Enhanced SBOM for Optimized Software Sustainment (E-BOSS)

Dr. Sergey Bratus
Program Manager
Information Innovation Office (I2O)

Proposers Day

December 13, 2023

Program objective

Develop Enhanced Software Bill of Material (eSBOM) metadata technology to enable rapid triage-and-remediation of vulnerabilities in software at scale

Key technical hypothesis:

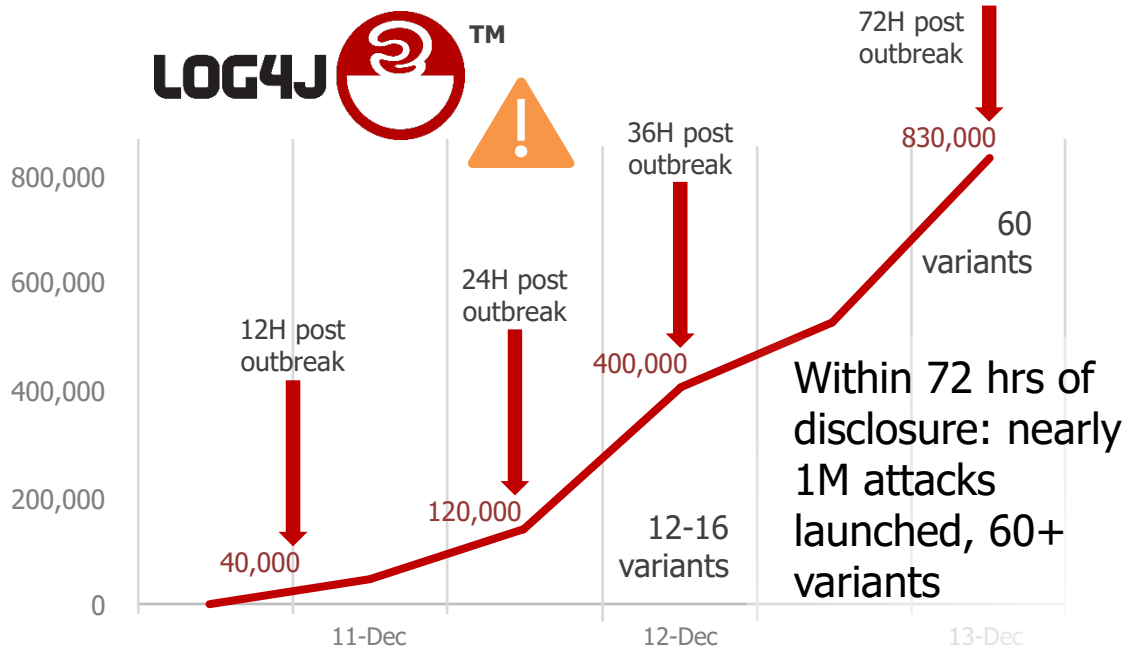
New metadata* and algorithms added to a SOTA software tool chain** will dramatically accelerate triage and remediation at scale

* Data flows, control flows, pre- and post-conditions, aliasing, and separation conditions

** Consisting of optimizing compiler, linker, CI/CD pipeline, and multiple programming language runtimes

(U) Acronym list:
CI/CD - Continuous Integration and Continuous Delivery
SOTA - State-Of-The-Art

We fail at triage and remediation at scale



Log4Shell vulnerability in Log4j: response did not scale

- Nearly 1M attacks launched in 72 hours since disclosure
- Average 12-17 days to patch
- Over 30% remained unpatched in over 3 months
  - 98 distinct Log4j versions in the wild, 55% vulnerable
- Unnoticed in the open-source code base for **7 years**
- **Gap:** No automated tools to decide if the flawed code is actually reachable and triggerable

https://blog.qualys.com/qualys-insights/2022/03/18/qualys-study-reveals-how-enterprises-responded-to-log4shell

Ground truth of today's large software ecosystems:

- ~10,000s of crash reports per day, up to 1 month of bespoke analysis to recover trigger for a crash
  - Vendors typically will not repair bugs without a reproducible trigger
  - **Gap:** Automated analyses of potential paths to the crash site don't scale, a.k.a. "state explosion"

ShellShock: direct insertion of hostile commands into web app gateways was unnoticed for **20 years**

- **Gap:** No support for data path analyses between components of a software system

Critical need to protect software supply chains, Executive Order 14028

THE WHITE HOUSE

Administration Priorities The Record

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

- Executive Order (EO) 14028 aims to reduce cyber threats and improve maintainability of software purchased by the Government
- EO 14028 creates a policy foundation for software component transparency in software supply chains

```
2   "bomFormat": "CycloneDX",
3   "specVersion": "1.2",
4   "serialNumber": "urn:uuid:b4f2954f-a96d-4578-9509-1
5   "version": 1,
6   "metadata": {
7     "timestamp": "2020-08-02T21:27:04Z",
8     "tools": [{
9       "vendor": "CycloneDX",
10      "name": "CycloneDX Maven plugin",
11      "version": "2.0.2",
12      "hashes": [
13        {
60  "components": [
61    {
```

