OpenSSF
OPEN SOURCE SECURITY FOUNDATION

6 Months In:
Building and Using the Security Toolbelt

OSS-NA 2024

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Sarah Evans

Security Innovation Research, Dell Office CTO

20 year Air Force vet

music and business degree

John Kjell, adv

Pronunciation: 🇸🇪(🐚)

Eagle Scout

“Director” @ a startup

Hoodie Connoisseur

CRob, n, adj, and v

Pronunciation: U.S. (K-robe)

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Agenda

01 - Origin Story

02 - Personas, use cases, capabilities, threats, patterns

03 - Where we're going

04 - PoC

05 - Call to Action

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Origin Story

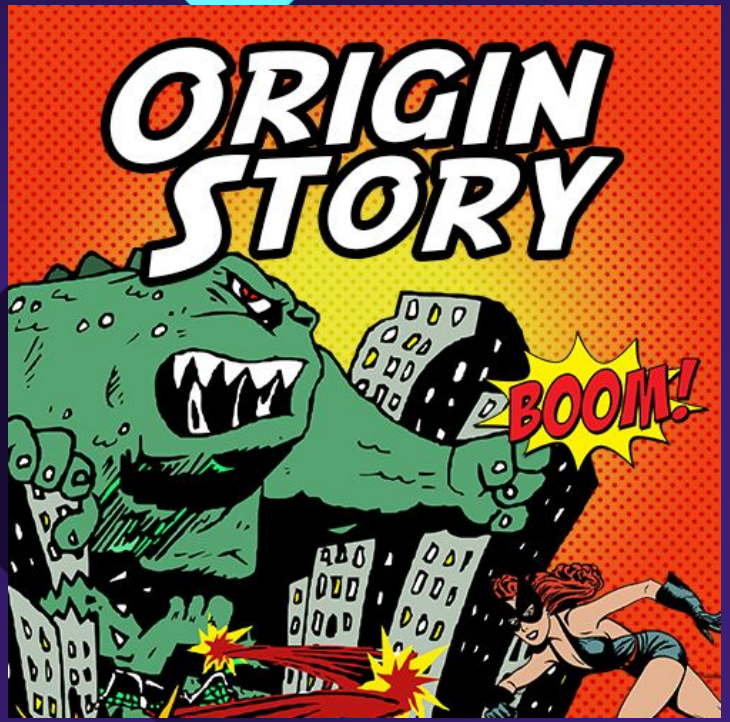
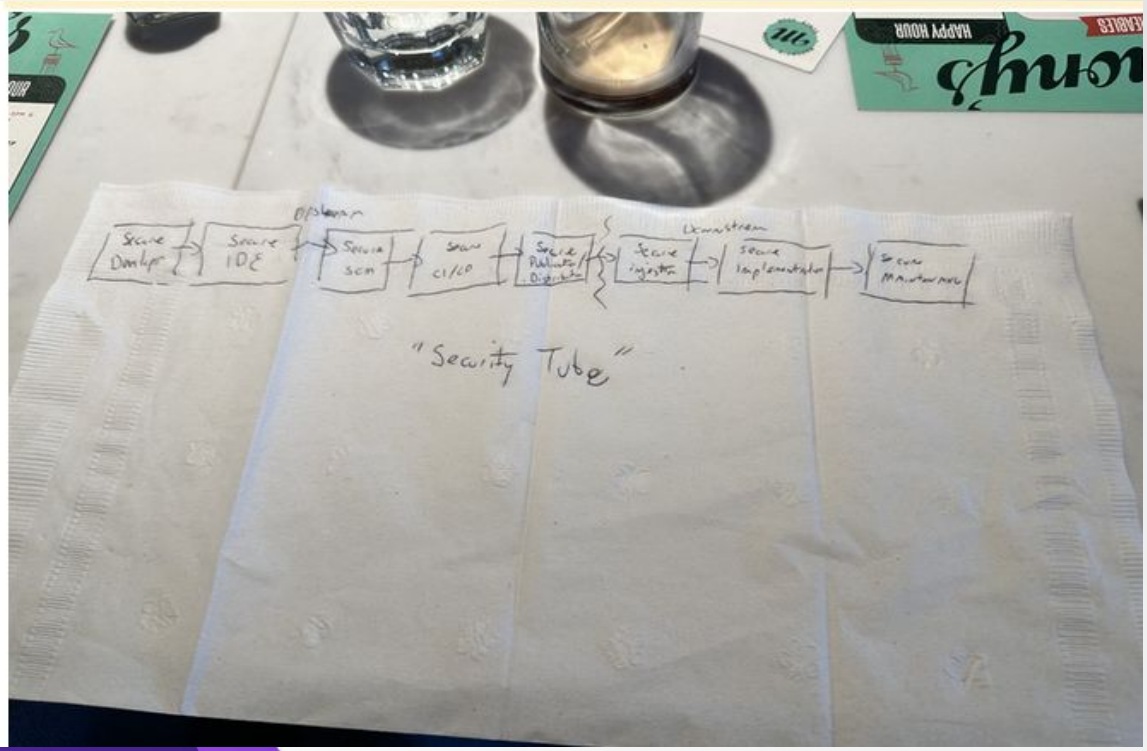


