Village Standards Sprint

Overviews of Standards and Subprojects


OCA
HDF
CACAO
CSAF/VEX
PACE
STIXSHIFTER
SADX
OPENC2
NIEM
STIX/TAXII
CAW
CYCLONEDX
TAC
SBOM
VSMI
KESTREL

Marlon Taylor &
Kartikey Desai

Supporting automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis

Quick Start

Charter

Define a **set of information representations and protocols** to address the need to model, analyze, and share cyber threat intelligence.

Define composable information sharing services for peer-to-peer, hub-and-spoke, and source subscriber **threat intelligence sharing models**

Develop formal models that **allow organizations to develop their own standards-based sharing** architectures to meet specific needs

Audience

Vendors of **products and services** that produce, consume, or process cyber threat intelligence

Organizations that produce or consume cyber threat intelligence

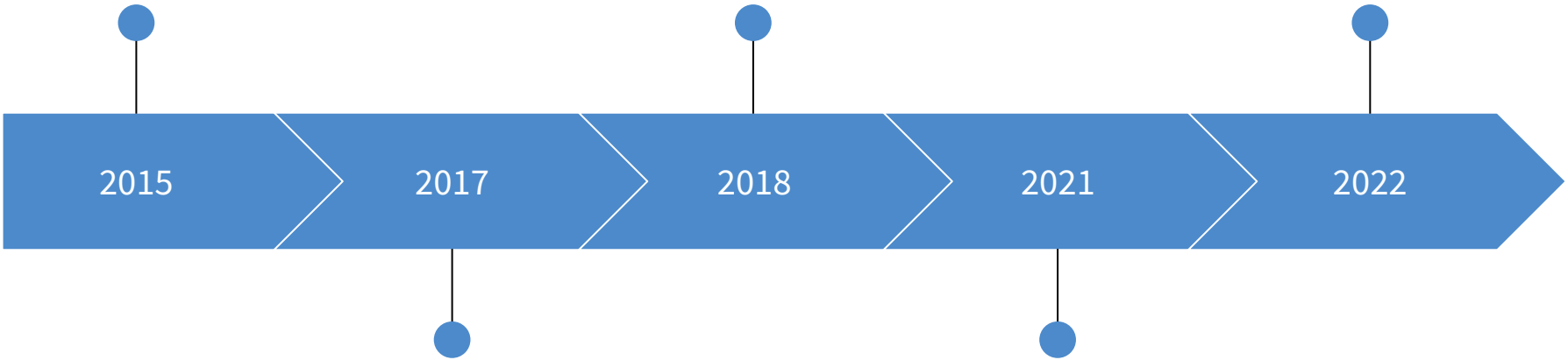
Communities Information Sharing and Analysis Organizations (ISAOs), including Information Sharing and Analysis Centers (ISACs)

Work Products

Structured Threat Information Expression (**STIX**)

Trusted Automated Exchange of Indicator Information (**TAXII**)

Others as deemed appropriate by the OASIS CTI TC as a whole.



US DHS Transitioned STIX and TAXII to OASIS Open, forming the CTI-TC

STIX/TAXII 2.0 Interoperability Test Documents (Part 1 & 2)

- STIX v2.1 and TAXII v2.1 submitted to ITU-T
- TAXII 2.1 Interop

STIX 2.0 Committee Specification approved

- STIX 2.1 and TAXII 2.1 become full OASIS Standards
- STIX 2.1 Interop

Goals

Standard → Extensibility → Interoperability

STIX

TAXII

TAXII Filtering Match Fields

OASIS OPEN

STIX 2.1 Interoperability Test Document Version 1.0

Committee Specification Draft 01

23 October 2021

This stage:

https://docs.oasis-open.org/cti/stix/v2.1/interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.docx (Authoritative)

https://docs.oasis-open.org/cti/stix/v2.1/interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.html

Previous

N/A

Latest

Technica

OASIS C

OASIS OPEN

TAXII 2.1 Interoperability Test Document Version 1.0

Committee Specification Draft 01

30 March 2022

This stage:

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/csd01/taxii-2.1-interop-v1.0-csd01.docx (Authoritative)

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/csd01/taxii-2.1-interop-v1.0-csd01.html

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/csd01/taxii-2.1-interop-v1.0-csd01.pdf

Previous stage:

N/A

Latest stage:

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/taxii-2.1-interop-v1.0.docx (Authoritative)

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/taxii-2.1-interop-v1.0.html

https://docs.oasis-open.org/cti/taxii/v2.1/interop/v1.0/taxii-2.1-interop-v1.0.pdf

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Charlie Frick

A structured representation of reusable adversary behaviors, detections of those behaviors, and correlation workflows to aid network defenders

Overview of Indicators of Behavior

Motivation

- Network defenders struggle to obtain and use Cyber Threat Intelligence
- STIX provides a useful standard for packaging the data, but the proper context is needed
- MITRE ATT&CK and D3FEND provide a necessary but not sufficient capability
- There is a need for something more general than an IOC and more specific than a high level Attack Pattern that can be shared and utilized by various community stakeholders

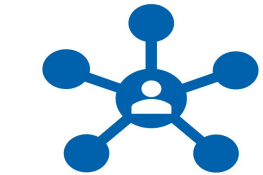
Concept

- Intelligence context provided in standardized (STIX) machine-readable graph representation
- Relationships to relevant ATT&CK attack pattern objects
- Relationships to detection analytics
- Includes **correlation workflows** to address false-positives
- Includes response COAs and cybersecurity operations playbooks in standardized formats

Solutions

- Reference implementation STIX bundles provided on IOB GitHub Site

  https://github.com/opencybersecurityalliance/oca-iob
- Also provides technical documentation and open tools for reading IOB bundles
- Use of open standards to quickly work with additional open tools



Ryan Hohimer

Threat Actor Context Technical Committee

Semantic Graph Analysis of Threat Actors

The Problem:

Human Analysis Takes Time

Human Cybersecurity Analysts are a valuable asset.

- There are not enough of them to go around.
- The rapid pace of data flow overwhelms our systems.

Automation is Paramount

To keep up, we must automate detection and analysis.

- Expert knowledge in machine readable and executable form

Local Environment Relevancy

Enterprise Knowledge in relation to the Threat Intelligence is important.

- Confidentiality
- Integrity
- Availability

Challenges deep-dive

Challenge 1

Challenge 2

Challenge 3

Creating a Graph Representation

To apply semantic graph analysis to STIX content it must be represented in an RDF Graph.

- STIX.OWL (ontology)
- STIX 2.1 JSON -> RDF Conversion (data fa

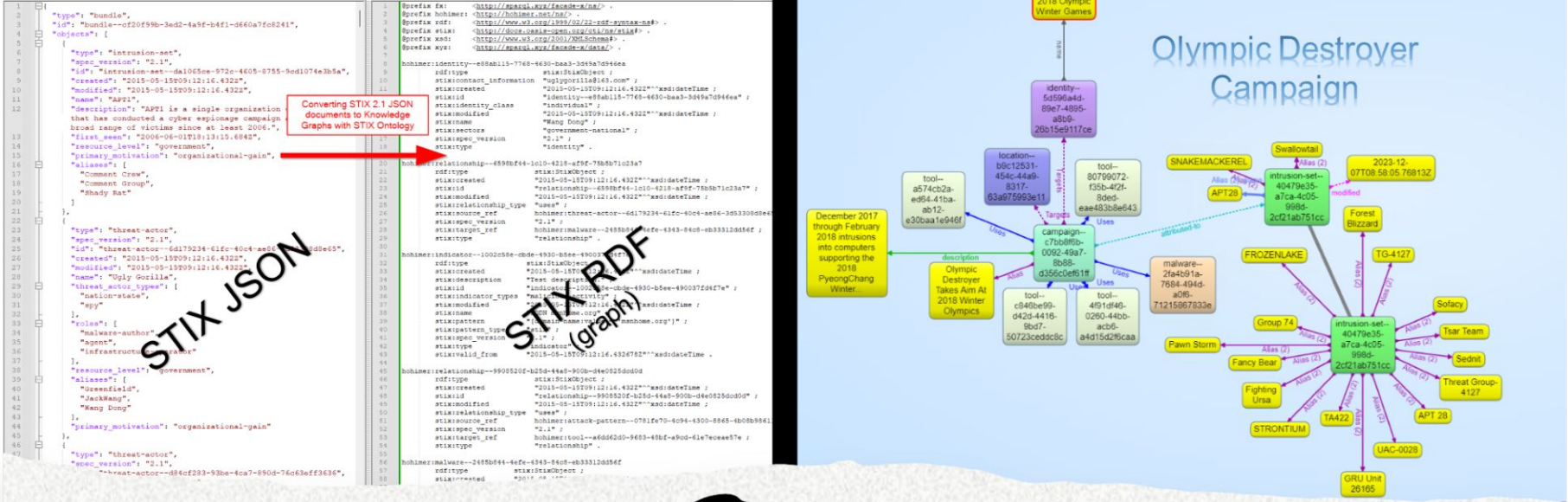
Merging the STIX data with related data

Data from MITRE, NIST, and others is important

- CVE
- CWE
- ATT&CK
- CAPEC
- Shared Indicators
- Etc.

Intuitive Interface

Querying the graph and presenting results is useful only if it is easy to understand.



Converting STIX JSON to STIX Knowledge Graph

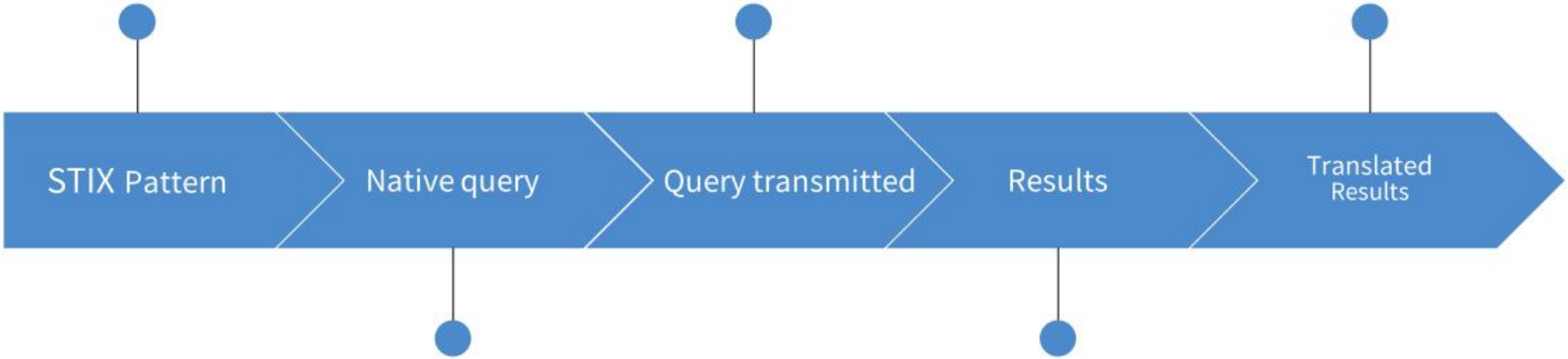
Md Azam

STIX-shifter is an open source python library allowing software to connect to products that house data repositories by using STIX Patterning and return results as STIX Observations.

STIX pattern is submitted.

Native query is sent via data source API.

JSON results are translated into bundles of STIX objects.



Pattern is translated into native query for target data source.

Search results are fetched from data source via API.

What can I do with STIX-Shifter?

As a CLI Tool

- Script searches for orchestration workflow
- Integrate workflow between multiple tools.
- Create cross platform playbook.

As a Library

- Provide standard way to integrate with the product.
- Provide a common way to query data.
- Add query or enrichment functionality.

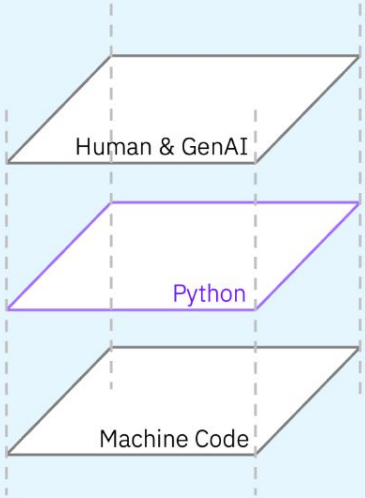
Connectors

- 35+ connectors to search a wide range of datasources
  https://github.com/opencybersecurityalliance/stix-shifter/blob/develop/docs/CONNECTORS.md

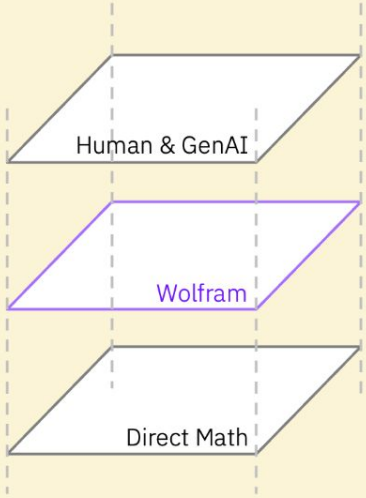
Michael Le &
Xiaokui Shu

Kestrel is a language designed for **cyber threat hunting** and an open-sourced compiler/runtime to take Kestrel huntbooks into action against a variety of data sources, threat intelligence sources, and hunting analytics.

