

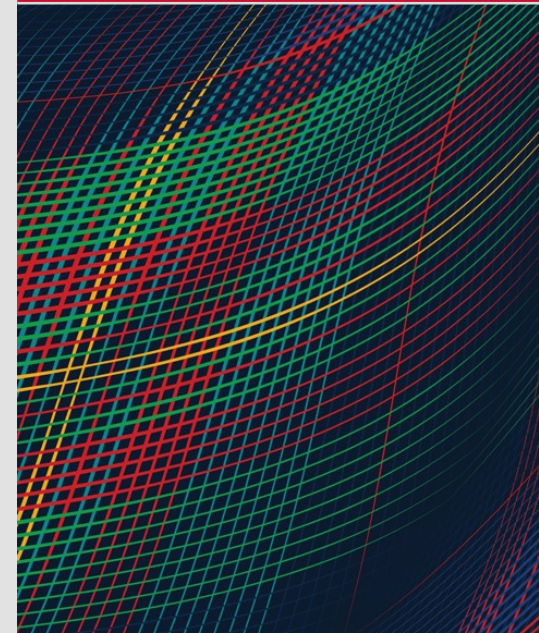
Vultron Update

APRIL 24, 2023

Allen Householder
Threat Ecosystem Analysis, CERT/CC
<https://infosec.exchange/@adh>

© 2023 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.



Copyright © 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

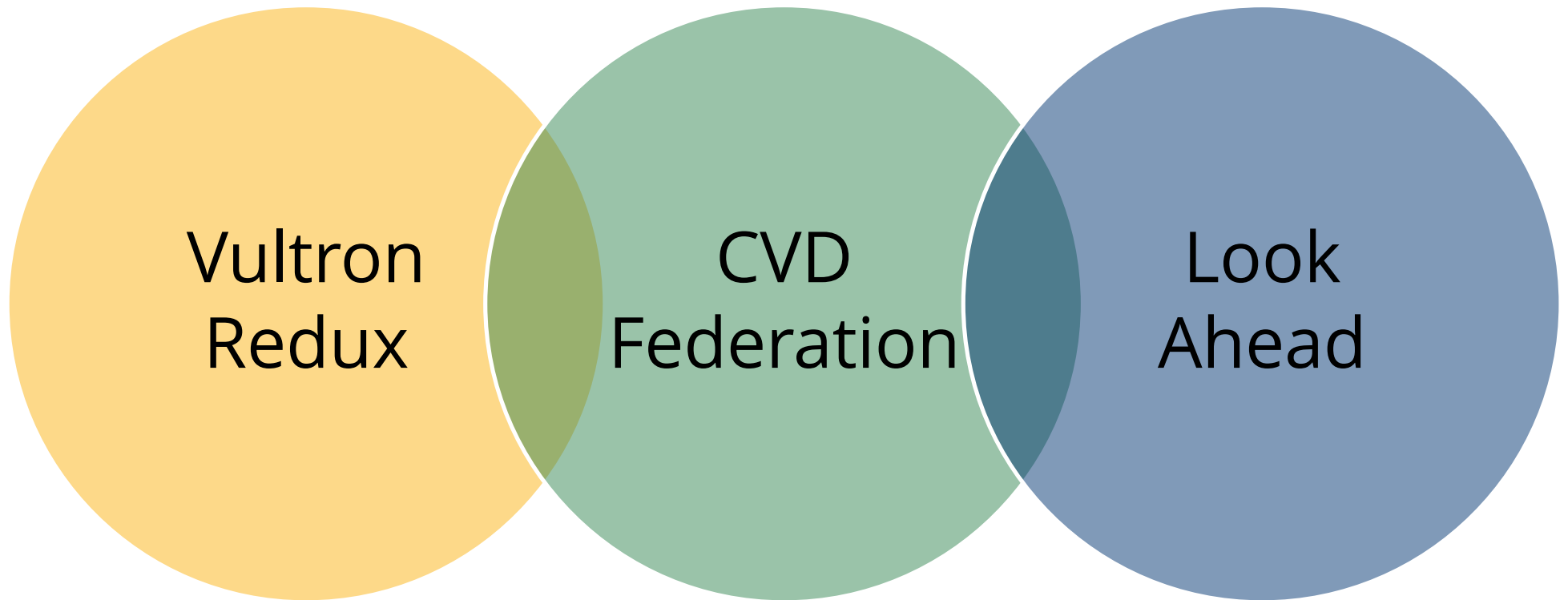
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0415

Agenda



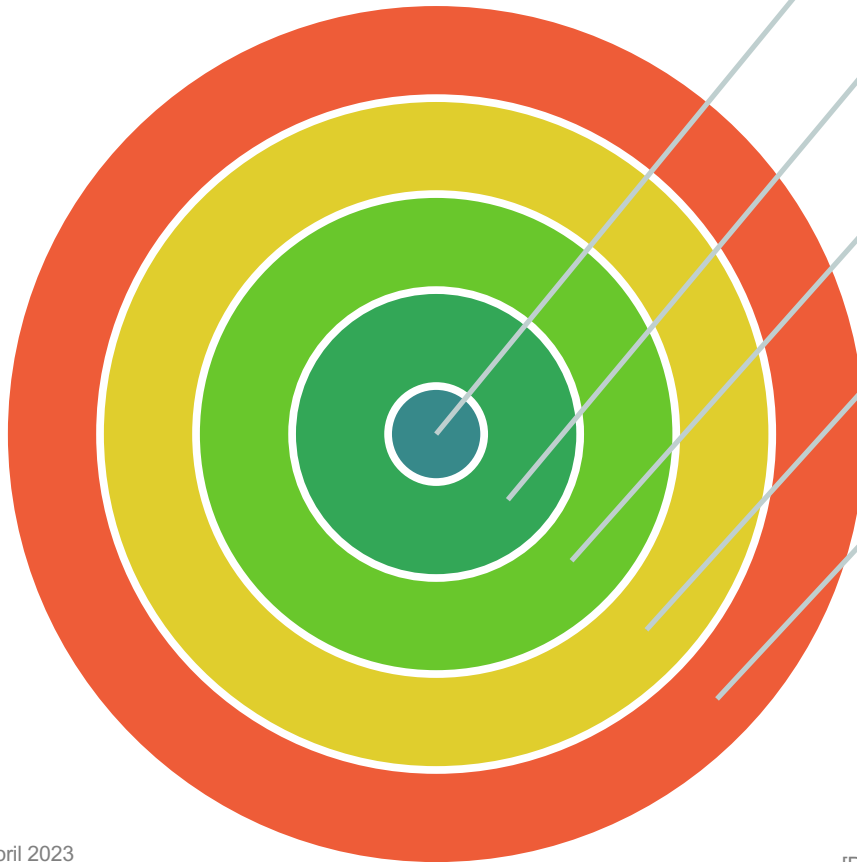
Vultron Update

What is Vultron?

**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Vultron: The Story So Far



CVD Process Description

CVD Guide

Process Models
(report, embargo, case)

Behavior Logic
(what to do when)