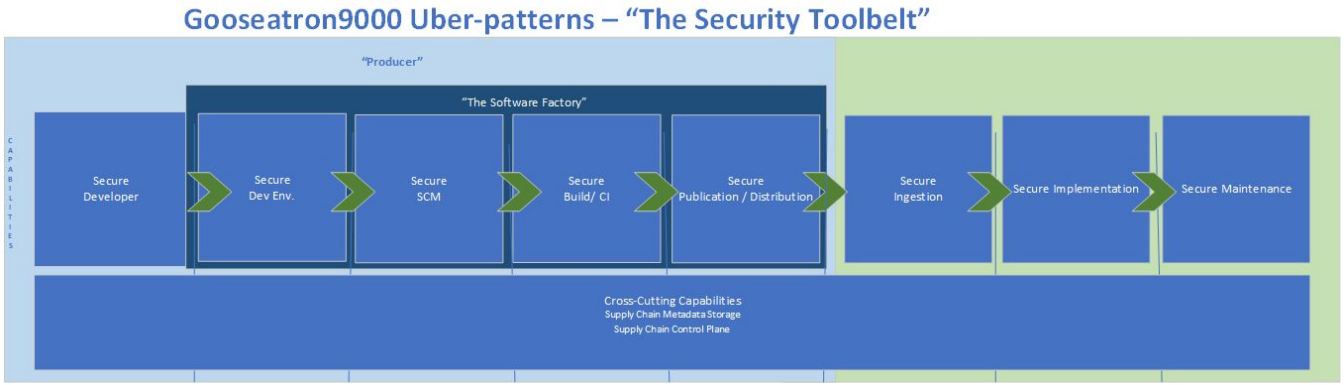
Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

As with all great projects, it started.....



