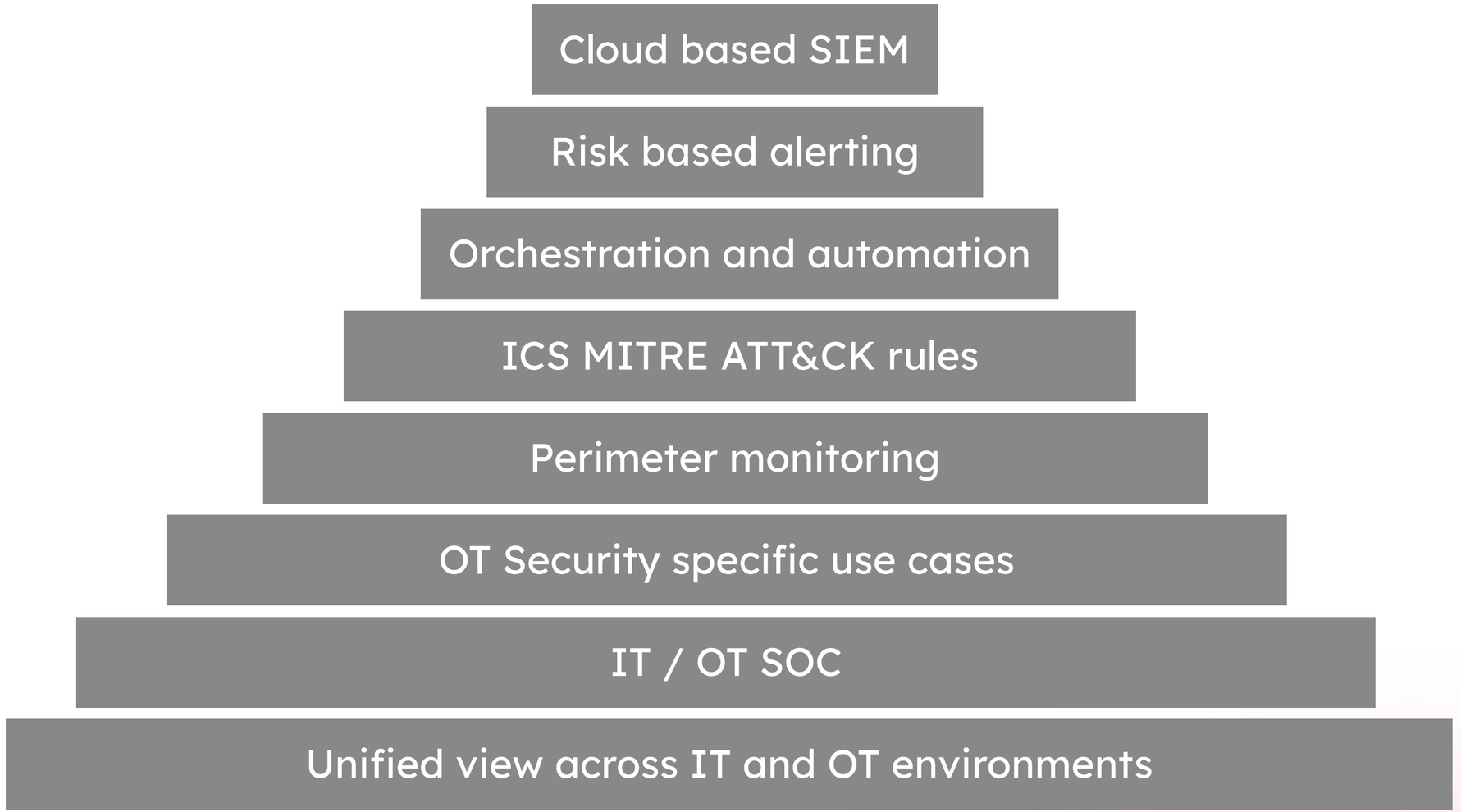
splunk> turn data into doing

Earthquake-Proof Towers

They bend, but don’t break.

Japan is home to some of the most resilient buildings in the world

Building Resilience with OT Security



… it isn't just about dealing with the issues and challenges of today.

Rather, it's also creating a culture fortified with technology and digital tools that enable (organizations) to see around corners, to be ready for the changes that are yet to come.

Source: McKinsey, The Need for Resilience

How Can Splunk Help with IT / OT Cybersecurity?