Vultron 0.4.0

Message Types
and Formats

Today

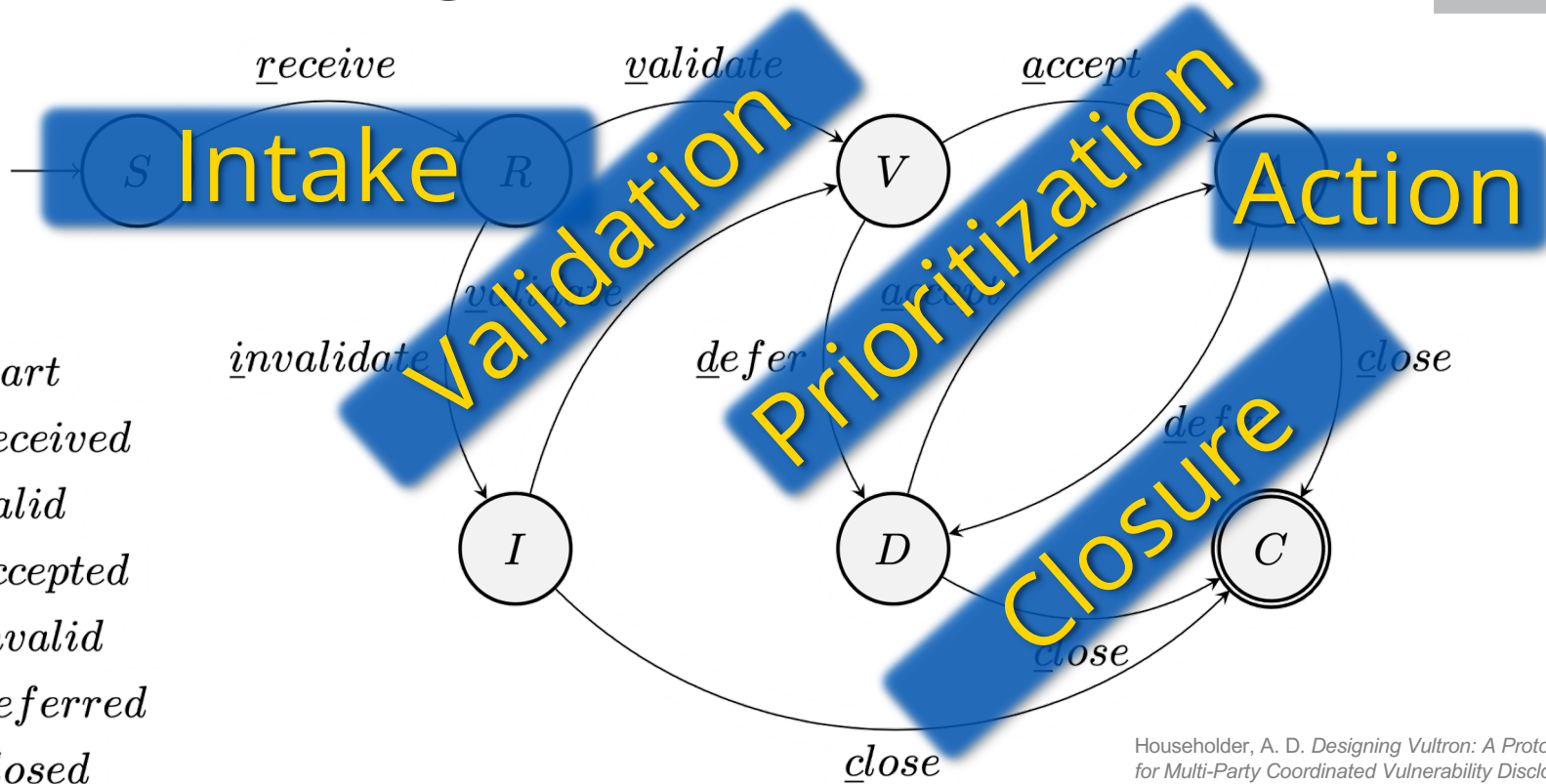
Reference API

Future

Report Management

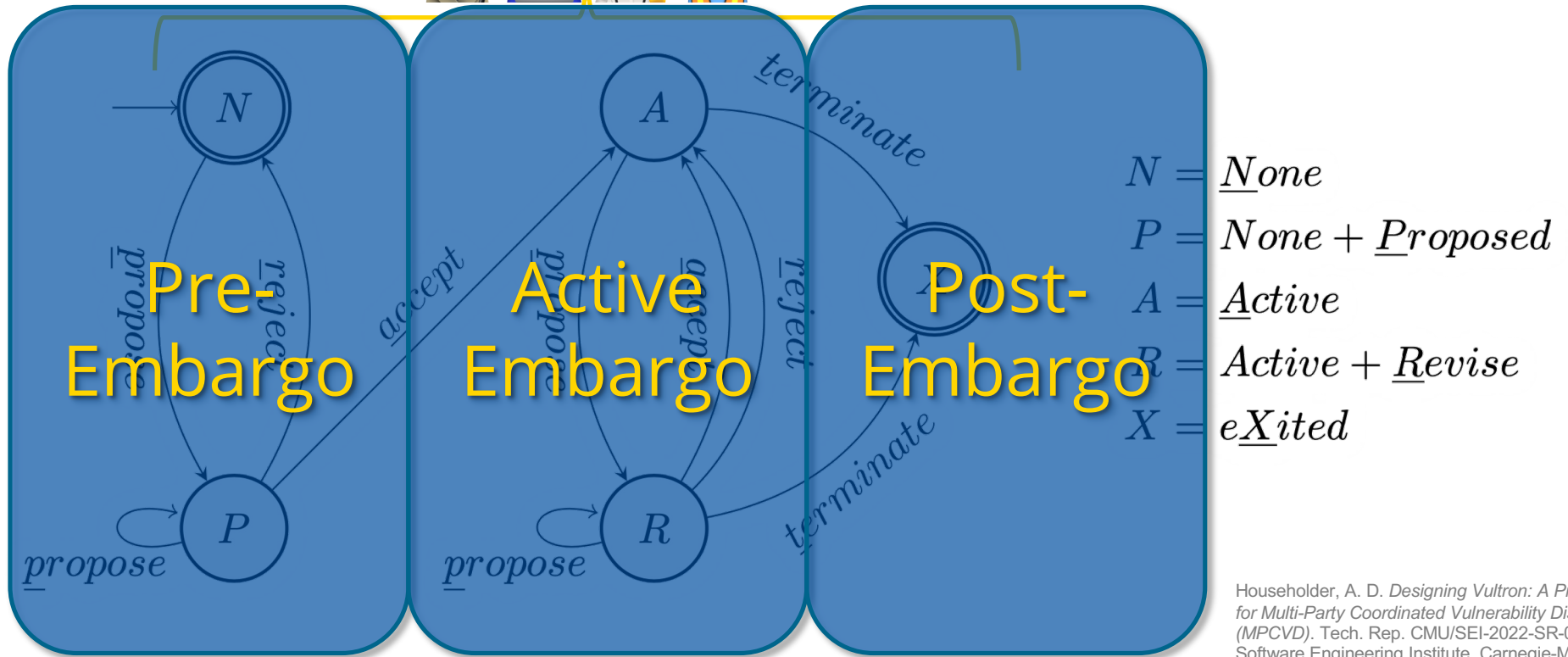


- S = Start*
- R = Received*
- V = Valid*
- A = Accepted*
- I = Invalid*
- D = Deferred*
- C = Closed*



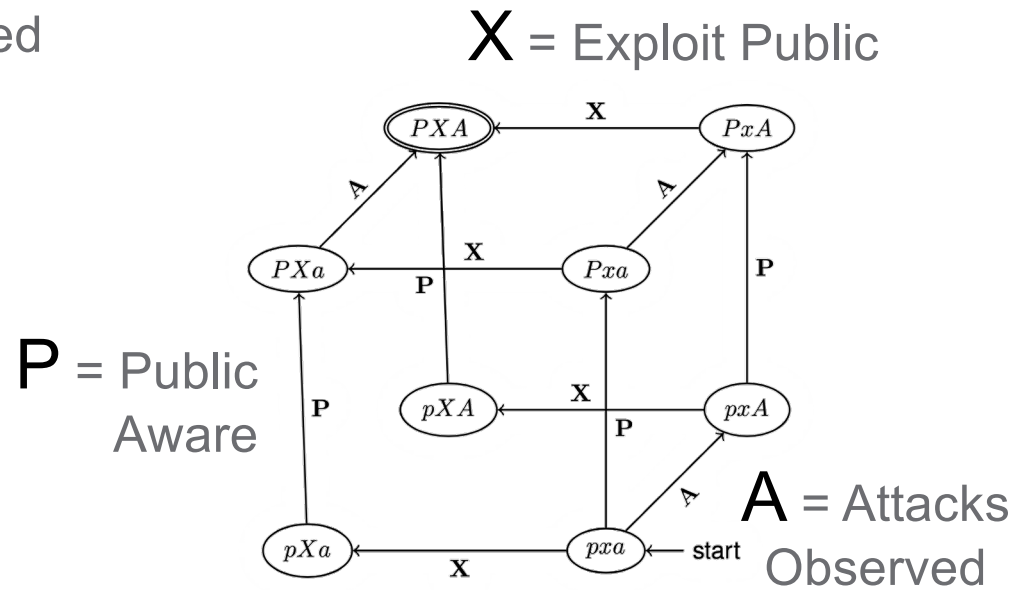
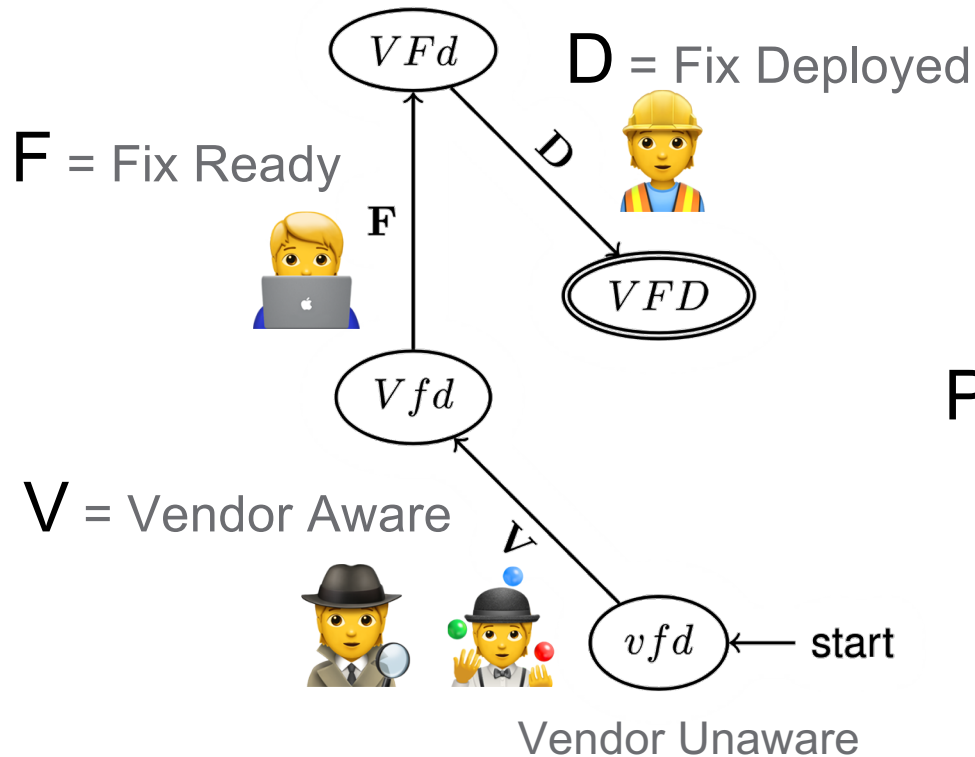
Householder, A. D. *Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Tech. Rep. CMU/SEI-2022-SR-012, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 2022.

Embargo Management



Householder, A. D. *Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Tech. Rep. CMU/SEI-2022-SR-012, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 2022.

Case State Model



Householder, A. D., and Jonathan Spring. *A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Tech. Rep. CMU/SEI-2021-SR-021, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 2021.

Case State Ordering Preferences

Vendor Aware,
Fix Ready,
Fix Deployed

...before...

Public Aware,
Exploit Public,
Attacks Observed

Householder, A. D., and Jonathan Spring. *A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Tech. Rep. CMU/SEI-2021-SR-021, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 2021.