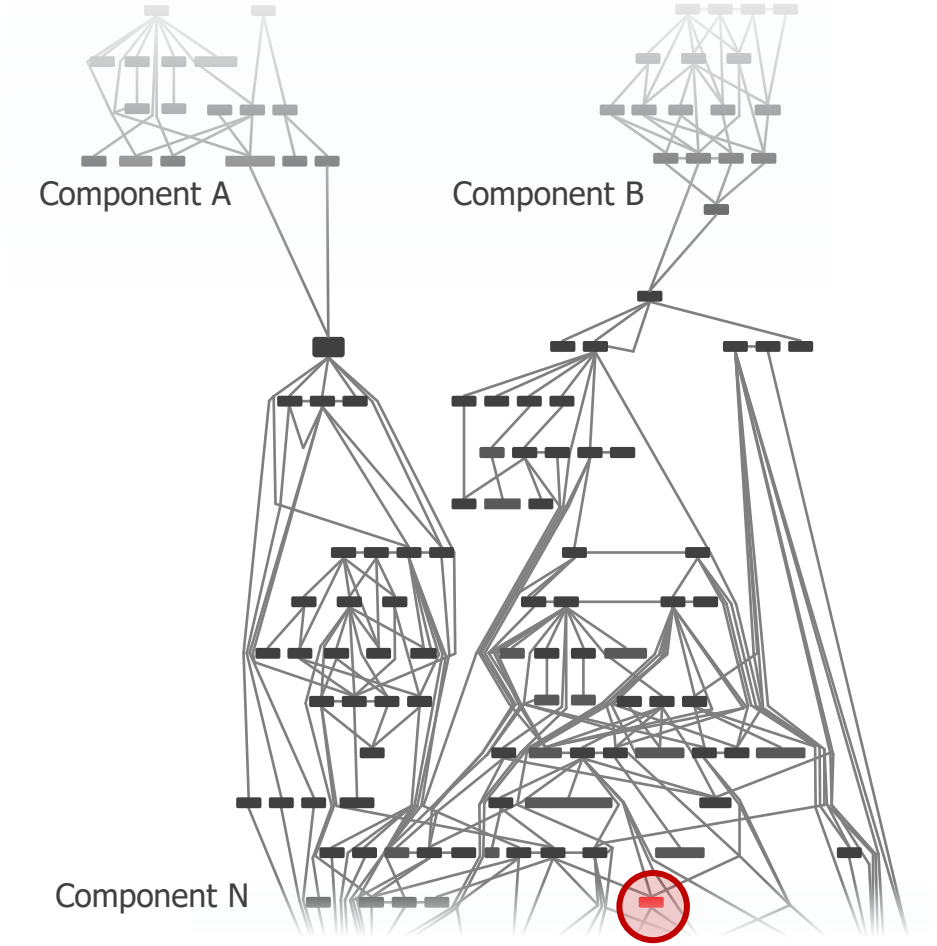
Sample SBOM: is a manifest

Has limited utility for cyber reasoning

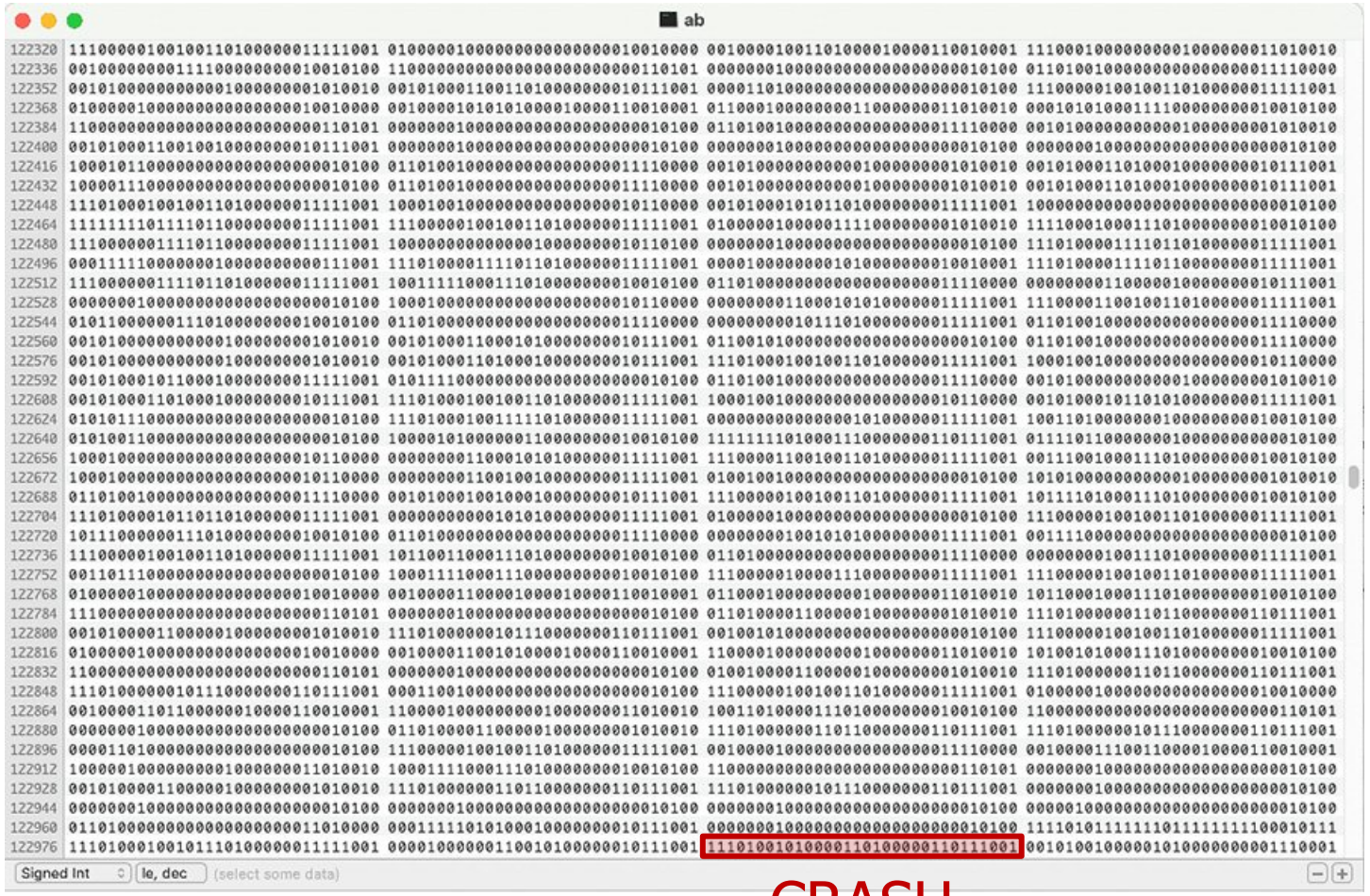
- Caveat: SBOM is **a list of parts**. However a system is more than the sum of its parts.

Enhanced SBOM and new tools are needed to respond to vulnerabilities at scale and optimize system sustainment and modernization

