OASIS OPEN

Setting the standard for open collaboration

OASIS Open Supply Chain Information Modeling (OSIM)

- Goal and scope
- Relationship with other standards
- Comments, questions, open discussion
- Participation options
- Timeline and next steps

On the call today…

Carol Geyer
Chief Development Officer
OASIS Open
carol.geyer@oasis-open.org

Duncan Sparrell
Founder
sFractal Consulting
duncan.sparrell@oasis-open.org

Holly Petersen
Business Development Manager
OASIS Open
holly.petersen@oasis-open.org

OSIM Mission

To standardize and promote information models about software aspects of supply chains.

Goal

To bring clarity to supply chain partners and eliminate inefficiencies that come from using so many disparate implementations.

To make it easier for companies to plan for upgrades and contingencies and help reduce vulnerabilities, disruptions, and security risks.

Open Supply Chain Information Model

To standardize and promote information models about software supply chains.

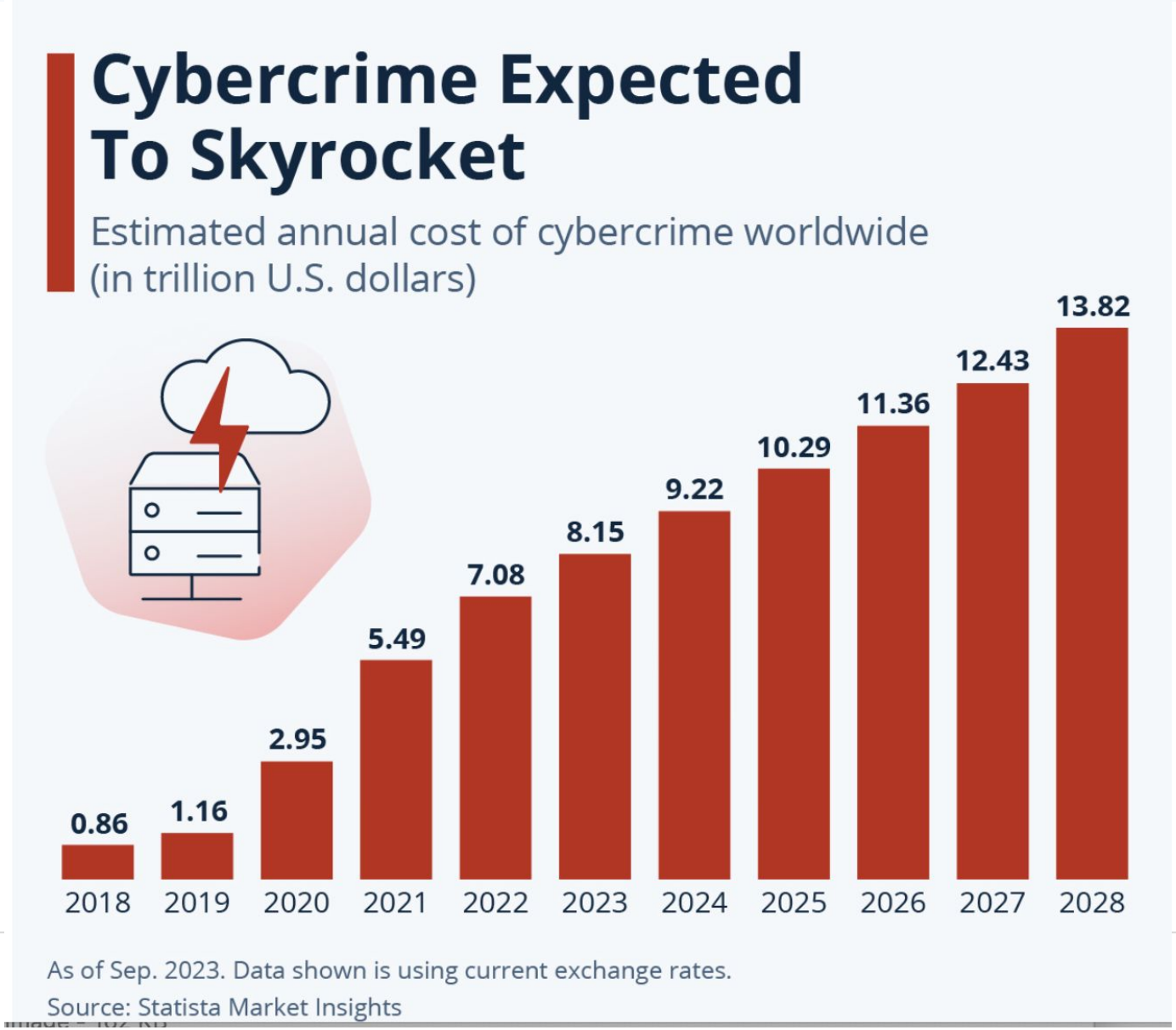
OSIM Mission


SHOW
ME THE
MONEY!

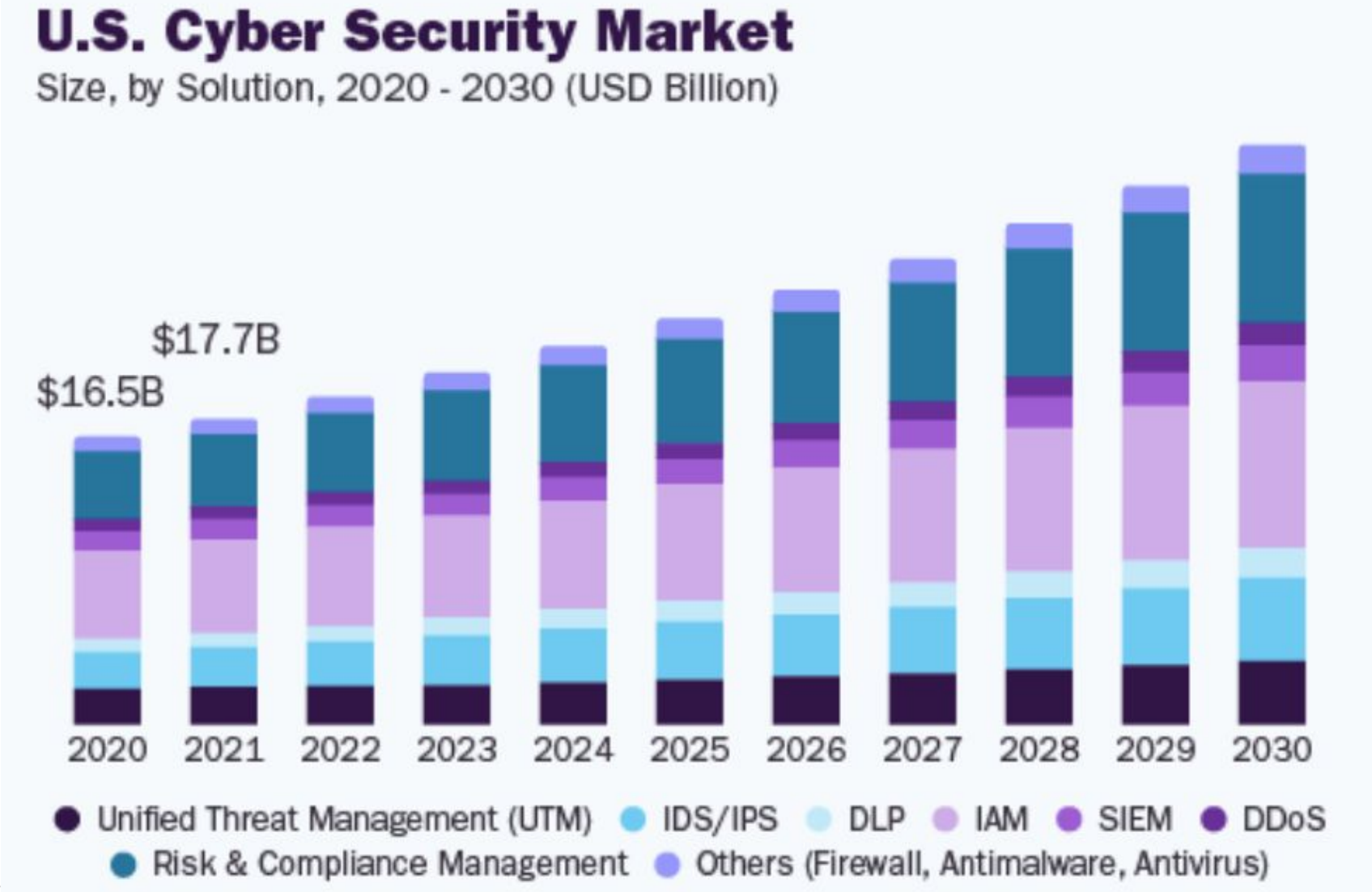
Why?