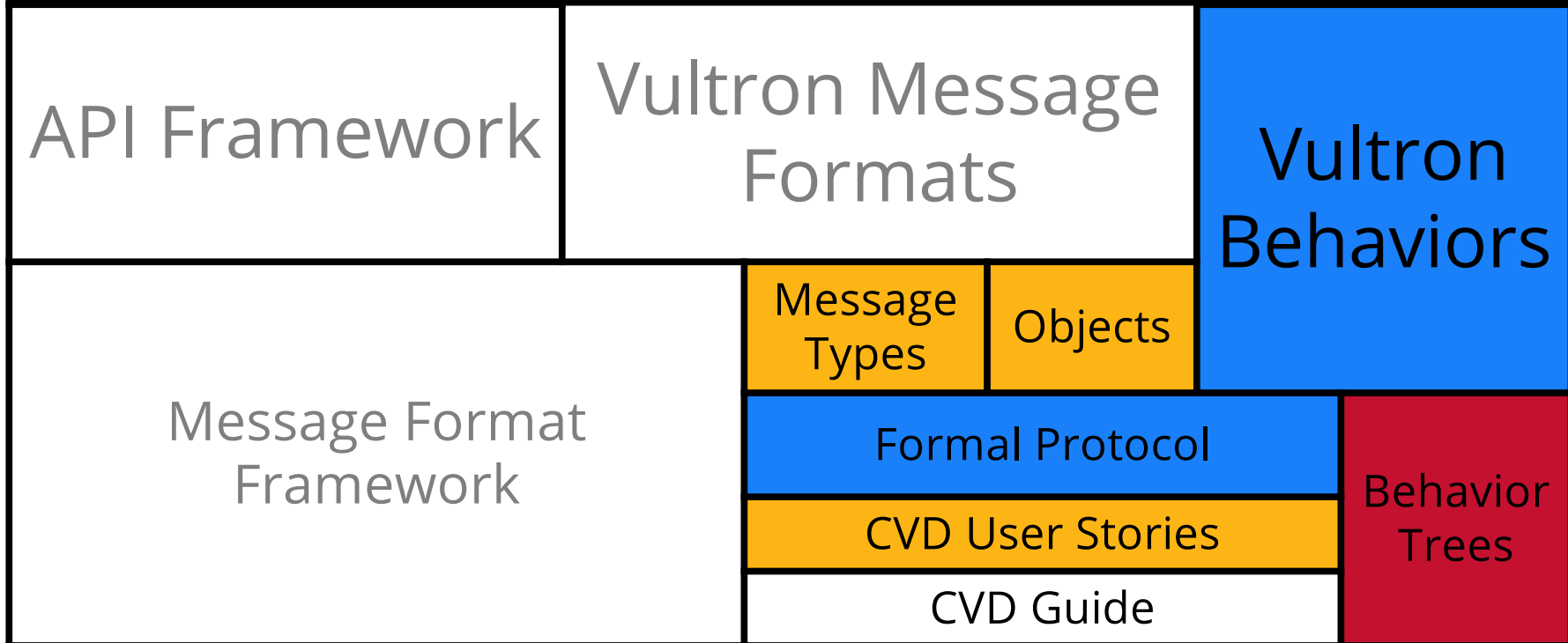
Vultron Message Types

Report Mgt

RS	Report Submission
RI	Report Invalid
RV	Report Valid
RA	Report Accepted
RD	Report Deferred
RC	Report Closed
RK	Report Ack
RE	Report Error

Householder, A. D. *Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Tech. Rep. CMU/SEI-2022-SR-012, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 2022.

Vultron API



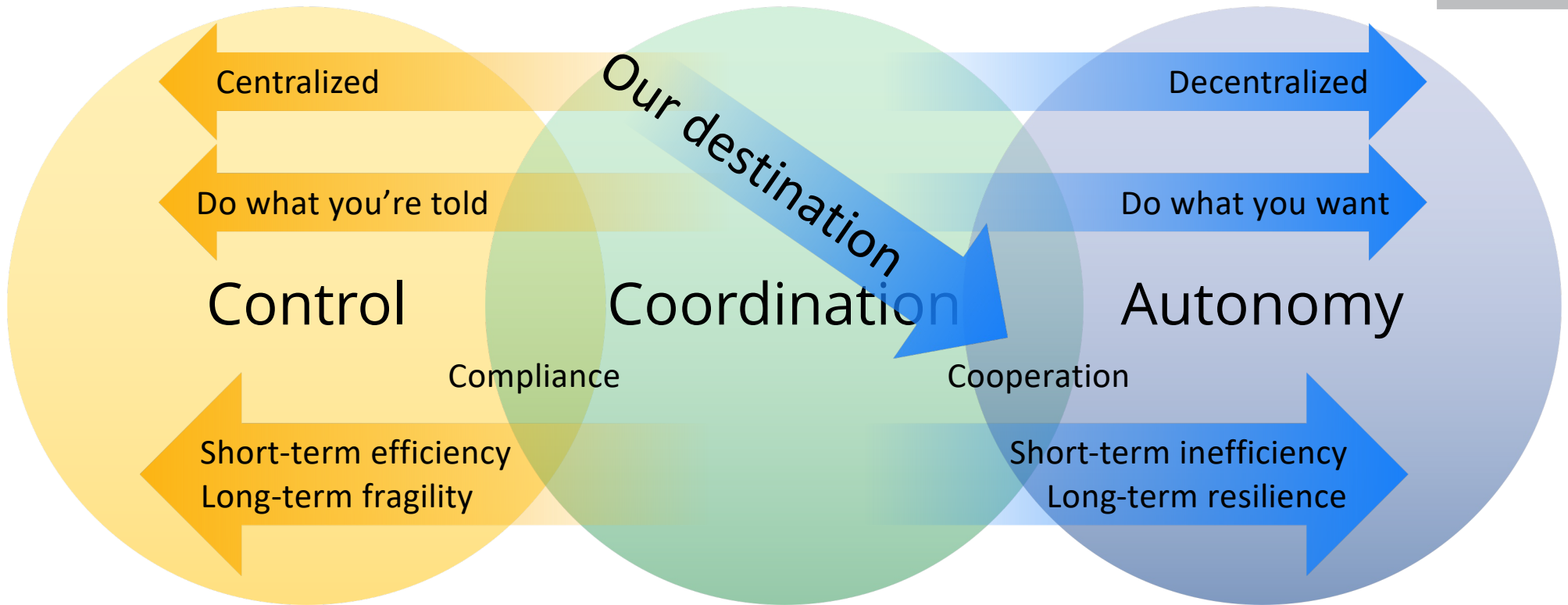
What we talked about last time...

Vultron Update

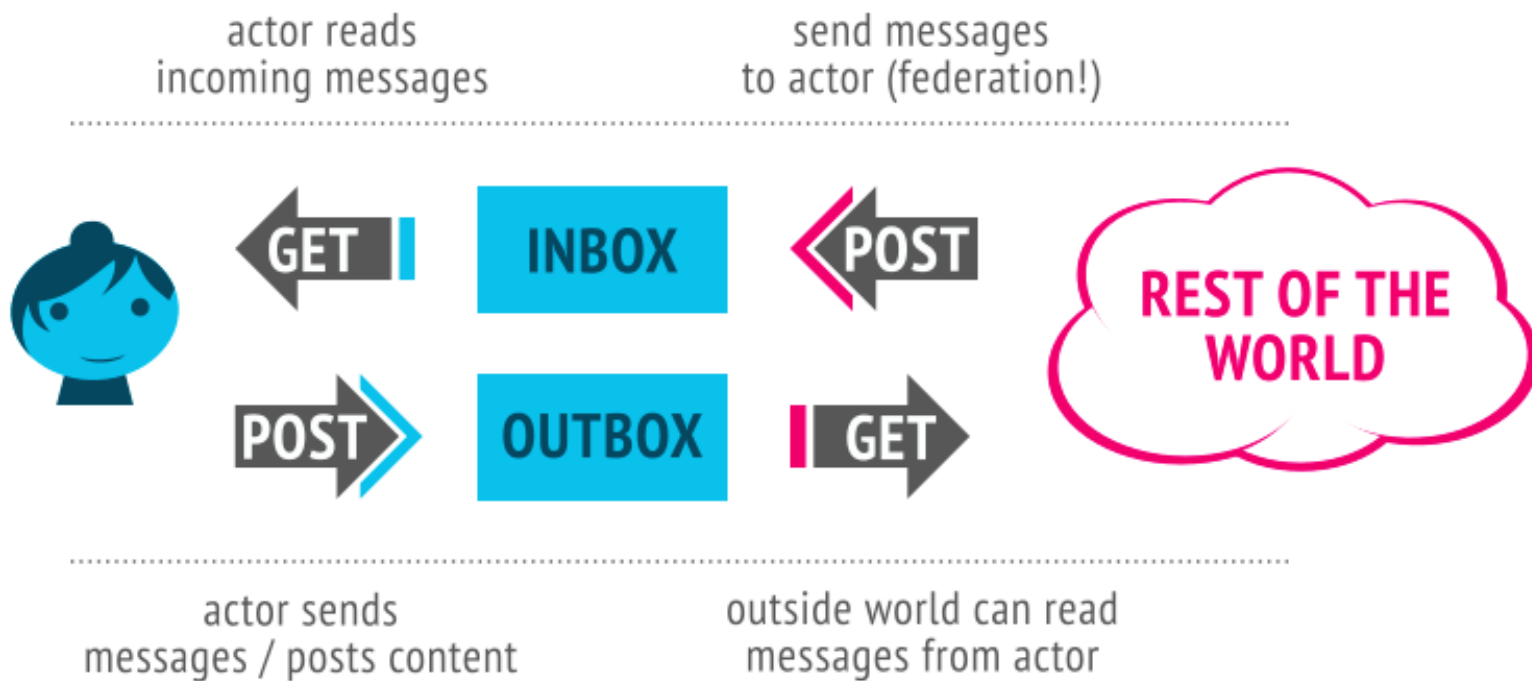
Forward the Federation

**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.



ActivityPub



<https://www.w3.org/TR/activitypub/>

Alyssa places a Note in her outbox



```
{"@context": "https://www.w3.org/ns/activitystreams",  
  "type": "Note",  
  "to": ["https://chatty.example/ben/"],  
  "attributedTo": "https://social.example/alyssa/",  
  "content": "Say, did you finish reading that book I lent you?"}
```