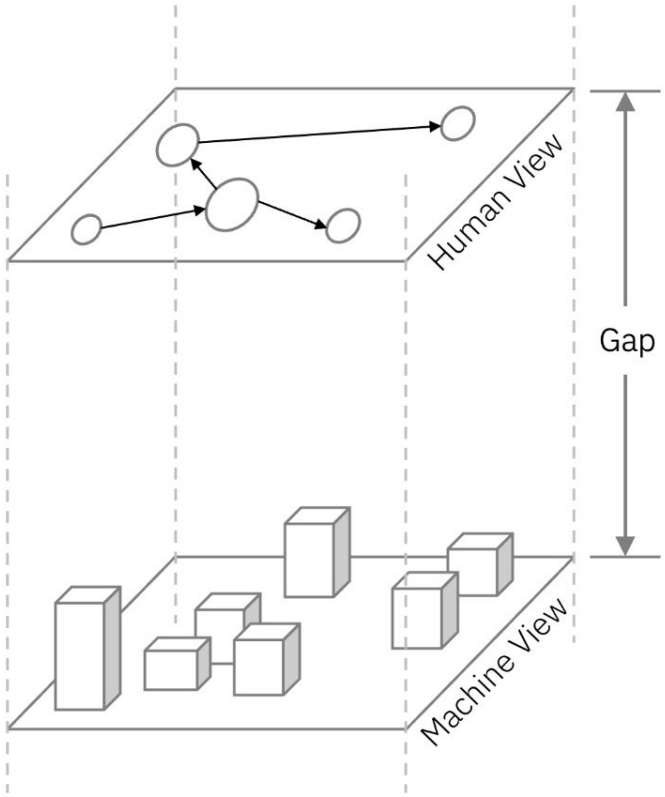
Generic Problem Solving

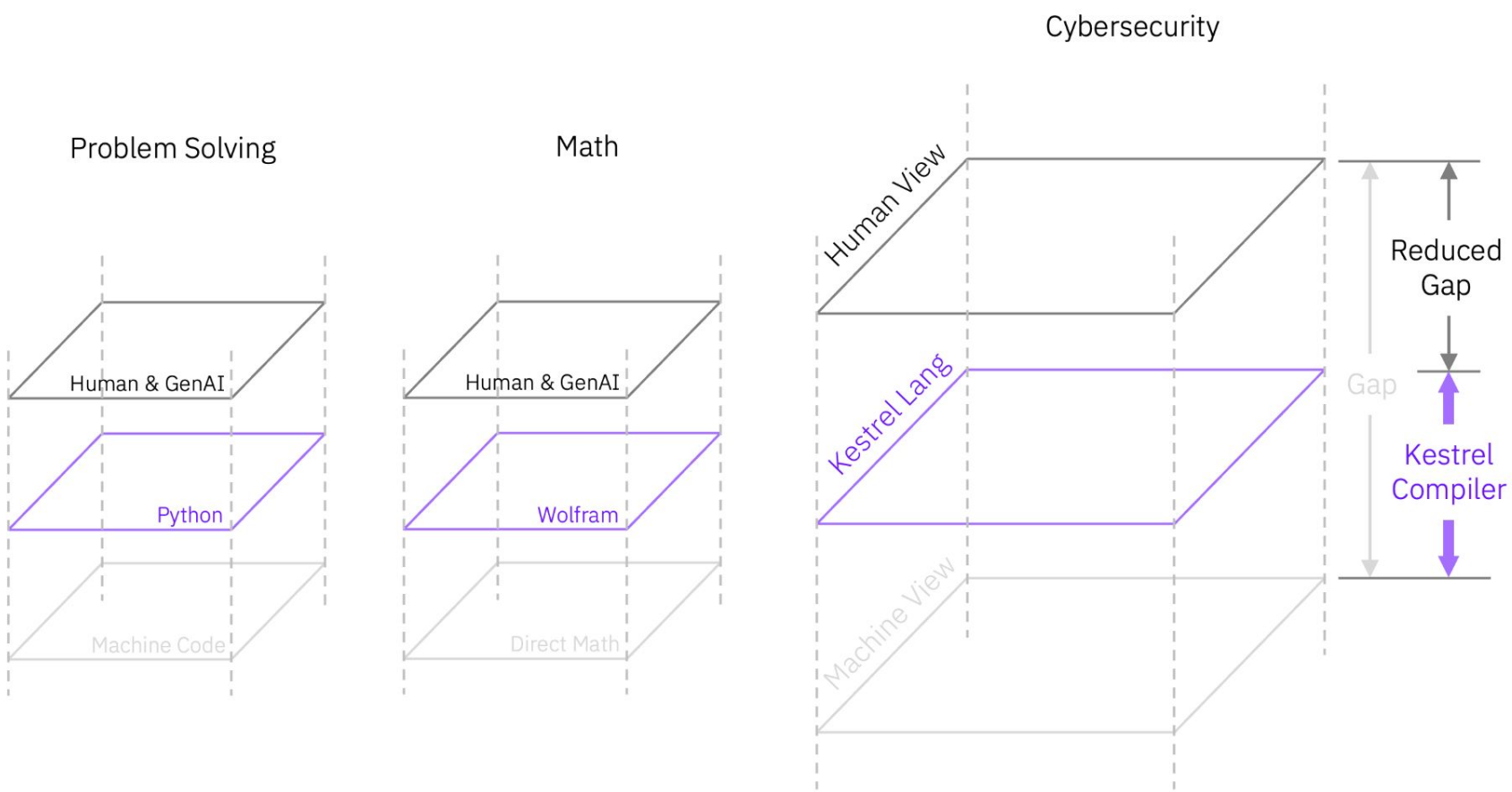


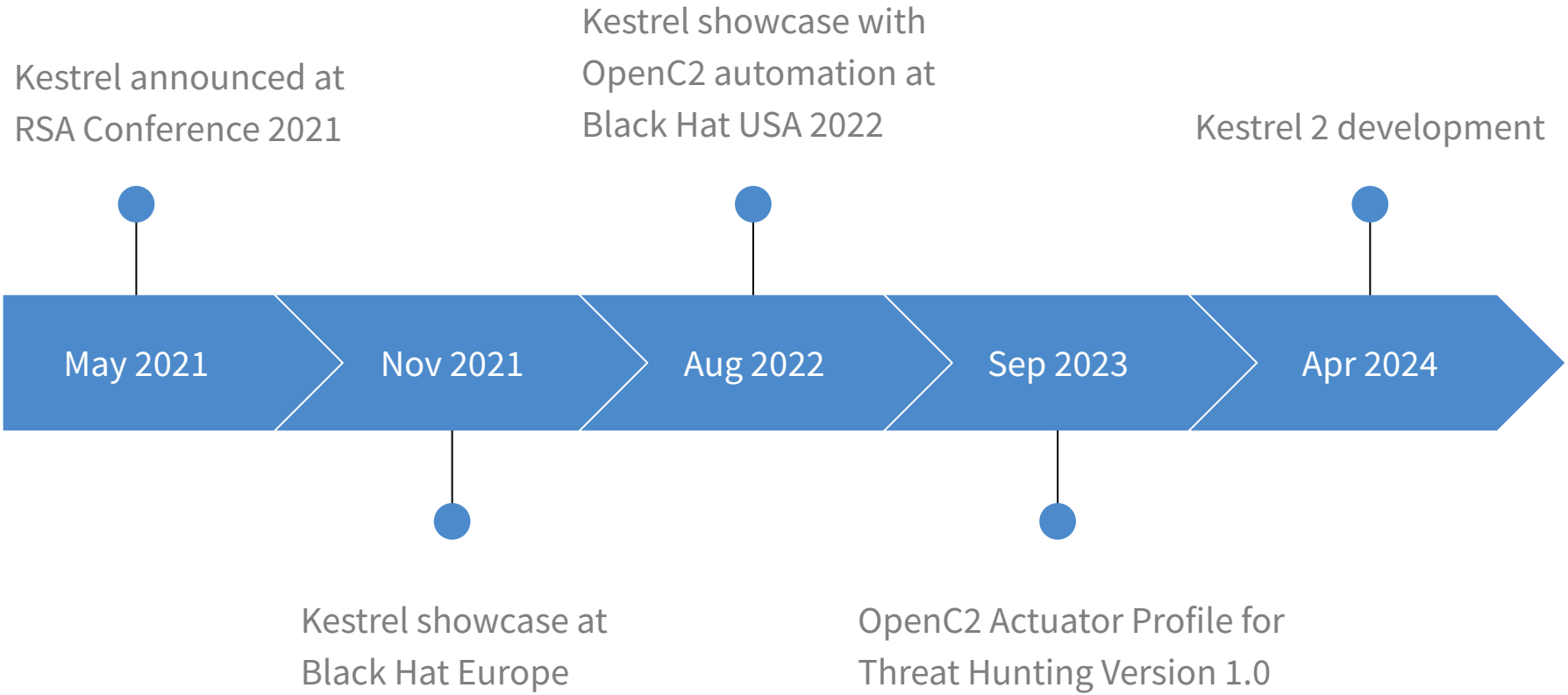
Math Problem Solving



Cybersecurity






Kestrel announced at RSA Conference 2021
Kestrel showcase with OpenC2 automation at Black Hat USA 2022
Kestrel 2 development
May 2021
Nov 2021
Aug 2022
Sep 2023
Apr 2024
Kestrel showcase at Black Hat Europe
OpenC2 Actuator Profile for Threat Hunting Version 1.0

Alexandre Dulaunoy &
Christian Studer

MISP is an open-source platform and standard designed for threat intelligence sharing, providing a structured environment to aggregate, model, store and distribute information.

A full ecosystem

Platform

The core platform comes with several automation tools such an advanced API and integrations with many other tools and formats.

Standard format

The standard MISP JSON format provides enhanced consistency and interoperability in data sharing.

Modulable components

MISP is complemented by various components such as taxonomies for classification, Galaxies that offer clusters of related threat information, or object templates to describe specific data.

Challenges deep-dive

Ensuring flexibility

Long-term stability

Interoperability

Community builds intelligence

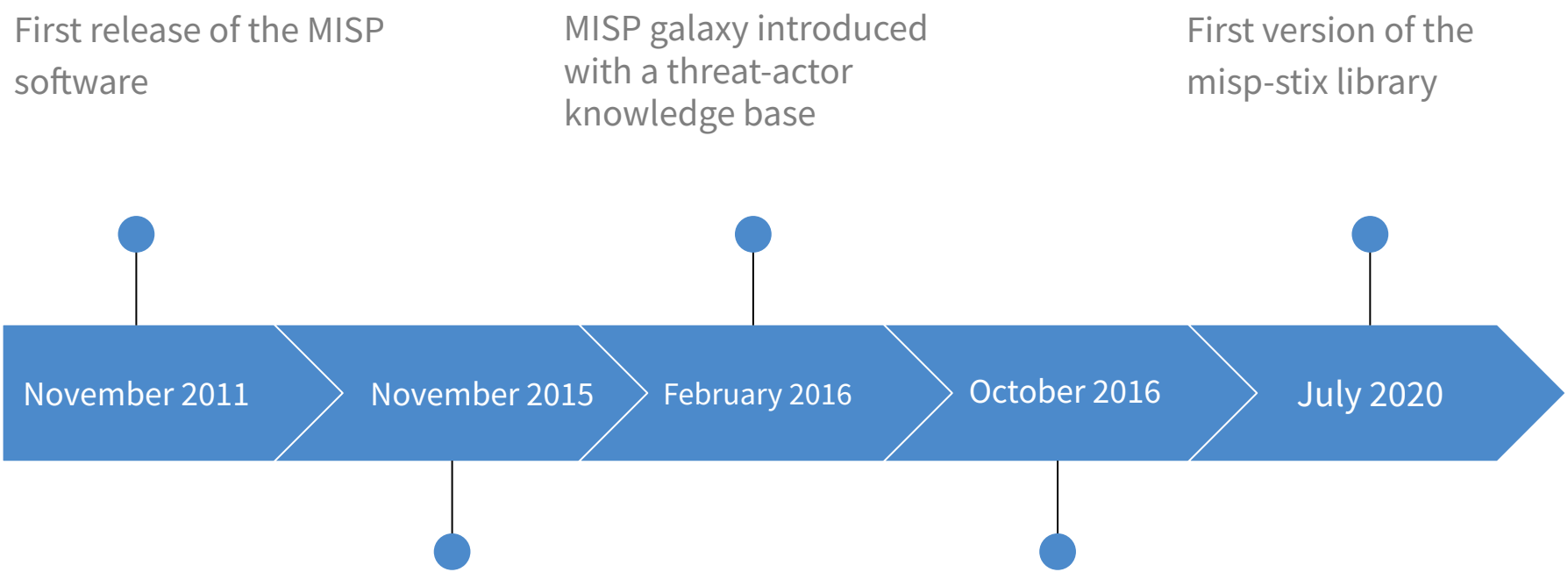
The MISP project established a comprehensive community to not only facilitate contributions to the software but also to the MISP standard.

12+ years

Numerous users depend on MISP, whether from a software perspective, as a knowledge base (including galaxy and taxonomy), or for its API capabilities. Therefore, it's essential to maintain long-term compatibility and interoperability with a wide range of tools.

Extend to all new open standards

MISP has developed a comprehensive library, known as misp-stix, to ensure compatibility and facilitate mapping with the STIX standards. The aim is to assist other software that faces challenges with standard formats by providing them with an easy-to-use library.


First release of the MISP software
MISP galaxy introduced with a threat-actor knowledge base
First version of the misp-stix library
November 2011
November 2015
February 2016
October 2016
July 2020
Starting modular JSON file called misp-taxonomy
First version of the MISP standard IETF ID misp-core-format

OpenCTI

Samuel Hassine

OpenCTI is an open source platform providing enterprise-grade threat knowledge management capabilities from technical to strategic use cases.

What is OpenCTI?

Knowledge management

Organizing and managing large threat intelligence datasets

Data visualization

Complex data into intuitive visualizations, enabling users to grasp complex patterns and insights

IOCs management automation

Automates the management of Indicators of Compromise, streamlining the detection and response

Case management

Advanced incident response capabilities, facilitating efficient case management and response orchestration

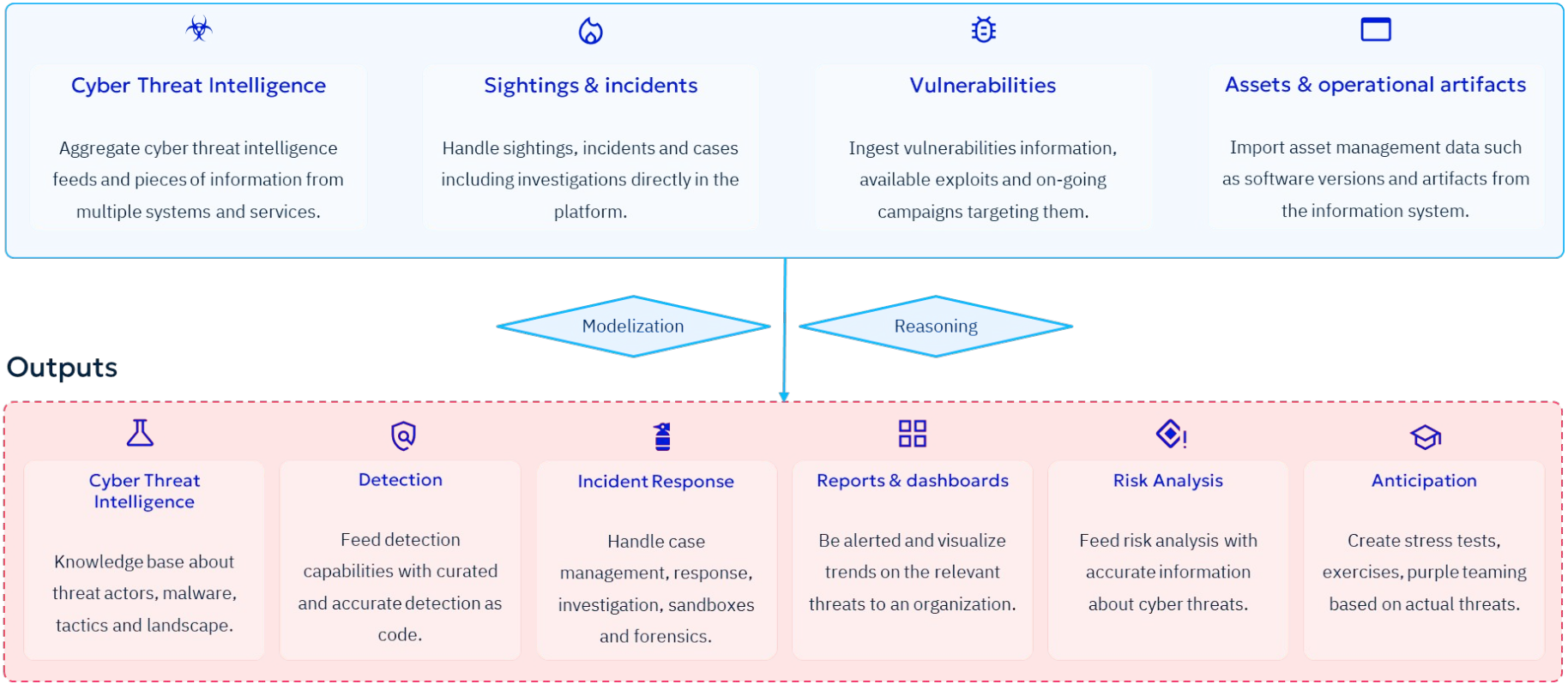
Integration

Seamlessly integrates with various cybersecurity solutions and intelligence source

Intelligence sharing

Effortless sharing of threat intelligence through seamless, secure, and controlled sharing capabilities

Use Cases


Cyber Threat Intelligence
Aggregate cyber threat intelligence feeds and pieces of information from multiple systems and services.
Sightings & incidents
Handle sightings, incidents and cases including investigations directly in the platform.
Vulnerabilities
Ingest vulnerabilities information, available exploits and on-going campaigns targeting them.
Assets & operational artifacts
Import asset management data such as software versions and artifacts from the information system.
Modelization
Reasoning
Outputs
Cyber Threat Intelligence
Knowledge base about threat actors, malware, tactics and landscape.
Detection
Feed detection capabilities with curated and accurate detection as code.
Incident Response
Handle case management, response, investigation, sandboxes and forensics.
Reports & dashboards
Be alerted and visualize trends on the relevant threats to an organization.
Risk Analysis
Feed risk analysis with accurate information about cyber threats.
Anticipation
Create stress tests, exercises, purple teaming based on actual threats.

