

Building Resilience with IT/OT Security

2025



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, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2024 Splunk Inc. All rights reserved.

Agenda

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



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

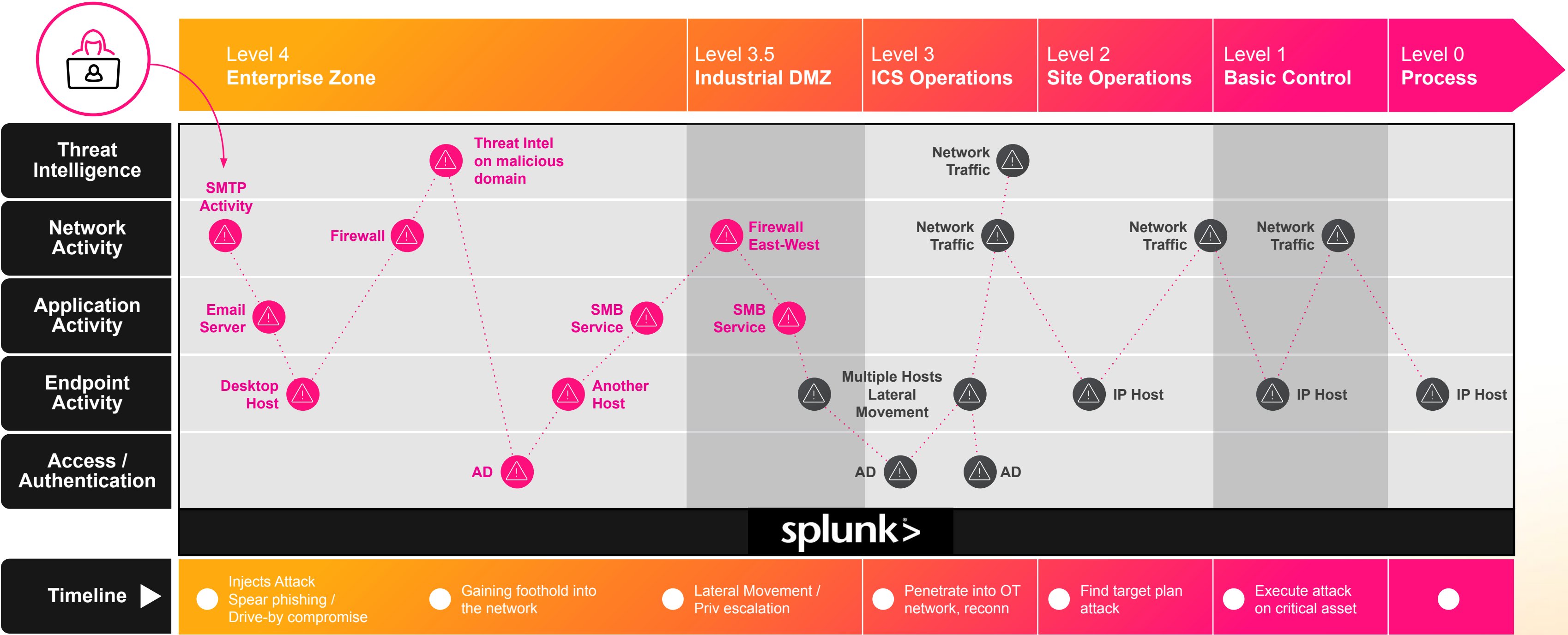
Best Practices

IT / OT SOC: VISIBILITY ACROSS IT AND OT