<https://www.w3.org/TR/activitypub/>

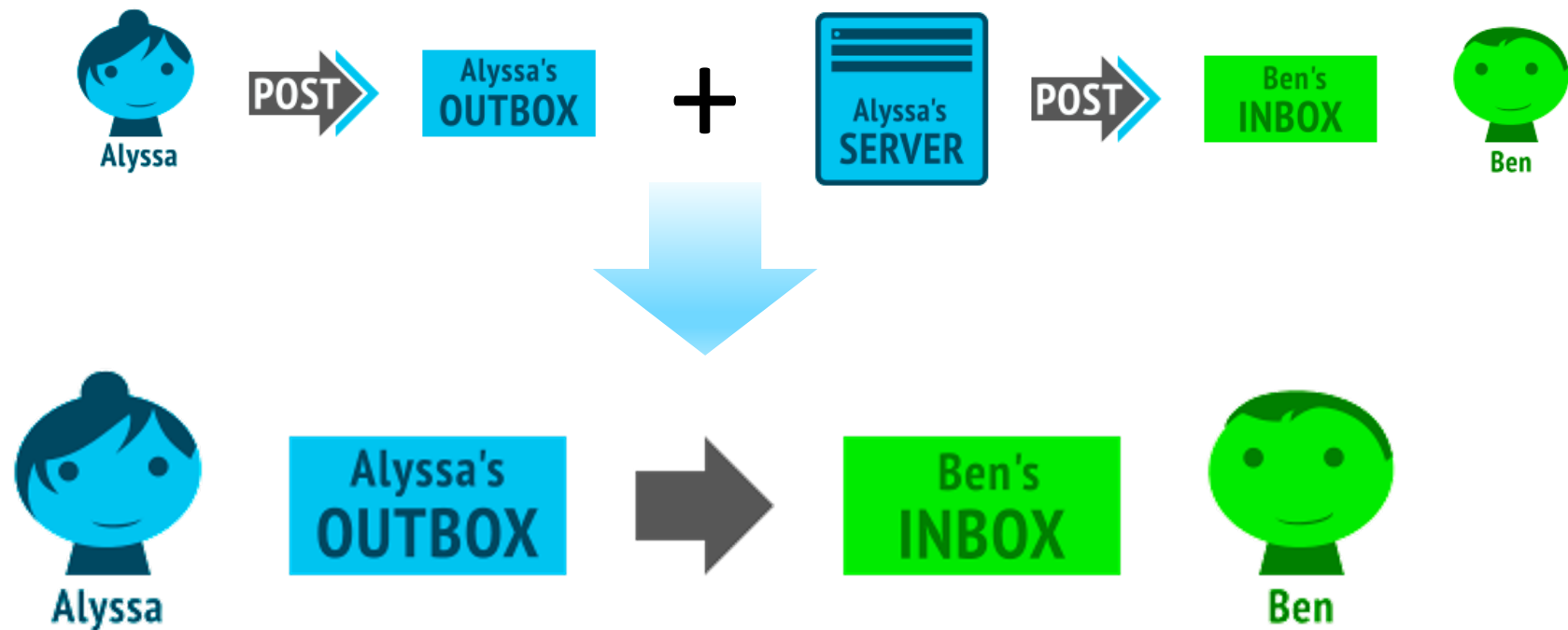
Alyssa's server wraps her Note in a Create activity and places it in Ben's Inbox



```
{ "@context": "https://www.w3.org/ns/activitystreams",  
  "type": "Create",  
  "id": "https://social.example/alyssa/posts/a29a6843-9feb-4c74-a7f7-081b9c9201d3",  
  "to": ["https://chatty.example/ben/"],  
  "actor": "https://social.example/alyssa/",  
  "object": { "type": "Note",  
              "id": "https://social.example/alyssa/posts/49e2d03d-b53a-4c4c-a95c-94a",  
              "attributedTo": "https://social.example/alyssa/",  
              "to": ["https://chatty.example/ben/"],  
              "content": "Say, did you finish reading that book I lent you?" } }
```

<https://www.w3.org/TR/activitypub/>

ActivityPub builds seamless distributed interaction via client-server and server-server



<https://www.w3.org/TR/activitypub/>

Ben replies to Alyssa with a Note

```
{"@context": "https://www.w3.org/ns/activitystreams",
  "type": "Create",
  "id": "https://chatty.example/ben/p/51086",
  "to": ["https://social.example/alyssa/"],
  "actor": "https://chatty.example/ben/",
  "object": {"type": "Note",
    "id": "https://chatty.example/ben/p/51085",
    "attributedTo": "https://chatty.example/ben/",
    "to": ["https://social.example/alyssa/"],
    "inReplyTo": "https://social.example/alyssa/posts/49e2d03d-b53a-4c4",
    "content": "<p>Argh, yeah, sorry, I'll get it back to you tomorrow.
      <p>I was reviewing the section on register machines,
        since it's been a while since I wrote one.</p>"}}}
```

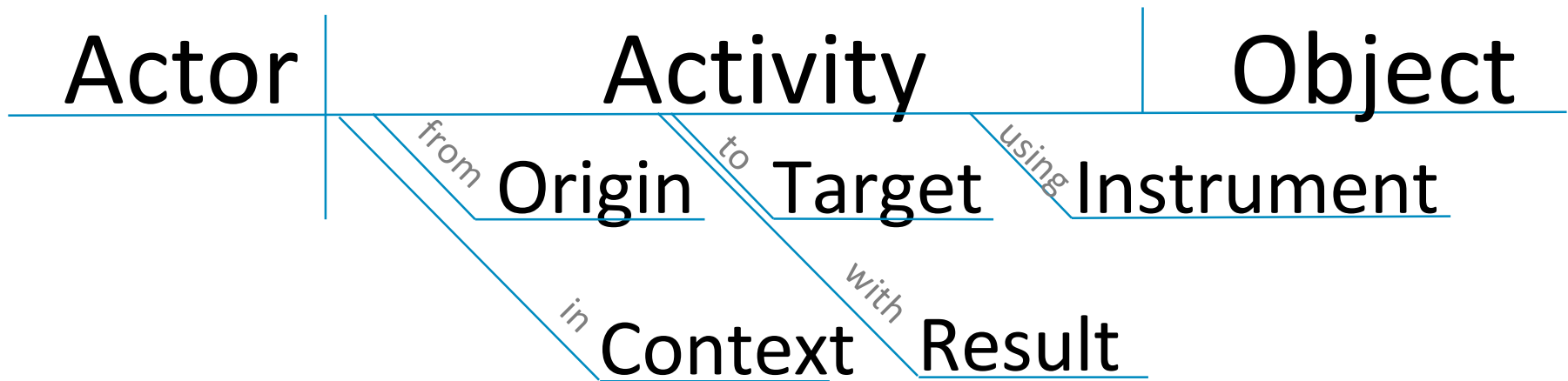
<https://www.w3.org/TR/activitypub/>

Alyssa Likes Ben's reply

```
{"@context": "https://www.w3.org/ns/activitystreams",  
  "type": "Like",  
  "id": "https://social.example/alyssa/posts/5312e10e-5110-42e5-a09b-934882b3",  
  "to": ["https://chatty.example/ben/"],  
  "actor": "https://social.example/alyssa/",  
  "object": "https://chatty.example/ben/p/51086"}
```

<https://www.w3.org/TR/activitypub/>

Activity Vocabulary brings sentence structure



Actor Types

Person	Represents an individual person.
Group	Represents a formal or informal collective of Actors.
Organization	Represents an organization.
Application	Describes a software application.
Service	Represents a service of any kind.

Activity Types

Offer, Invite

Accept, Reject

Add, Move, Remove

Like, Dislike

Follow, Ignore, Block

Announce

Leave, Travel, Arrive

Create, Update, Delete

Join, Leave

Read, View, Listen

Question

Undo

Object Types

Article

Audio

Document

Event

Image

Note

Page

Place

Profile

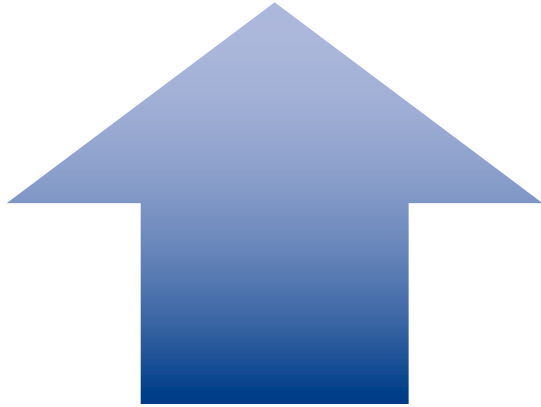
Relationship

Tombstone

Video

+ Actor types and Activity types

Activity Vocabulary is Extensible



All Objects, Actors,
Activities are extensible

- You can define arbitrary new types



Custom types might inhibit
interoperability

- Reuse existing types whenever possible

Vultron Update April 2023

Vultron + Activity Vocabulary Objects (Nouns)

**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Vultron + Activity Vocabulary: Actors

CVD participants are just *Actors**...



Finder/Reporters



Vendors



Coordinators



Deployers



Others

...they can be represented as

- Person

- Group

- Organization

- Application

- Service

Can a threat feed participate in a case? 💡

Can an **Application** be a **Deployer**? ✓



Can a **Service** be a **Coordinator**? ⚡

*Well, almost. We'll address how to represent their roles in different cases in a moment



```
"type": "Person",
  "id": "https://vuls.example.com/finder-reporter",
  "name": "Finn der Reporter",
```

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "Person",
  "id": "https://vuls.example.com/finder-reporter",
  "name": "Finn der Reporter",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "inbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/7346501d-c5e9-4b53-9835-e23de794557a",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "outbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/3a177852-2739-4b45-9ae4-cef7a8752e19",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "following": null,
  "followers": null,
  "liked": null,
  "streams": null,
  "preferredUsername": null,
  "endpoints": null
}
```



```
"type": "Organization",
  "id": "https://vendor.example/psirt",
  "name": "Vendor 0'Product",
```

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "Organization",
  "id": "https://vendor.example/psirt",
  "name": "Vendor 0'Product",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "inbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/498b6ab6-9ac2-4557-b3fc-6ae5a8e4d367",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "outbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/d17cbe44-0cf0-440e-ad1b-32212c8c42c5",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "following": null,
  "followers": null,
  "liked": null,
  "streams": null,
  "preferredUsername": null,
  "endpoints": null
}
```




```
"type": "Organization",
  "id": "https://coordinators-r-us.example",
  "name": "Coordinators R Us",
```

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "Organization",
  "id": " https://coordinators-r-us.example",
  "name": "Coordinators R Us",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "inbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/498b6ab6-9ac2-4557-b3fc-6ae5a8e4d367",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "outbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/d17cbe44-0cf0-440e-ad1b-32212c8c42c5",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "following": null,
  "followers": null,
  "liked": null,
  "streams": null,
  "preferredUsername": null,
  "endpoints": null
}
```



```
"type": "Organization",
  "id": "https://weedyploy.example",
  "name": "Weedy Ploy Infrastructure",
```

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "Organization",
  "id": " https://weedyploy.example",
  "name": "Weedy Ploy Infrastructure",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "inbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/498b6ab6-9ac2-4557-b3fc-6ae5a8e4d367",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "outbox": {
    "@context": "https://www.w3.org/ns/activitystreams",
    "type": "OrderedCollection",
    "id": "https://for.example/d17cbe44-0cf0-440e-ad1b-32212c8c42c5",
    "published": "2023-04-07T13:58:54+00:00",
    "updated": "2023-04-07T13:58:54+00:00",
    "items": [],
    "current": 0
  },
  "following": null,
  "followers": null,
  "liked": null,
  "streams": null,
  "preferredUsername": null,
  "endpoints": null
}
```

Vultron + Activity Vocabulary: Objects

We're going to need a few customized objects...

- Vulnerability Report

No...the **Report** object is just a small wrapper object...

Are you suggesting yet another vul report format?

