Beyond Open Standards

—

What is needed to Make Open, Distributed Cybersecurity Systems Architecture a Reality?

Jason Keirstead / Matthias Vallentin

IBM Security

OPEN CYBERSECURITY ALLIANCE

TENZIR

Quick Intro

Jason Keirstead is an IBM Distinguished Engineer and CTO of Threat Management in IBM Security. His role encompasses threat management products under the IBM QRadar, ReaQta, and XForce brands. Jason also sits on the OASIS Board of Directors and serves as a co-chair of the Open Cybersecurity Alliance project governing board.

Matthias is co-founder and CEO of Tenzir, a startup empowering defenders to build scalable SOC architectures. He holds a PhD in computer science from UC Berkeley and has over a decade of hands-on experience in network security and engineering large-scale distributed systems.

@BlueTeamJK

in https://www.linkedin.com/in/jasonkeirstead/

@mavam

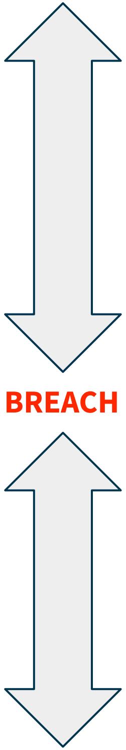
in https://www.linkedin.com/in/matthias-vallentin