splunk> turn data into doing™



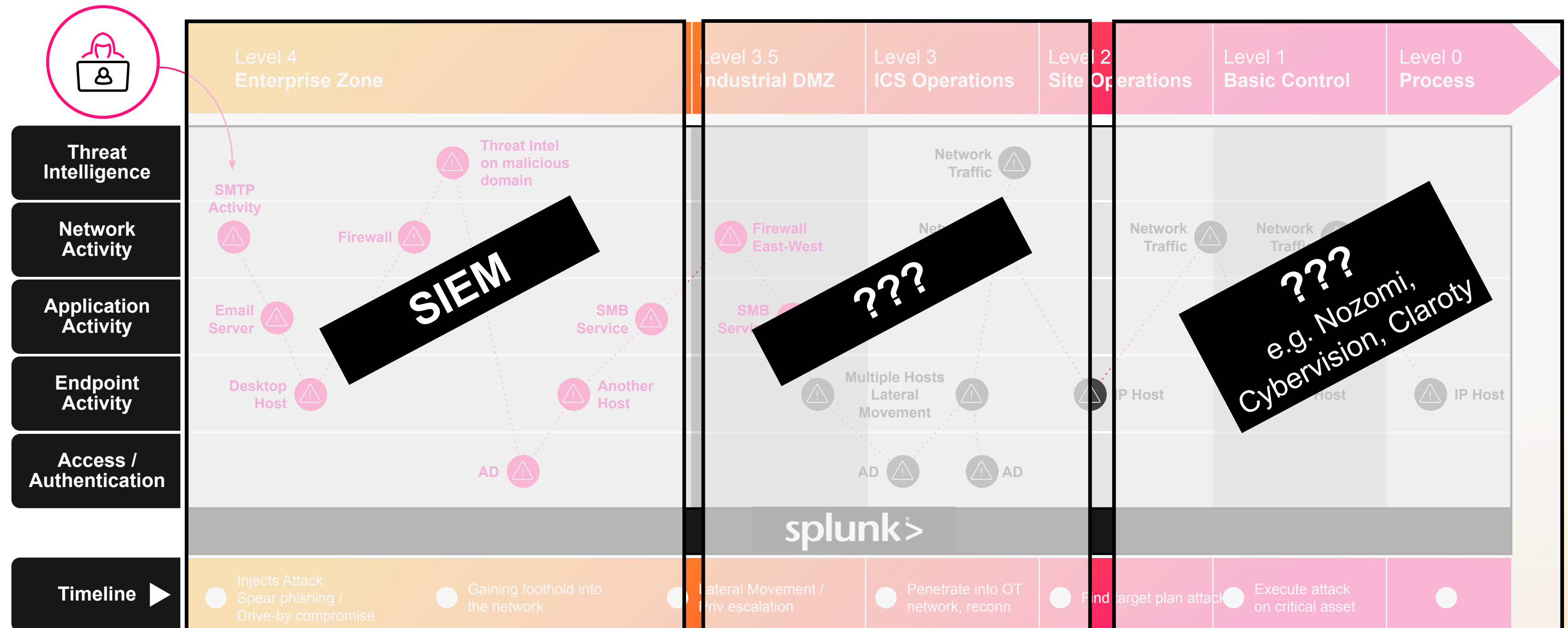
During a Cyberattack Visibility Across Zones is Essential



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 <i>Things we are aware of and understand.</i>	Known Unknowns <i>Things we are aware of but don't understand.</i>
Unknown Knowns <i>Things we understand but are not aware of.</i>	Unknown Unknowns <i>Things we are neither aware of nor understand.</i>