...that can contain a well-defined format like CSAF or just plain text

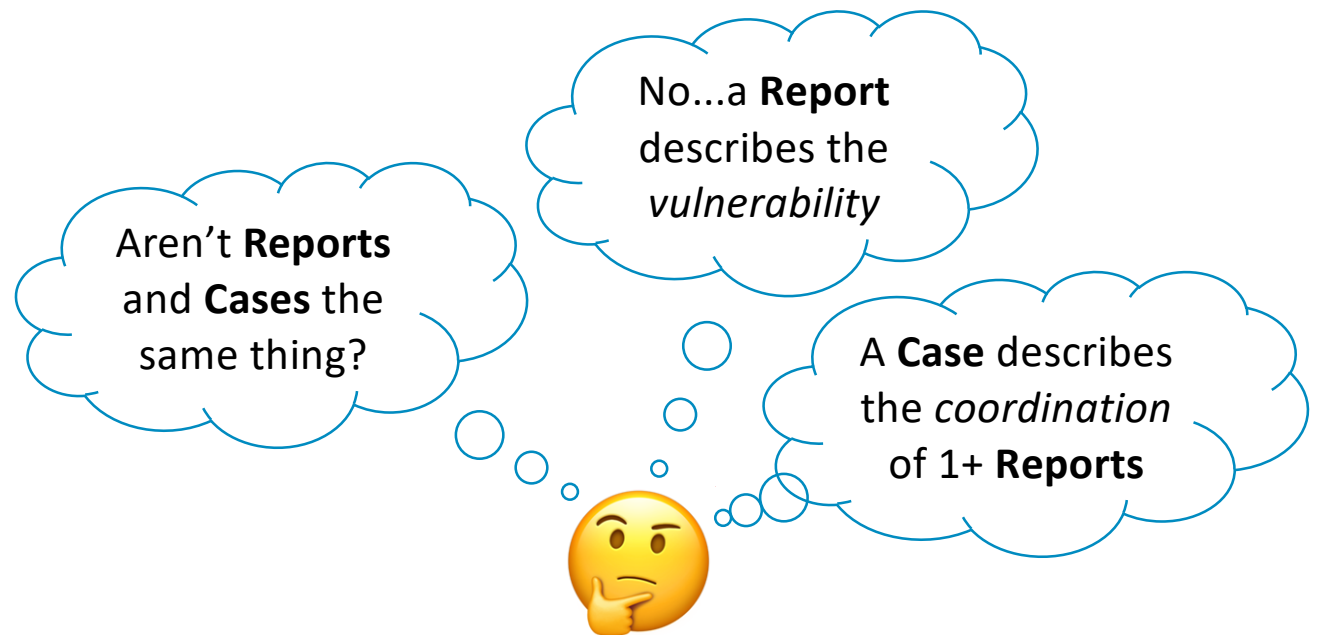


```
{  
  "@context": "https://www.w3.org/ns/activityst",  
  "type": "VulnerabilityReport",  
  "id": "https://finder.reporter.example/report",  
  "name": "finding-101029",  
  "published": "2023-04-07T18:22:56+00:00",  
  "updated": "2023-04-07T18:22:56+00:00",  
  "content": "I found a vulnerability!",  
  "attributedTo": [  
    "https://vuls.example.com/finder-reporter"  
  ]  
}
```

Vultron + Activity Vocabulary: Objects

We're going to need a few customized objects...

- Vulnerability Report
- Vulnerability Case



Report

```
{
  "@context":
    "https://www.w3.org/ns/activitystreams",
  "type": "VulnerabilityReport",
  "id":
    "https://finder.reporter.example/report/101029",
  "name": "finding-101029",
  "published": "2023-04-07T18:22:56+00:00",
  "updated": "2023-04-07T18:22:56+00:00",
  "content": "I found a vulnerability!",
  "attributedTo": [
    "https://vuls.example.com/finder-reporter"
  ]
}
```

Case

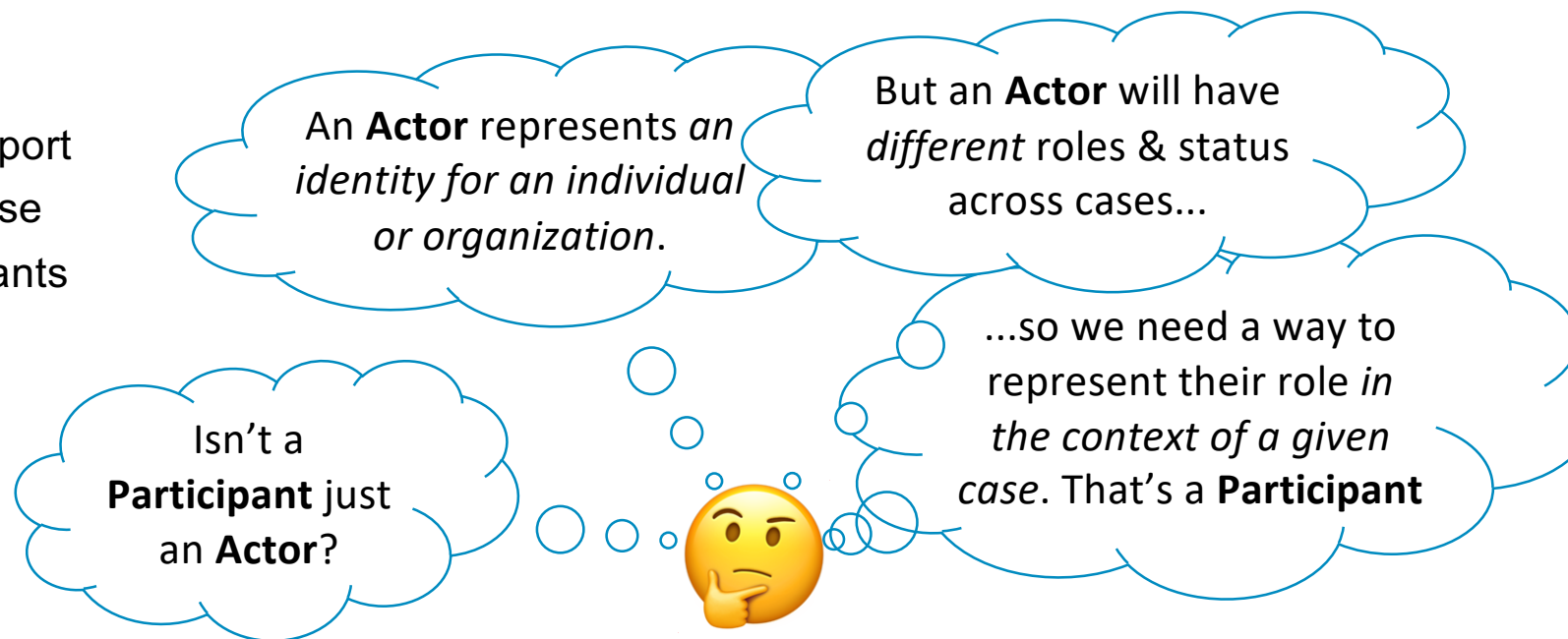
```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "VulnerabilityCase",
  "id": "https://vendor.example/psirt/case/18283771",
  "name": "vendor-case-18283771",
  "published": "2023-04-07T18:31:00+00:00",
  "updated": "2023-04-07T18:31:00+00:00",
  "attributedTo": "https://vendor.example/psirt",
  "caseParticipants": [...],
  "vulnerabilityReports": [
    "https://finder.reporter.example/report/101029"
  ],
  "caseStatus": [
    {
      "type": "CaseStatus",
      "id": "https://for.example/6d88fda5-d392-4c90-a77d-3209d5f2550a",
      "name": "EMBARGO_MANAGEMENT_NONE
CS_PUBLIC_UNAWARE__NO_EXPLOIT__NO_ATTACKS",
      "published": "2023-04-07T18:31:00+00:00",
      "emState": "EMBARGO_MANAGEMENT_NONE",
      "pxaState":
"CS_PUBLIC_UNAWARE__NO_EXPLOIT__NO_ATTACKS"
    }
  ],
  "activeEmbargo": null
}
```



Vultron + Activity Vocabulary: Objects

We're going to need a few customized objects...