IBM Security

OPEN CYBERSECURITY ALLIANCE

TENZIR

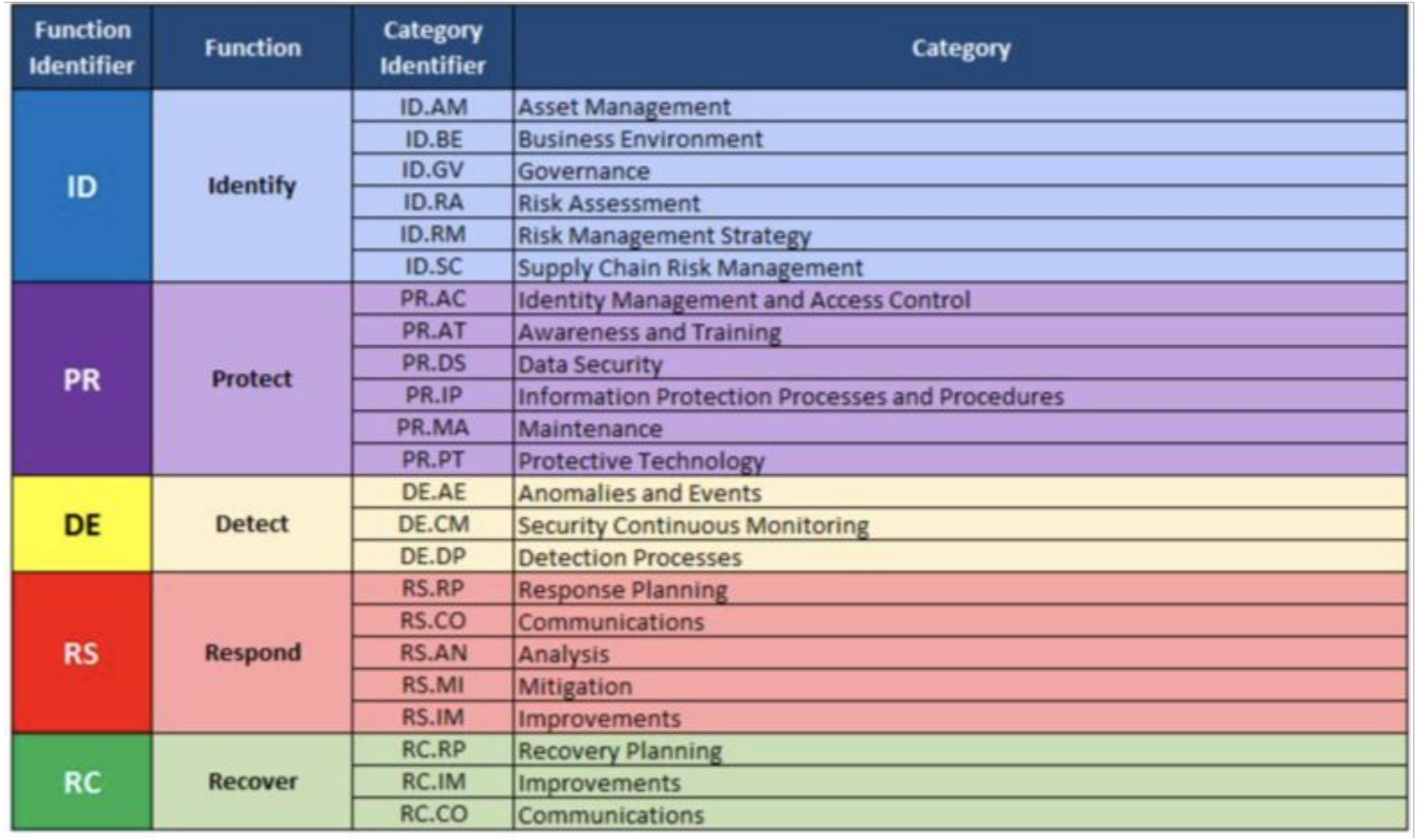
Level Setting



Cyber Resiliency

BREACH

Cybersecurity Operations



Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

CSA Themes

Market Themes

> ENISA shall promote the use of European cybersecurity certification, with a view to **avoiding the fragmentation of the internal market**. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework [..], with a view to **increasing the transparency of the cybersecurity of ICT products**, ICT services and ICT processes, thereby **strengthening trust in the digital internal market** and its competitiveness.
>
> — Article 4(6)

> ENISA shall support and promote the development and implementation of **Union policy on cybersecurity certification** of ICT products, ICT services and ICT processes [..]
>
> — *Article 8(1)*

"avoiding [market] fragmentation"

- cybersecurity reality, caused by
  - monolith tech stacks
  - vendor lock-in
  - incompatible products

"transparency of cybersecurity"

- response to supply chain attacks
- e.g., SBOM

"trust in the digital internal market"

- a European trusted cyber brand
- a European cyber certification

Operational Themes

ENISA shall **promote cooperation**, including **information sharing and coordination at Union level**, [..] **on matters related to cybersecurity.**

— *Article 4(4)*

[ENISA shall assist] that [..] each CSIRT possesses **a common set of minimum capabilities** and operates according to best practices;

— Article 6(1g)

ENISA shall support **information sharing** in and between sectors [..] by providing **best practices and guidance on available tools, procedures**, as well as on how to **address regulatory issues related to information-sharing**.

— Article 6(2)

"information sharing"

- Threats
- Telemetry (network traffic, app logs, etc.)
- Alerts
- Detections
- Behavior models

"coordination at the Union level"

- Investigations & IR
- Joint response
- Best practices
- Cross-border, cross-tool, cross-CSIRT

When are standards insufficient?

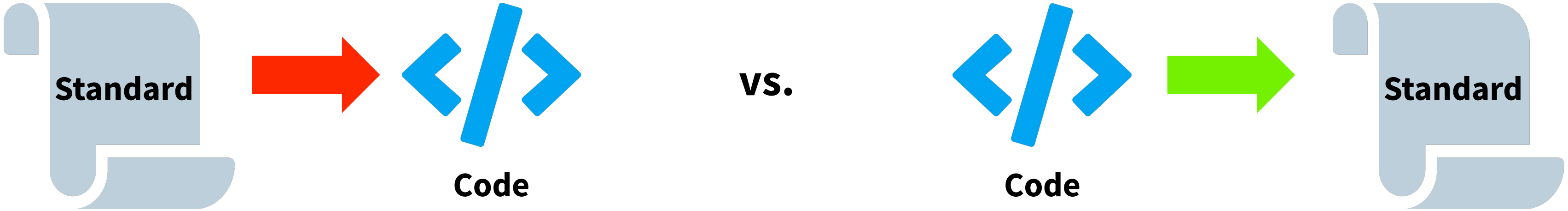
When are standards insufficient?

- An "open API" counts as standard
- Often just a RFP checkbox
- Implementation ⇏ interoperability
- Process: shouldn't something be known to work *before* it is standardized?