Flaw evidence is far removed from the initial entry-point and triggers

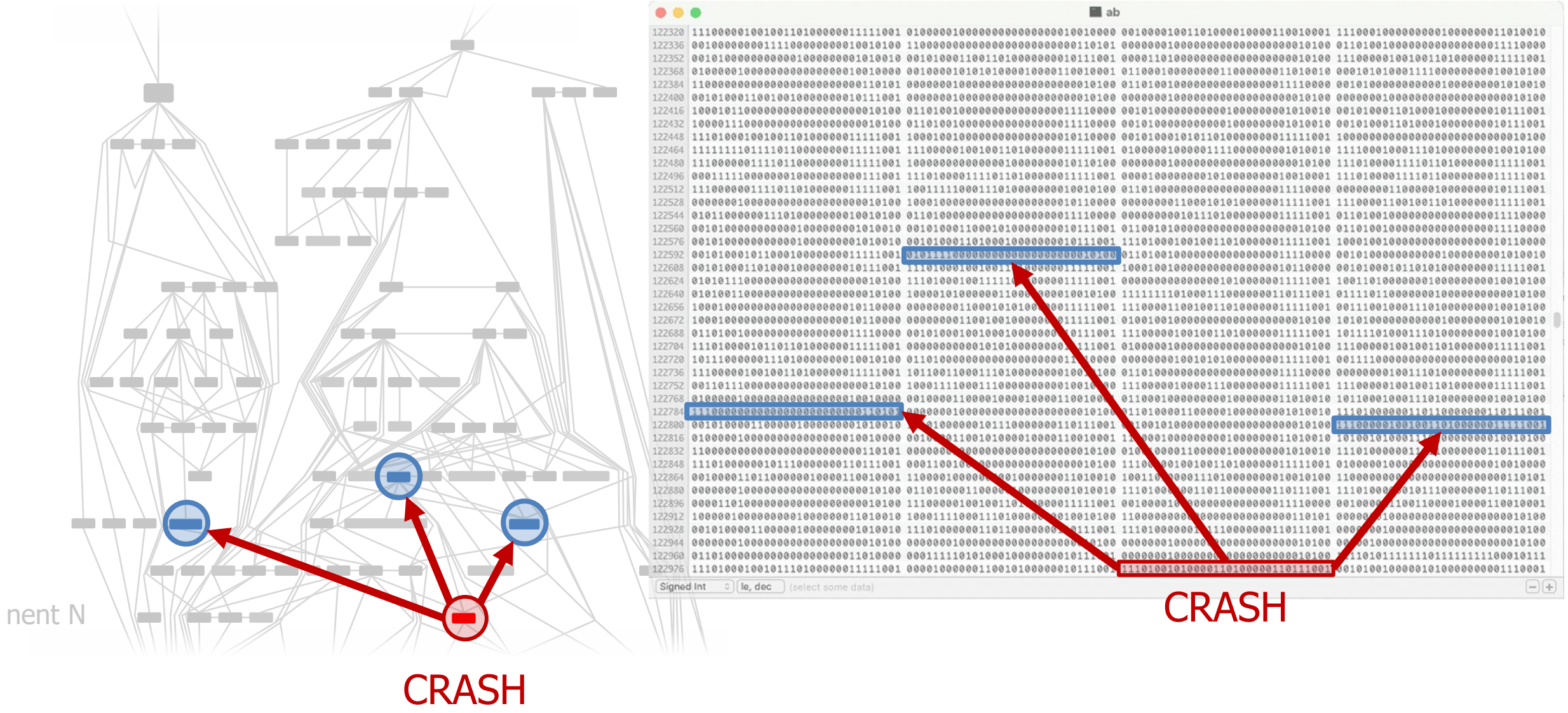


CRASH

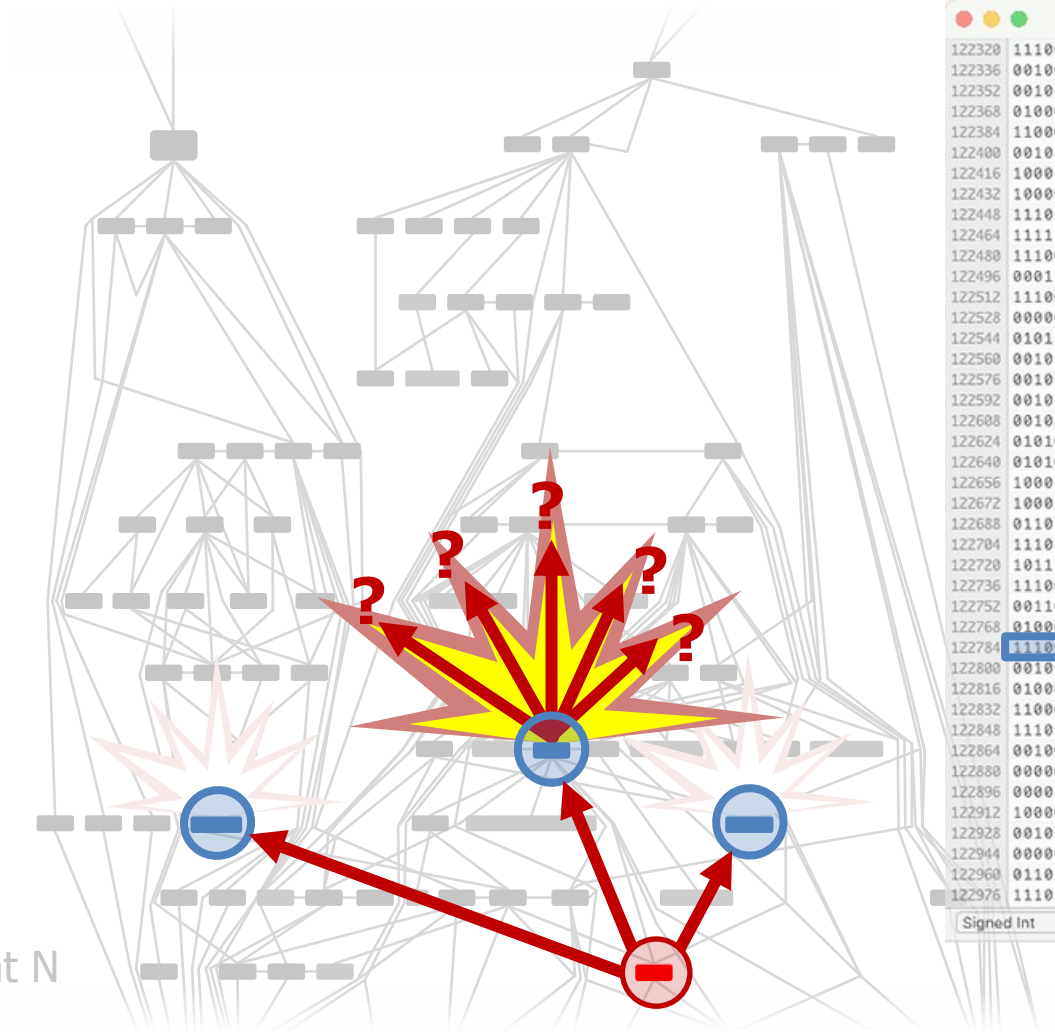


CRASH

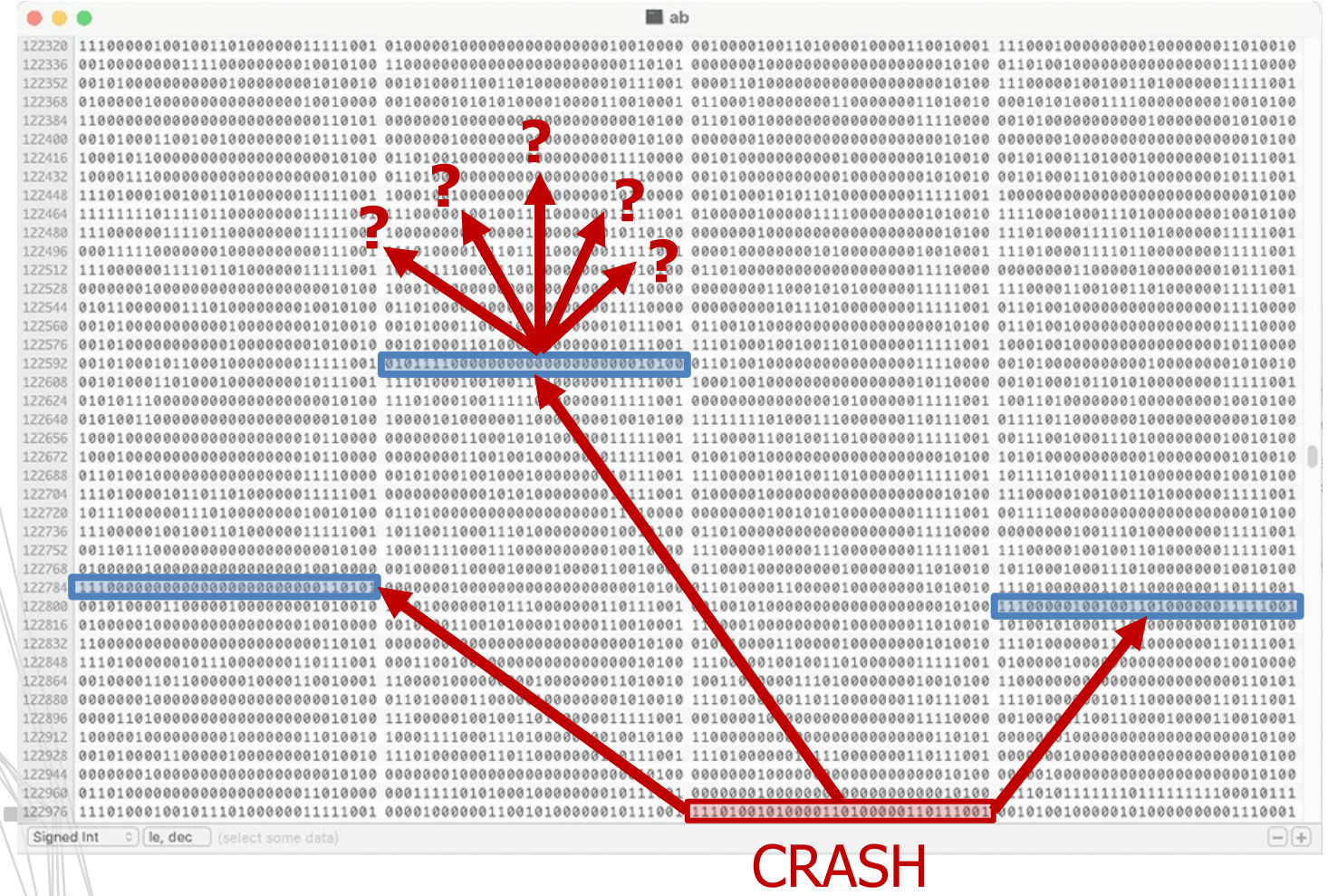
Working back along code paths quickly leads to state explosion