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™

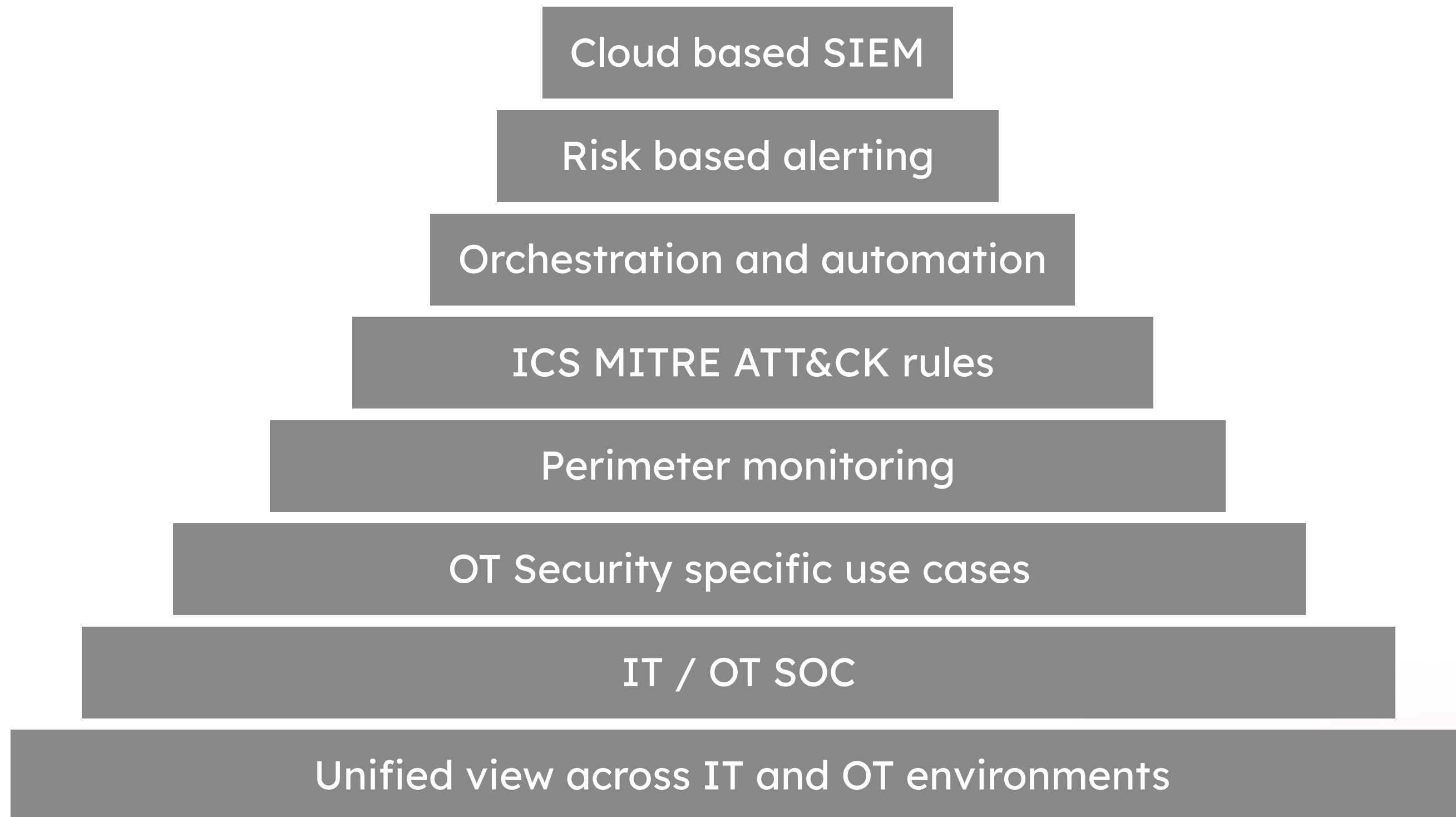


Earthquake-Proof Towers

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

THE FORRESTER WAVE™

Operational Technology Security Solutions

Q2 2024



Cisco/Splunk is a Leader in OT Security

[Link to Report](#)

with detailed vendor profiles



Cisco Cyber Vision Splunk Add On

The Cyber Vision Splunk Add On provides the ability for organizations to pull information from Cisco Cyber Vision leveraging it's RESTful API Interface. Leveraging the Add On, organizations can configure and pull component information, vulnerabilities, activities and events from Cyber...

Built by [Dan Behrens](#)



 Login to Download



Latest Version 1.1.0

March 1, 2023

[Release notes](#)