Value for SOCs

Reduce Mean Time To Qualify

- Standard correlation engine, amplified to a next level with Advanced Correlation (AI)
- Automation engine (# false positives)
- Intel assessement based on powerful confidence level system and deduplication mechanism

Reduce Mean Time To Detect

- Automation engine (automated IOCs management)
- NLP (reduce ingestion & patterning time)
- Full Text Indexing (data exhaustivity)

Reduce Mean Time To Respond

- NLP (reduce ingestion & patterning time)
- Complete mapping with MITRE ATT&CK
- Case management / incident response with the immediate threat context

Analyst Efficiency / Fatigue – SOC effectiveness

- NLP, Advanced Correlation, Automation
- Significant amount of time saving

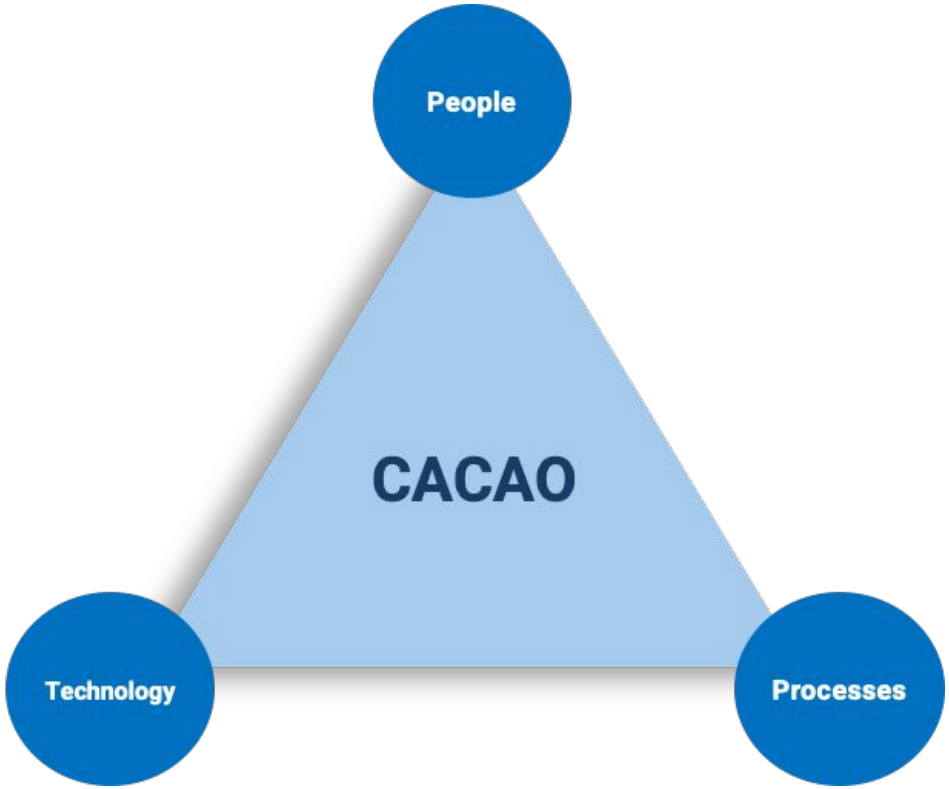
Vasileios Mavroeidis

Collaborative **A**utomated
Course of **A**ction **O**perations

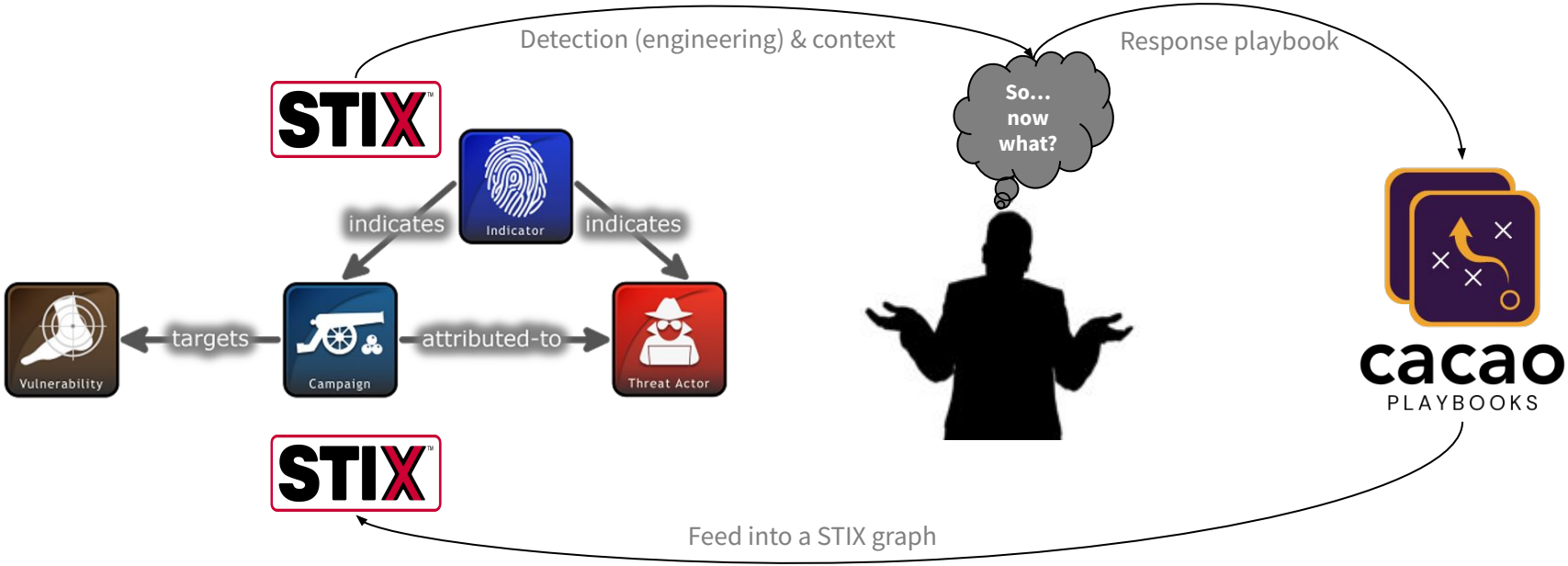
A standardized machine-readable schema for cybersecurity playbooks

The problem

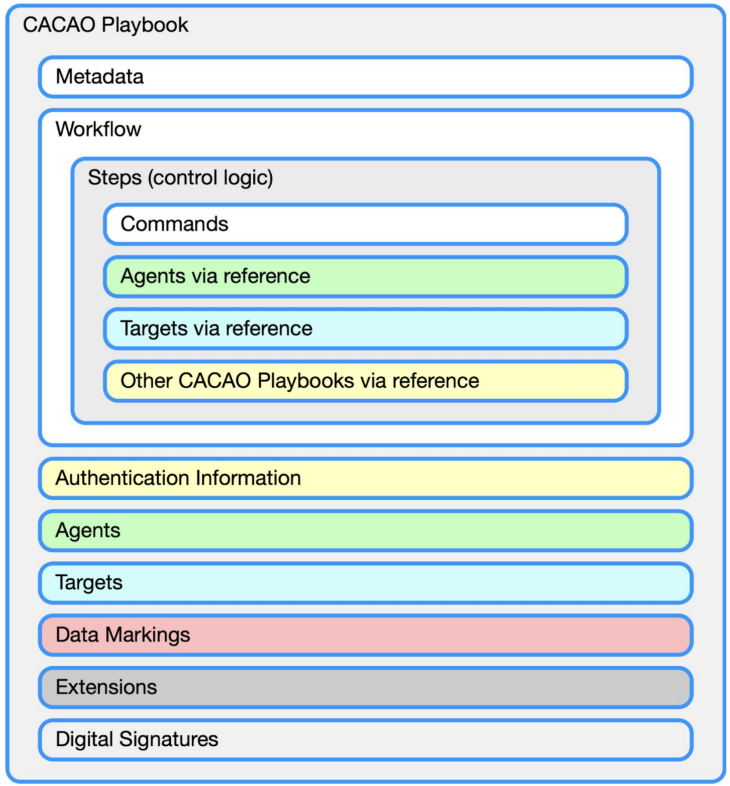
Playbooks have been used for decades	Need to be able to share playbooks	Need for Automation
• Often in paper or wiki • Searching blog posts for mitigation and remediation steps is not scalable and is time consuming • No workflow or ability to track progress	• Teams are siloed and isolated • Many different groups inside and outside of organizations are part of the response • Need to do for playbooks what STIX and TAXII did for CTI	• Manual incident response is painful and slow • Need to be able to respond in cyber-relevant time

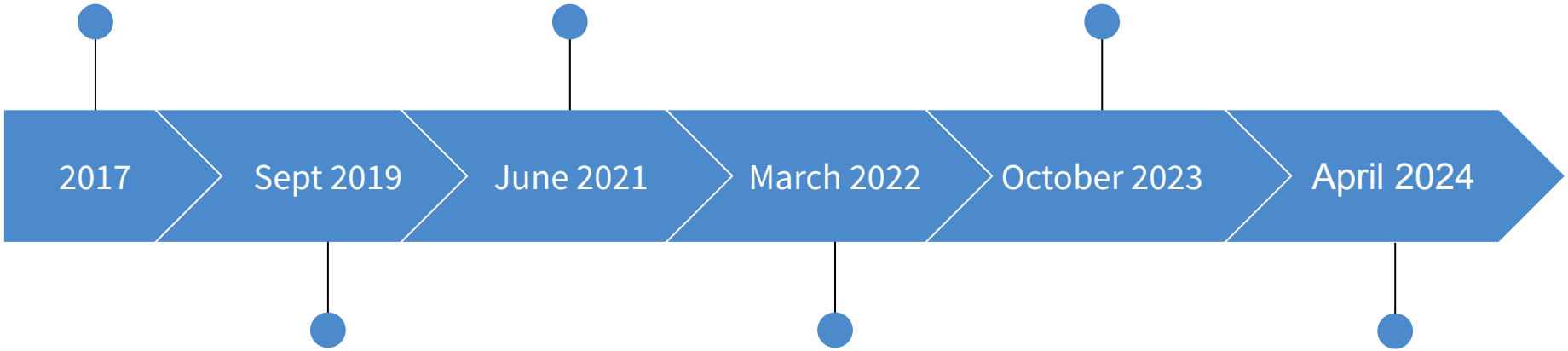

People
CACAO
Technology
Processes

CACAO & cyber threat intelligence



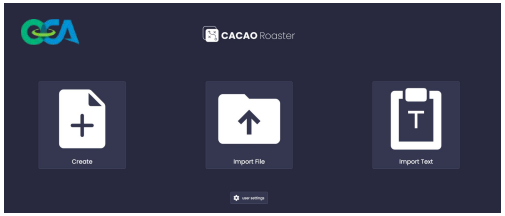
CACAO high-level architecture




Initial ideas worked out that led to industry partnerships in early 2018
CACAO version 1.0 released
CACAO version 2.0 released
2017
Sept 2019
June 2021
March 2022
October 2023
April 2024
OASIS CACAO TC was formed with 72 initial members
CACAO version 1.1 released
CACAO Layout Extension version 1.0

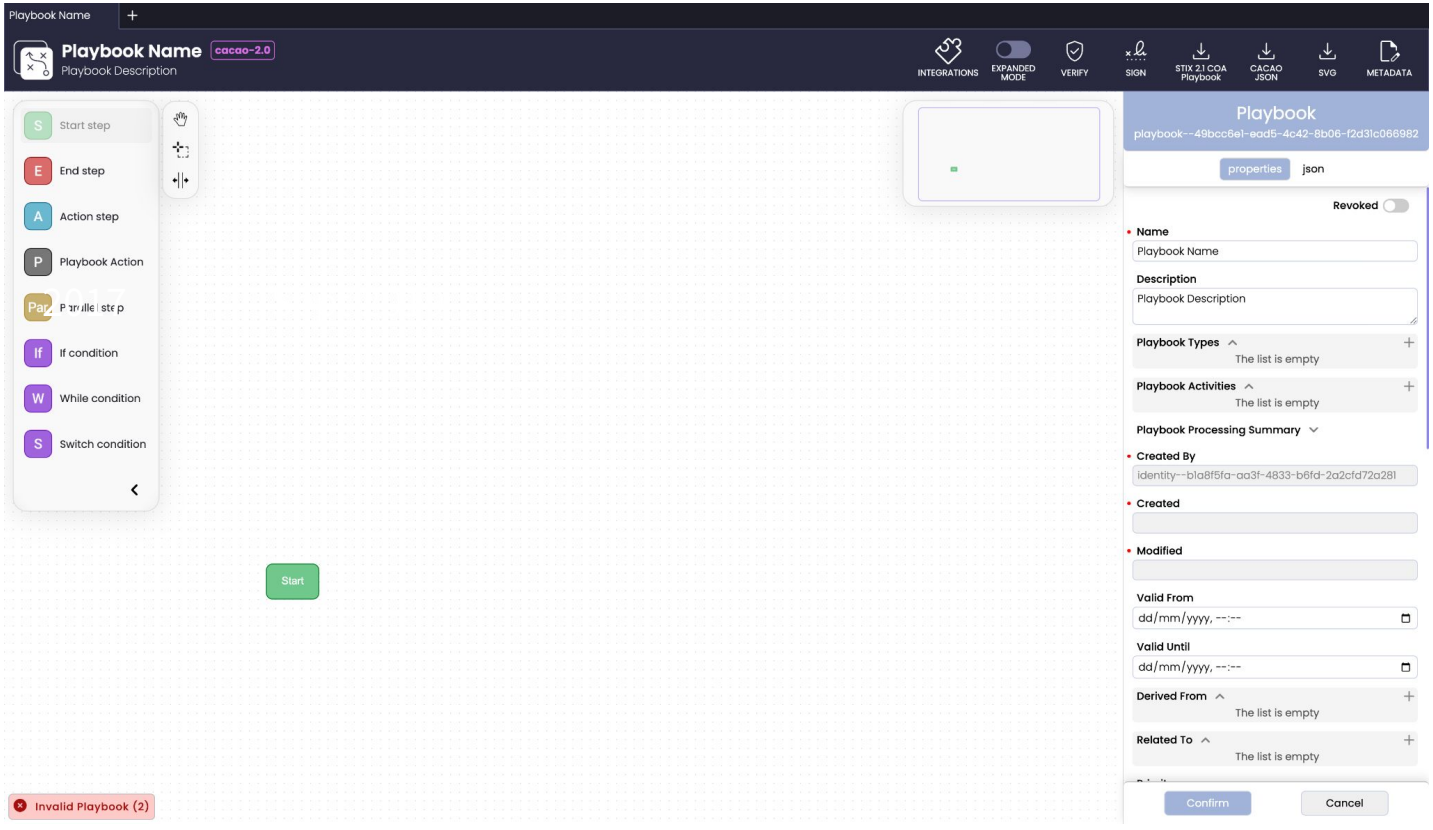
Vasileios Mavroeidis

Open-source web application for designing, generating, modifying, digitally signing, and verifying CACAO playbooks



Jan 2024 …

Release of CACAO Roaster version 1.0.0



- CACAO Roaster
- **CACAO v2 library**
- **JSON validation schemas**
- Layout extension
- Integrations with SOAR!
  - SOARCA

Live Instance

https://github.com/opencybersecurityalliance/cacao-roaster

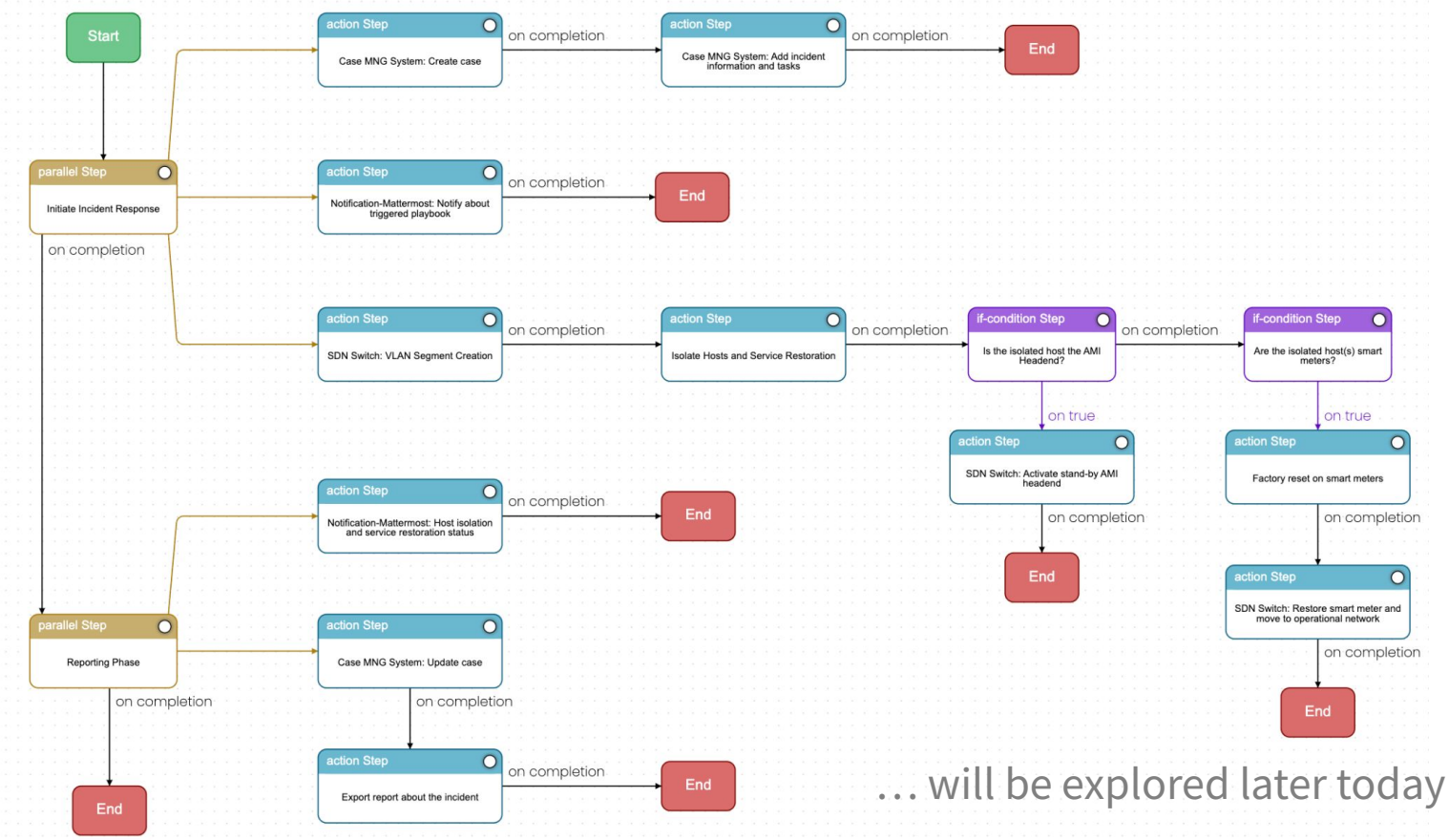
https://opencybersecurityalliance.github.io/cacao-roaster/