Backward analysis quickly becomes intractable, requires weeks, often fails

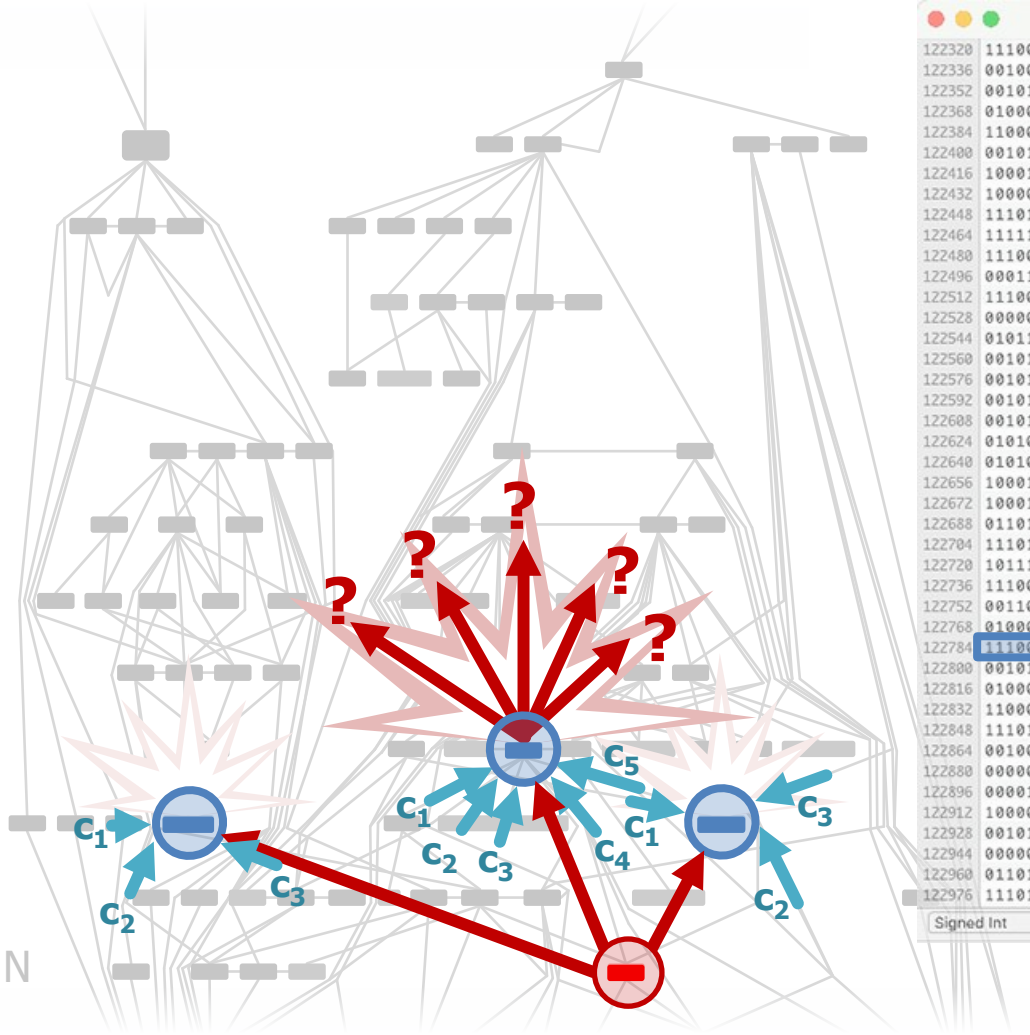


Flow analysis

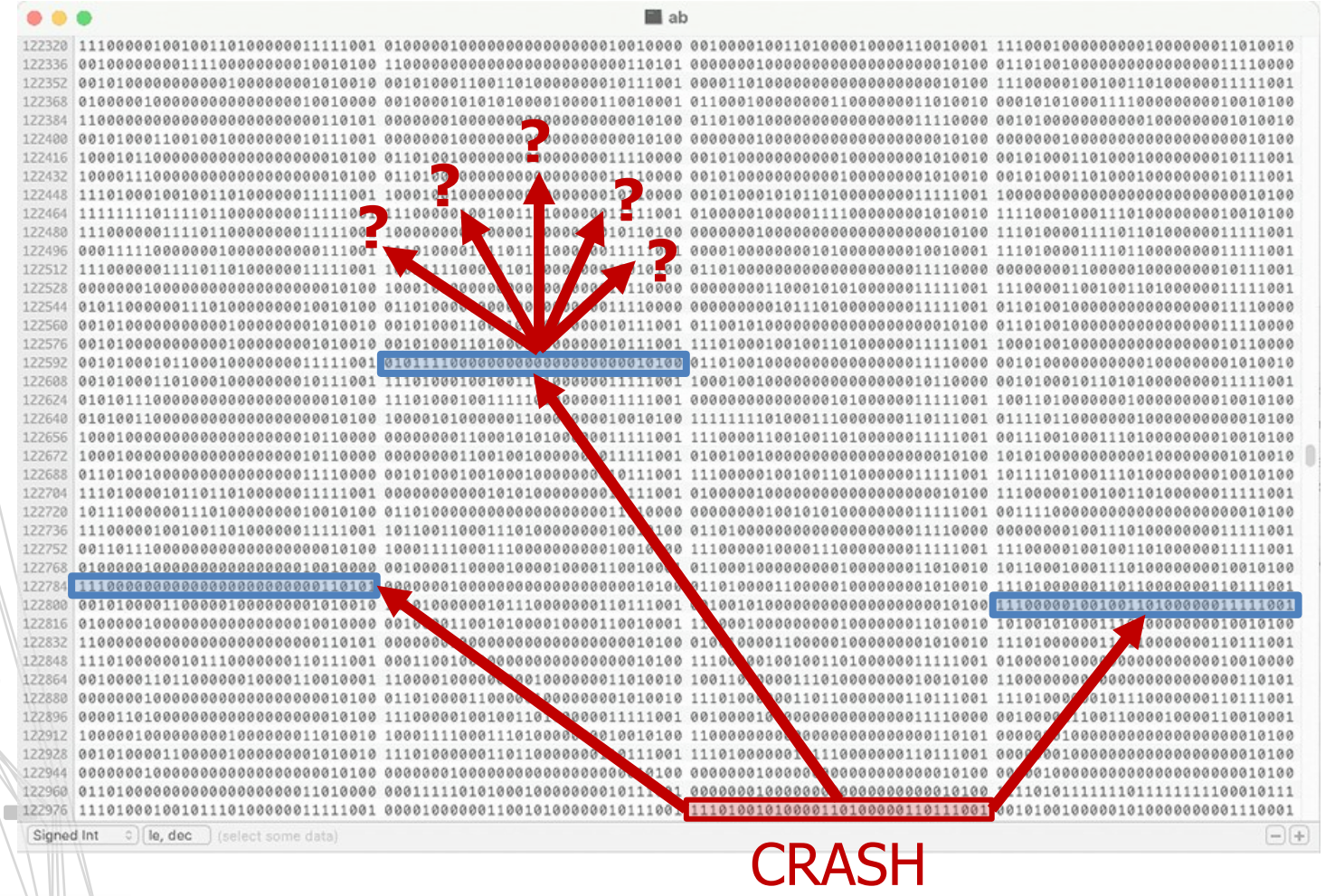


Traceback becomes **intractable**

