

CSAF COMMUNITY DAYS 2024

WELCOME & OPENING REMARKS

Justin Murphy
DHS/CISA



TLP:CLEAR

Justin Murphy
May 8, 2025

Justin Murphy

- Vulnerability Analyst @CISA
- Passion for:
 - Service
 - International Cooperation
 - CVD
 - OASIS Open: CSAF/OpenEoX/OSIM
 - SBOM/VEX



TLP:CLEAR

Justin Murphy
May 8, 2025

BLOG

Transforming the Vulnerability Management Landscape

Released: November 10, 2022**Revised:** November 14, 2022

Eric Goldstein, Executive Assistant Director for Cybersecurity

In the current risk environment, organizations of all sizes are challenged to manage the number and complexity of new vulnerabilities. Organizations with mature vulnerability management programs seek more efficient ways to triage and prioritize efforts. Smaller organizations struggle with understanding where to start and how to allocate limited resources. Fortunately, there is a path toward more efficient, automated, prioritized vulnerability management. Working with our partners across government and the private sector, we are excited to outline three critical steps to advance the vulnerability management ecosystem:

- First, we must introduce greater automation into vulnerability management, including by expanding use of the Common Security Advisory Framework (CSAF)
- Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)

TLP: CLEAR

BLOG

Transforming the Vulnerability Management Landscape

Released: November 10, 2022

Revised: November 14, 2022

Eric Goldstein, Executive Assistant Director for Cybersecurity



In the current risk environment, organizations of all sizes are challenged to manage the number and complexity of new vulnerabilities. Organizations with mature vulnerability management programs seek more efficient ways to triage and prioritize efforts. Smaller organizations struggle with understanding where to start and how to allocate limited resources. Fortunately, there is a path toward more efficient, automated, prioritized vulnerability management. Working with our partners across government and the private sector, we are excited to outline three critical steps to advance the vulnerability management ecosystem:

- First, we must introduce greater automation into vulnerability management, including by expanding use of the Common Security Advisory Framework (CSAF)
- Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)

Search



Search

BLOG

Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories

Released: September 29, 2023

By Lindsey Cerkovnik, Chief of Vulnerability Response and Coordination, and Daniel Larson, Justin Murphy, and Brandon Tarr

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [CYBER THREATS AND ADVISORIES](#)



In our pursuit to "[transform the vulnerability management landscape](#)," CISA is excited to announce that our security advisories for **Industrial Control Systems (ICS)**, **Operational Technology (OT)**, and Medical Devices now include the OASIS Common Security Advisory Framework (CSAF) Version 2.0 standard.

In the current risk environment, organizations are challenged to manage the growing number and complexity of new vulnerabilities. A critical step in helping organizations achieve better efficiency in triaging and prioritizing vulnerability management efforts is introducing greater automation into the ecosystem. CSAF supports automation of the production, distribution, and consumption of security advisories — reducing the time between when vulnerabilities are disclosed and when businesses remediate them and enabling future tooling for automated vulnerability information sharing.

The CSAF standard is "[the definitive reference for the language which supports creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties.](#)"¹

CISA now provides machine-readable CSAF documents alongside every new ICS Advisory and those dating back to 2017. Our ICS CSAF advisories will be located within the

TLP: CLEAR



BLOG

Transforming the Landscape



Released: November 10, 2022

Revised: November 14, 2022










Eric Goldstein, Executive Assistant Director






In the current risk environment, organizations face the complexity of new vulnerabilities. Organizations are seeking more efficient ways to triage and prioritize efforts, determine where to start and how to allocate limited resources, and implement automated, prioritized vulnerability management. In the private sector, we are excited to outline three key elements of our ecosystem:




- First, we must introduce greater automation and efficiency, including by expanding use of the Common Security Advisory Framework (CSAF)
- Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)



  cisagov / CSAF

Search Type / to search


 Code  Issues  Pull requests  Actions  Projects  Wiki  Security  Insights  Settings