[Utility]-FDI-business-continuity

cacao-2.0 TLP:GREEN

Generic mitigation, remediation, & business continuity playbook for FDI

fdi smart-meter ami-headend standard-operating-procedure



… will be explored later today

Luca Morgese Zangrandi

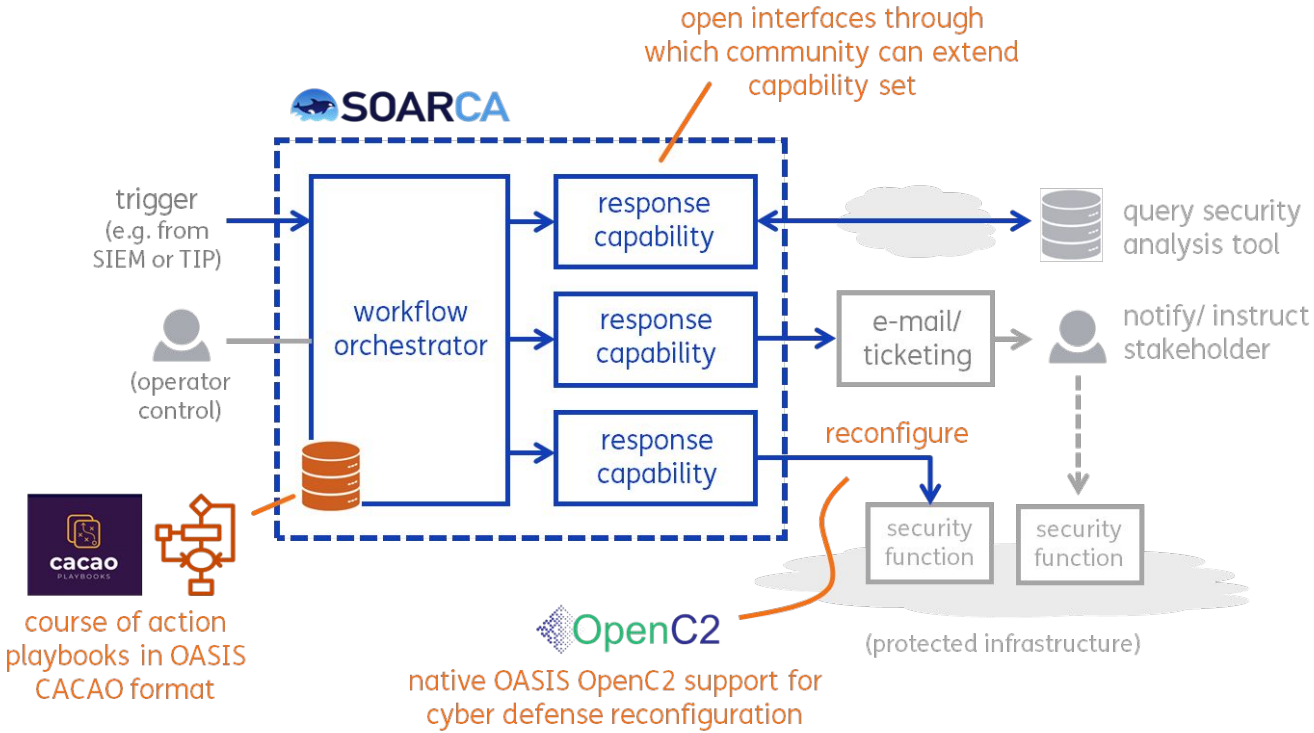
Security **O**rchestrator for
Advanced **R**esponse to **C**yber
Attacks

An execution Engine for CACAO V2 Playbooks

Raison d'être

Raison d'être

Raison d'être



TNO

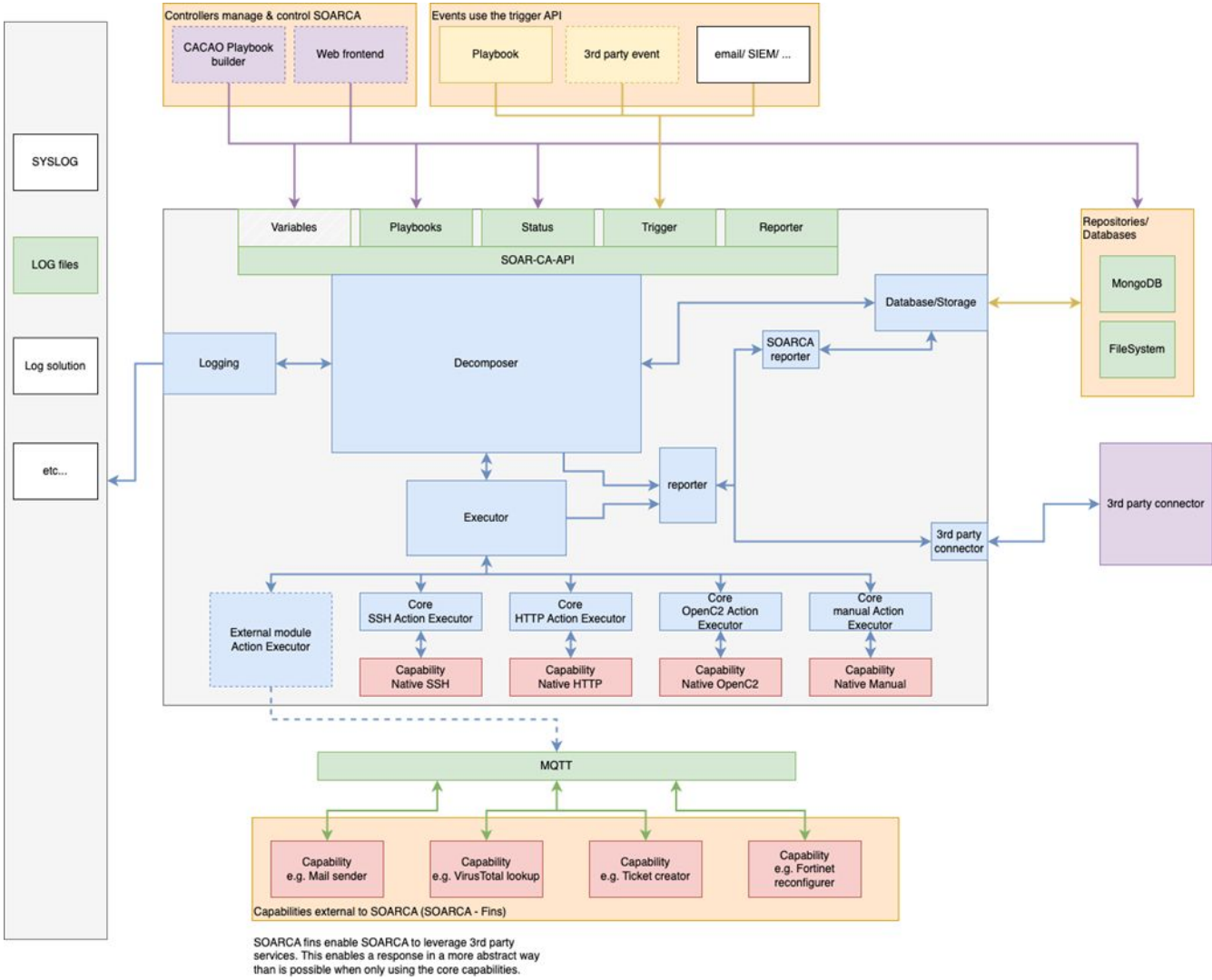
Dutch Organization for Applied Scientific Research

SOARCA

objectives

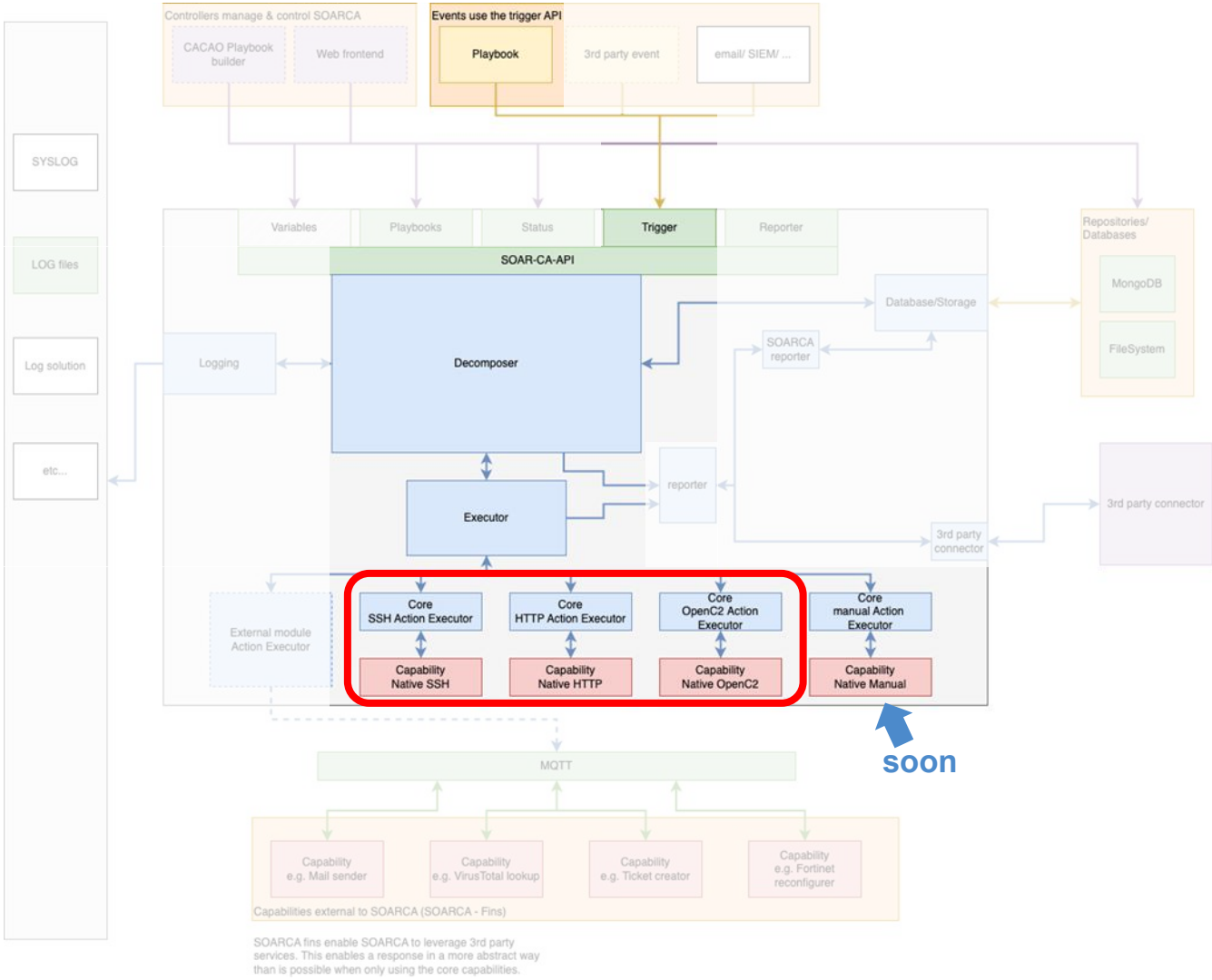
- support research and innovation in security automation
- allow community to experiment with open (vendor-agnostic) orchestration capability

What does SOARCA do?



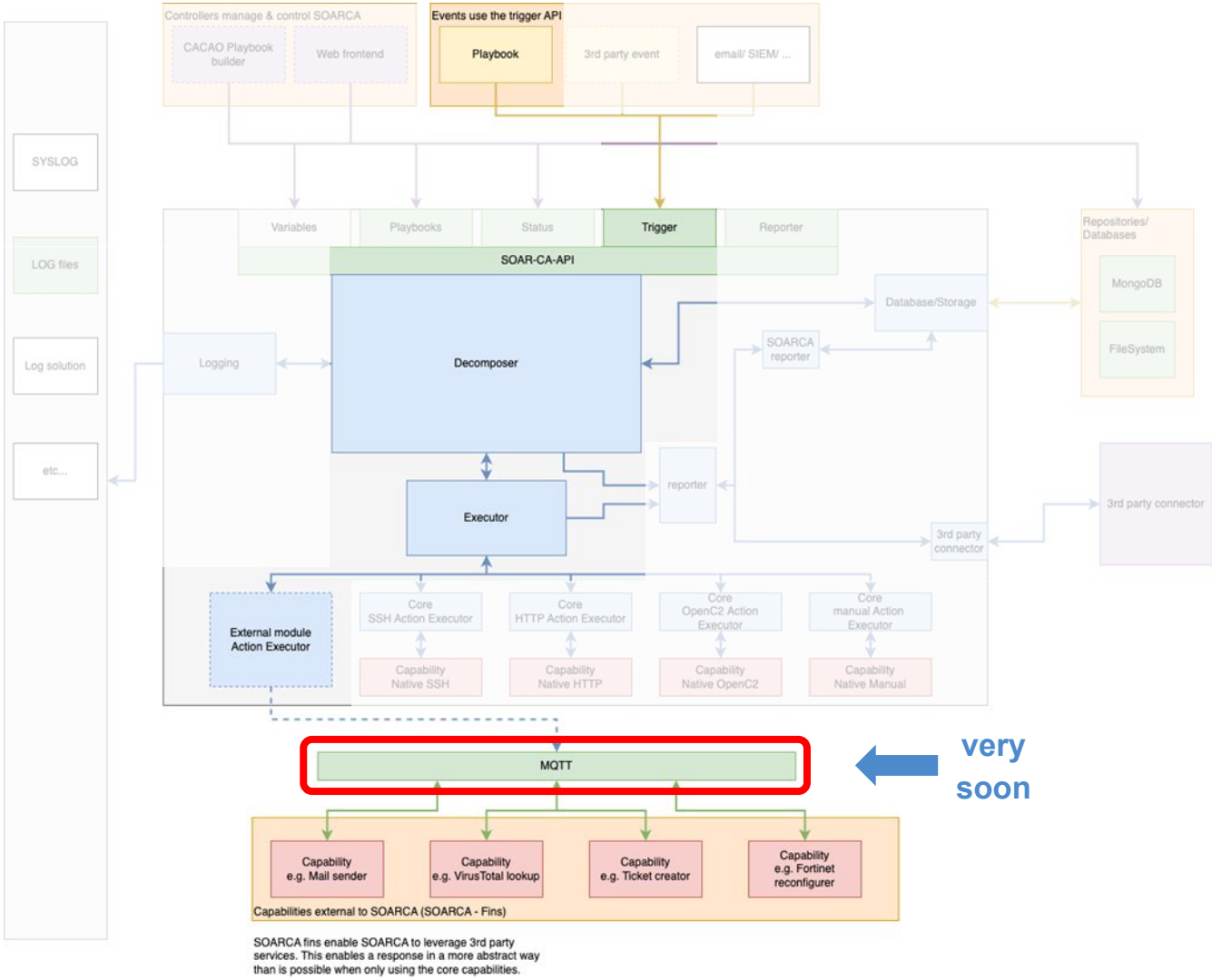
What does SOARCA do?