Backward analysis quickly becomes intractable, requires weeks, often fails

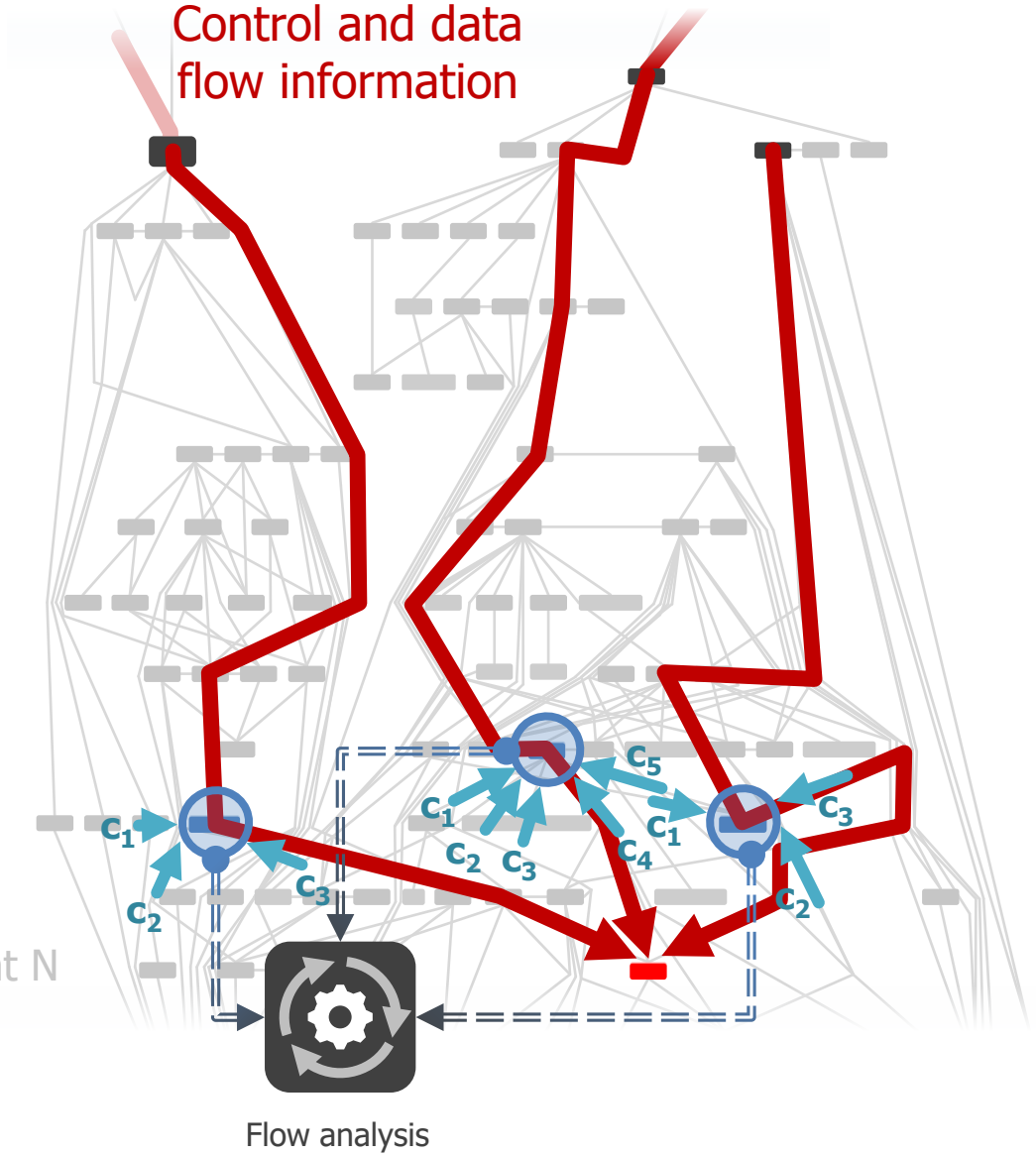


Flow analysis

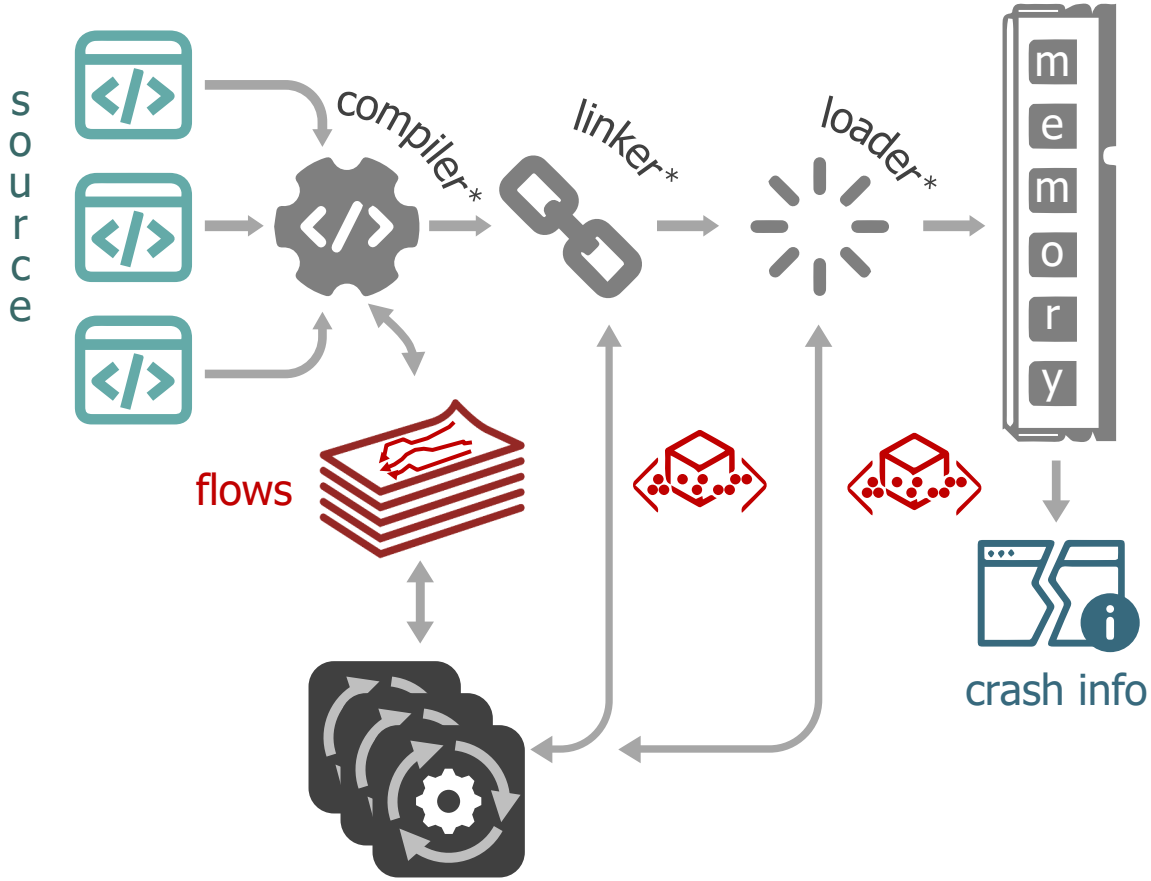


Hypothesis: Additional program analysis and metadata can control state/path explosion