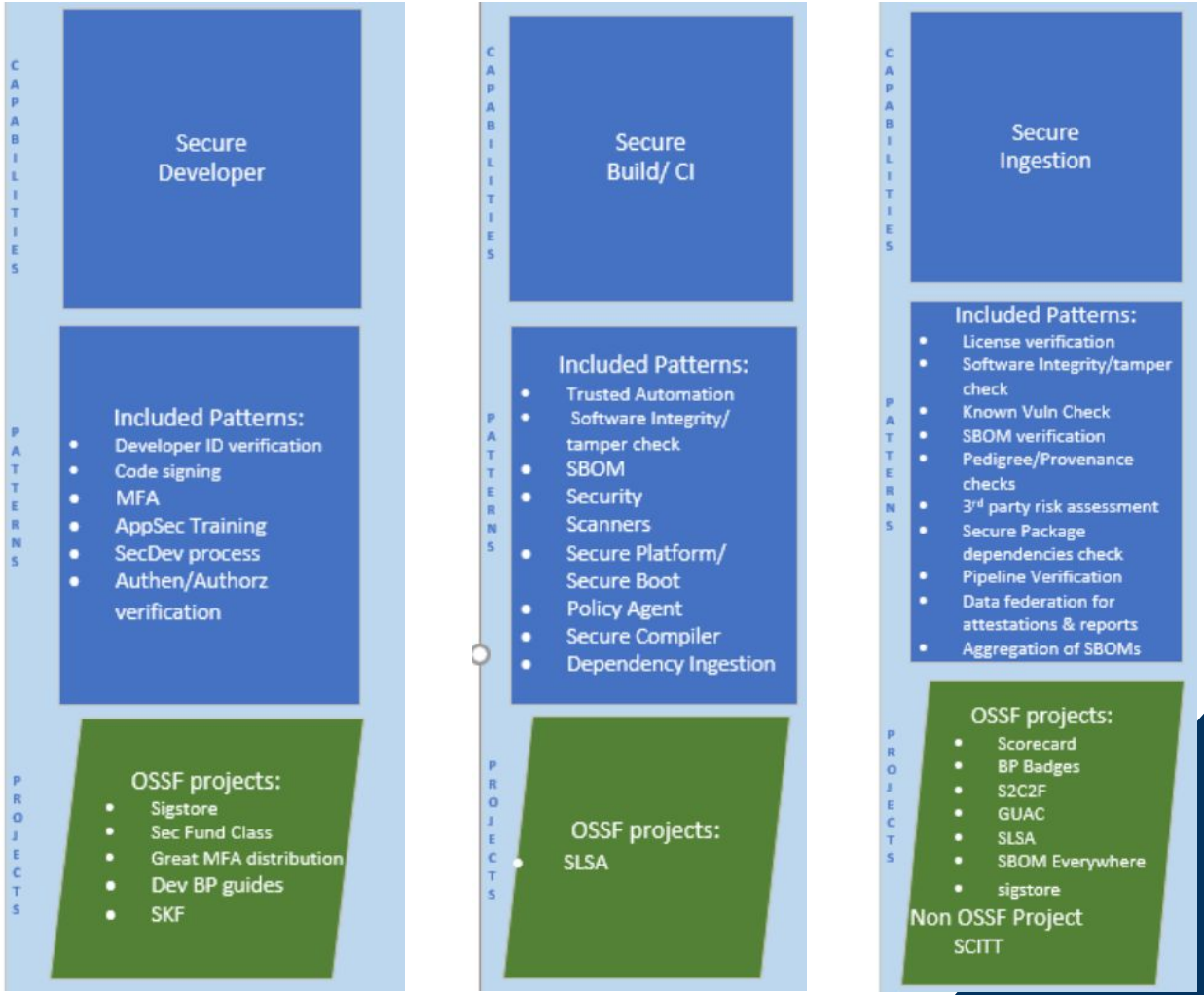
Gooseatron, Diagrammer's Society



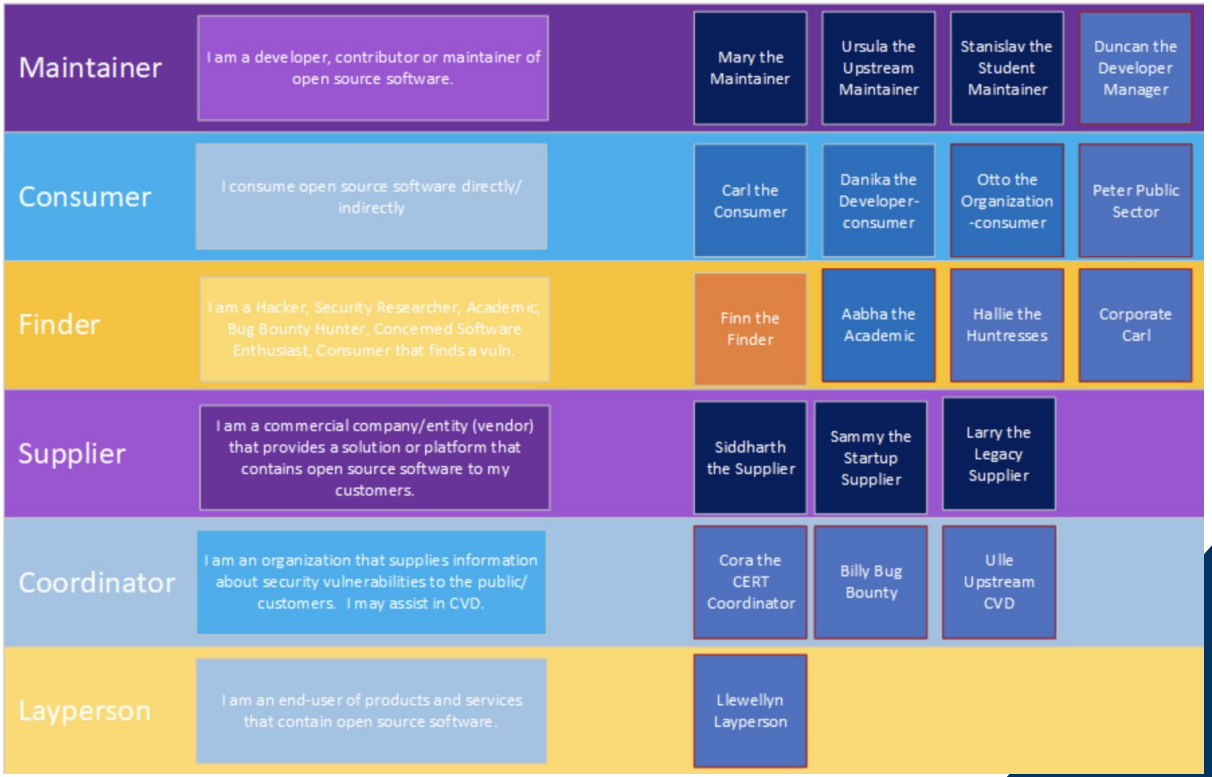
Personas, use cases, capabilities, threats, patterns