ransomware
spyware
crime
antivirus
malware
online
information
data theft
law
safety
firewall
DDOS
internet
personal data
virus
hacking
security
personal data
private information
CYBER ATTACK
private information
hacking
identity
law
online
technology
password
crime
future
virus
spyware
malware
future
DDOS
malware
ransomware
hacking
cyberattack
cyberattack
digital
virus
computer
problem
computer
internet
computer
security
password
data theft
spyware
technology
crime
problem
firewall
private information
security
computer
technology
information
law
website
ransomware
password
computer
computer
antivirus
future
website
digital
information
safety
safety
firewall
website
identity
digital

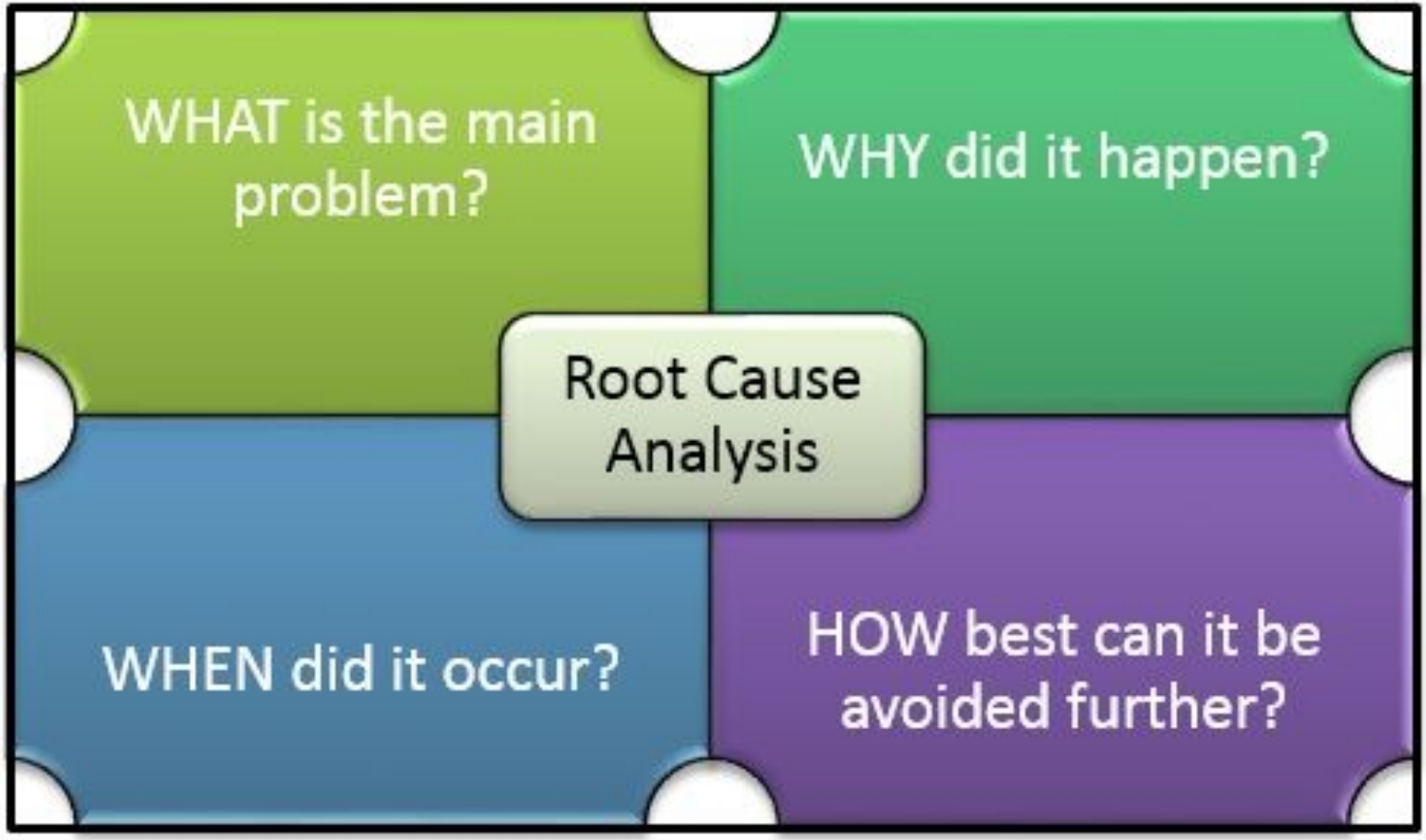
Cost Lost to Crime Increasing



Cost to thwart increasing



Instead of Bolting on Security, Fix the Problem



Attack Evolution

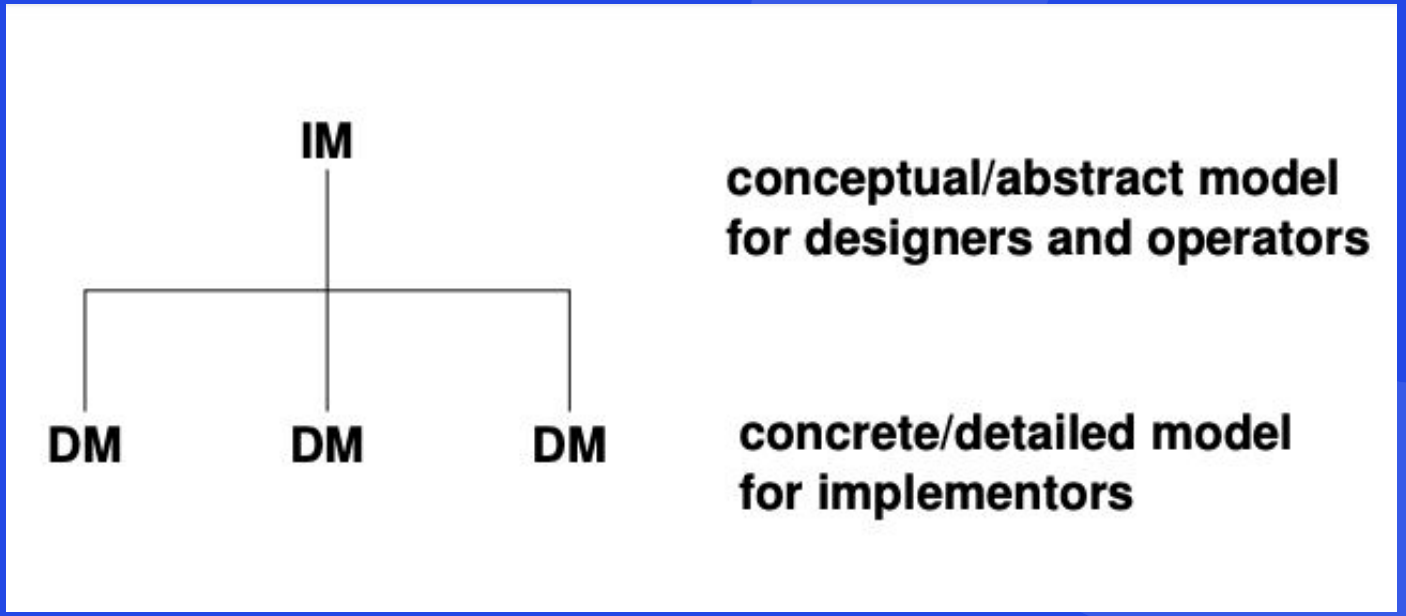
Open Supply Chain Information Model

To standardize and promote information models about software supply chains.