- **Playbook Execution**



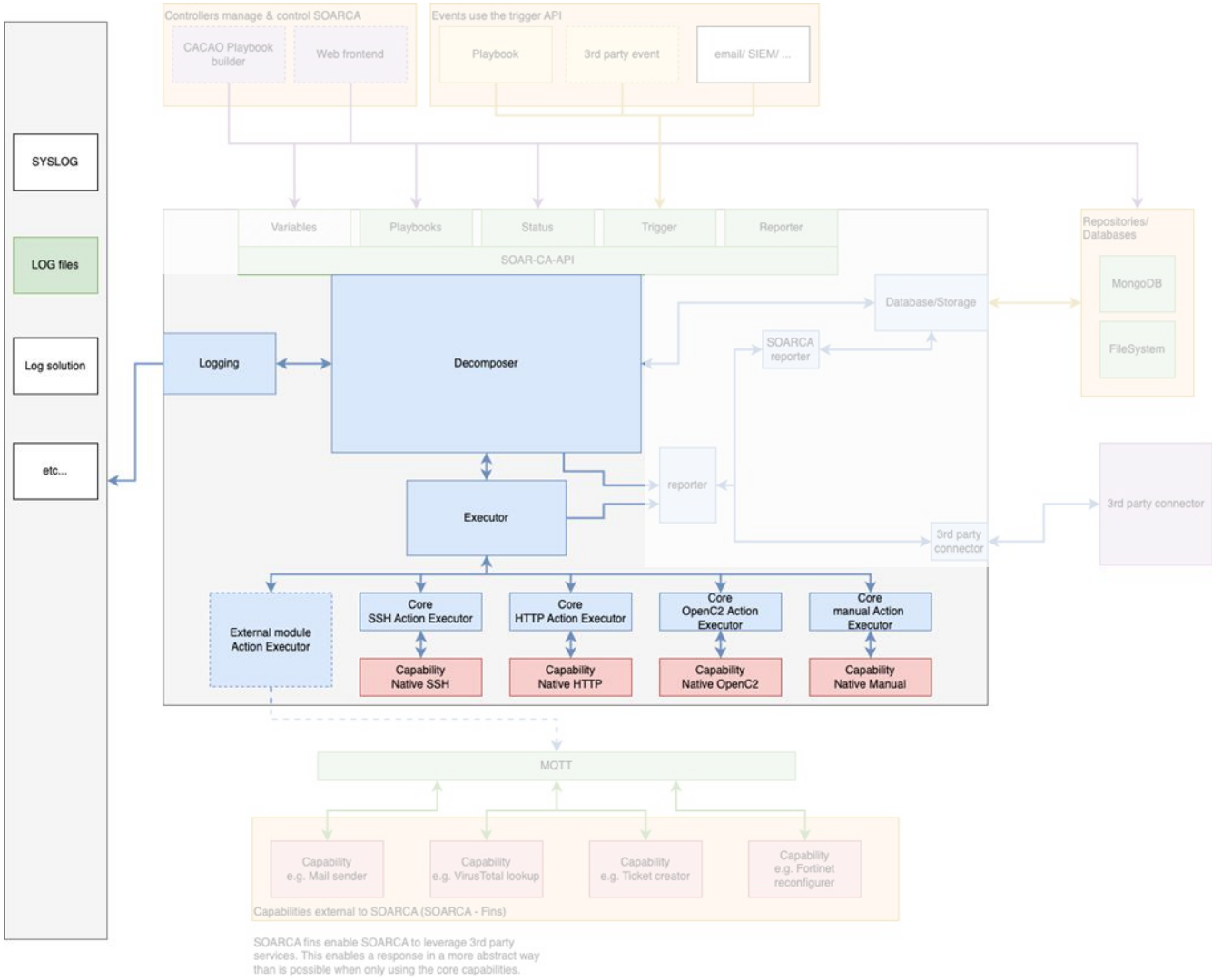
What does SOARCA do?

- Playbook Execution
- **Pluggable extensions via “fins”**



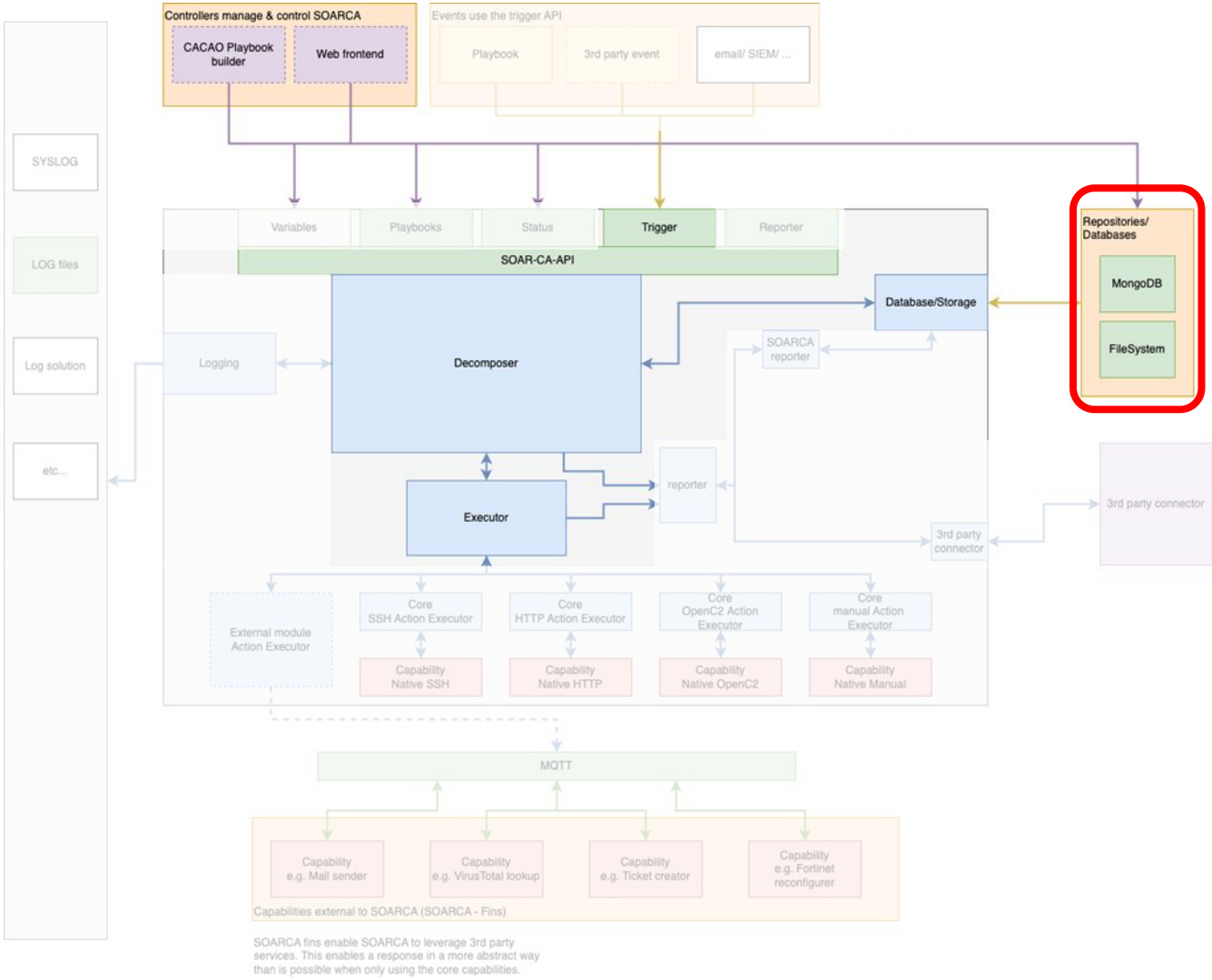
What does SOARCA do?

- Playbook Execution
- Custom extensions via “fins”
- **Flexible logging framework**



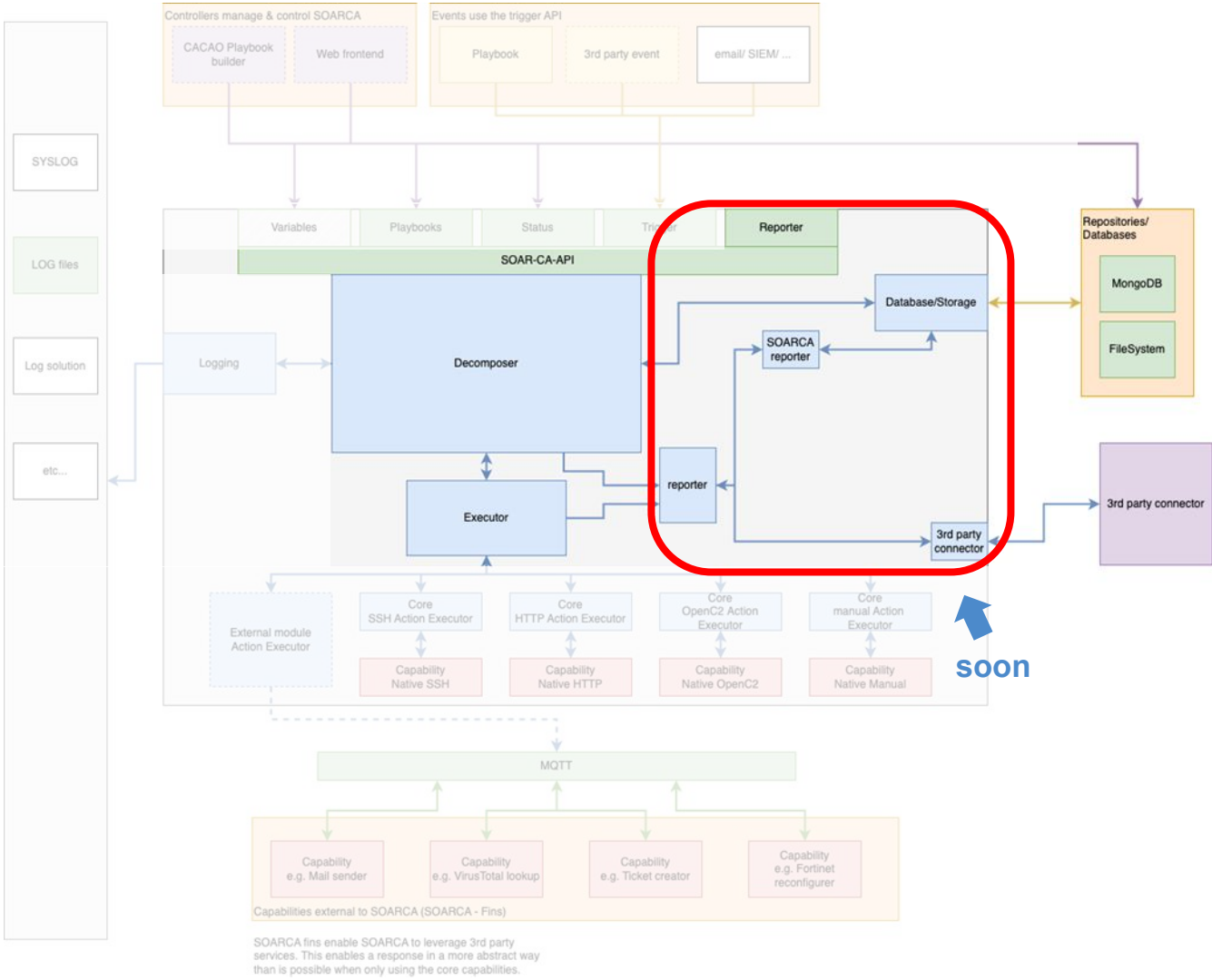
What does SOARCA do?

- Playbook Execution
- Custom extensions via “fins”
- Flexible logging framework
- **Database for storing and retrieving playbooks**



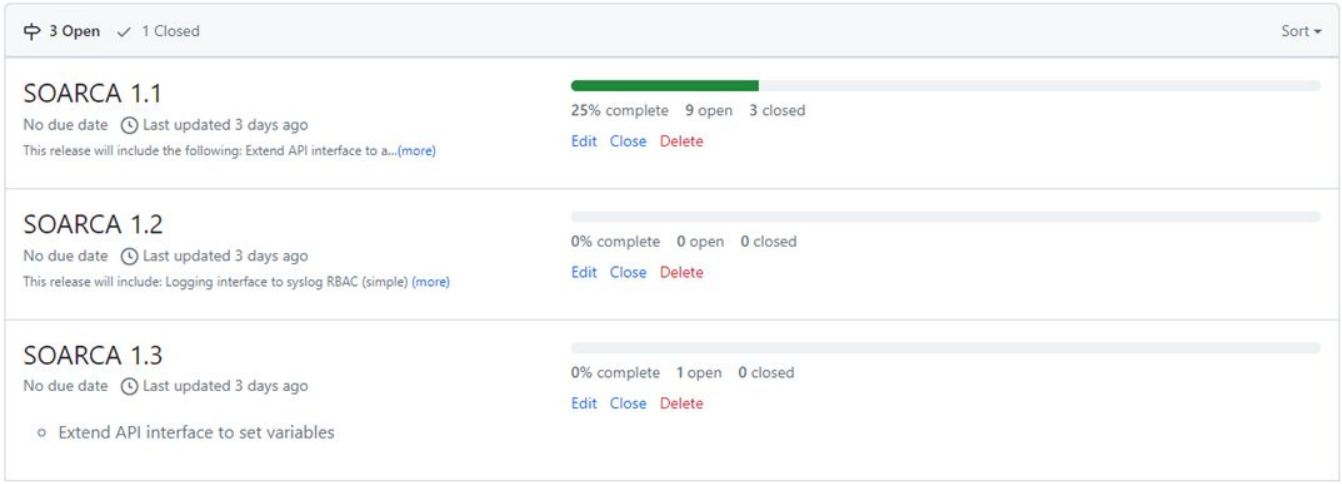
What does SOARCA do?

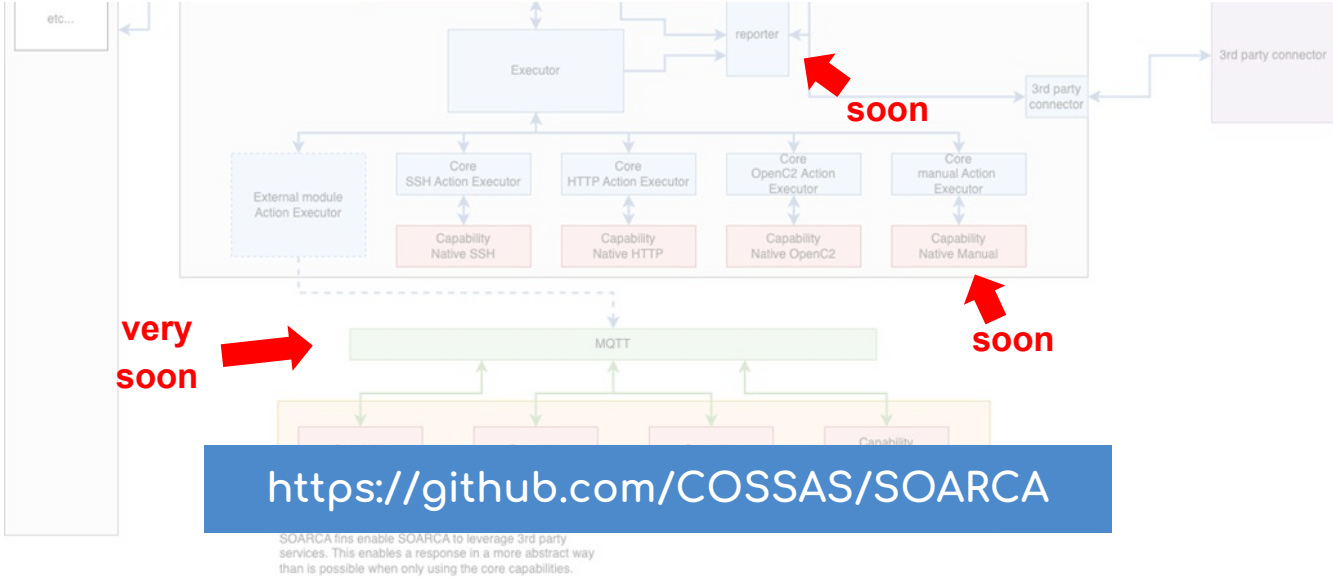
- Playbook Execution
- Custom extensions via “fins”
- Flexible logging framework
- Database for storing and retrieving playbooks
- **Push-, pull-, connection-based 3party integrations**



What does SOARCA do?

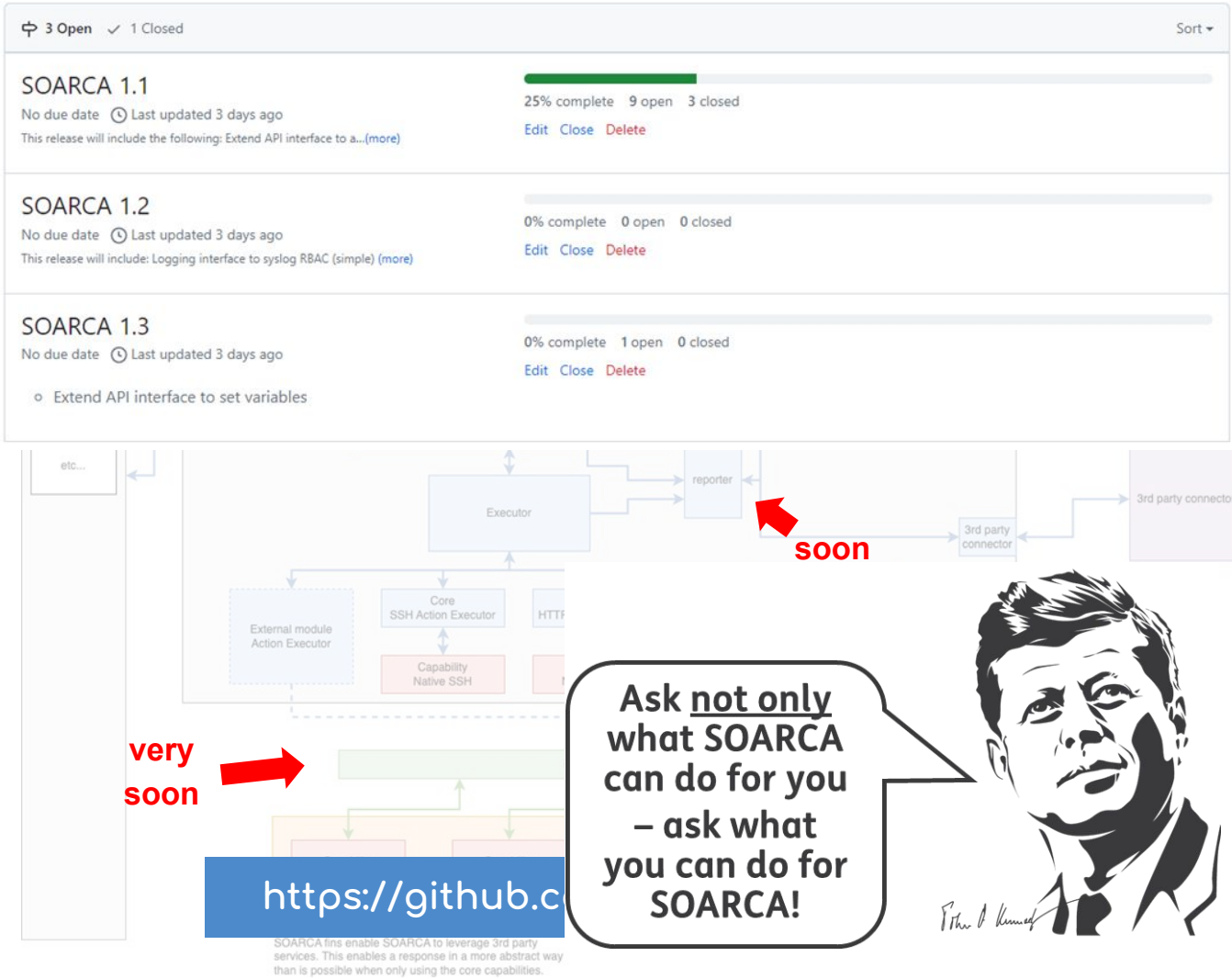
- Playbook Execution
- Custom extensions via “fins”
- Flexible logging framework
- Database for storing and retrieving playbooks
- Push-, pull-, connection-based 3party integrations
- ...