Splunk Enterprise Security (ES)

+

Splunk OT Security Add-On

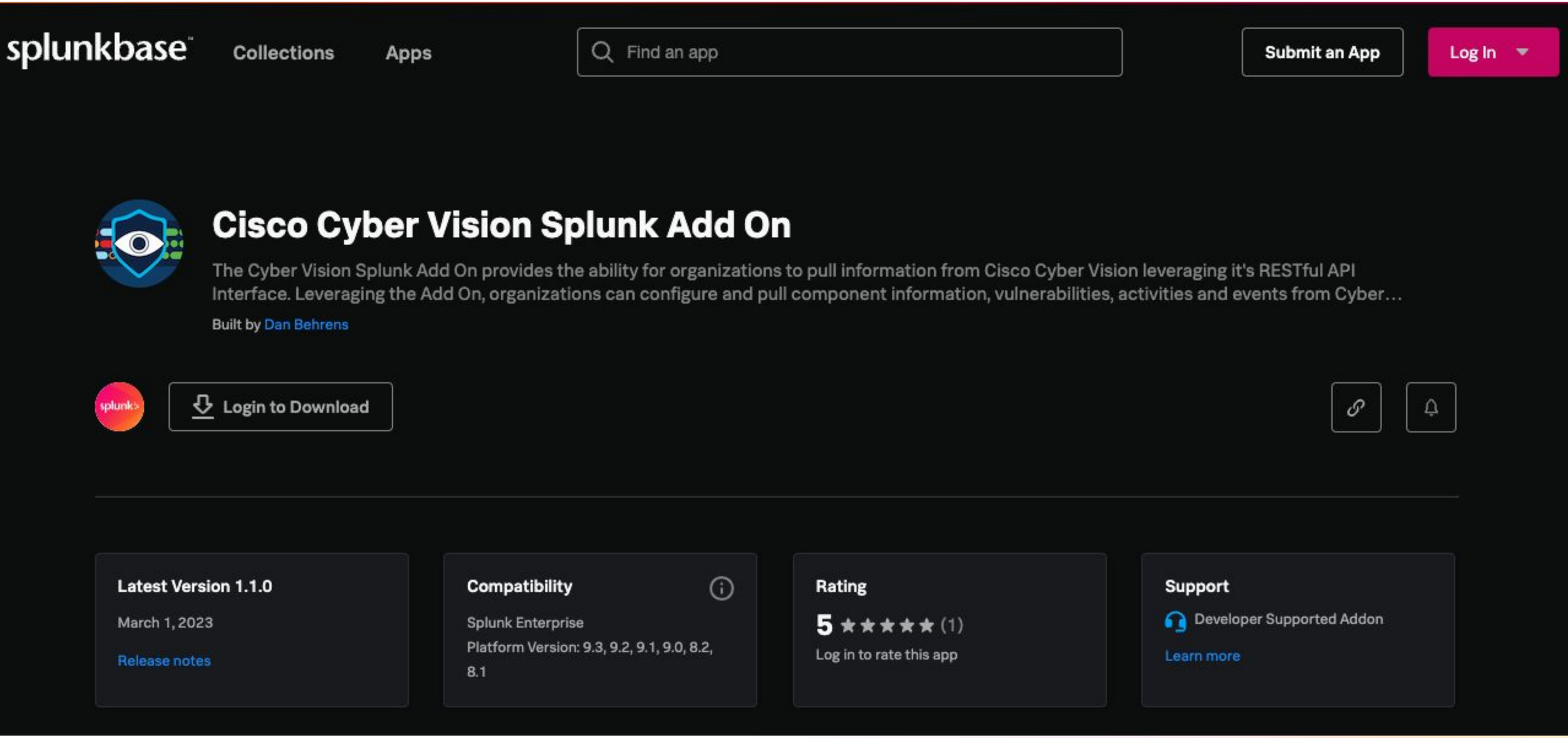
Free OT Security Add-on for ES Customers