Compatibility




Splunk Enterprise
Platform Version: 9.3, 9.2, 9.1, 9.0, 8.2, 8.1

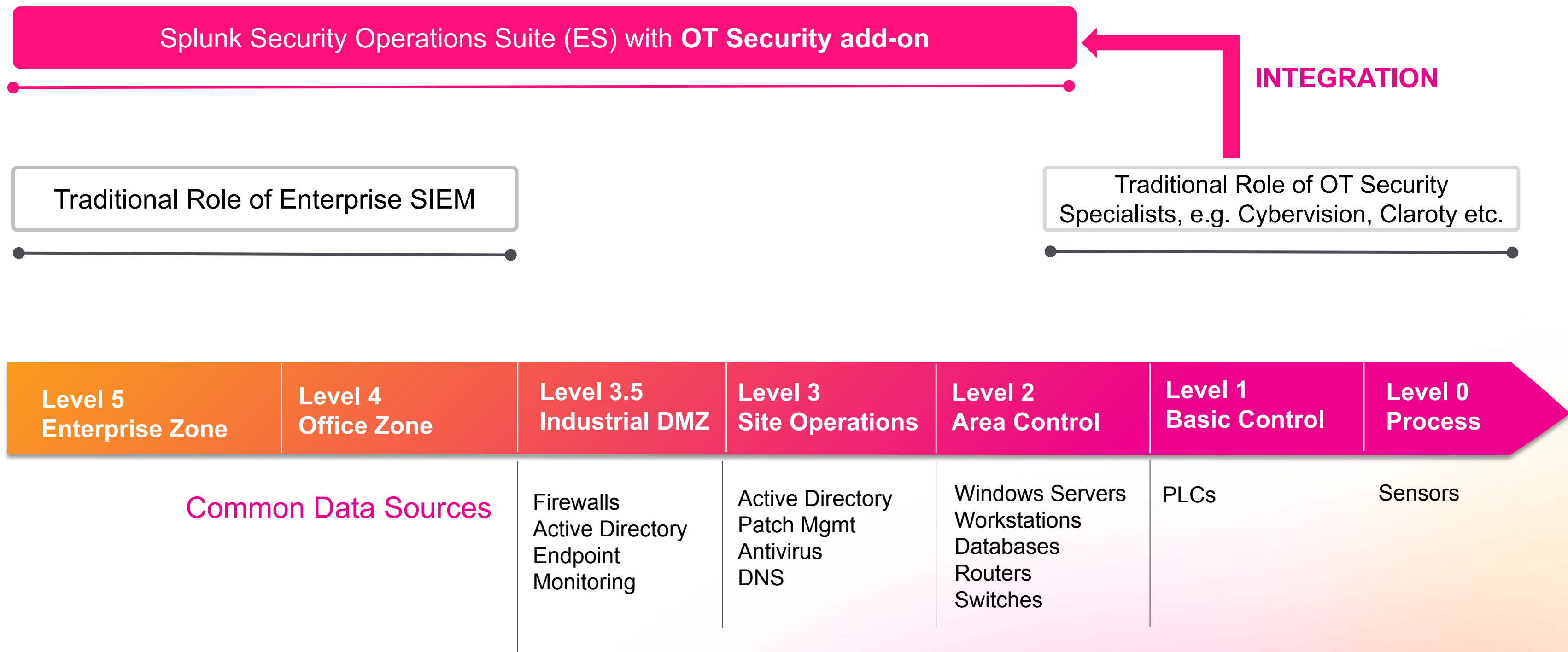
Rating

5 ★★★★★ (1)
Log in to rate this app

Support

 Developer Supported Addon
[Learn more](#)

Splunk Provides Holistic Visibility Across IT & OT Environments



OT Security Data Sources

Data Type	Data Source
Network Data Authorization data and alerts generated from network traffic for diagnosing system or security issues	Network Traffic Netflow/sflow Zeek Suricata Stream
Event Data Alerts to system issues, such as routers/switches reaching capacity (memory, disk space, CPU), Windows Events, Linux Security Events	SNMP traps Windows Event store Linux security logs
OS Data Installed software/version, patching logs, and OS changes	Services installed and state Applications Installed Process Tracking Registry monitoring OS Configuration File Shares
ICS Application logs Indications of the health of an application (e.g. application and services failures)	Logs created by ICS (access, system logs, etc) Database system and user usage ICS System Configuration files
Referential Data Clue to system health (e.g. data being replicated and security issues (e.g. access logs)	Files created by the system Database, Log, Text, Spreadsheet, etc Scripted output for state of ICS
OT/ICS System Data Generated by OT Equipment (e.g. PLC), OT Security Solutions, or ICS Solutions	OT Solution Products (Dragos, Nozomi, Claroty, etc) Alerts OT Solution Asset Data CMDB Spreadsheets Maintenance Inventory Systems

Data Type	Data Source
OT/ICS Alerts/Alarms Alerts Generated by OT Security Solutions or other ICS Monitoring solutions	OT Solution Alerts ICS System Alerts ICS Alarms/Events
Communications logs Problems with communications between control systems and PLCs / RTUs, such as timeouts, number of retries and failed attempts	Industrial protocols servers (OPC server, Kepware) Databases (MS SQL, Oracle) communication statistics Communication logs
Endpoint protection logs Generated by antivirus and whitelisting programs	Antivirus Whitelisting Patching Info & Logs
USB usage logs	Windows registry (USB) Endpoint Products with USB Monitoring
Firewall, IDS/IPS Communications external to the OT network and intrusion attempts into the network	Firewall Traffic Firewall system logs Firewall configurations Firewall rules IPS/IDS alerts
Remote access logs Records of VPN access, remote desktop and VNC server access	Windows AD Audit Information Windows AD Events Remote access application (e.g. VNC, TeamViewer, NextNine, etc) VPN Logs Custom File Transfer Logs (e.g. FTP, SFTP)
Remote server management logs Used for rack monitoring to track who is accessing which server	Datacenter logs (iLo, iDRAC, etc) Virtual Infrastructure Access (e.g. vcenter)

 **Essential** Data Source

 **Recommended** Data Source

 **Additional** Data Source

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



security

Customer References

threats manufacturers
ow.

splunk> turn data into doing™

Customer Case

Johnson Matthey (JM)