What does SOARCA do?

- Playbook Execution
- Custom extensions via “fins”
- Flexible logging framework
- Database for storing and retrieving playbooks
- Push-, pull-, connection-based 3party integrations
- ...



Next Steps

Long term plans:

- Continue SOARCA developments based on current & future public/private funded research + provide contract research to integrate in your environment!
- Support the community as much as possible with questions, bug fixes, feature requests, maintenance, etc.
- … but we are non-for-profit research organization.

Community role:

- We made it open source such that others can join and contribute!
- Please contact us if you want to join SOARCA development team.
  - GitHub: Development takes place here!
  - Slack: Chat with other developers
  - **E-mail us:** info@cossas-project.org

https://github.com/COSSAS/SOARCA

Thank You!

https://github.com/COSSAS/SOARCA

Luca Morgese Zangrandi

Mike Rosa

Open Command and Control

A standardized language for the command and control of technologies that provide or support cyber defenses.

Overview

Vision

- Define a language at a level of abstraction
- Support automated action/response
- Flexible and lightweight

Context

Remediation Cycle (OODA Loop):

- Sense
- Analyze
- Decide
- Act

OpenC2: vendor-agnostic vocabulary of core and extension commands, integrable into response playbooks.

Current Specs/CNs

- OpenC2 Language Spec v1.0
- OpenC2 Profile for Stateless Packet Filtering v1.0
- Specification for Transfer of OpenC2 Messages via HTTPS 1.0
- Specification for Transfer of OpenC2 Messages via MQTT 1.0
- JSON Abstract Data Notation (JADN) Version 1.0
- Information Modeling with JADN Version 1.0 (CN01)
- OpenC2 Actuator Profile Development Process Version 1.0 (CN01)

Current Development

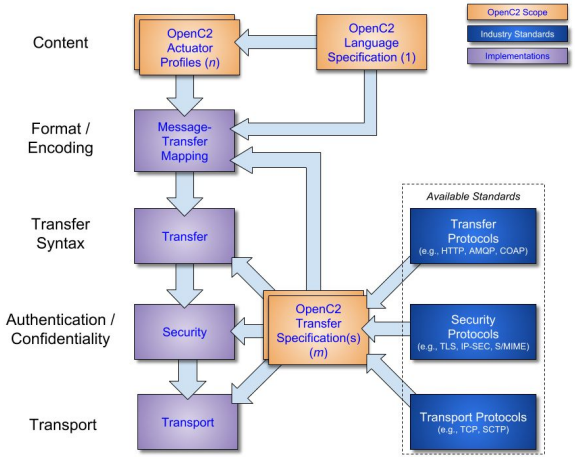
Standardization

Actuator profiles in development:

- Endpoint Detection and Response
- Software Bill of Materials (SBOM)
- Threat Hunting

Information Modeling:

- JADN Updates

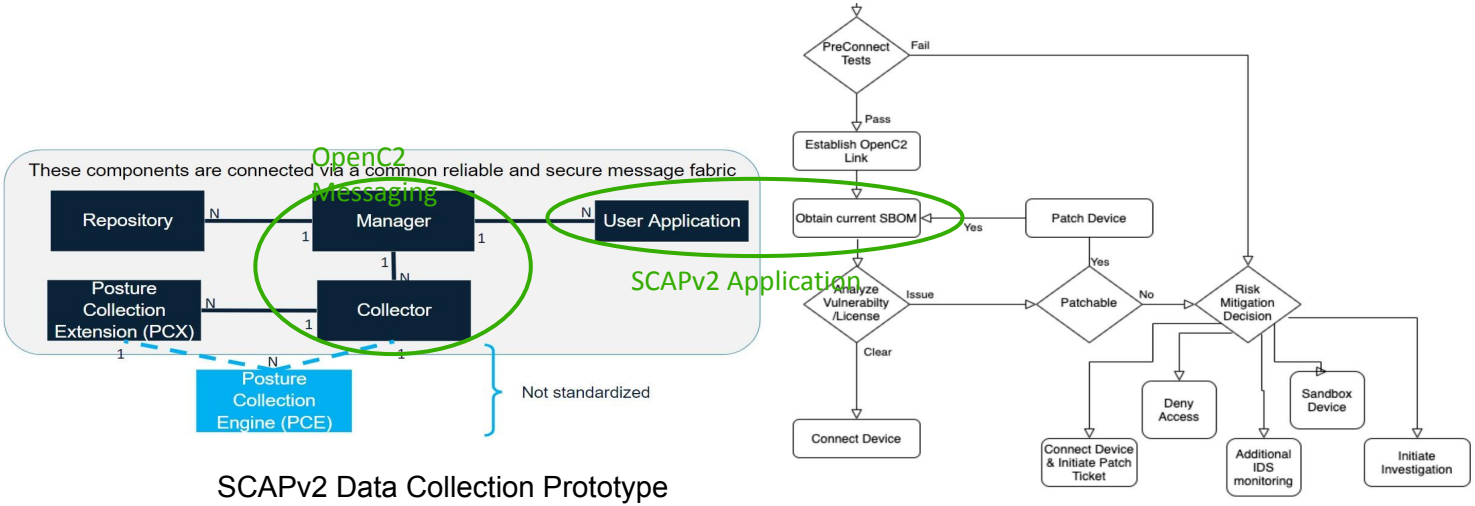


Awareness and Adoption

Coordinating with TCs and OSS:

- PACE
- CASP
- Kestrel
- SBOM community
- etc.

Interoperability with OpenC2



SCAPv2 Data Collection Prototype

OpenC2 Software Bill of Materials Proof of Concept

https://github.com/oasis-tcs/openc2-usecases/tree/master/SBOM-PoC

David Bizeul

OXA stands for **Open XDR Architecture.**

The goal is to facilitate interactions between security products, using open standards and APIs and with a special focus on Detection and Response. This project aims to define the architecture of an ideal eXtended Detection and Response approach.

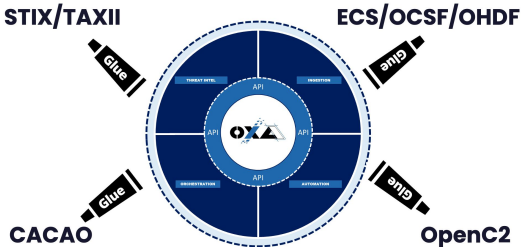
The problem

Motivation

- In XDR, CTI dissemination is required
- Integration teams take SO MUCH time on 1-to-1 integrations
- XD(R) means understanding incoming events
- X(D)R means thinking about interoperable playbooks

Concepts

- Glue existing standards and focus on what is missing



Main benefits

For users: Ability to plug solutions easily without waiting vendor integration

For customers: No vendor lock-in

For cybersecurity vendors: no more integration struggle

For MSSP: SOC ready in one day

For products: CTI enabled detection

Challenges deep-dive

Make it real

The project has been bootstrapped but not announced.

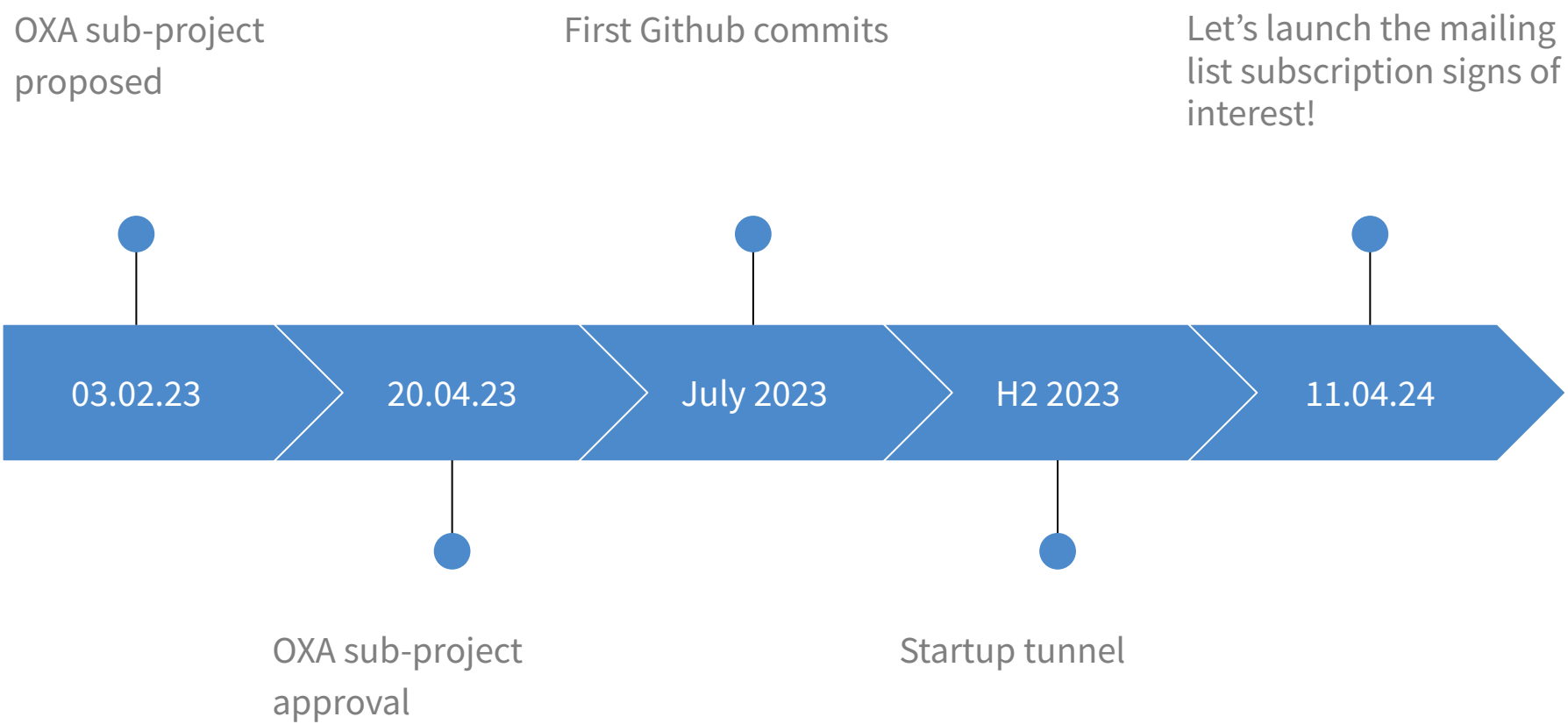
The early group constitution will be important

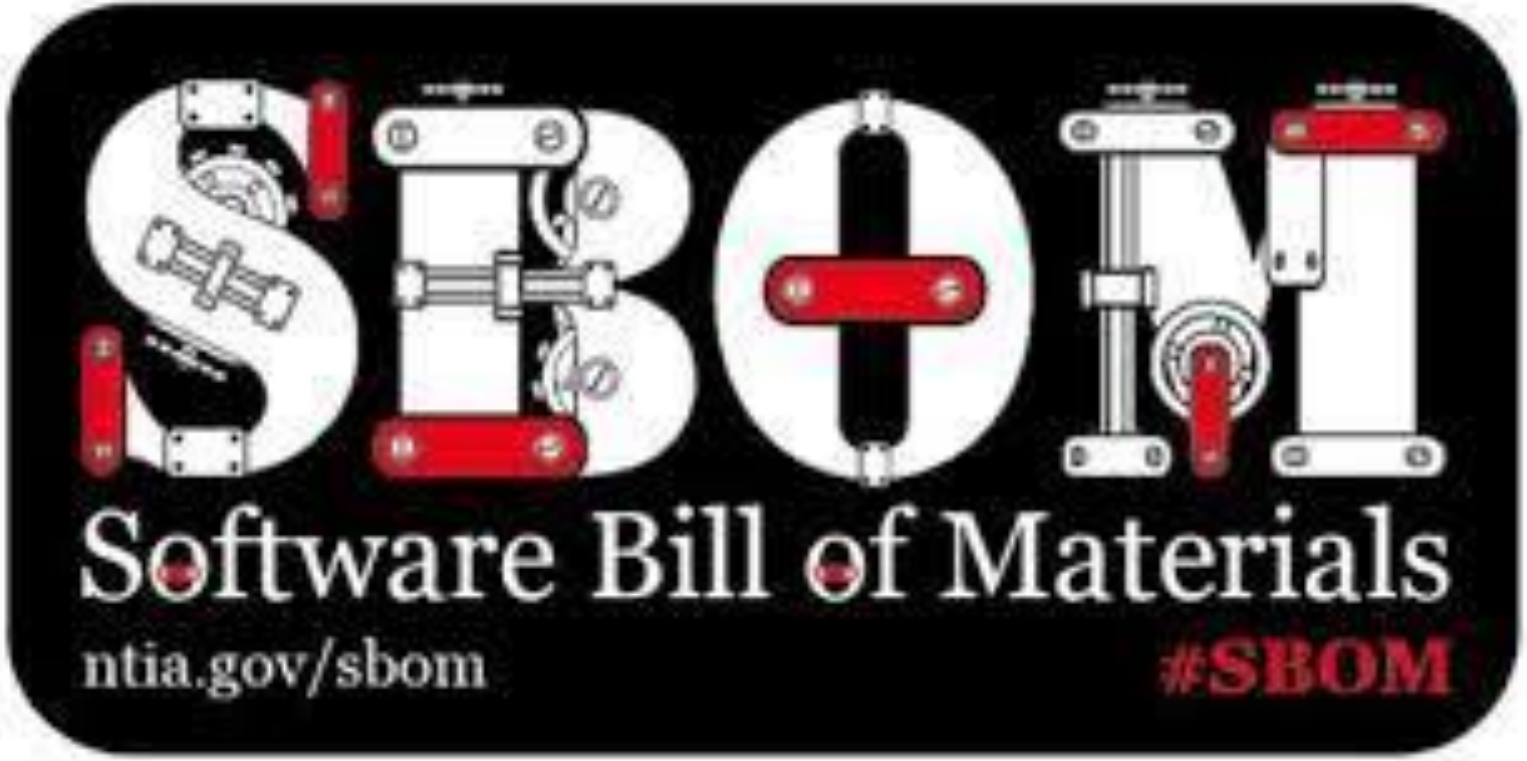
Make it run

We need to make sure everyone can bring their ideas and at the same time, have them aligned with something that can be run in a product

Make it useful

Collect implementation tests, disseminate the feedbacks and improve


OXA sub-project proposed
First Github commits
Let’s launch the mailing list subscription signs of interest!
03.02.23
20.04.23
July 2023
H2 2023
11.04.24
OXA sub-project approval
Startup tunnel