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The “Stovepipes”



Personas


Maintainer
I am a developer, contributor or maintainer of open source software.
Mary the Maintainer
Ursula the Upstream Maintainer
Stanislav the Student Maintainer
Duncan the Developer Manager
Consumer
I consume open source software directly/ indirectly
Carl the Consumer
Danika the Developer-consumer
Otto the Organization-consumer
Peter Public Sector
Finder
I am a Hacker, Security Researcher, Academic, Bug Bounty Hunter, Concerned Software Enthusiast, Consumer that finds a vuln.
Finn the Finder
Aabha the Academic
Hallie the Huntresses
Corporate Carl
Supplier
I am a commercial company/entity (vendor) that provides a solution or platform that contains open source software to my customers.
Siddharth the Supplier
Sammy the Startup Supplier
Larry the Legacy Supplier
Coordinator
I am an organization that supplies information about security vulnerabilities to the public/ customers. I may assist in CVD.
Cora the CERT Coordinator
Billy Bug Bounty
Ulle Upstream CVD
Layperson
I am an end-user of products and services that contain open source software.
Llewellyn Layperson

Case Study Persona: Diana the Weekend Warrior

Role:

- working on open source software in their "spare time"
- maintains the project(s) by themselves
- started out as a way to learn new things for fun, has grown beyond that

Background:

- I maintain a couple of small packages and contribute new medium size but impactful features to my underlying ecosystem. (Think a compiler optimisation for floats that takes a few months of work and extremely niche knowledge to get right) This is a really common and critical profile.
- Diana is in a loose network of other niche people doing the same in my ecosystem.
- Diana has challenges keeping their toolchain and CI systems up-to-date and running. C was not made for this kind of work, nor are most of the packaging ecosystem, and they have to fight with them all the time.

Goals:

- keep the project going and as maintained as possible, given constraints of budget, time, and resources.

https://github.com/ossf/toolbelt/tree/main/personas#name-diana-the-weekend-warrior

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Diana continued

Challenges:

- Diana usually gets something like 2 hours per month to spend on FOSS. Sometimes up to 4h, sometimes less. 1 to 2h per month are dedicated to simply updating base dependencies. This is when it is just a few patches or minor versions. Sometimes up to 4 hours are taken for this. Sometimes a big major version in an important dependency happens and it takes us 10h to fix, over a quarter. This means that nearly all our *time* is spent handling dependency stuff. Basic stuff. Not security emergencies or anything like that. Releasing a new version that just is kept up to date basically.
- Diana does not have more *time* to give. Life is what it is; they have family, a job, friends, etc.
- Diana's tests for the project are in poor shape. This is very well known. They want to make them better, but per the above, there is no additional *time* to devote to this task. Even something like fuzzing would be incredibly challenging to deal with the additional bugs that could be found, prioritized, and eventually (maybe) fixed.
- Diana has no additional *time* to read security-oriented material or the use.
- Most of Diana's *time* is spent fighting build and dependency management tools. This is a constant problem. These tools often break in new and obscure ways. Oftentimes, features of the tool need to be disabled to even make things work and not break their builds. There are probably ways around this, but again, see above, there is no additional time to troubleshoot, research, and adjust. Even the basic tools break too much and eat Diana's *time*.
- Reviewing and reacting to user reports is challenging.