- Vulnerability Report
- Vulnerability Case
 - Case Participants



Actor

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "Organization",
  "id": "https://vendor.example/psirt",
  "name": "Vendor 0'Product",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "inbox": {
    "type": "OrderedCollection",
    "id": "https://for.example/498b6ab6-9ac2-4557-b3fc-6ae5a8e4d367",
    "items": [],
    "current": 0
  },
  "outbox": {
    "type": "OrderedCollection",
    "id": "https://for.example/d17cbe44-0cf0-440e-ad1b-32212c8c42c5",
    "items": [],
    "current": 0
  },
  "following": null,
  "followers": null,
  "liked": null,
  "streams": null,
  "preferredUsername": null,
  "endpoints": null
},
```

Participant

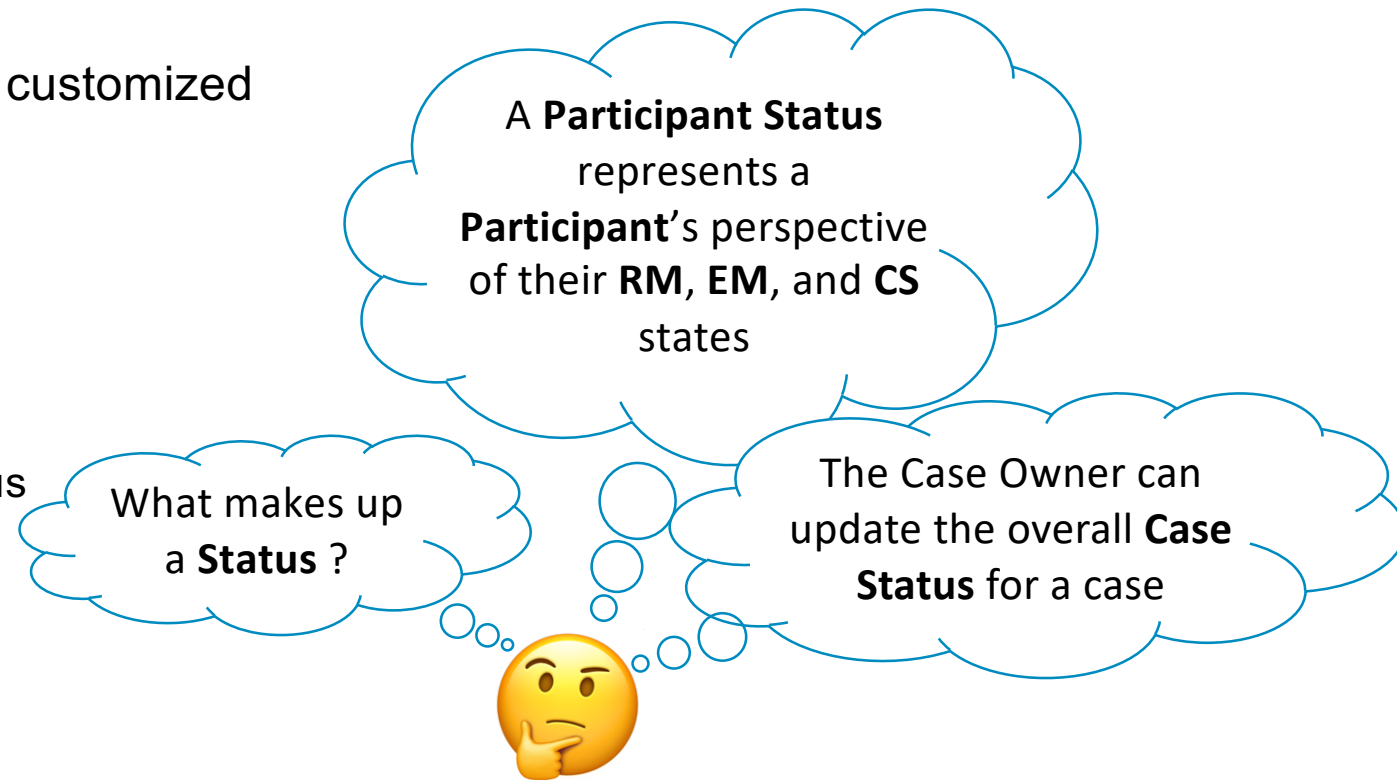
```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "CaseParticipant",
  "id": "https://for.example/9977b4dd-76b4-4727-9b24-f1b8d5adc2b0",
  "name": "Vendor 0'Product",
  "published": "2023-04-07T18:31:00+00:00",
  "updated": "2023-04-07T18:31:00+00:00",
  "actor": "https://vendor.example/psirt",
  "context": "https://vendor.example/psirt/case/18283771",
  "caseRoles": [
    "CVD_ROLE_VENDOR"
  ],
  "participantStatus": [...]
},
```



Vultron + Activity Vocabulary: Objects

We're going to need a few customized objects...

- Vulnerability Report
- Vulnerability Case
 - Case Participants
 - Case & Participant Status



Participant Status

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "ParticipantStatus",
  "id": "https://for.example/8ce1b298",
  "name": "REPORT_MANAGEMENT_RECEIVED
CS_VENDOR_AWARE__NO_FIX__NOT_DEPLOYED",
  "context": "https://vendor.example/psirt/case/18283771",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "actor": "https://vendor.example/psirt",
  "rmState": "REPORT_MANAGEMENT_RECEIVED",
  "vfdState": "CS_VENDOR_AWARE__NO_FIX__NOT_DEPLOYED",
  "caseEngagement": true,
  "embargoAdherence": true
}
```

Case Status

```
{
  "@context": "https://www.w3.org/ns/activitystreams",
  "type": "CaseStatus",
  "id": "https://for.example/adcc7597",
  "name": "EMBARGO_MANAGEMENT_NONE
CS_PUBLIC_UNAWARE__NO_EXPLOIT__NO_ATTACKS",
  "context": "https://vendor.example/psirt/case/18283771",
  "published": "2023-04-07T13:58:54+00:00",
  "updated": "2023-04-07T13:58:54+00:00",
  "emState": "EMBARGO_MANAGEMENT_NONE",
  "pxaState": "CS_PUBLIC_UNAWARE__NO_EXPLOIT__NO_ATTACKS"
}
```

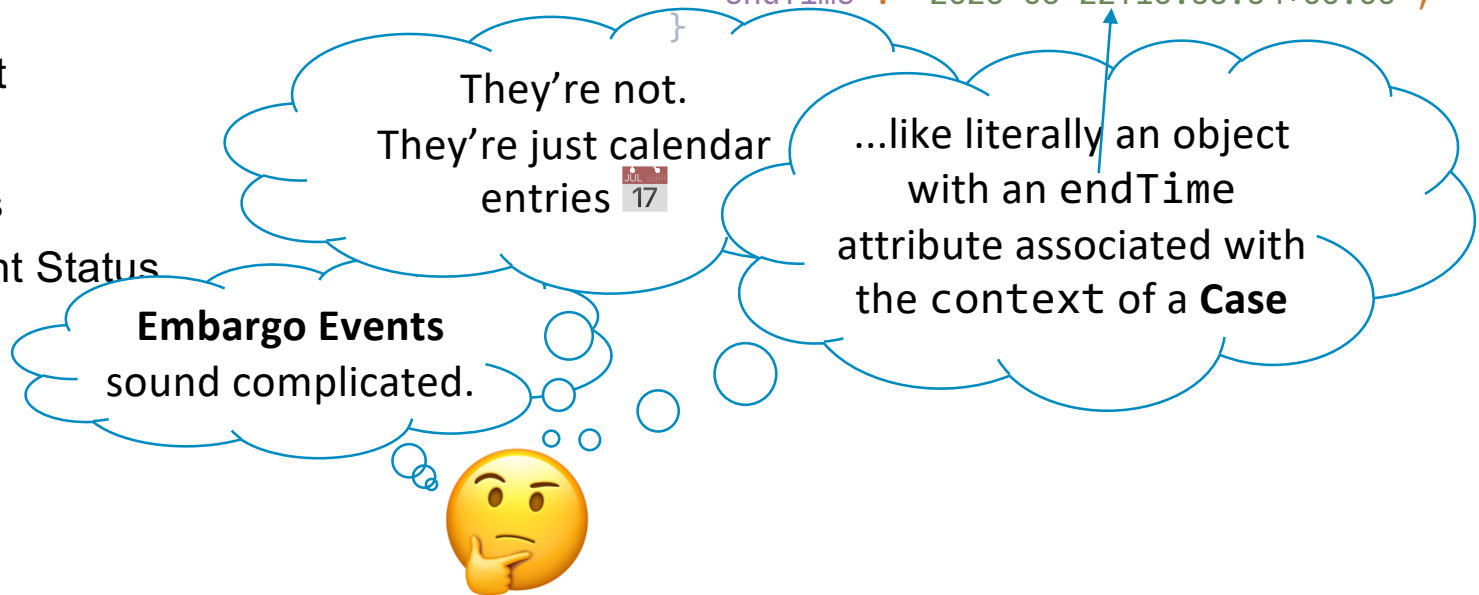


Vultron + Activity Vocabulary: Objects

We're going to need a few customized objects...

```
{
  "@context": "https://www.w3.org/ns/activityst
  "type": "EmbargoEvent",
  "id": "https://for.example/86caf69a",
  "name": "Embargo for https://vendor.example/c
  "context": "https://vendor.example/case/18283
  "startTime": "2023-04-07T13:58:54+00:00",
  "endTime": "2023-05-22T13:58:54+00:00",
}
```

- Vulnerability Report
- Vulnerability Case
 - Case Participants
 - Case & Participant Status
 - Embargo Events



Vultron Update April 2023

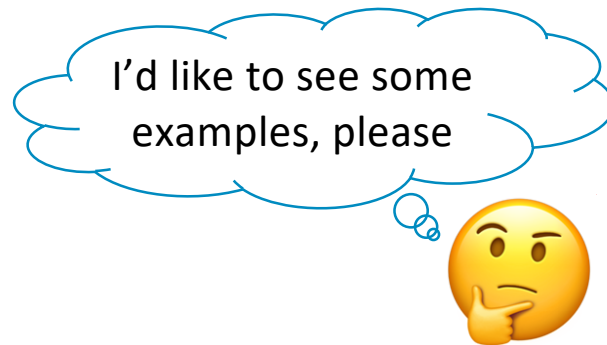
Vultron + Activity Vocabulary Verbs



**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Turns out most of the verbs (Activities) defined in the vocabulary are good enough for most of what we need.

There are a few where we need to clarify semantics.