 CSAF Public  Edit Pins  Unwatch 10  Fork 13  Starred 55


 develop  2 Branches  0 Tags


Go to file  Add file  Code

About

 mstrad Merge pull request #145 from cisagov/Harwood 3d82f2a · yesterday 354 Commits

 csaf_files Advisories for 2024-12-10. yesterday





 README.md Correct misspelling of repository 5 months ago




README  Security

CISA CSAF Repository

The purpose of this repository is to provide machine-readable security advisories using the [OASIS Common Security Advisory Framework \(CSAF\) Version 2.0 standard](#) for CISA's Information Technology (IT) and Operational Technology (OT) advisories. By providing machine-readable advisories using CSAF v2.0, vendors and providers of software and hardware can join [CISA and many other leading organizations](#) in taking [proactive steps to enable automation and](#)

CISA CSAF Security Advisories





 Readme  Security policy  Activity  Custom properties

 55 stars  10 watching  13 forks

Report repository

Releases

No releases published [Create a new release](#)

SHARE:    

TLP: CLEAR

The CSAF standard is *the definitive reference for the language which supports creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties.*"

CISA now provides machine-readable CSAF documents alongside every new ICS Advisory and those dating back to 2017. Our ICS CSAF advisories will be located within the

NATIONAL CYBERSECURITY STRATEGY



MARCH 2023

Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)

TLP: CLEAR

products, vulnerabilities and the status of impact and remediation among interested parties.”³

CISA now provides machine-readable CSAF documents alongside every new ICS Advisory and those dating back to 2017. Our ICS CSAF advisories will be located within the

ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY



CISA

STRATEGIC PLAN 2023–2025



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search



products, vulnerabilities and the status of impact and remediation among interested parties.”¹³

TLP: CLEAR

CISA now provides machine-readable CSAF documents alongside every new ICS Advisory and those dating back to 2017. Our ICS CSAF advisories will be located within the



OSIM



CSAF



TLP:CLEAR

Justin Murphy
May 8, 2025

Common Security Advisory Framework (CSAF)

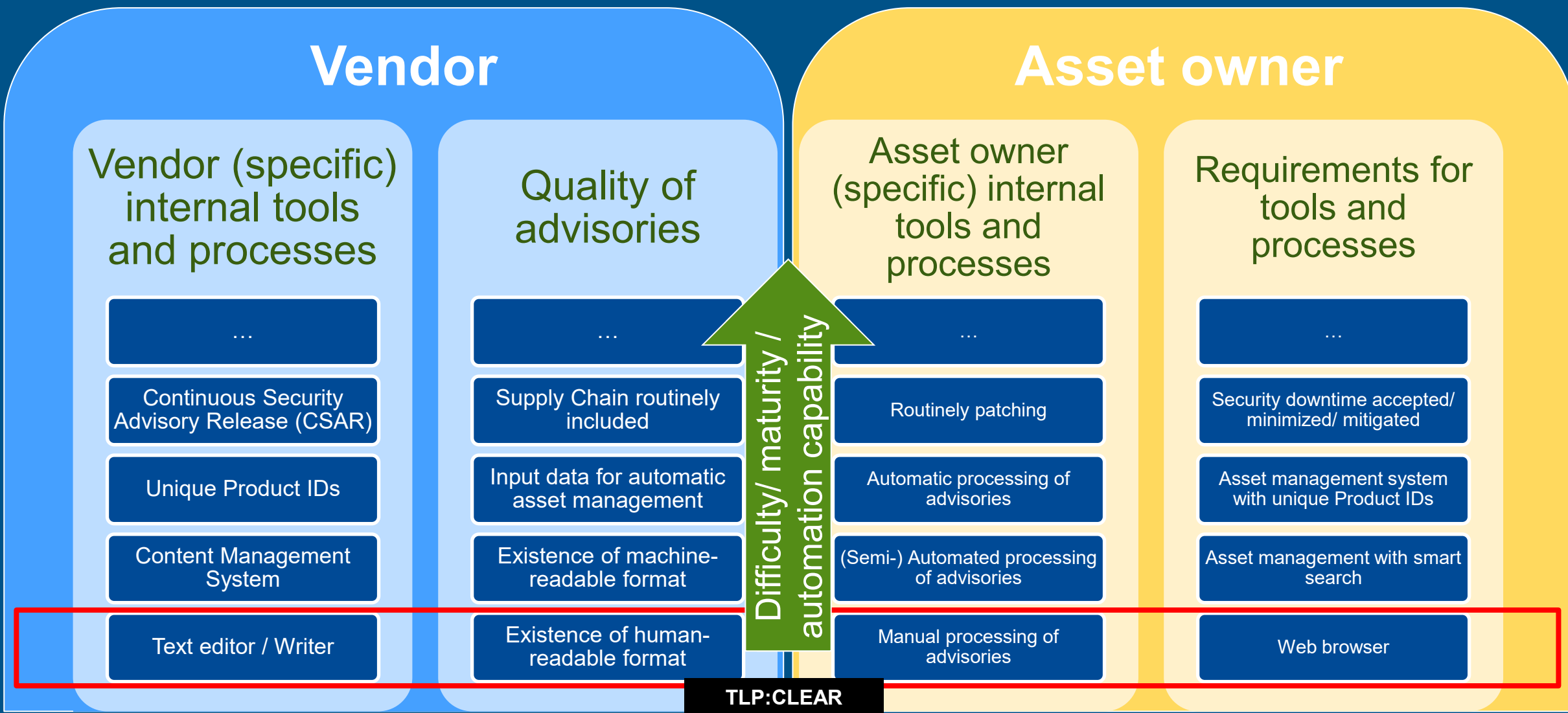
- International, open and free OASIS standard
- Machine-readable format for security advisories (JSON) and VEX
- Standardized way for distribution of security advisories
- Build with automation in mind
- Standardized tool set
- Guidance to actionable information
- Allows for linking to SBOM data
- Successor of CVRF 1.2