https://github.com/ossf/toolbelt/tree/main/personas#name-diana-the-weekend-warrior

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Where we're going

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Rising Tide lifting all boats

- The OpenSSF is a cross-industry collaboration that brings together leaders to improve the security of open source software (OSS) by building a broader community, targeted initiatives, and best practices
- The OpenSSF brings together open source security initiatives under one foundation to accelerate work through cross-industry support. This is beginning with the Core Infrastructure Initiative and the Open Source Security Coalition, and will include new working groups that address vulnerability disclosures, security tooling and more.
- OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.

https://openssf.org/

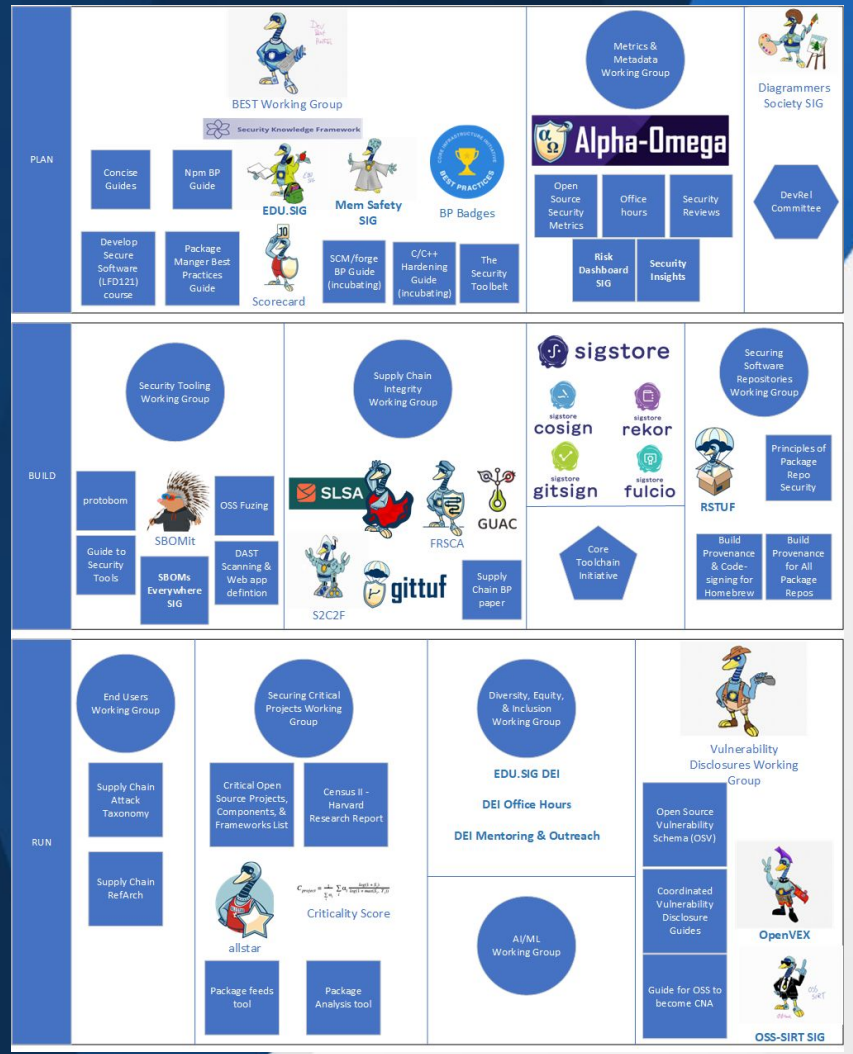
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

A Gaggle of Geese!