Fighting Phishing and Closing Investigations 83% Faster

Key Challenges

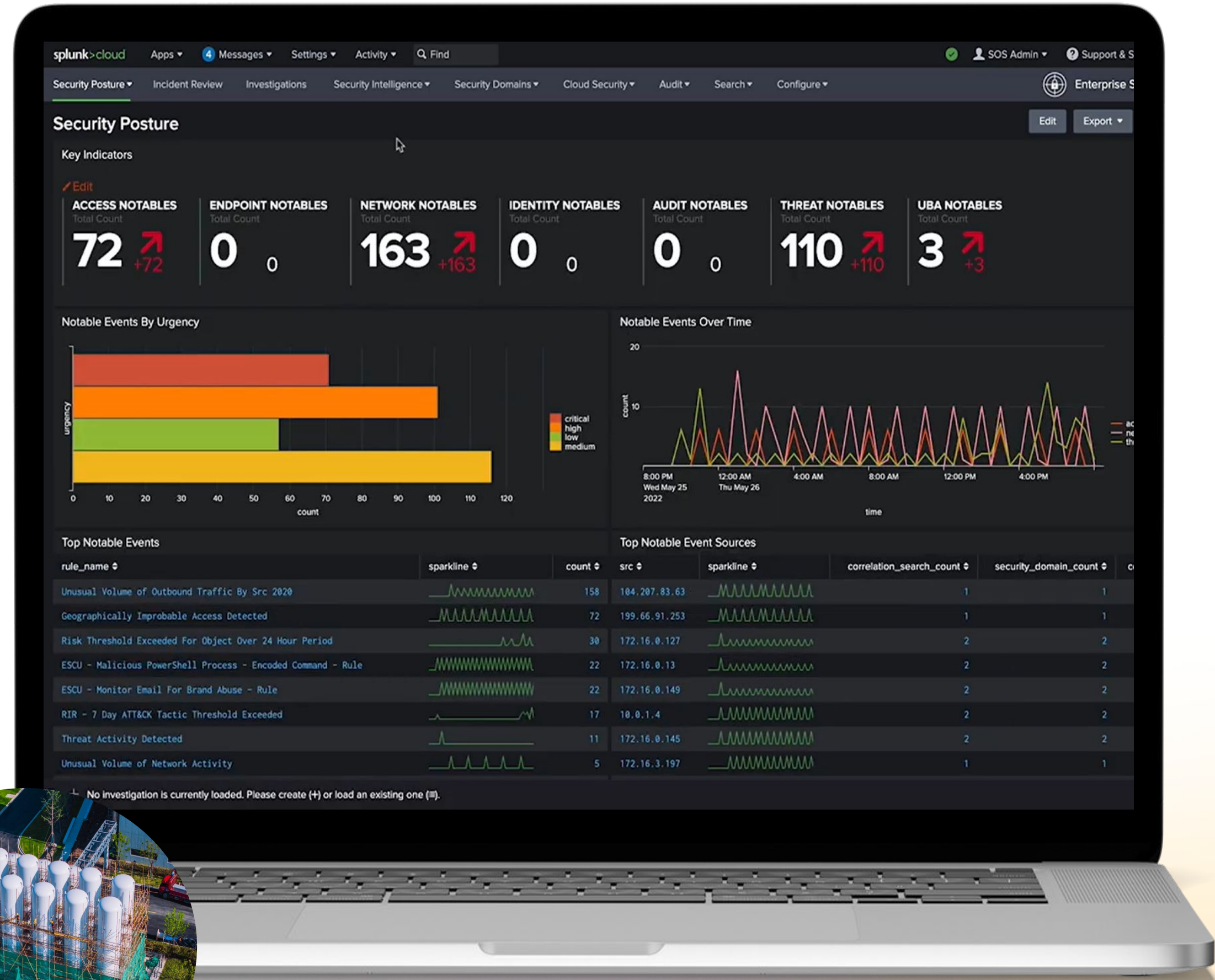
JM's security team faced an overwhelming number of alerts without a means to effectively filter through and prioritize

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

Splunk Lantern Customer Success Center

Let Splunk experts light your path toward gaining valuable data insights, achieving your key use cases, and managing Splunk more efficiently.

[Click here to learn more.](#)



Solution Accelerator for Operational Technology (OT) Security

The Solution Accelerator for **OT Security** helps you get started with common use cases for **OT** environments and ensure your **security** controls are working.

Last update: 11/12/2024

[Link](#)

[Link Dashboard](#)

Thank you