Missing requirement:
open-source reference implementation

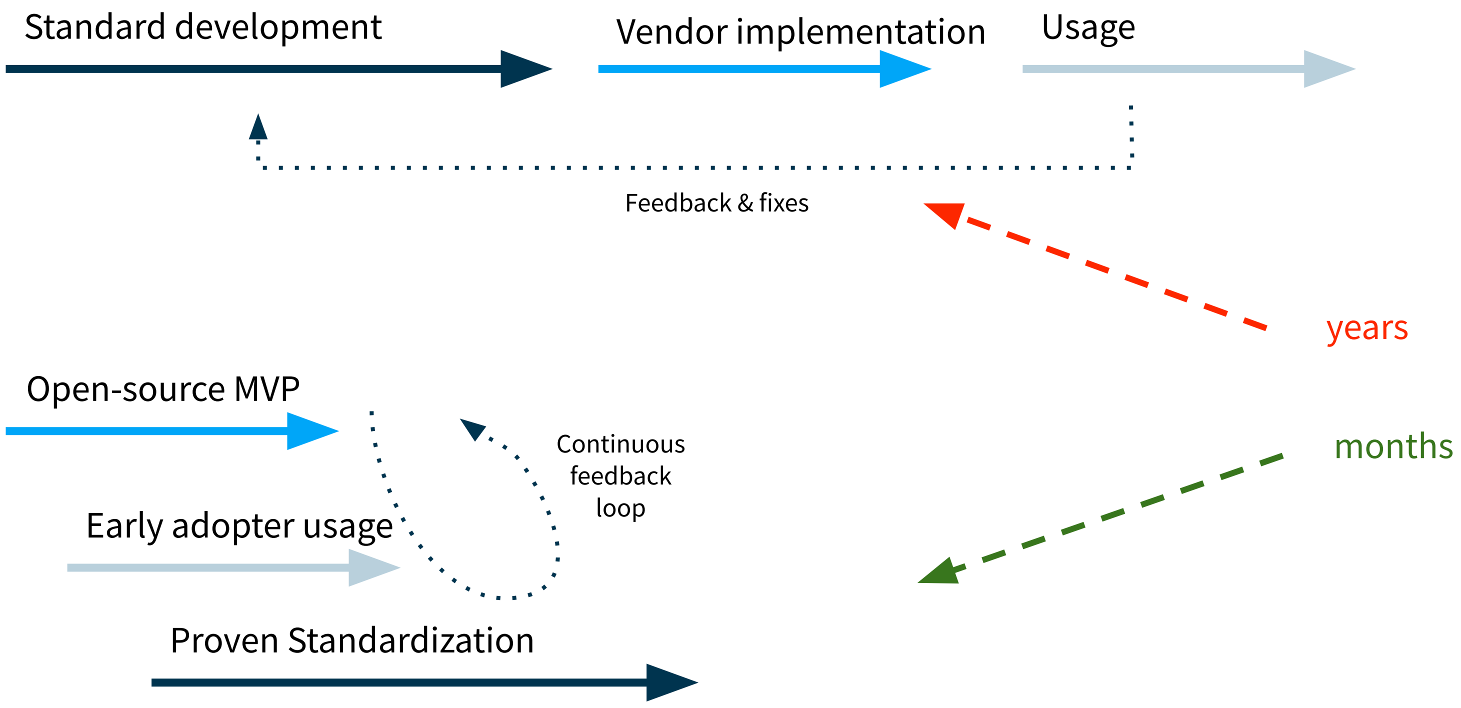
✓ **Guaranteed interoperability for a use case**