We have numerous software projects, guidelines, specs, and experts to help both upstream OSS developers AND downstream OSS consumers

https://openssf.org/community/openssf-working-groups/

What's up with all the Geese?



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Turn on

- Does it support:
  - Who?
    - Single person project
  - What?
    - Language
  - Where?
    - GitHub/GitLab
    - Air gap server in your basement
- Why?

OpenSSF DevRel Community partnership

-call for Maintainers (PoC prep)

- Build out a generic OSS security presentation deck with notes that can be used by anyone to raise awareness (e.g. local DevOps Days)

https://github.com/ossf/DevRel-community
https://github.com/ossf/DevRel-community/issues/36

PoC

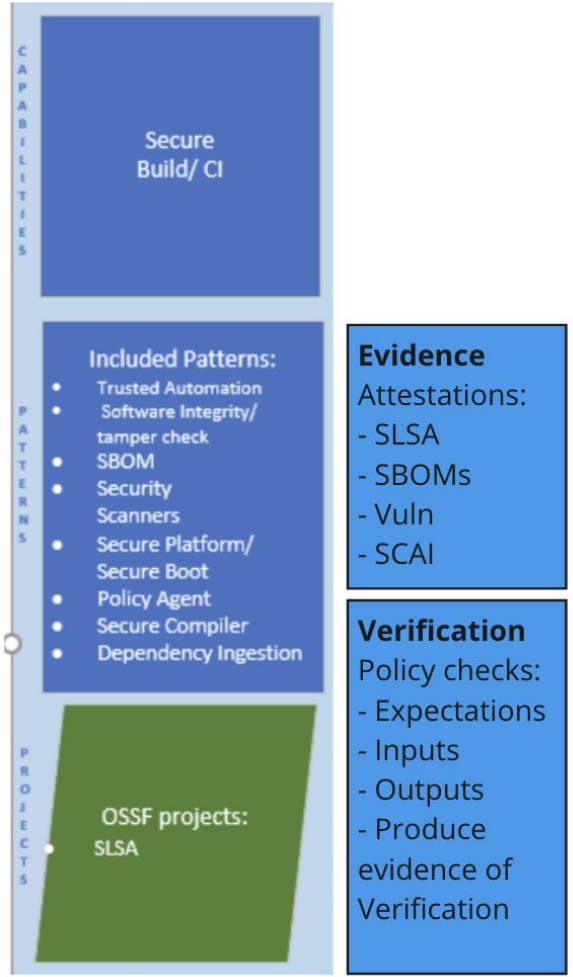
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Goals

- Understand the needs of **maintainers**
  - Blockers in them adopting OpenSSF security tooling and best practices?
  - Why won't they adopt Scorecards?
  - Why won’t they generate SBOMs?
- Understand the needs of **end users**
  - How can they safely consume open source software?
  - What information do they need?
    - What do they keep asking of OSS maintainers?
- Understand where there are gaps in open source security frameworks, tools, etc., intended to secure production, distribution, and consumption of open source software