https://splunkbase.splunk.com/app/5151/

IT + OT Security

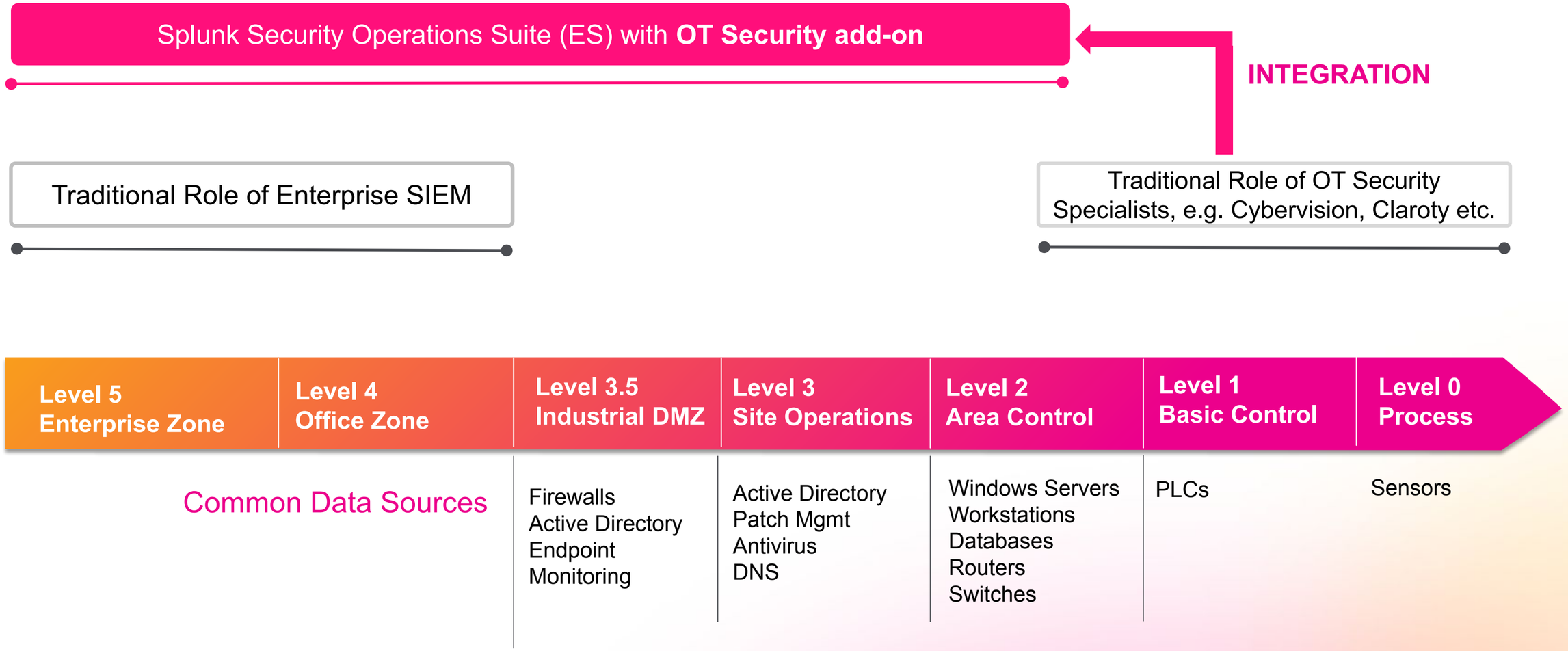
Cisco/Splunk is a Leader in OT Security

Link to Report
with detailed vendor profiles



https://splunkbase.splunk.com/app/5748

Splunk Provides Holistic Visibility Across IT & OT Environments



Customer Benefits of IT / OT Security with Splunk

Holistic Visibility across IT and OT Environments

via an central IT / OT SOC - on-premise, hybrid oder aaS (Splunk Cloud)

OT Environments Coverage

via implementation of the latest ICS MITRE ATT&CK rules
and integration of OT Security vendors, e.g. Nozomi as data sources

Security Automation & Orchestration Technologies

Risk-based Alerting
Orchestration - Automation - Response (SOAR)
Attack Analyzer

Customer References

splunk> turn data into doing

Customer Case

Johnson Matthey (JM)

Fighting Phishing and Closing Investigations 83% Faster

Key Challenges

JM's security team faced an overwhelming number of alerts without a means to effectively filter through and prioritize

Solution

Adopted ES, SOAR, RBA, Attack Analyzer

Business Impact

- 61% of phishing cases closed by automation with SOAR
- Reduced case management time by 83%

“Using SOAR and Splunk Attack Analyzer has enabled us to automate part of our phishing process. Our analysts deal with fewer cases because we now automatically close the ones that aren’t a real threat.

Using risk-based alerting, we’re able to fine tune precisely what we want out of the system, so all the data keeps coming for analysis, but without bombarding our SOC with irrelevant alerts.”

Nathan Lowey, Cybersecurity Engineer
Johnson Matthey

Saudi Aramco
In a COVID-19 World - Lessons Learned with OT CyberSecurity

Israeli Ministry of Energy
How Israel's Ministry of Energy applies Machine Learning to protect their Critical Infrastructure and OT Operations

EY
Splunk in P&U: Empowering OT and the Grid

Transport for New South Wales, Australia
NSOC for Your OT & IT Government Services

Blog: [OT Security is the New Avenger]

Image generated by Deep Dream Generator, edited

Thank you

splunk> a cisco company