OSIM Mission

Information Model

Information Models (per RFC 3444) are
used to model managed objects at a conceptual level,
independent of any specific protocols
used to transport the data
(protocol agnostic).



https://github.com/oasis-tcs/openc2-jadn-im/blob/published/imjadn-v1.0-cn01.md#2-information-modeling-overview

Open Supply Chain Information Model

To standardize and promote information models about software supply chains.

OSIM Mission

Software Supply Chain

VEX Fields Comparison

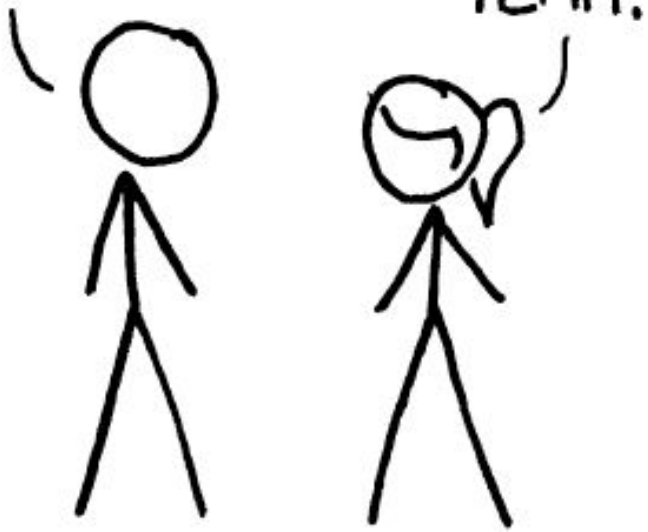
	CSAF	CycloneDX	OpenVEX
Metadata	Publisher (name, website, contact details) Title, version, Revision history	Version, Revision history (as property) *More to be added*	Publisher name, version
Product	Product Id, Vendor, Name, version, SBOM (ref to URL)	Name *(more to be added)*	
Vulnerability	ID (cve), status, date, product affected (ref to product Id), justification/analysis	ID (cve), status, date (created/updated), product affected (ref to SBOM), justification/analysis	ID (cve), status, date, product (only components), action statement

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.

