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!
Cost Lost to Crime Increasing

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)

As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights
Cost to thwart increasing

**U.S. Cyber Security Market**
Size, by Solution, 2020 - 2030 (USD Billion)

- 2020: $16.5B
- 2021: $16.7B
- 2022: $17.0B
- 2023: $17.3B
- 2024: $17.6B
- 2025: $18.0B
- 2026: $18.4B
- 2027: $18.9B
- 2028: $19.5B
- 2029: $20.3B
- 2030: $21.2B

- Unified Threat Management (UTM)
- IDS/IPS
- DLP
- IAM
- SIEM
- DDoS
- Risk & Compliance Management
- Others (Firewall, Antimalware, Antivirus)
Instead of Bolting on Security, Fix the Problem

WHAT is the main problem?

WHY did it happen?

Root Cause Analysis

WHEN did it occur?

HOW best can it be avoided further?
Attack Evolution

- Ukraine Power Grid
- Colonial Pipeline
- JBS Meat
- SolarWinds
- Melissa
- Equifax
- Log4j
- XZ
- Wannacry
- Target
- OPM
Open Supply Chain Information Model

To standardize and promote information models about software supply chains.
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

<table>
<thead>
<tr>
<th>Field</th>
<th>CSAF</th>
<th>CycloneDX</th>
<th>OpenVEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata</td>
<td>Publisher (name, website, contact details)</td>
<td>Version, Revision history (as property)</td>
<td>Publisher name, version</td>
</tr>
<tr>
<td></td>
<td>Title, version, Revision history</td>
<td><em>More to be added</em></td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Product Id, Vendor, Name, version, SBOM (ref to URL)</td>
<td>Name <em>(more to be added)</em></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>ID (cve), status, date, product affected (ref to product Id), justification/analysis</td>
<td>ID (cve), status, date (created/updated), product affected (ref to SBOM), justification/analysis</td>
<td>ID (cve), status, date, product (only components), action statement</td>
</tr>
</tbody>
</table>
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.

Yeah!

**Situation:**
There are 15 competing standards.

Soon:
Supply Chain Information Model

To standardize and promote information models about software supply chains.

OSIM Mission
Current OSIM Supporters
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:

1. Involve an unlimited number of staff (as TC members or observers)
2. Be represented in OSIM and any other OASIS TCs of interest
3. Start new TCs
4. Nominate, serve, and vote on OASIS Board of Directors
5. Vote to approve final deliverables and request de jure submissions
Sponsor Members also receive:

1. Logo visible throughout OASIS website
2. Inclusion and quotes in OSIM press releases issued by OASIS
3. Recognition on OSIM TC homepage
4. Participation in Interop demos and expo showcases
5. Opportunities to speak at conferences
<table>
<thead>
<tr>
<th>Organization size (total employee headcount)</th>
<th>Contributor</th>
<th>General Sponsor</th>
<th>Premier</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 + employees</td>
<td>$13,500</td>
<td>$27,000</td>
<td></td>
</tr>
<tr>
<td>100–500 employees</td>
<td>$12,500</td>
<td>$22,500</td>
<td></td>
</tr>
<tr>
<td>10–99 employees</td>
<td>$10,500</td>
<td>$19,000</td>
<td></td>
</tr>
<tr>
<td>Fewer than 10 employees</td>
<td>$5,300</td>
<td>$9,500</td>
<td>$70,000</td>
</tr>
<tr>
<td>University, local government agency, nonprofit association</td>
<td>$1,800</td>
<td>$16,000</td>
<td></td>
</tr>
</tbody>
</table>

- **Contributor**: Technical participation only for non-commercial entities and SME users.
- **General Sponsor**: Technical participation + marketing benefits for vendors, stakeholder users, national government agencies.
- **Premier**: Technical participation + exclusive marketing and event benefits for industry leaders and innovators.
Launch timeline and next steps

<table>
<thead>
<tr>
<th>Charter</th>
<th>Call for Participation</th>
<th>First TC Meeting</th>
<th>Press release</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 March – 22 April</td>
<td>24 April – 4 May</td>
<td>4 June</td>
<td>Mid-June</td>
</tr>
<tr>
<td>All received comments have been addressed</td>
<td>30 days to join in order to attend first TC meeting</td>
<td>Chair(s) elected, meeting cadence set, agenda prioritization begins</td>
<td>All Sponsor members are featured and may provide quotes</td>
</tr>
</tbody>
</table>
## Related Projects

<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CES</strong></td>
<td><strong>Computing Ecosystem Supply-Chain</strong>: Developing use cases, standards (data schemas, ontologies) and APIs that enable end-to-end visibility for computing supply chains</td>
</tr>
<tr>
<td><strong>CSAF</strong></td>
<td><strong>Common Security Advisory Framework</strong>: Standardizing automated disclosure of cybersecurity vulnerability issues</td>
</tr>
<tr>
<td><strong>Open EoX</strong></td>
<td><strong>OpenEoX</strong>: Standardizing the language for managing end-of-life information for commercial and open source software and hardware.</td>
</tr>
<tr>
<td><strong>SARIF</strong></td>
<td><strong>Static Analysis Results Interchange Format</strong>: Defining a standard output format for static analysis tools</td>
</tr>
<tr>
<td><strong>UBL</strong></td>
<td><strong>Universal Business Language</strong>: Defining a common XML library of business documents (purchase orders, invoices, etc.)</td>
</tr>
</tbody>
</table>