Compilers, linkers and loaders should aid remediation at scale

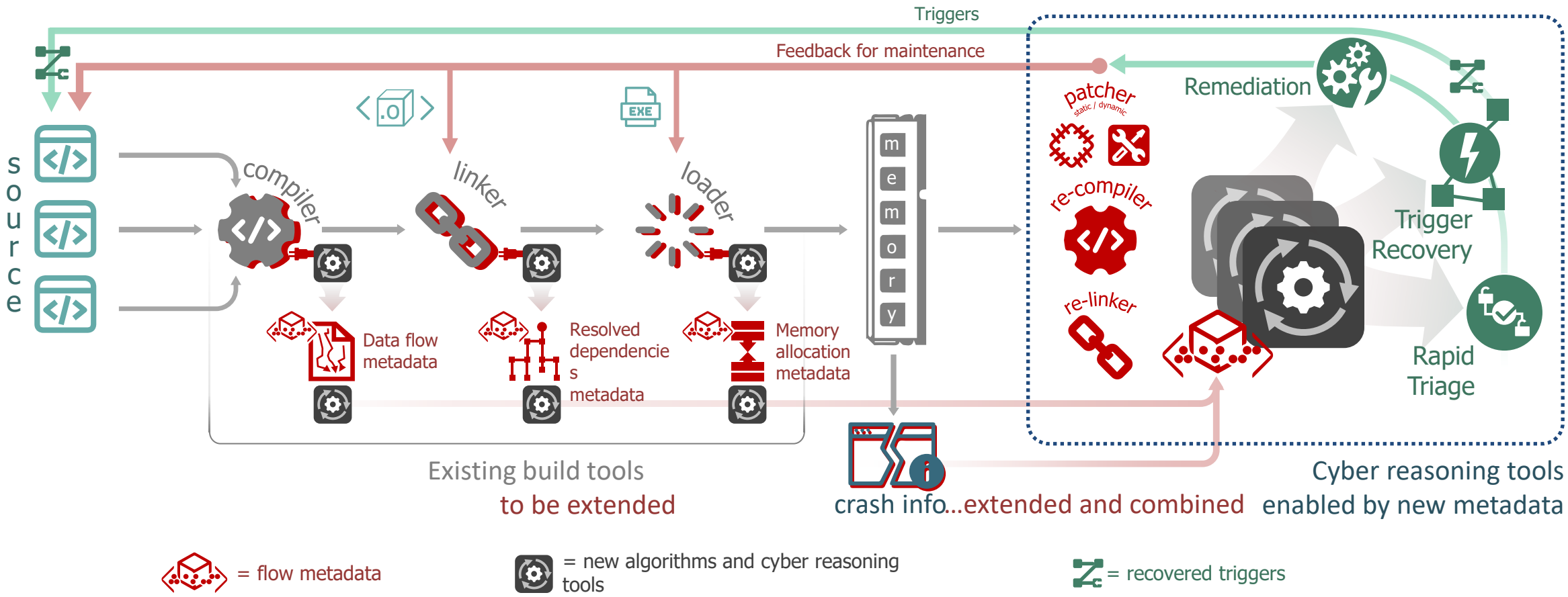


Flow analysis



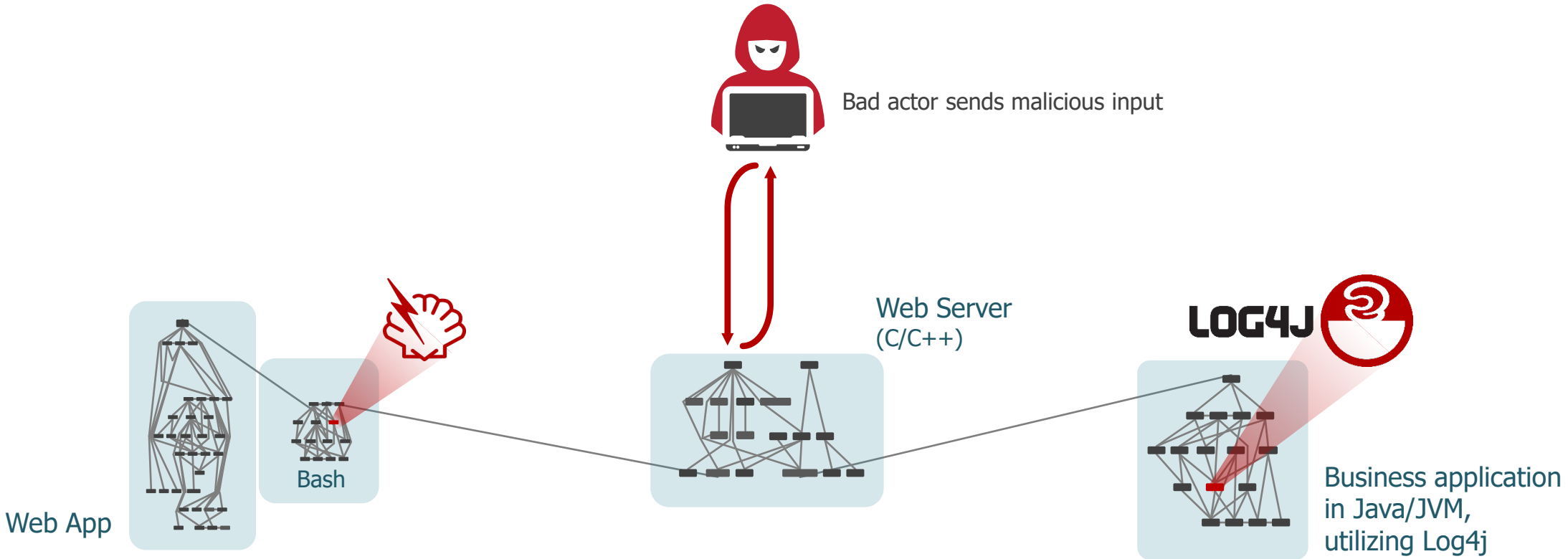
Novel analysis and metadata throughout the toolchain will enable triage and trigger recovery