✓ **Faster iteration cycle**



Proven Standardization

Use open–source to bootstrap a standard, rather than the vice-versa



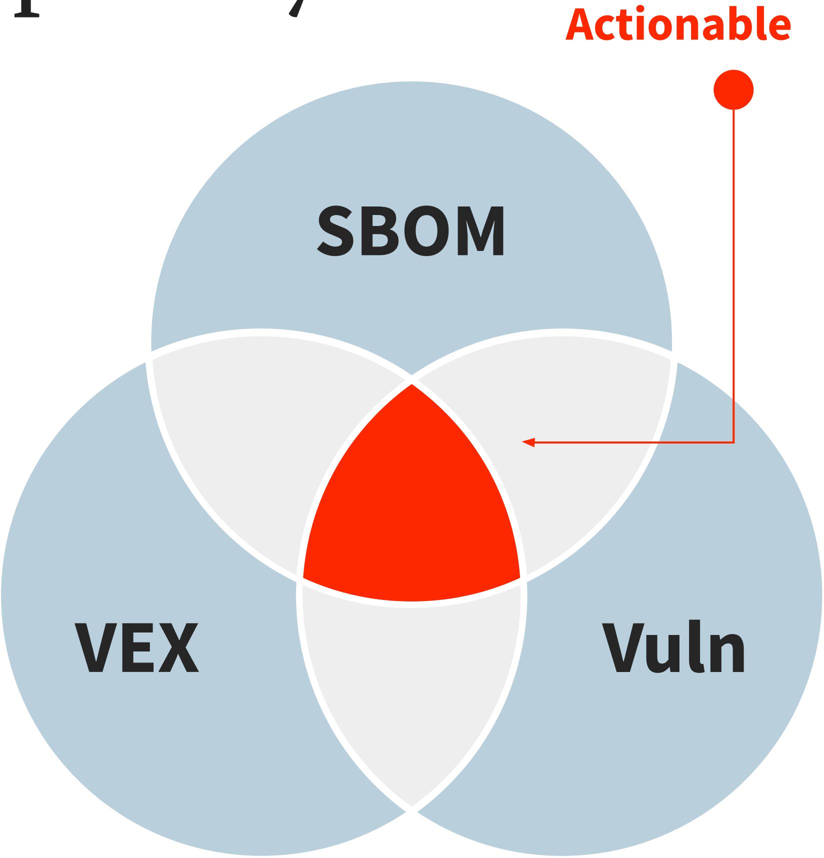
Enabling Transparency

Software Bill of Materials (SBoM) standards:

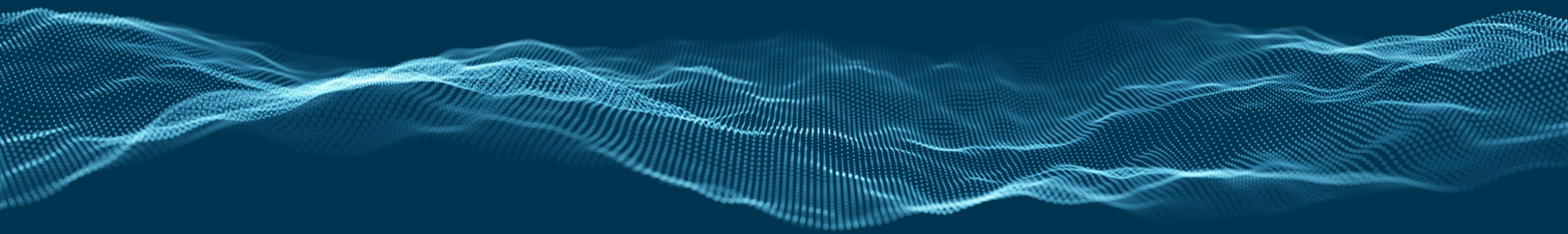
- **SPDX**, Linux Foundation / ISO - https://spdx.dev/
- **CycloneDX**, OWASP - https://cyclonedx.org/

SBoM is just the *beginning*:

- **VEX**: Vulnerability Exploitability eXchange
- **PACE** Project: https://github.com/opencybersecurityalliance/PACE
- OWASP Dependency Track: https://dependencytrack.org/



How to cooperate on information sharing?



Standards For Sharing Data (too many!)

Data sharing considerations:

- Do I have *any influence at all* on the source data?
- What is my toolchain? Does it work best with a preferred model or format?
- What are my use cases? Am I hunting or detecting? Or both?
- Do I have any pre-existing expertise to leverage?
- Are there pre-existing communities I or should be leveraging?