TLP:CLEAR


Justin Murphy
May 8, 2025

Manual Processes



Variety of Formats & Structures

An official website of the United States government [Here's how you know](#)

 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

Search

Services Report

Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Advisories > Emerson Rosemount X-STREAM

ICS Advisory (ICSA-21-138-01)

More ICS-CERT Advisories

Emerson Rosemount X-STREAM

Original release date: May 18, 2021

[Print](#) [Tweet](#) [Send](#) [Share](#)

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" without warranty of any kind, either expressed or implied, including but not limited to the accuracy, completeness, or timeliness of the information. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial products or services. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see [https://www.dhs.gov/tlp](#).

1. EXECUTIVE SUMMARY


- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Emerson
- **Equipment:** Rosemount X-STREAM Gas Analyzer
- **Vulnerabilities:** Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information, modify configuration, or affect the availability of the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Life is On 

Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

11 May 2021

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure Geo SCADA Expert products (formerly known as ClearSCADA).

The [EcoStruxure Geo SCADA Expert](#) product is an open, flexible and scalable software system for telemetry and remote SCADA solutions.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

Affected Products and Versions

- ClearSCADA, all versions
- EcoStruxure Geo SCADA Expert, all versions
- EcoStruxure Geo SCADA Expert, all versions

Vulnerability Details

CVE ID: CVE-2021-22741

CVSS v3.1 Base Score 6.7

A CWE-916: Use of Passwords in URLs vulnerability exists that could cause the exposure of sensitive information. The vulnerability is present in the EcoStruxure Geo SCADA Expert product. The vulnerability is present in the EcoStruxure Geo SCADA Expert product. The vulnerability is present in the EcoStruxure Geo SCADA Expert product.

Remediation

Geo SCADA Expert 2020 April 2021 (83.7787.1) includes a fix for this vulnerability. The security of stored passwords in the servers is significantly strengthened. It is available for download here: <https://projects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads>

Installation of new server software will require system restart or changeover of redundant servers. Consult the Release Notes and Resource Center for advice on the procedure.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure.