Vision: enhance SBOMs with flow metadata to trace flaws to triggers

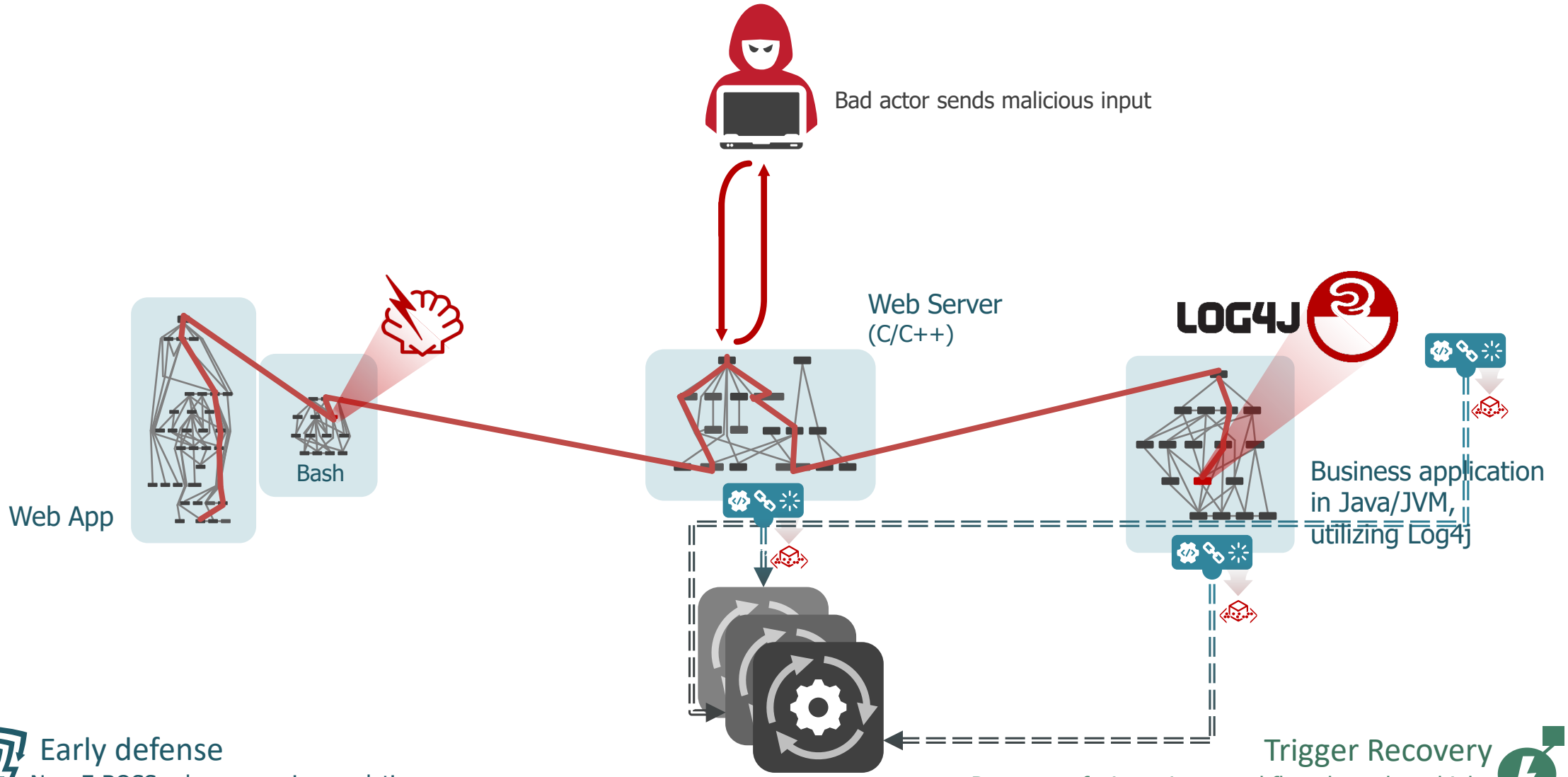


- Keep advanced metadata in addition to symbols to effectively trace back flaw evidence to triggers
- Enhance SBOMs with new types of rich metadata, enabling cyber reasoning for triage and remediation
- Remediate with eSBOMs: Recover paths and triggers to crash site from crash snapshots ("crash dumps"), remediate by blocking triggers once recovered
  - Block triggers and flows leading to quick remediation

Rapidly mitigating vulnerabilities in multi-runtime environments



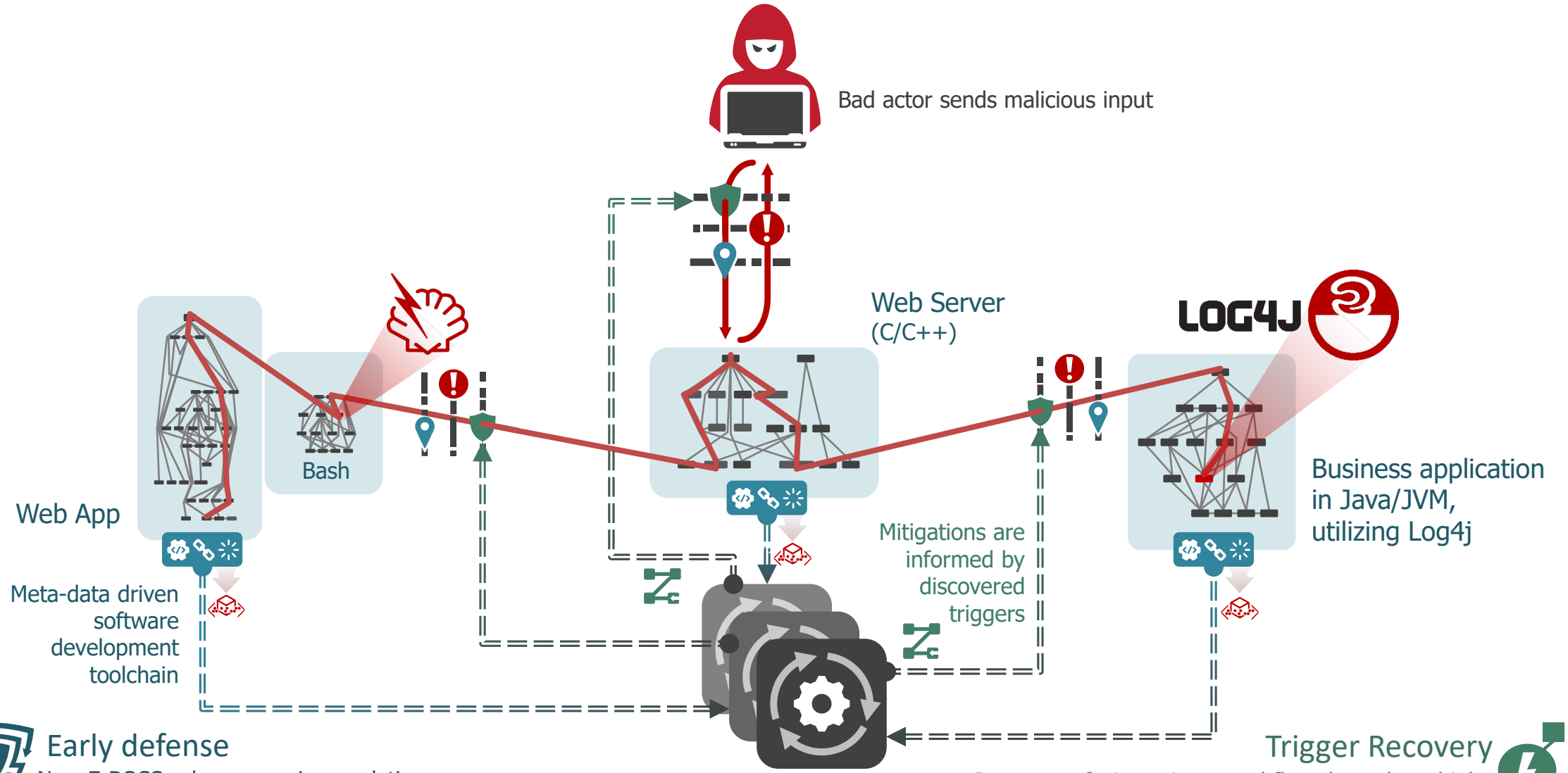
Rapidly mitigating vulnerabilities in multi-runtime environments