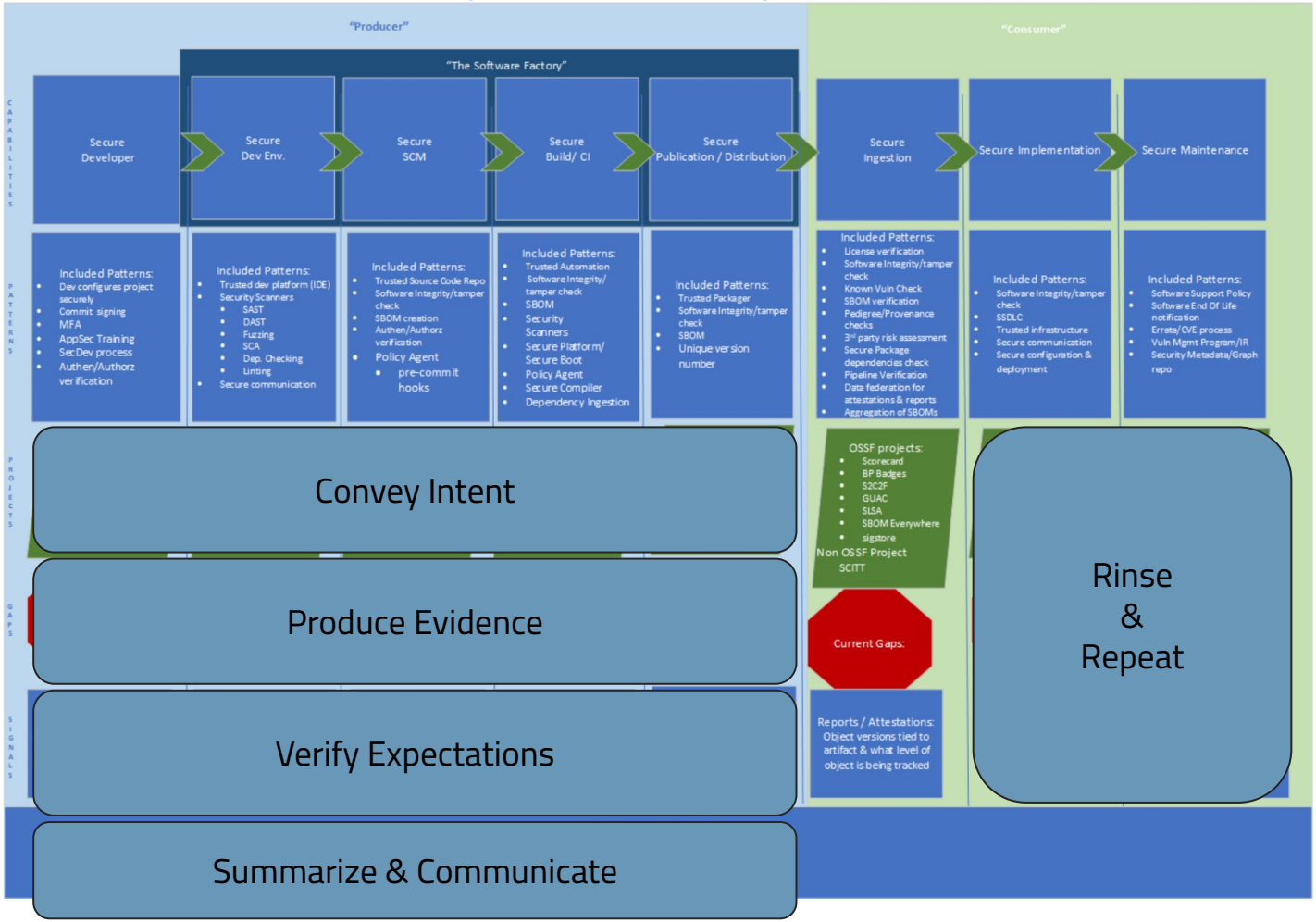
API for Needs?

- Start with one “stovepipe”
- Define intent
- Do “the thing”
- Generate evidence
- Verify expectations
- Aggregate all of the stovepipes.