11-May-21 Document Reference Number – SEVD-2021-130-07 Page 1 of 3

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

SSA-344983: Vulnerability in WPA2 Key Handling affecting SCALANCE W700 and SCALANCE W1700 Devices

Publication Date: 2019-12-10
Last Update: 2019-12-10
Current Version: 1.0
CVSS v3.1 Base Score: 6.5

SUMMARY
=====

The latest firmware updates for the SCALANCE W700 and W1700 wireless device families fix a vulnerability affecting WPA/WPA2 key handling. It might be possible to, by manipulating the EAPOL-Key frames, decrypt the Key Data field without the frame being authenticated.

This has impact on WPA/WPA2 architectures using TKIP encryption. The attacker must be in the wireless range of the device to perform the attack.

AFFECTED PRODUCTS AND SOLUTIONS
=====

- * SCALANCE W1700
- Affected versions: All versions < V1.1
- Remediation: Update to V1.1 or an later version
- Download: <https://support.industry.siemens.com/cs/qa/qa/09762253>
- * SCALANCE W700
- Affected versions: All versions < V6.4
- Remediation: Update to V6.4 or an later version
- Download: <https://support.industry.siemens.com/cs/qa/qa/09773308>

WORKAROUNDS AND MITIGATIONS
=====

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- * Whenever possible, use AES-CCMP instead of TKIP in the WPA/WPA2 networks. This can be configured for both SCALANCE W700 and W1700 families over the Web Based Management (web server). For more information, go for the respective Manual.

GENERAL SECURITY RECOMMENDATIONS
=====

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/ics/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.