 **Offer**  **this
Vulnerability Report**



 **Read the
Vulnerability Report**



 Offer  this
Vulnerability Report



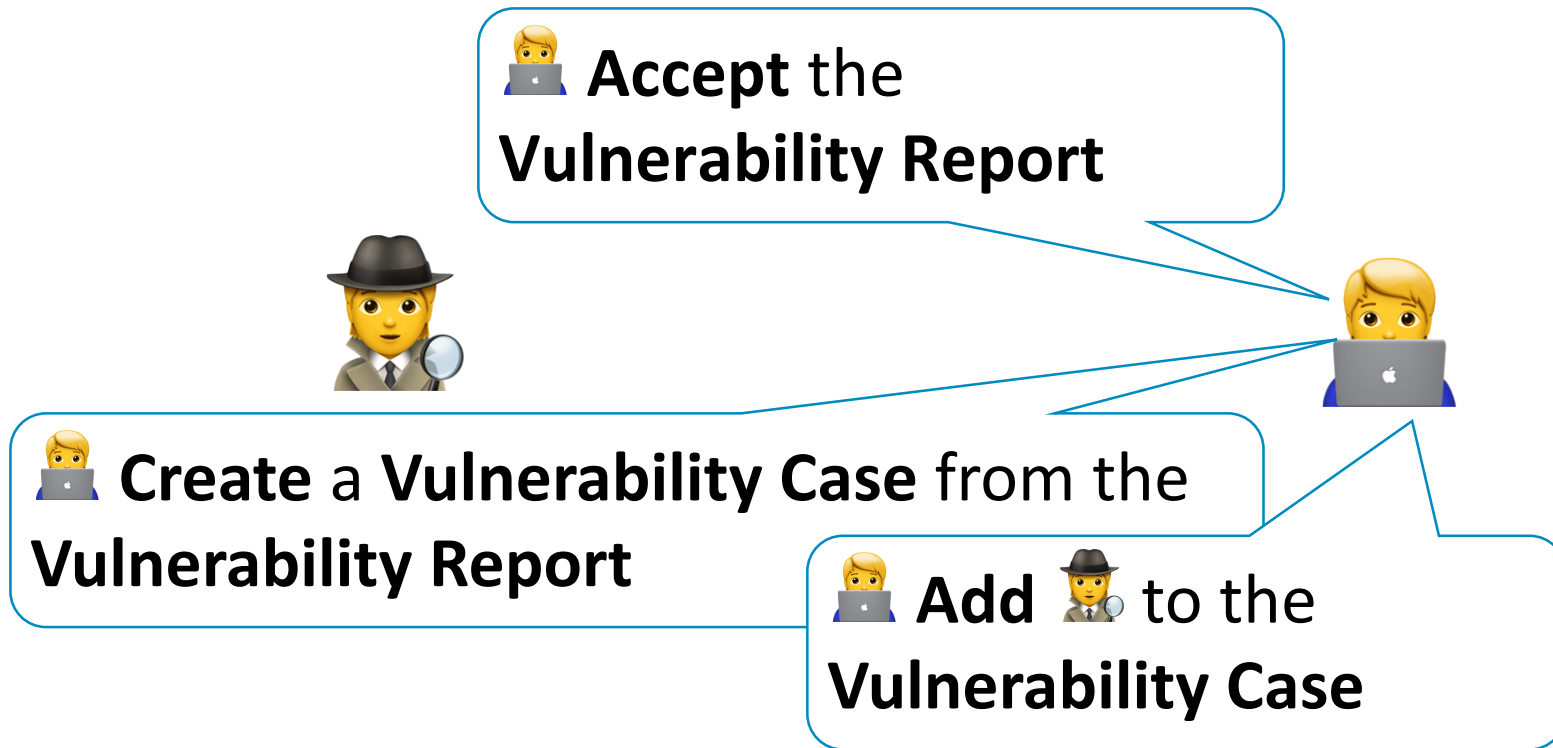
```
"@context": "https://www.w3.org/ns/activitystreams",  
"asType": "Offer",  
"id": "https://for.example/a2d22497-67b8-4893-9bba-51e1b72ccc4d",  
"name": "https://vuls.example.com/finder-reporter Offer https://finder.  
https://vendor.example/psirt",  
"published": "2023-04-17T19:34:46+00:00",  
"updated": "2023-04-17T19:34:46+00:00",  
"to": [  
  "https://vendor.example/psirt"  
],  
"actor": "https://vuls.example.com/finder-reporter",  
"target": "https://vendor.example/psirt",  
"object": "https://finder.reporter.example/report/101029"  
}
```




```
{  
  "@context": "https://www.w3.org/ns/activitystreams",  
  "asType": "Read",  
  "id": "https://for.example/6a21c203-18cf-499f-bd3f-0614b597dcb1",  
  "name": "https://vendor.example/psirt Read  
https://finder.reporter.example/report/101029",  
  "published": "2023-04-17T19:34:46+00:00",  
  "updated": "2023-04-17T19:34:46+00:00",  
  "to": [  
    "https://vuls.example.com/finder-reporter"  
  ],  
  "actor": "https://vendor.example/psirt",  
  "object": "https://finder.reporter.example/report/101029"  
}
```



**Read the
Vulnerability Report**




 **Create a Note to the Vulnerability Case**



 **Create a new Status**
(indicating that  has a fix ready) to the **Vulnerability Case.**




 **Close (Leave) the Vulnerability Case**



 **Offer**  **Add**  to the
Vulnerability Case

 **Join the
Vulnerability Case**


 **Accept the
Vulnerability Report**





 **Create a Vul**
from the Vulne

 **Invite**  to the
Vulnerability Case



 **Reject (decline) the Vulnerability Case**

 **Invite**  **to the Vulnerability Case**

Report Management Message Types

	Activity	Object	Indirect Object(s)
RS	Offer	Vulnerability Report	Target: Actor
	Invite	Actor	Target: Vulnerability Case
RI	Invalidate (Reject)	Vulnerability Report	
	Invalidate (Reject)	Vulnerability Case	
RV	Validate (Accept)	Vulnerability Report	
	Validate (Accept)	Vulnerability Case	
RA	Engage (Join)	Vulnerability Case	
RD	Defer (Leave)	Vulnerability Case	
RC	Close (Leave)	Vulnerability Case	
RK	Read	Vulnerability Case	
RE	Create	Note	Target: Vulnerability Case



Embargo Management Message Types

	Activity	Object	Indirect Object(s)
EP	Offer/Invite	Embargo Event	Context: Report or Case Target: Case (as appropriate)
ER	Reject	Embargo Event	
EA	Accept	Embargo Event	
	Add	Embargo Event	
EV	Offer/Invite	Embargo Event	
EJ	Reject	Embargo Event	
EC	Accept	Embargo Event	
ET	Terminate (???)	Embargo Event	
EK	Read	Embargo Event	
EE	Create	Note	Target: Vulnerability Case



Case State Message Types

	Activity	Object	Indirect Object(s)
CV	Create	Participant Status	Target: Participant Context: Case
CF			
CD			
CP	Create	Case Status	Target: Participant or Case Context: Case
CX			
CA			
CK	Read	Status	
CE	Create	Note	Target: Case



General Inquiry Message Types

	Activity	Object	Indirect Object(s)
GI	Create	Note	Target: Case Context: Case
GK	Read	Note	Context: Case
GE	Create	Note	Target: Case Context: Case

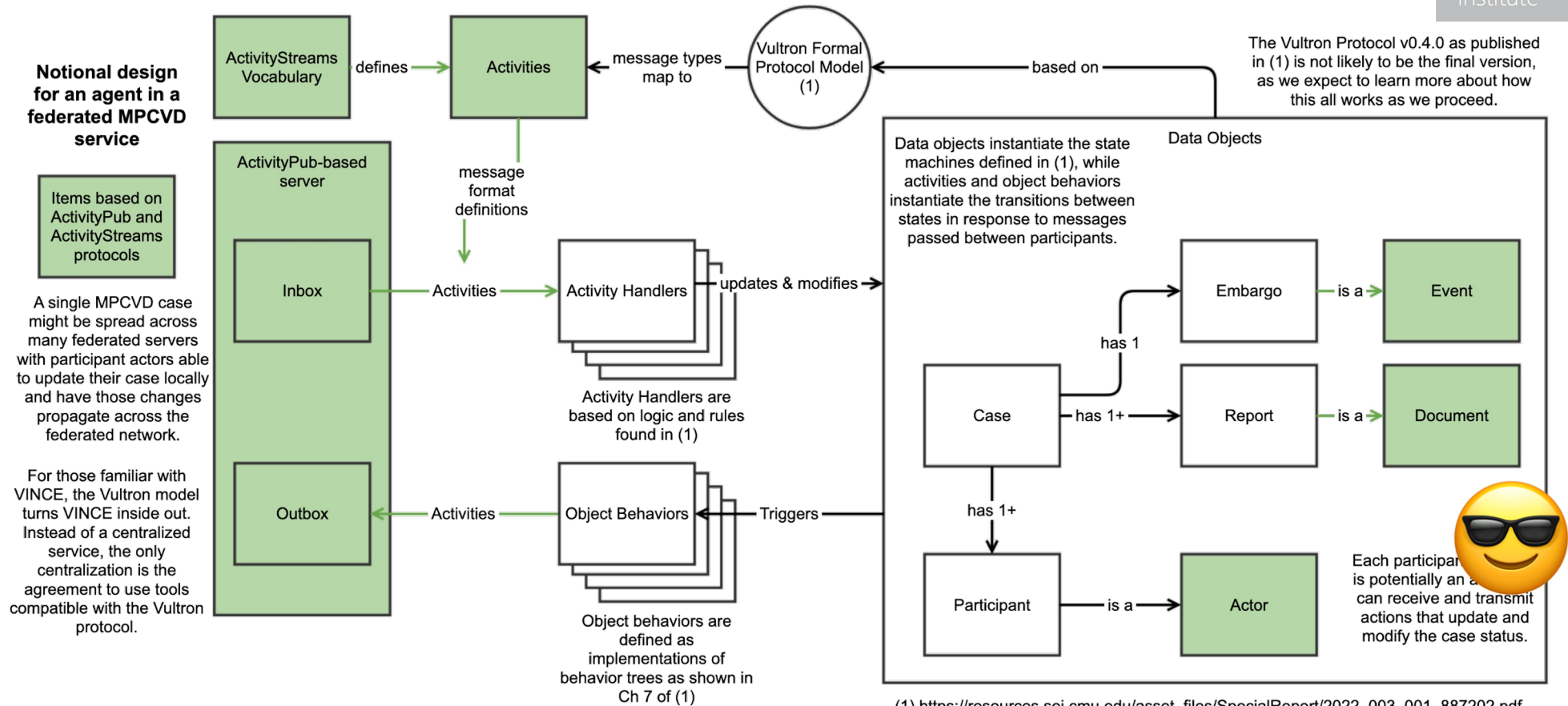


Activity Vocabulary opens up possible expansions to things Vultron 0.4.0 left out:

- Ownership transfer of cases
- Suggesting new case participants
- Polling case participants (e.g., about Embargo changes)
- Probably more we haven't thought of yet



Vultron Notional Architecture



(1) https://resources.sei.cmu.edu/asset_files/SpecialReport/2022_003_001_887202.pdf

