Software Transparency in SaaS Environments

SBOM-a-rama 2024

Doug Cavit
Nisha Kumar

https://docs.google.com/document/d/1_yQgLhOEw-H5w9Dr3XbNYIIX8vLs59IJwLvJm4aHDVY/edit#heading=h.3kcprhiiv0b8

SBOM Differences and Limitations

1. Frequency of change for SaaS
2. Volume and shared origin of software and services involved – who is responsible?
3. Lack of definitive boundaries both horizontally and vertically
4. The opacity of SaaS systems

SBOM Benefits by Persona

Producer:

- Transparency for managing risk both for themselves and customers.
- Communicate information about services and practices.

Operators:

- Transparency for managing risk both for themselves and customers.
- Communicate information about services and practices.
- Vulnerability Management.
- Accountability for vendors.

Chooser:

- Accountability for vendors.
- Transparency in risk management.

Subscribers (unique to cloud):

- Transparency in risk management.

Examples of Where It Would be Useful

- CVE-2023-4863 – Webp Vulnerability Risk Identification
- Simplifying job of different personas
- Thin clients
- Web applications with 3rd party services
- Cloud Services

Call to Action

- There are identified areas where more standardization is needed including an software interchange format to increase transparency. Advocate for this with your providers and peers.
- Everyone has a role in being part of the ownership/responsibility chain. Understand your own role and your providers.
- Request SBOM's from both your upstream and downstream solutions.

Future Work

- Data Governance
- Service Availability Indicators
- Risk Indicators
- Transitive Service Dependency Considerations

Acknowledgements

Adrian Diglio, Microsoft
Bhargav Vivekanandan, Blue Shield of California
Cassie Crossley, Schneider Electric
Charles Kelly, SAP
Christine O'Leary, Intel
Craig Rubin, HPE
Daniel Bardenstein, Manifest
Deanna Medina, Honeywell
Doug Cavit, Cavit and Hohman
Duncan Sparrell, sFractal Consulting
Emily Fesnak, Deloitte
Henry Yandell, AWS
Isaac Hepworth, Google
Ivana Atanasova, VMware
Ixchel Ruiz
Jeremiah Stoddard, INL
Jim Routh, Saviynt
Joerg Eschweiler
Joyabrata Ghosh, CARIAD SE
Lynn Westfall
Michael Greco, ServiceNow
Nisha Kumar, Oracle
Rene Pluis, Philips
Ricardo Reyes, Tidelift
Scott Armstrong, Interos
Shafia Zubair, JCI
Steve Springett, ServiceNow/OWASP
Tom Alrich
Trevi Housholder, Prudential
Victoria Ontiveros, CISA