TLP: CLEAR

Justin Murphy
May 8, 2025

12

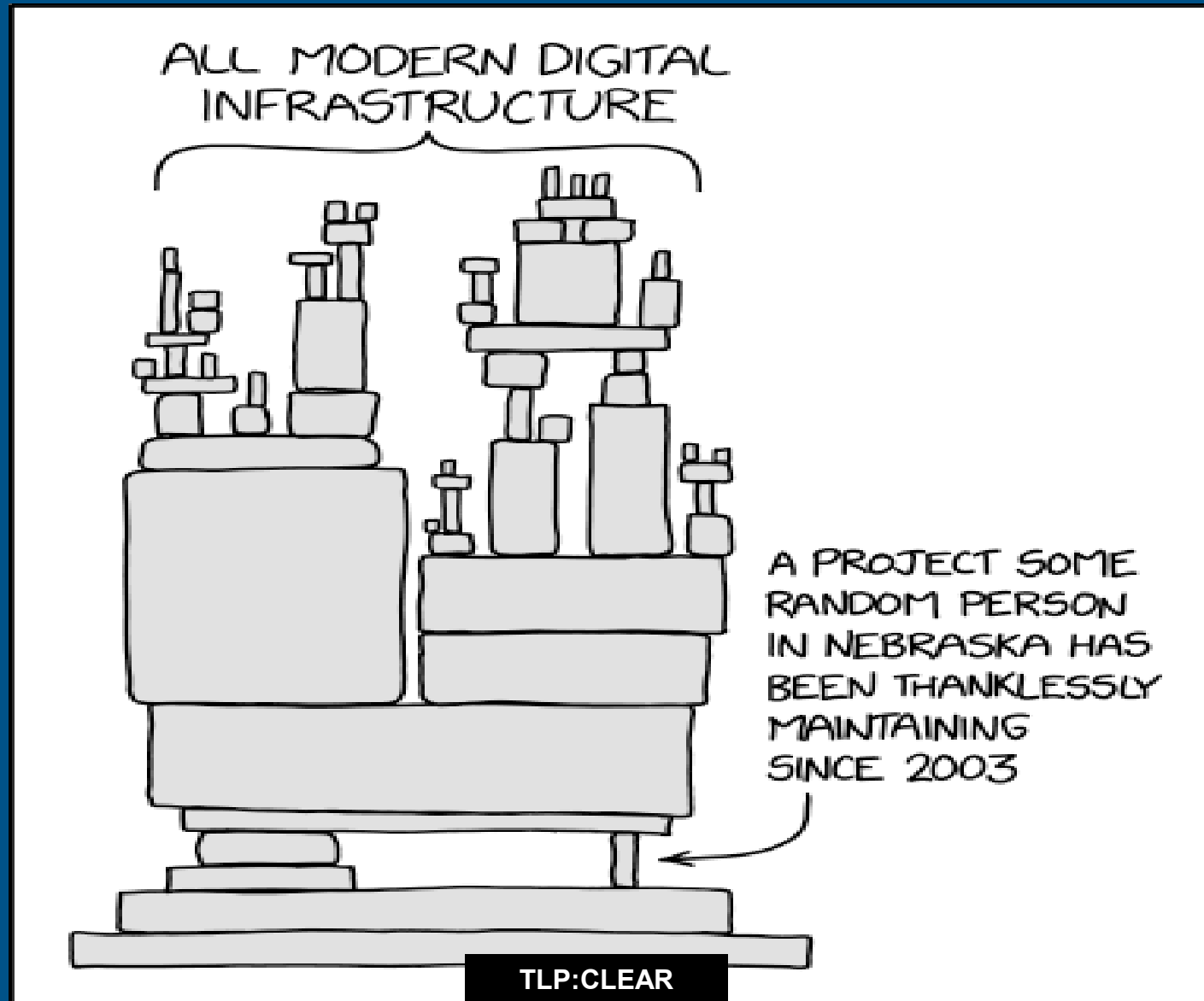
Does Not Scale



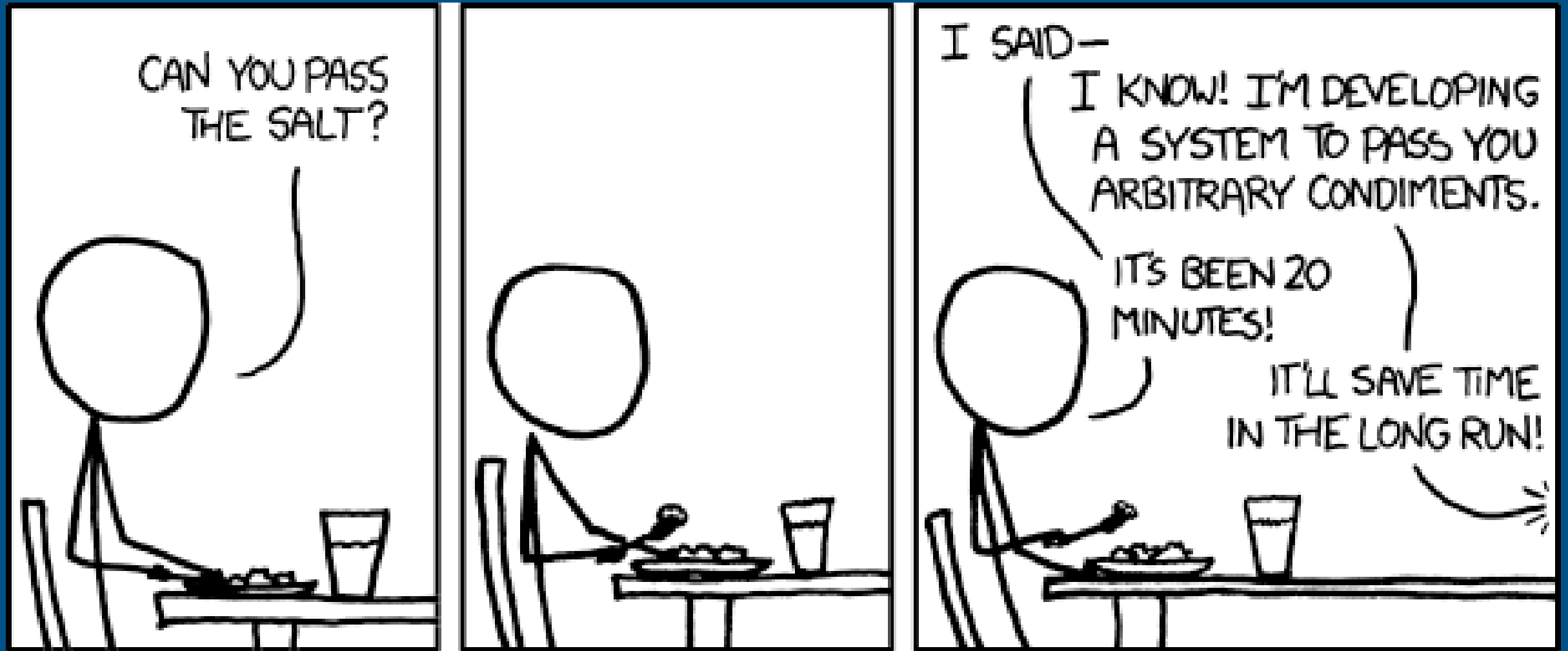
TLP:CLEAR

Justin Murphy
May 8, 2025

Challenges of Supply Chain Security



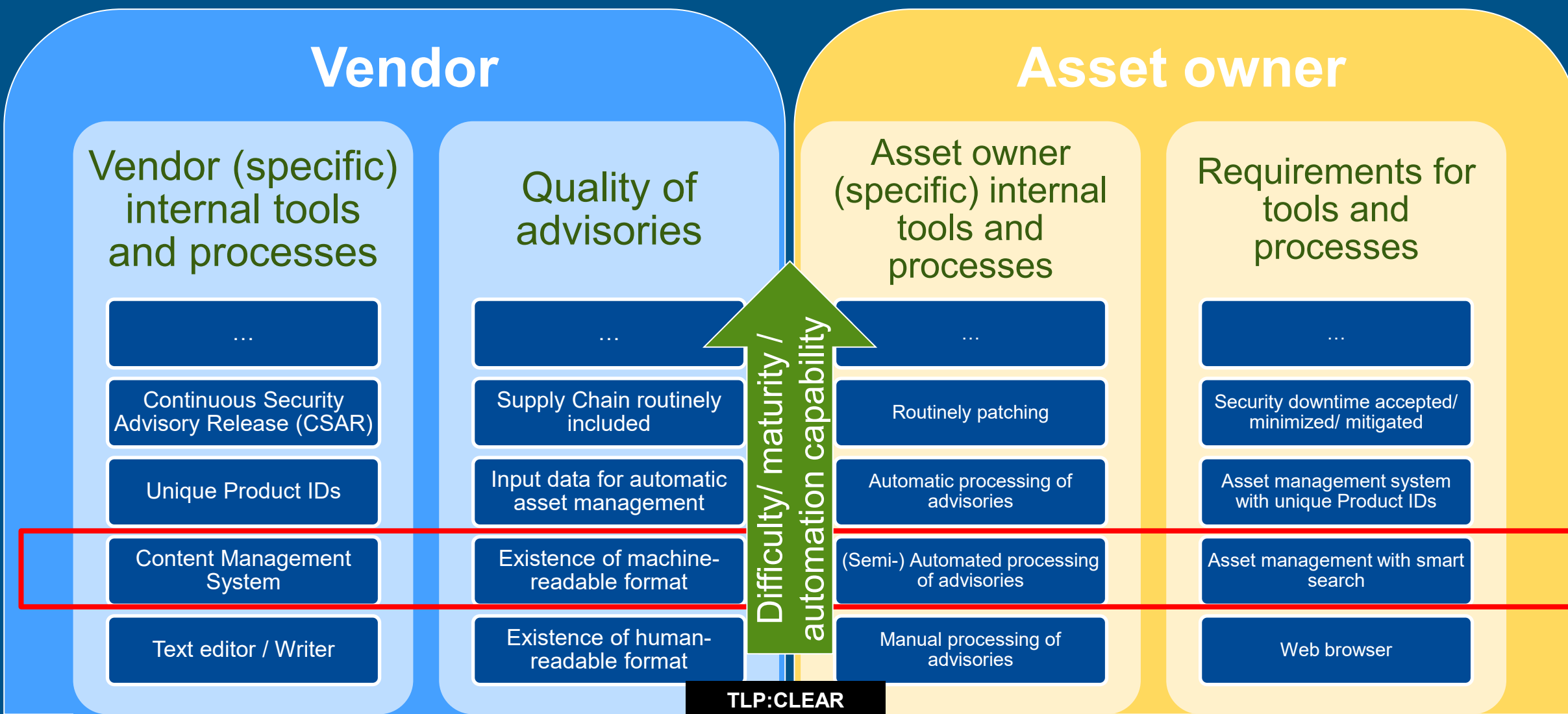
Automation



Importance of Standardization



Next Step: Reach Stage 2 Across Ecosystem



Transparency & Trust



TLP:CLEAR

Tooling and Interoperability



TLP:CLEAR

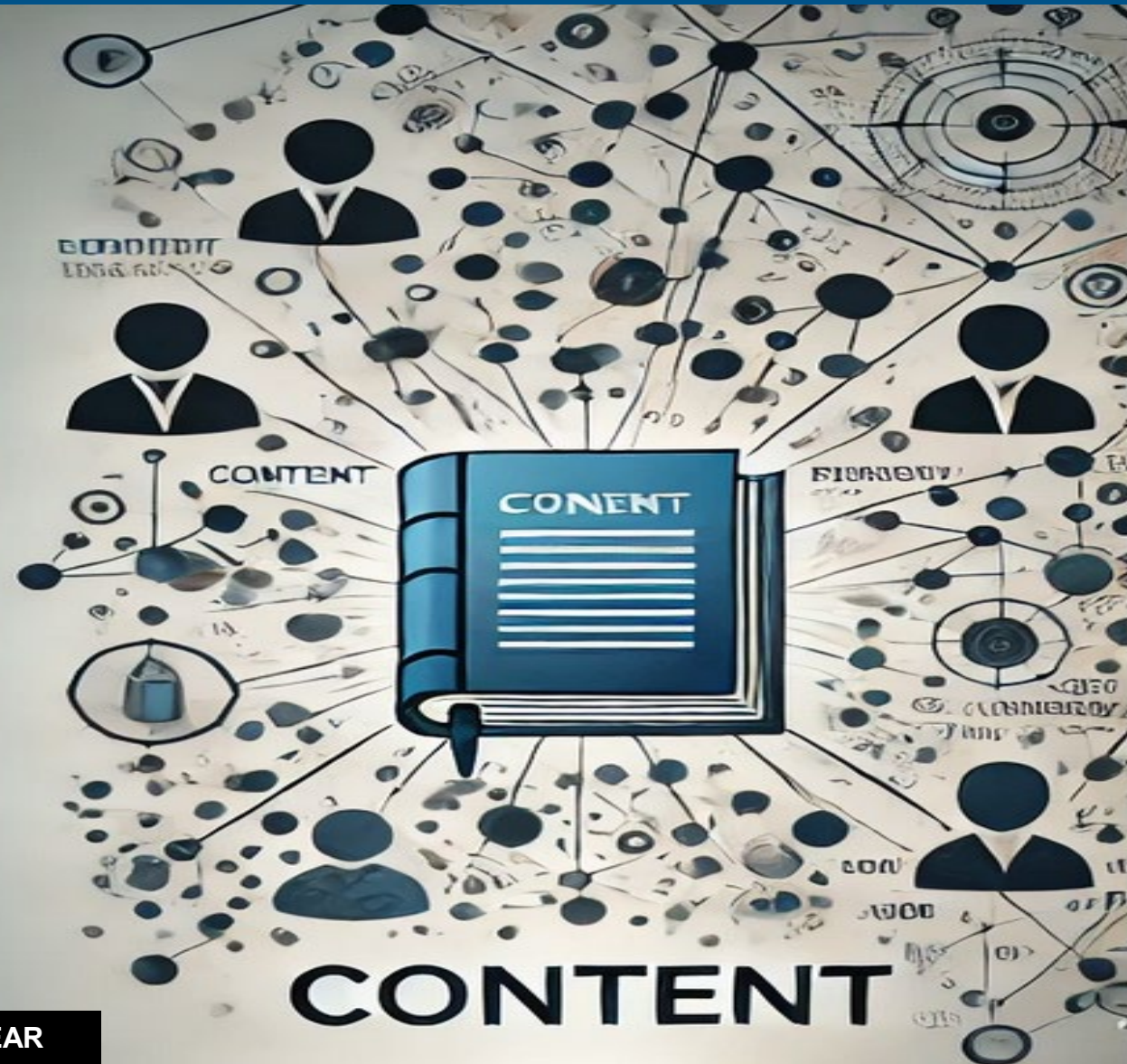
Importance of Partnership/Collaboration



Call to Action



Context vs Content



Thank You!



CSAF Community Day 1

TLP: CLEAR

CSAF Community Day 1 (December 12, 2024)

Time	Session	Speaker