CIM
ECS
LEEF
OpenIOC
OSSEM
CEF
SIGMA
IPFIX
ASIM
STIX

"Alphabet Soup" of data sharing standards

Existing Methodologies & Forums

Open Security Standards

Open security standards to facilitate interoperability of security tools

fido ALLIANCE

SAML SECURITY ASSERTION MARKUP LANGUAGE

STIX TAXII

OASIS STANDARD KMIP

OpenC2

OpenID

cacao PLAYBOOKS

TRUST Over IP FOUNDATION

Open Source Code

Open-source code to quickly fix gaps in commercial products

nifi

MISP Threat Sharing

CONFIDENTIAL COMPUTING CONSORTIUM

OCA OPEN CYBERSECURITY ALLIANCE

OPENCTI

Sysflow

falco

Intelligence & Analytics

Comprehensive Threat Intelligence for quickly responding to threats

MITRE ATT&CK™

THREAT HUNTER Playbook

Quad9

OPENCTI

jupyter

MISP Threat Sharing

Frameworks & Governance

Bring the power of industry expertise to your security team

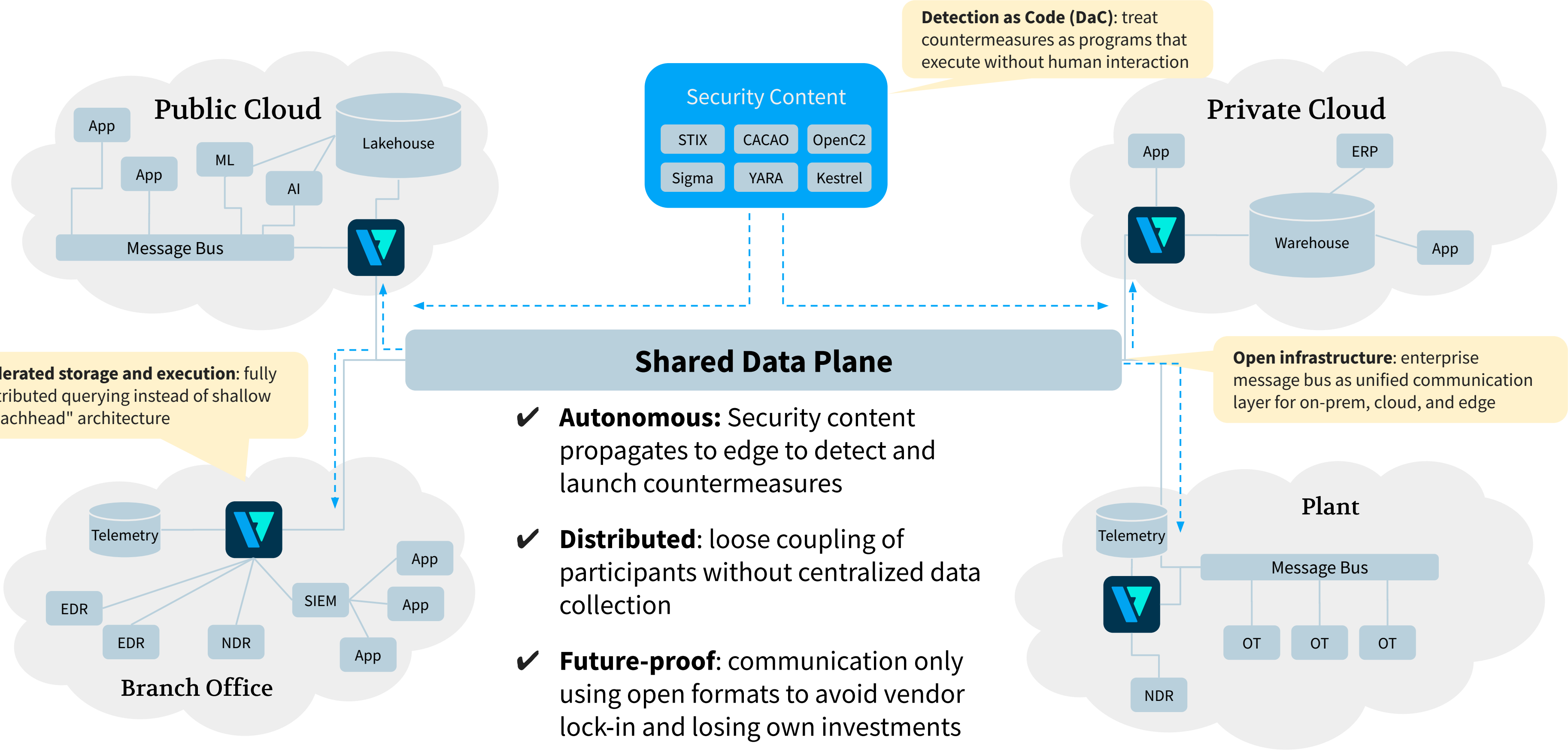
CYBERSECURITY FRAMEWORK: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

CIS Center for Internet Security

enisa

OWASP™

Enabling Data Sharing



Detection as Code (DaC): treat countermeasures as programs that execute without human interaction