Duncan Sparrell

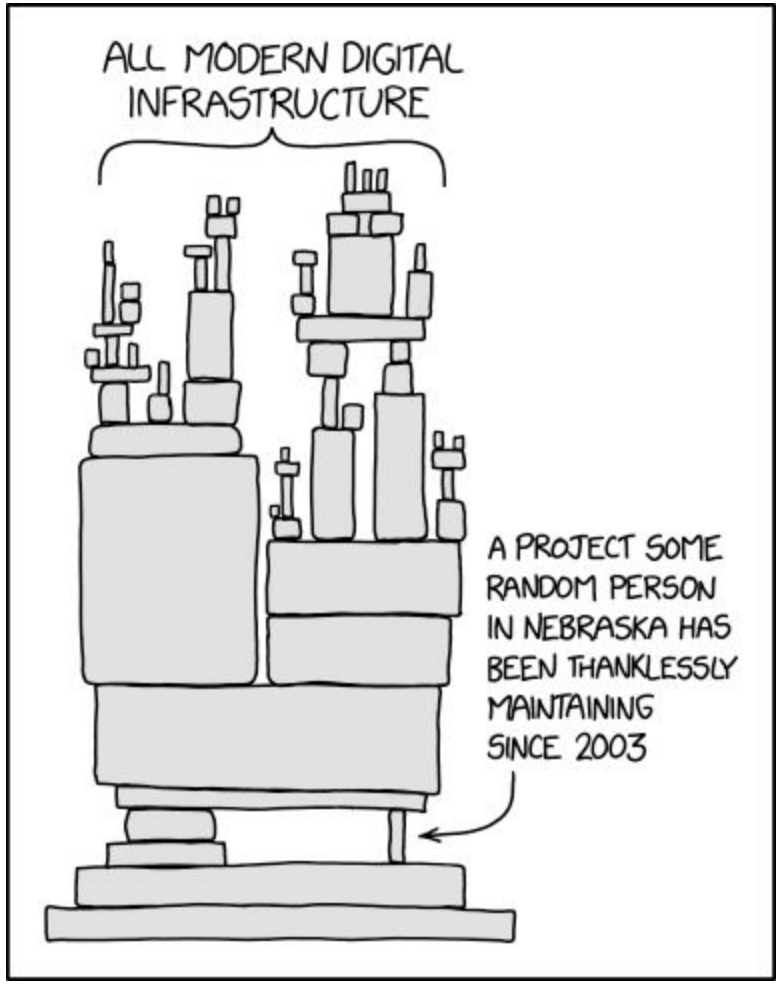

CISA
SBOM
CISA.GOV/SBOM

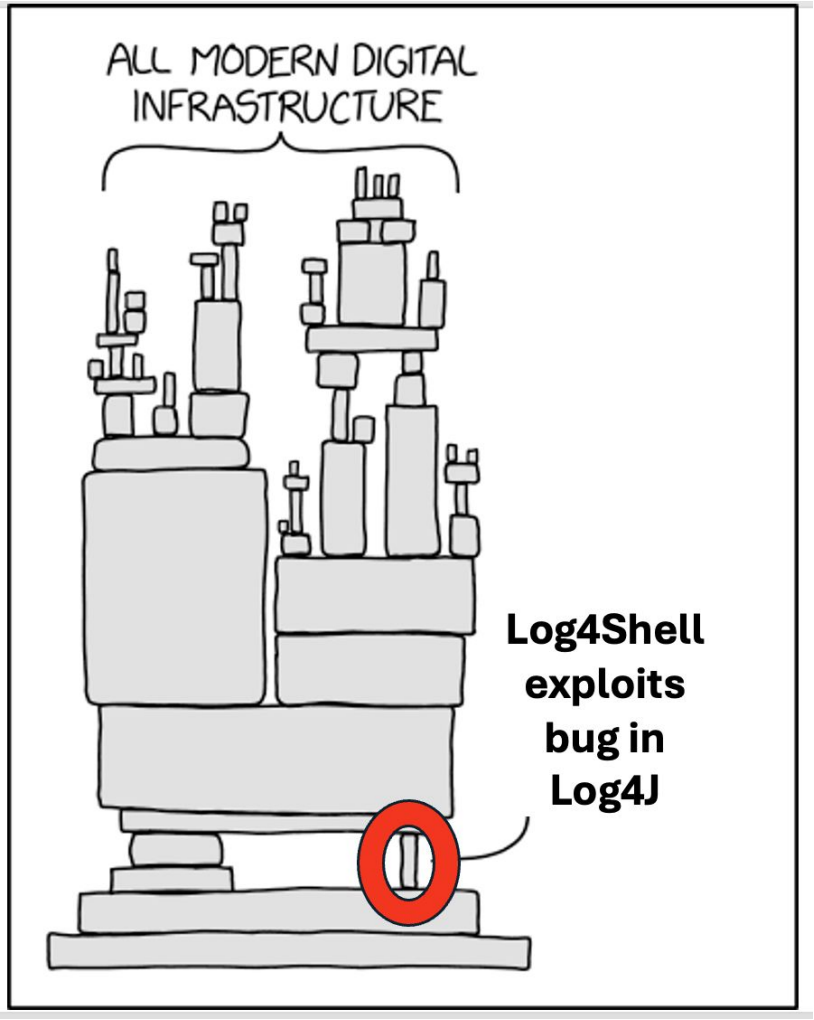
SBOM Facts

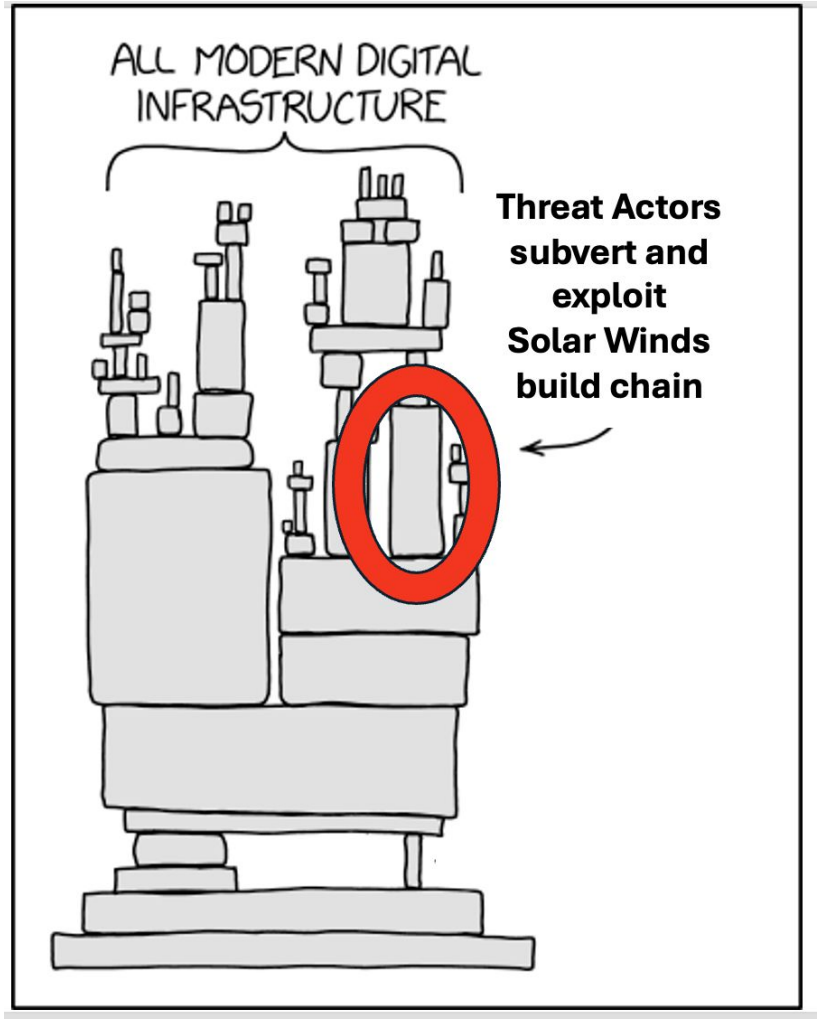
At its most simplistic level, an SBOM is a list of "ingredients" that describes the components in a software application.

Elements

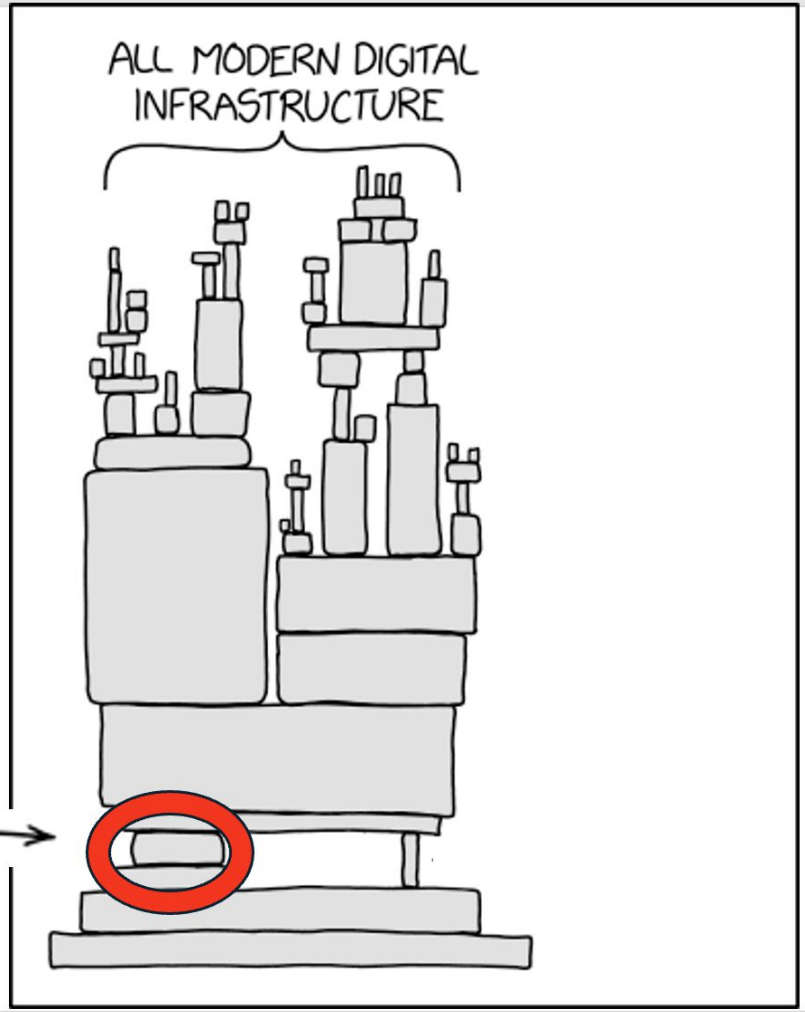
		% Daily Value*
Supplier Name	The name of an entity that creates, defines, and identifies components.	%
Component Name	Designation assigned to a unit of software defined by the original supplier.	
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.	%
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.	%
Dependency Relationship	Characterizing the relationship that an upstream componentX is included in software Y.	%
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.	
Timestamp	Record of the date and time of the SBOM data assembly.	%


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003


ALL MODERN DIGITAL INFRASTRUCTURE
Log4Shell exploits bug in Log4J


ALL MODERN DIGITAL INFRASTRUCTURE
Threat Actors subvert and exploit Solar Winds build chain

Threat Actors subvert (2021) and exploit (2024) xz open source




SHOW
ME THE
MONEY!

Why *SBOM* and why now?

- Increasing supply chain cybersecurity threats
- New SEC Rules, Government Regulations
- Increasing third-party and supply chain, 8k filings, etc.
- EO 14028 (for Federal Business... or everyone)
- Increased director risk
- Increased cyber physical risk increases safety risk

For $STUFF we Buy

Cost Risk/Opportunity

- Maximizing CAPEX/OPEX
- Shifting/sharing burden with suppliers / rebalancing cyber risk
- Resilience
- Reduce elective risks:
  - brand/reputation
  - regulatory
  - legal
  - revenue

For $STUFF we Sell

Revenue Risk/Opportunity

- Federal Gov Direct Sales
- Sales to Federal Gov Suppliers
- Healthcare, Energy, Transportation Sector Sales
- Sales to Regulated Industries
- Brand Reputation
- Direct/Indirect Impact of Compromise
- Marketshare
- Shifting/sharing burden with suppliers / rebalancing cyber risk

There is never enough time.

Thank you for yours.

Omar Santos &
Justin Murphy

https://csaf.io

Common Security Advisory Framework (CSAF) is a language to exchange Security Advisories and Vulnerability eXploitability Exchange (VEX) information. It plays a crucial role in the cybersecurity arena since it allows stakeholders to automate the creation and consumption of security vulnerability information and remediation.

Common Security Advisory Framework (CSAF)

- International, open and free OASIS standard
- Machine-readable format for security advisories (JSON) and VEX
- Standardized way for distribution of security advisories
- Built with automation in mind
- Standardized tool set
- Guidance for actionable information
- CSAF allows for linking to SBOM data
- Successor of CVRF 1.2

https://www.cisa.gov/news-events/news/transforming-vulnerability-management-landscape

BLOG

Transforming the Vulnerability Management Landscape

Released: November 10, 2022

Revised: November 14, 2022

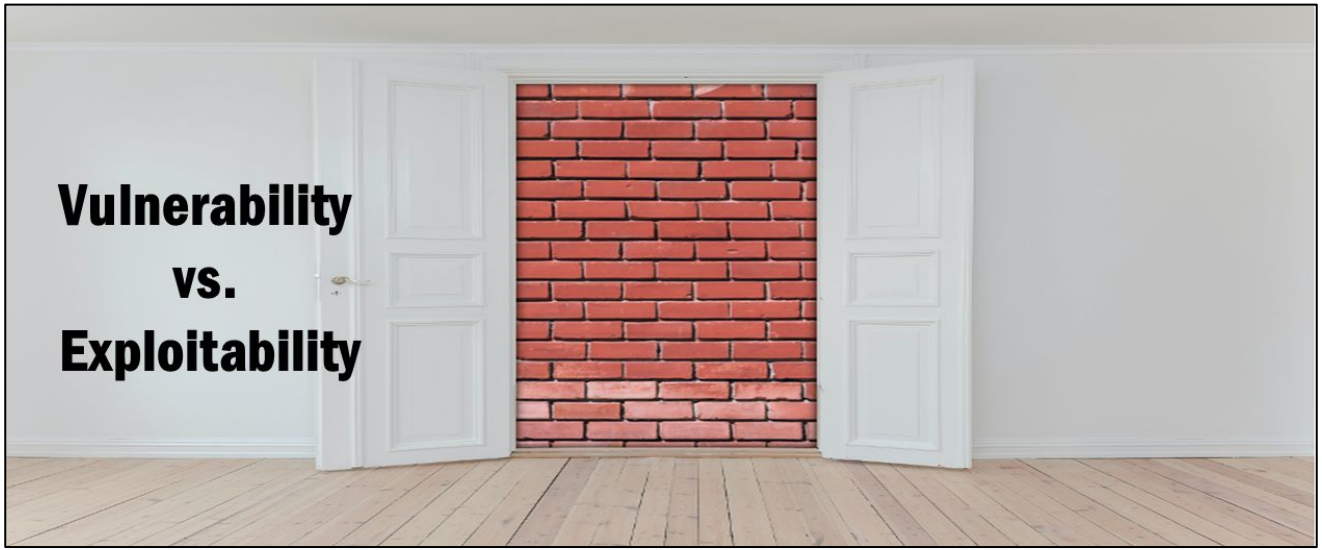
Eric Goldstein, Executive Assistant Director for Cybersecurity

In the current risk environment, organizations of all sizes are challenged to manage the number and complexity of new vulnerabilities. Organizations with mature vulnerability management programs seek more efficient ways to triage and prioritize efforts. Smaller organizations struggle with understanding where to start and how to allocate limited resources. Fortunately, there is a path toward more efficient, automated, prioritized vulnerability management. Working with our partners across government and the private sector, we are excited to outline three critical steps to advance the vulnerability management ecosystem:

- First, we must introduce greater automation into vulnerability management, including by expanding use of the Common Security Advisory Framework (CSAF)
- Second, we must make it easier for organizations to understand whether a given product is impacted by a vulnerability through widespread adoption of Vulnerability Exploitability eXchange (VEX)

What is VEX?

Vulnerability Exploitability eXchange (VEX) indicates the status of a software product or component with respect to a vulnerability.



https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/guidance/faq.md#what-is-vex-and-how-is-it-supported-in-csaf

What is VEX?

- A common VEX use case is to indicate that software is or is not affected by a vulnerability.
- Born from the SBOM work.
- Works with SBOM, or independently.
- One vulnerability, one status, one or more components.
- Machine-readable allowing technology consumers, vendors, providers, and coordinators to accelerate vulnerability management.

Current state of CSAF (and VEX)?

- CSAF 2.0 is now supported by several vendors, coordination agencies, government organizations (such as CISA)
- Several security vendors now support CSAF (e.g., Manifest, CyBeats, Trivy, SecOps Solutions, etc.).
- A few enhancements underway with CSAF 2.1.

What is next for CSAF 2.1?