13:30 - 13:45 CET	Welcome & Keynote	Justin Murphy (CISA)
13:50 - 14:20 CET	What is New in CSAF 2.1	Stefan Hagen (CSAF TC)
14:25 - 14:55 CET	Advisory, Quo Vadis?	Thomas Proell (Siemens)
15:00 - 15:30 CET	CSAF Trusted Provider - Huawei Solution, Progress and Sharing of Experience	Sonny van Lingen
15:30 - 15:45 CET	Break	
15:45 - 16:05 CET	Correlation between CSAF and CVEs	Cédric Bonhomme (CIRCL)
16:10 - 16:55 CET	CSAF Usage as Part of the EUVD and Beyond	Johannes Clos (ENISA)
16:55 - 17:05 CET	Break	
17:05 - 18:00 CET	Modernizing Vulnerability Management and Disclosure: Using CSAF in an "AI-Driven World" (Panel)	Omar Santos (CSAF TC (Chair)) and guests
18:00 - 18:05 CET	Day 1 Wrap Up	

Social Gathering: 19:00 CET at Wirtshaus Weißbräu Huber, General-von-Nagel-Straße 5, 85356 Freising, Germany (*Location changed*)

CSAF Community Day 2

TLP:CLEAR

CSAF Community Day 2 (December 13, 2024)

Time	Session	Speaker
08:00 - 08:05 CET	Welcome and Day 1 Recap	
08:05 - 08:35 CET	Oddities of finding and files (from an implementers view)	Bernhard Reiter (Intevation GmbH)
08:40 - 09:25 CET	OT Security in Sync: A CSAF Template Powering 40+ Vendors	Jochen Becker (CERT@VDE)
09:30 - 10:10 CET	Scaling CSAF: Building a Trusted Provider Network for 40+ Vendors	Christian Link (CERT@VDE)
10:10 - 10:25 CET	Break	
10:25 - 11:10 CET	VEX-supported Vulnerability Management with SecObserve	Stefan Fleckenstein & Lukas Voetmand
11:15 - 11:45 CET	Integrating the CSAF Standard into Dependency-Track with Kotlin-CSAF: Early Insights and Developments	Christian Banse
11:45 - 12:45 CET	Lunch	
12:50 - 13:20 CET	Handling lots of Incoming Documents as Team with ISDuBA — a CSAF Management System Web App	Bernhard Reiter (Intevation GmbH)
13:25 - 13:55 CET	Demonstrator with CSAF-Matching from the Project ZenSIM4.0	Dr. Salva Daneshgadeh Cakmakci
14:00 - 14:45 CET	Experiences in Consuming CSAFs & What is Still Missing	Tobias Limmer & Michael Pfurtscheller
14:50 - 15:15 CET	How to get CSAF into Contracts	Thomas Schmidt (BSI)
15:20 - 15:30 CET	Closing Remarks	Omar Santos (CSAF TC (Chair))



TLP:CLEAR