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

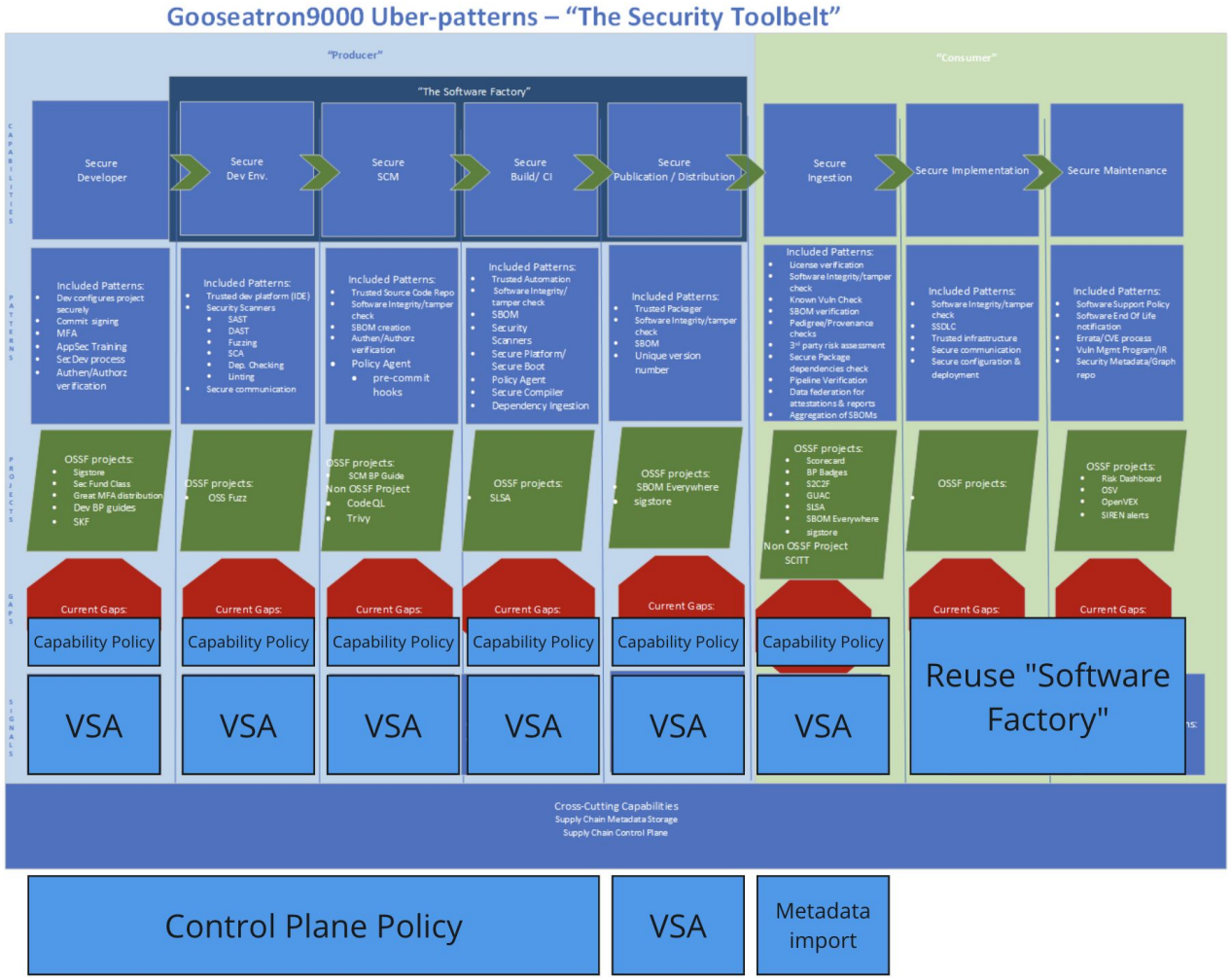
Gooseatron9000 Uber-patterns – "The Security Toolbelt"



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

in-toto

- Spec for evidence and policies
- Already used today in SLSA, SBOMit, and Gittuf
- Can communicate trust across boundaries w/ VSA



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Call to Action

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Contribute *asynchronously* to describe the OSS community and security outcomes

- Discussions
  - currently seeking input on high level security outcomes
    - Maintainers (bonus-round: what would Diana the Weekend Warrior say?)
    - Suppliers/consumers
- Building out a description of the OSS community and security outcomes
  - Personas
  - Use Cases
  - Threats
  - Capabilities
  - Patterns

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Contribute to a PoC to support making security outcomes easy for Diana the Weekend Warrior

- Looking for project maintainer volunteers!
  - https://github.com/ossf/toolbelt/issues/5
- Turn on any two tools!
  - Let us know how they (don't) work together
- "All problems in computer science can be solved by another level of indirection"
  - Defining the "Supply Chain Control Plane"
  - Defining the "Capability Intents"

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Contribute to a generic OSS Security presentation with speaker notes for distributed talks

- https://github.com/ossf/DevRel-community/issues/36

- Help build out generic OSS security presentation
- Enable anyone to give the presentation
- Distributed (e.g. local DevOps Days, BSides)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

- Join the OpenSSF Mailing List
- Follow us on Twitter
- Follow us on LinkedIn
- Follow us on Mastodon
- Follow us on Facebook
- Subscribe to our YouTube Channel
- Join a Working Group/Project
- Access the Public Meetings Calendar
- Participate on Slack
- Follow OpenSSF on GitHub
- Become an Organizational Member

Thank You

Security Toolbelt: https://github.com/ossf/toolbelt