Federated storage and execution: fully distributed querying instead of shallow "beachhead" architecture

Open infrastructure: enterprise message bus as unified communication layer for on-prem, cloud, and edge

- ✔ **Autonomous:** Security content propagates to edge to detect and launch countermeasures
- ✔ **Distributed**: loose coupling of participants without centralized data collection
- ✔ **Future-proof**: communication only using open formats to avoid vendor lock-in and losing own investments

Governance is a Success Factor

Open-source is a starting point, but open governance is critical:

- Reduces risk of project abandonment
- Eliminates single-vendor control
- Creates a safe place to innovate (IP rights)
- Allows projects to 'scale-up'
- Provides a path to standardization

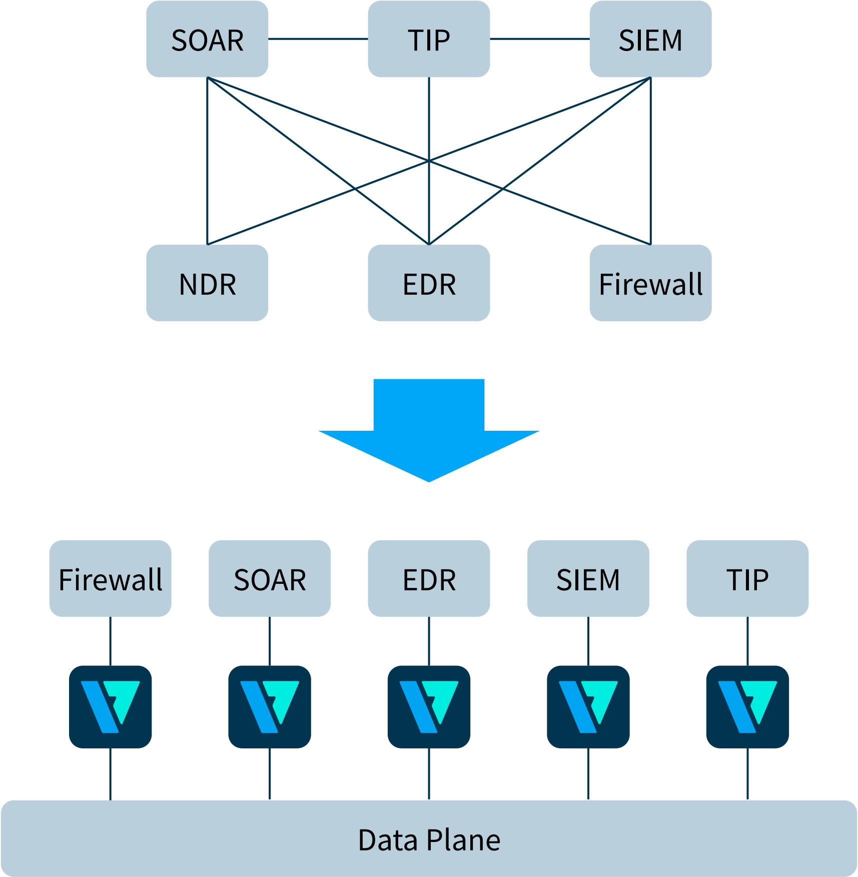
https://developer.ibm.com/articles/open-governance-community/
https://www.oasis-open.org/2021/12/17/minimum-viable-governance-is-great-but-not-always-sufficient/

Actions & Recommendations

Making Theory Reality

Leading analysts advocate for an **open mesh architecture** to security

- **CSMA**: Cyber Security Mesh Architecture (**Gartner**)
- **SPIF**: Security Platform Integration Framework (**Omdia**)
- **SOAPA**: Security Operations and Analytics Platform Architecture (**ESG**)



Actions & Recommendations

ENISA must play a more active role in defining **open standards for cybersecurity operations** and contribute with **open-source reference implementations**.

Communities must be enabled to extract value from their existing investments via **open collaboration**, driven by a **shared data plane**.

Organizations must consider **open & standardized interfaces** as critical capabilities during RFPs. Having an "open API" to a blackbox is not enough.

Thank you! Questions?

Join our communities and engage with us!

- OCA Slack
- Tenzir Community Slack

OPEN CYBERSECURITY ALLIANCE