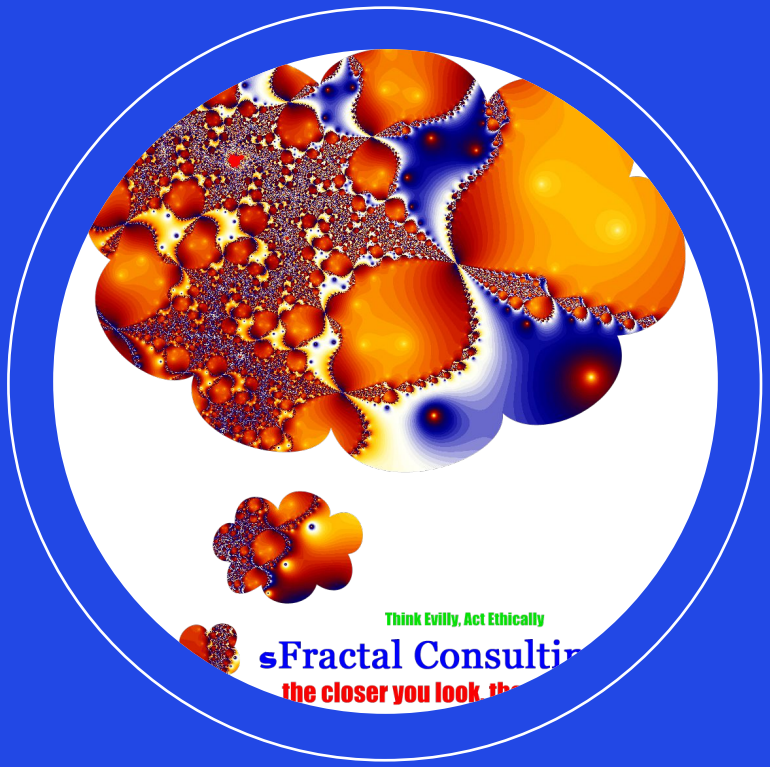


SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

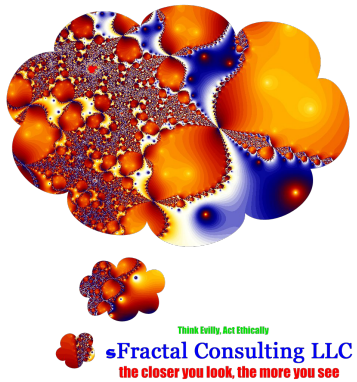
Supply Chain Information Model

To standardize and promote information models about software supply chains.



OSIM Mission

Current OSIM Supporters



Google

AT&T

cisco

CYWARE™

Microsoft

Why should you participate in OSIM?

a) It's good for your company.
b) It's good for you.

Benefits of Joining

Influence

Be sure your voice is heard, your use cases are addressed, and your requirements met.

Governance

Get things done with support and oversight that result in fair, transparent, and productive collaboration.

Safety

Develop under proven licensing policies, confident that the contributions you make and the work you produce can be adopted without concerns.

Recognition

Be seen as one of the leaders--or be conspicuous by your absence

Benefits of Membership

The Inside Track

Get a head start on compliance before the standards become final

Community

Collaborate with potential partners, customers, and policymakers. Extend your own knowledge base.

Glory

See your name attached to something that's relevant, respected, and adopted on a global scale...maybe all the way to ISO, IEC, or ITU

Sponsor Membership lets your company:

- Involve an unlimited number of staff (as TC members or observers)
- Be represented in OSIM and any other OASIS TCs of interest
- Start new TCs
- Nominate, serve, and vote on OASIS Board of Directors
- Vote to approve final deliverables and request de jure submissions

Sponsor Members also receive:

- Logo visible throughout OASIS website
- Inclusion and quotes in OSIM press releases issued by OASIS
- Recognition on OSIM TC homepage
- Participation in Interop demos and expo showcases
- Opportunities to speak at conferences

Annual Membership Dues

Organization size (total employee headcount)	**Contributor**	**General Sponsor**	**Premier**
	Technical participation only **For non-commercial entities and SME users**	*Technical participation + marketing benefits* **For vendors, stakeholder users, national government agencies**	*Technical participation + **exclusive** marketing and event benefits* **For industry leaders and innovators**
500 + employees	$13,500	**$27,000**	**$70,000**
100-500 employees	$12,500	**$22,500**	
10- 99 employees	$10,500	**$19,000**	
Fewer than 10 employees	$5,300	**$9,500**	
University, local government agency, nonprofit association	$1,800	**$16,00**	

Launch timeline and next steps

Charter

27 March - 22 April

All received comments have been addressed

Call for Participation

24 April - 4 May

30 days to join in order to attend first TC meeting

First TC Meeting

4 June

Chair(s) elected, meeting cadence set, agenda prioritization begins

Press release

Mid-June

All Sponsor members are featured and may provide quotes

Related Projects

CES

Computing Ecosystem Supply-Chain:

Developing use cases, standards (data schemas, ontologies) and APIs that enable end-to-end visibility for computing supply chains

CSAF

Common Security Advisory Framework:

Standardizing automated disclosure of cybersecurity vulnerability issues

Open EoX

OpenEoX:

Standardizing the language for managing end-of-life information for commercial and open source software and hardware.

SARIF

Static Analysis Results Interchange Format:

Defining a standard output format for static analysis tools

UBL

Universal Business Language:

Defining a common XML library of business documents (purchase orders, invoices, etc.)

OASIS OPEN

WEBSITE:
https://oasis-open.org

CHARTER:
Draft Charter

EMAIL:
carol.geyer@oasis-open.org
holly.petersen@oasis-open.org