- Integration of CVSSv4
- TLPv2 support
- Several enhancements to the schema.
- The current work items can be found at our GitHub repository:

  https://github.com/oasis-tcs/csaf/issues?q=is%3Aissue+is%3Aopen+label%3A%22csaf+2.1%22

Omar Santos &
Justin Murphy

https://openeox.org

The OASIS OpenEoX is an initiative aimed at standardizing the way End-of-Life (EOL) and End-of-Support (EOS) information is exchanged within the software and hardware industries. Covering both vendors and open-source maintainers, OpenEoX strives to provide a transparent, efficient, and unified approach to managing product lifecycle.

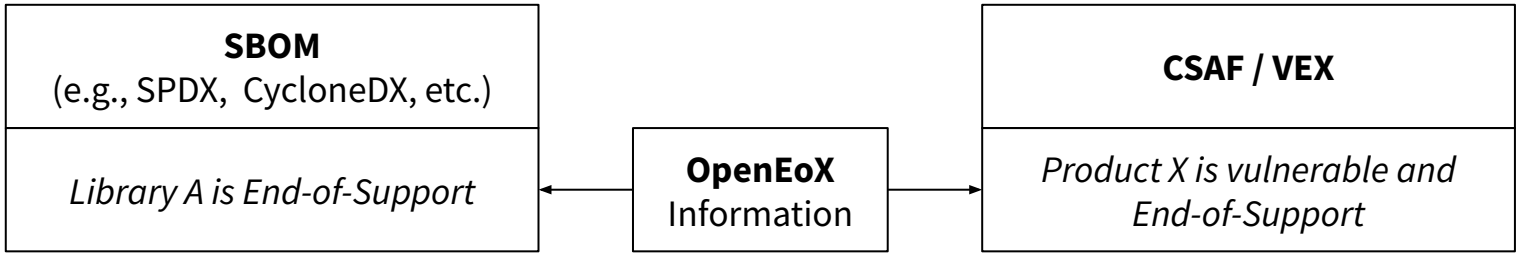
OASIS OpenEoX

- International, open and free OASIS standard effort
- Standardized, machine-readable method for exchanging EoX information
- Focused on providing transparent, efficient, and unified approach to managing product lifecycle.
- Built with automation in mind.
- Founding members of the OpenEoX Technical Committee include Cisco, Microsoft, Red Hat, Siemens, BSI, and CISA. Many organizations have joined since the OpenEoX TC was introduced.

https://openeox.org

Goal: Lightweight and Standalone Schema

A lightweight schema to allow the integration of OpenEoX information within an SBOM, CSAF/VEX document:



OpenEoX Standalone schema will also allow independent operation.

Get Engaged Today!

Whether you're a vendor, open-source maintainer, industry expert, or an enthusiastic volunteer, your contribution is invaluable.

Join us in our mission to create a more sustainable, predictable, and transparent technology ecosystem.

Get involved today to help define the OpenEoX standard and associated tools.

https://openeox.org

https://github.com/oasis-tcs/openeox

Duncan Sparrell

Posture **A**ttribute **C**ollection & **E**valuation

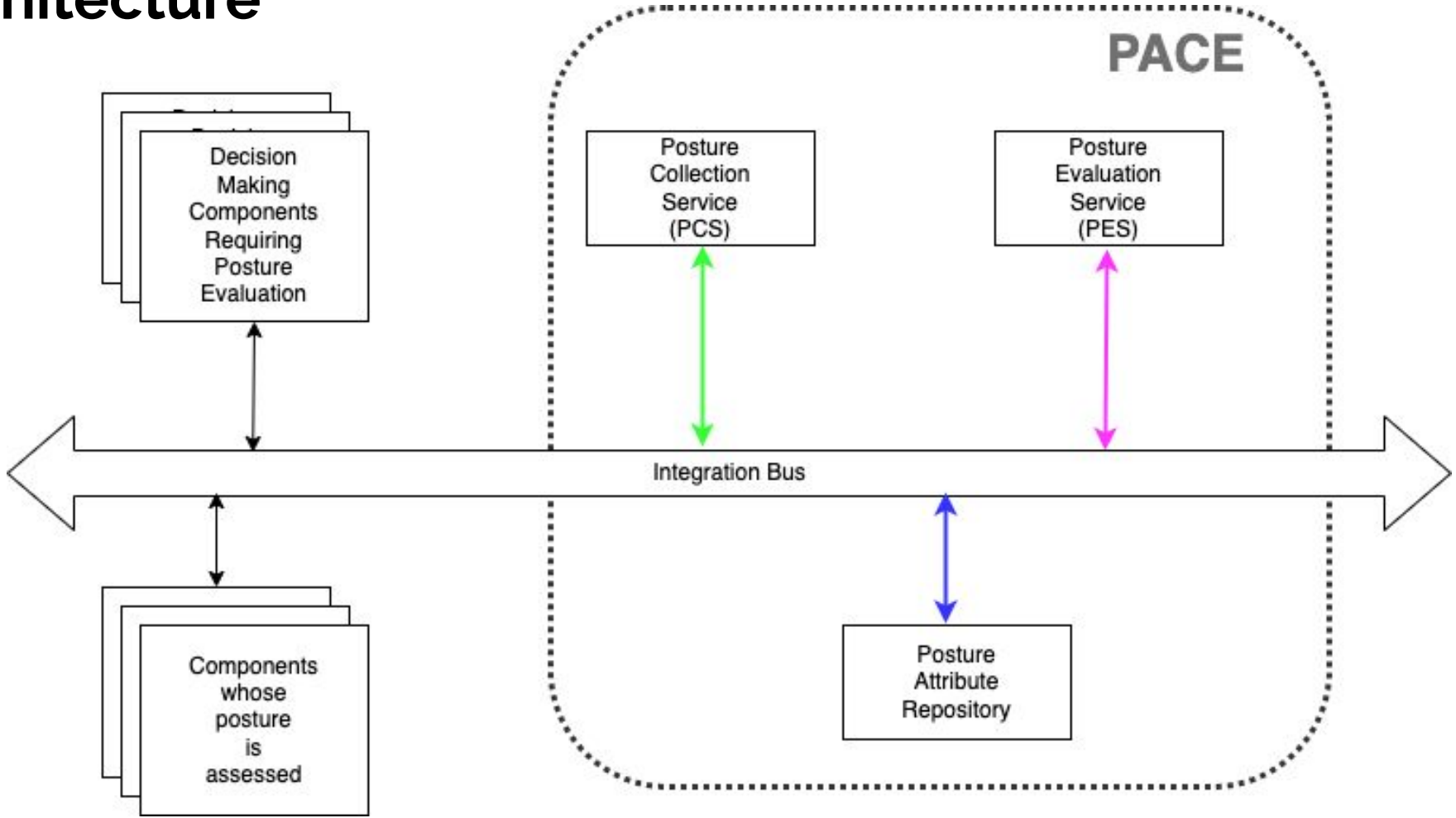
A comprehensive automated strategy for understanding security posture and what to do about it.

Security Posture

Attributes

Posture assessment generally consists of understanding, for a given computing resource (or set of computing resources), software load, composition of that software load, patch levels, vulnerability, and configuration state. Together, these attributes of a computing resource represent its cybersecurity posture.

Architecture



There is never enough time.

Thank you for yours.

Ian Craggs

MQTT is a Client Server publish subscribe messaging transport protocol. It is low overhead and designed so as to be easy to implement. Ideal for IoT contexts where a small code footprint is required and network bandwidth is at a premium.

The problem

Context

Collecting data from industrial devices used disparate, vendor-specific protocols.

Time to market was key, so each vendor developed their own method, usually based on polling.

Problem statement

Polling relies on the server regularly contacting all devices, whether or not their data has changed.

A server can be overloaded with communications to a large number of devices, even if their data changes infrequently.

Approach

MQTT:

- allows devices to only send changed data to a server
- TCP/IP for reliability
- implementation by any device vendor
- embedded devices need MQTT stability

Challenges deep-dive

Challenge 1

Challenge 2

Challenge 3

Expand beyond TCP/IP

MQTT 3.1.1 and 5.0 are laid over TCP/IP.

The goal of MQTT-SN is to allow MQTT-style solutions to incorporate non-TCP networks.

Security

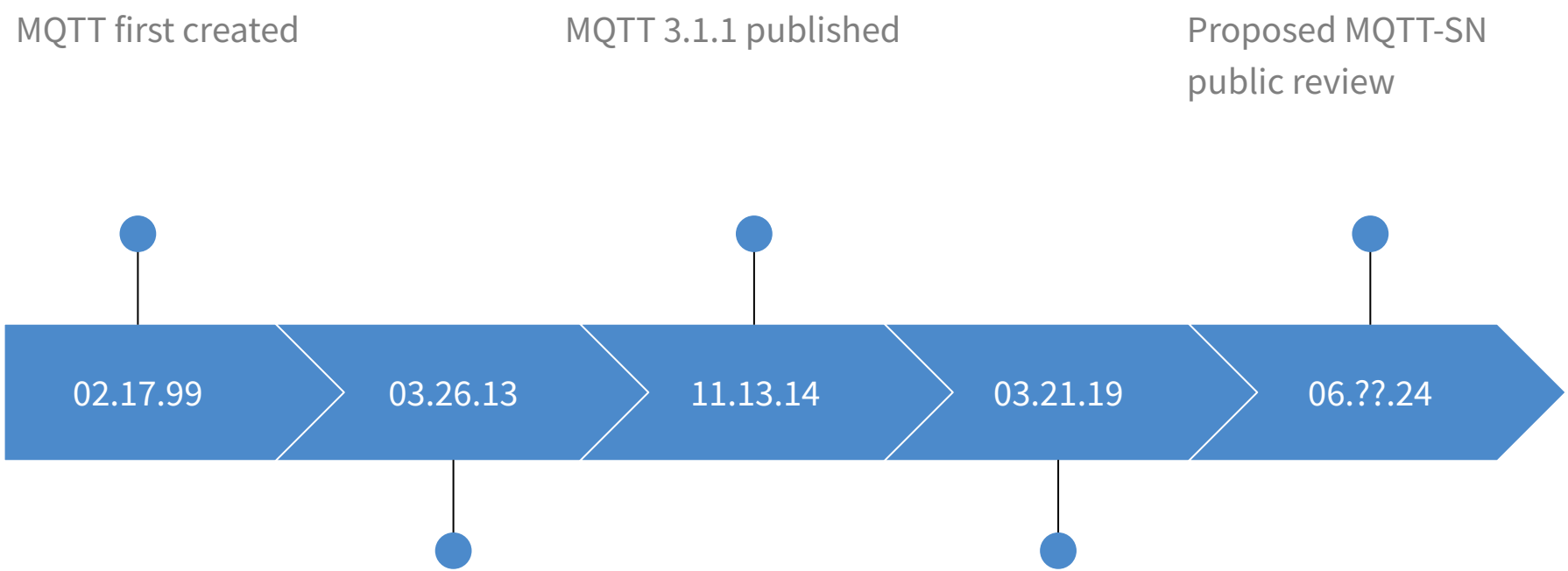
MQTT relies on TLS. DTLS is often too heavyweight.

MQTT-SN proposes a per-packet lightweight encryption and authentication mechanism.

MQTT family vision

MQTT-SN is a departure from previous MQTT versions.

Integrate with other MQTT based standards such as Eclipse Sparkplug.


MQTT first created
MQTT 3.1.1 published
Proposed MQTT-SN public review
02.17.99
03.26.13
11.13.14
03.21.19
06.??.24
MQTT Introduced to OASIS
MQTT 5.0 published

SCIM

Duncan Sparrell

Supply **C**hain

Information **M**odeling

Standardize and promote all aspects of supply chains.

Initial focus on SBOM, VEX and software supply chain

Or maybe?

OSIM

Duncan Sparrell

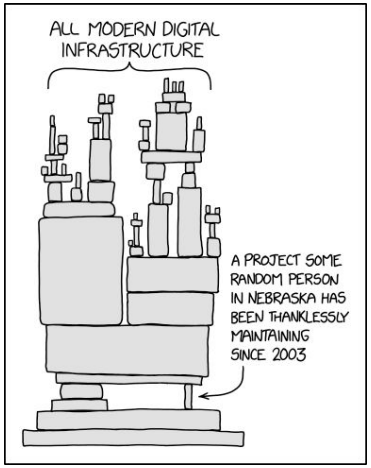
Open

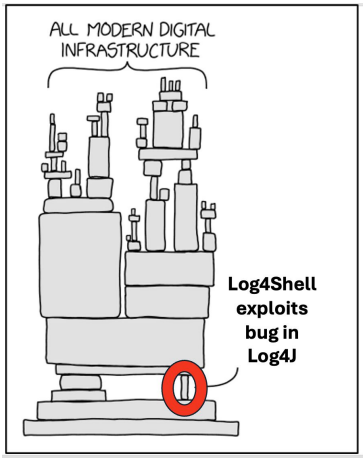
Supplychain

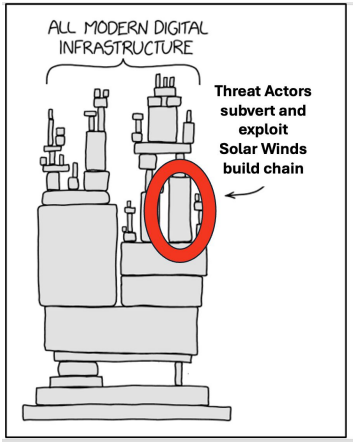
Information **M**odeling

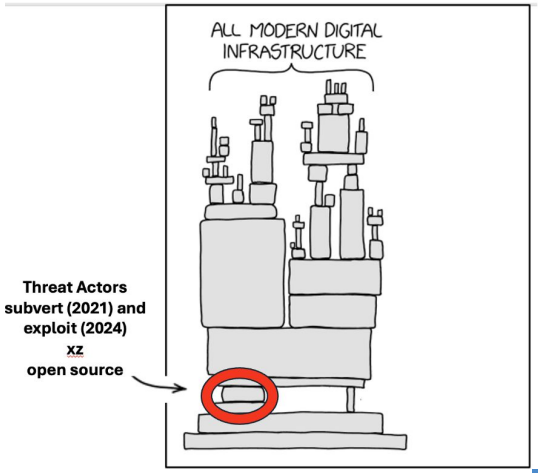
Standardize and promote all aspects of supply chains.

Initial focus on SBOM, VEX and software supply chain









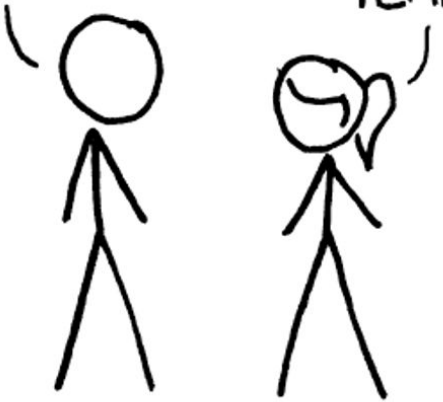
Why Supply Chain?

- The risk shown by lack of support in adjacent XKCD comic
- Log4J
- Solar Winds
- XZ

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

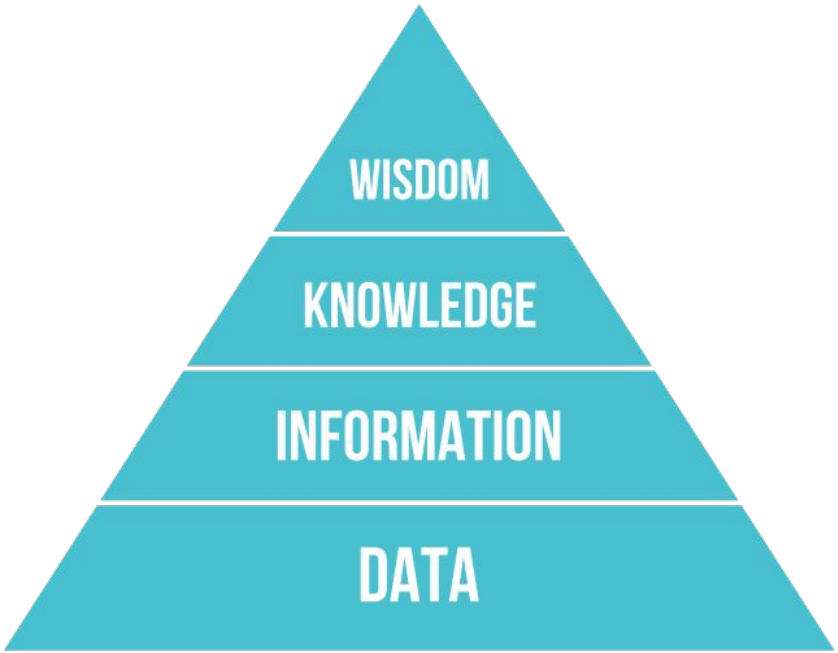
SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

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

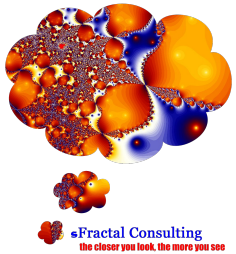


SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.



Why Information Modeling?



Co-proposers

There is never enough time.

Thank you for yours.

Thank you