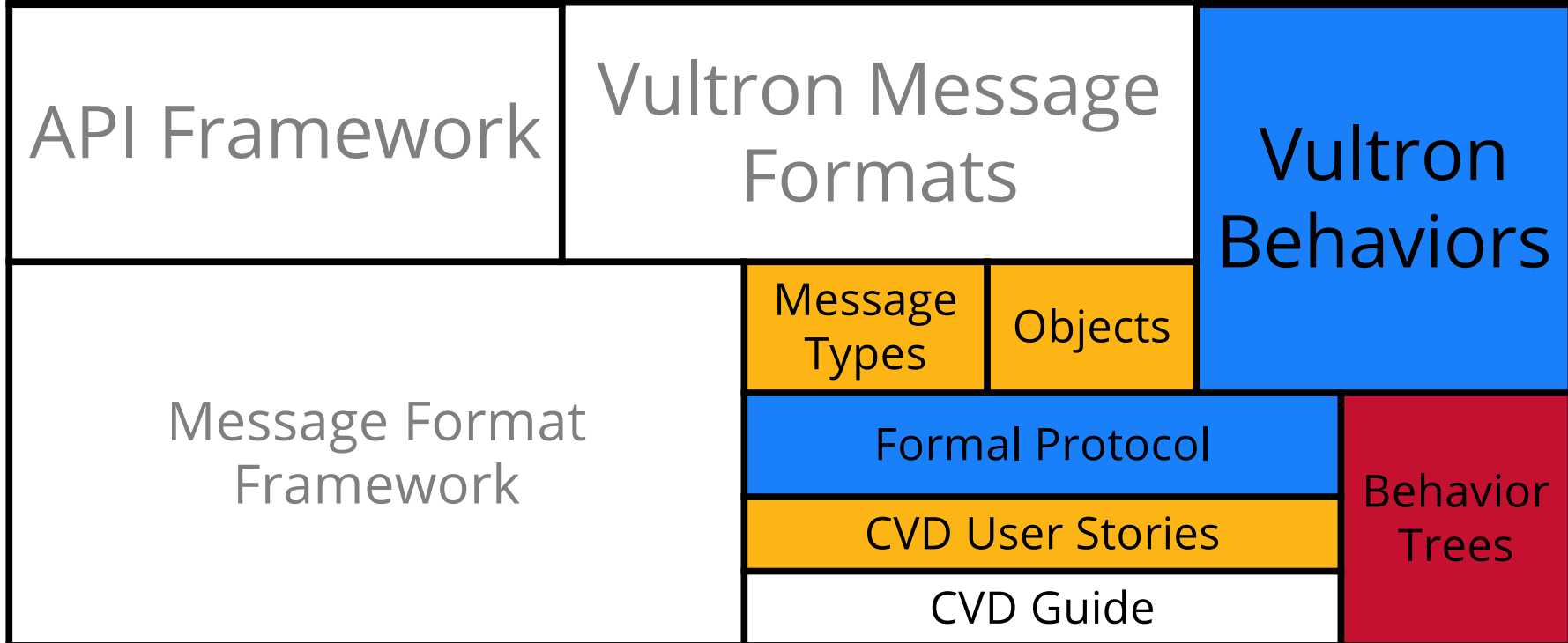
Vultron Update April 2023

Looking Ahead

**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Vultron API

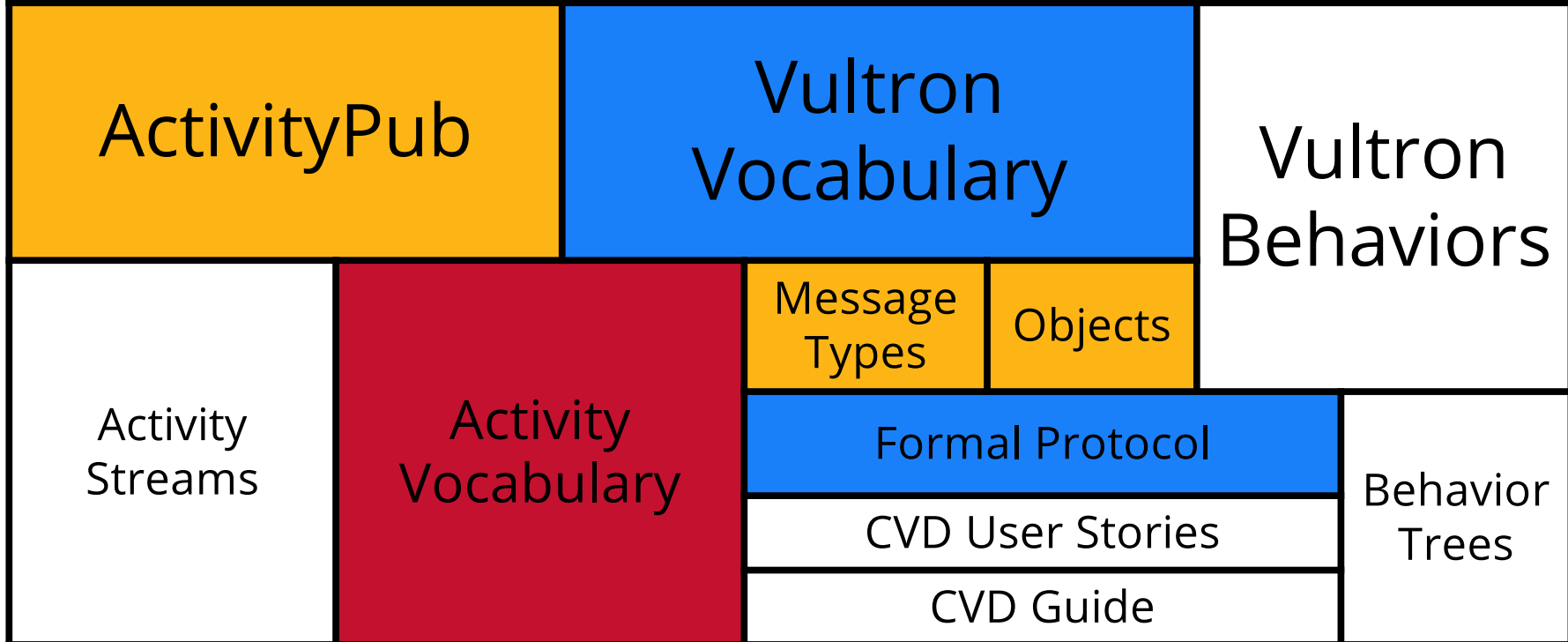


What we talked about last time...

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887198>

<https://youtu.be/8WiSmhxJ2OM>

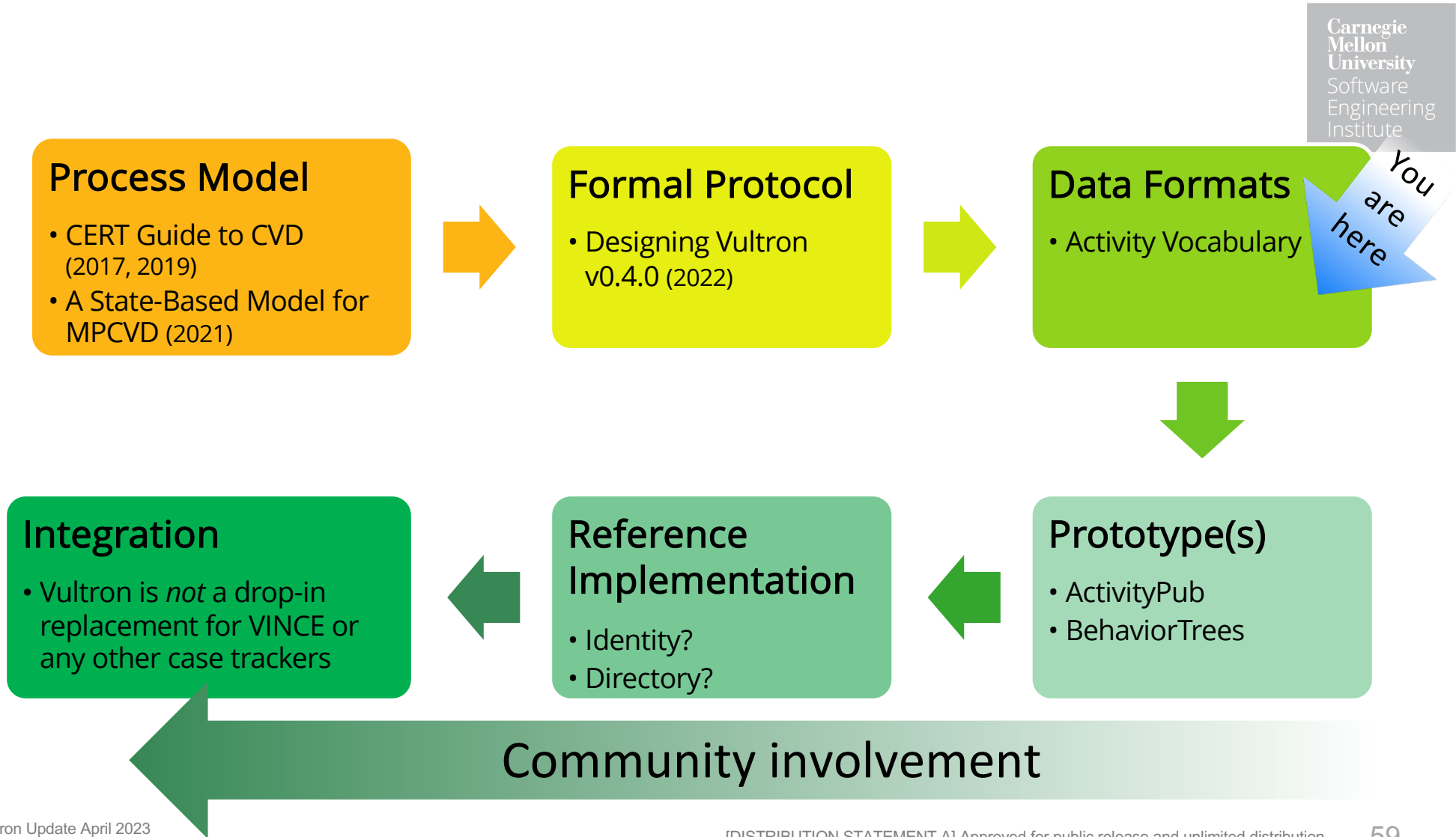
Vultron API



<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887198>

What I talked about today...

<https://github.com/CERTCC/Vultron>



You are here

What you can do next

- ✓ Ask Questions
- ✓ Read the report
- ✓ Watch the video
- ✓ Follow the work on Github

<https://youtu.be/8WiSmhxJ2OM>

<https://github.com/CERTCC/Vultron>

https://resources.sei.cmu.edu/asset_files/SpecialReport/2022_003_001_887202.pdf

Links

Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD) (Vultron v0.4.0) CMU/SEI-2022-SR-012

https://resources.sei.cmu.edu/asset_files/SpecialReport/2022_003_001_887202.pdf

Coordinated Vulnerability Disclosure User Stories

https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_887270.pdf

A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)
CMU/SEI-2021-SR-021

https://resources.sei.cmu.edu/asset_files/SpecialReport/2021_003_001_737890.pdf

CERT Guide to CVD CMU/SEI-2017-SR-022

<https://vuls.cert.org/confluence/display/CVD>

For further reading...

I didn't have time to talk about them today, but Vultron and much of my recent work on improving the Vulnerability Response Ecosystem relies on:

- Elinor Ostrom's Core Design Principles for managing common pool resources
- David Sloan Wilson et al's application of them into the group selection and evolution of organizations

Wilson, D.S., Philip, M.M., MacDonald, I.F. *et al.* Core design principles for nurturing organization-level selection. *Sci Rep* **10**, 13989 (2020). <https://doi.org/10.1038/s41598-020-70632-8>

“It was long unanimously held among economists that natural resources that were collectively used by their users would be over-exploited and destroyed in the long-term. Elinor Ostrom disproved this idea by conducting field studies on how people in small, local communities manage shared natural resources, such as pastures, fishing waters, and forests. She showed that when natural resources are jointly used by their users, in time, rules are established for how these are to be cared for and used in a way that is both economically and ecologically sustainable.”

<https://www.nobelprize.org/prizes/economic-sciences/2009/ostrom/facts/>