Early defense
New E-BOSS cyber reasoning analytics as part of DevSecOps pipeline

Trigger Recovery
Recovery of trigger input and flow through multiple components on various networks and systems

Rapidly mitigating vulnerabilities in multi-runtime environments



Early defense

New E-BOSS cyber reasoning analytics as part of DevSecOps pipeline

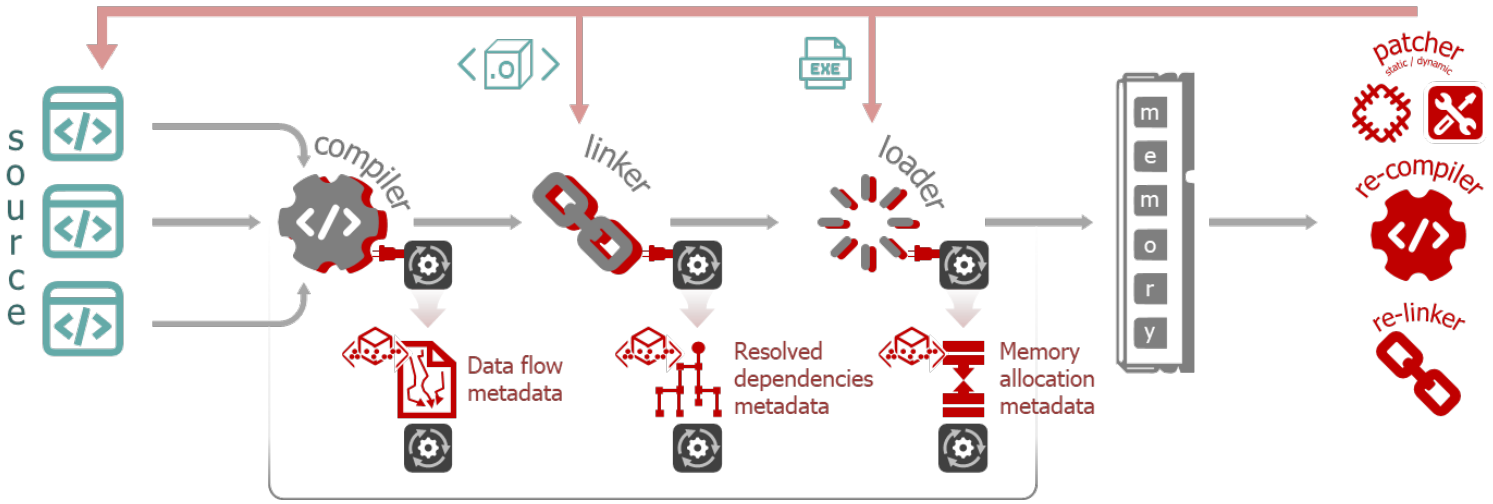
Trigger Recovery

Recovery of trigger input and flow through multiple components on various runtimes and systems

TA1: Production build chains for enriched SBOMs (eSBOMs) and cyber reasoning

TA1: BUILD WITH eSBOMs

Develop **enhanced SBOM with new types of metadata and compiler/linker/loader extensions** to generate them

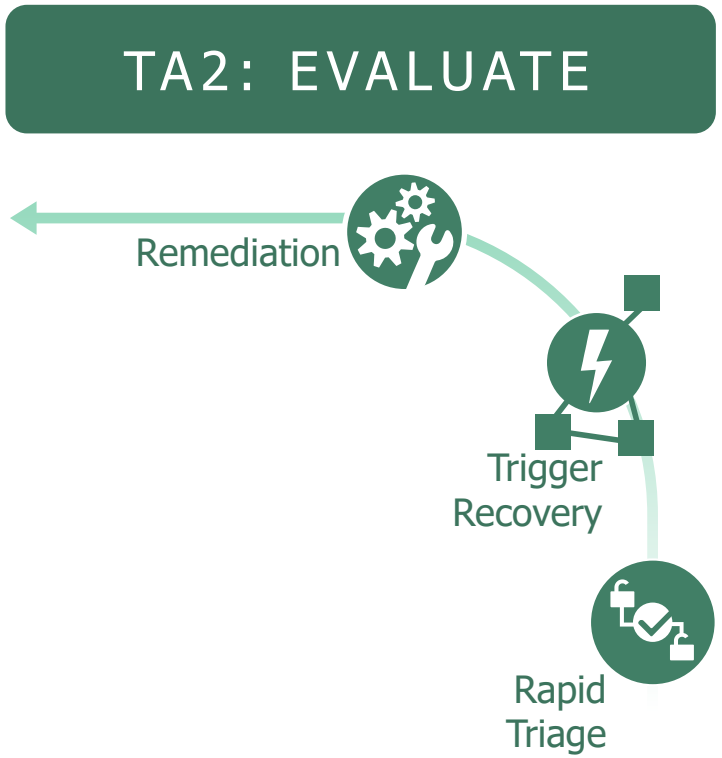


- Design and automatically generate fine-grained data about control and data flows, and inter-component interactions
- Design metadata tailored to software goals, mission requirements, and prioritization
- Develop algorithms in modern build chains and compiler extensions for unifying program analysis techniques
- Achieve adoptable performance

Develop **cyber reasoning and remediation tools** that use eSBOMs to enable rapid tactical remediation at scale

- Incorporate metadata-driven symbolic reasoning support into the software development toolchain to enable rapid testing
- Design interfaces for developers to easily specify critical properties of code units to facilitate proactive remediation
- Demonstrate translation of intended flows and structure encoded in eSBOMs into policies enforceable at runtime

TA2: Integration and cyber security sustainment evaluation



Performer team:

- Define program concept of operations (CONOPS) and design use cases, focusing on testing and evaluating TA1-created capabilities for trigger recovery at scale; construct and conduct corresponding series of challenge tests every 3 months
- Assess effectiveness of TA1 tooling via security analysis as part of (DevSecOps) pipeline
- Establish test range for TA1 testing and evaluation scalable to simulated 5M nodes
- Annual SOTA analysis of available SBOM tools

FFRDC partner:

- Engagement with transition partners to inform the design of DoD-relevant eSBOMs
- System engineering and integration with DoD platform

Experimental plan and metrics

Exemplar Experimental Plan

Evaluator will create emulated distributed deployments of software-under-test (SUT) with synthetic vulnerabilities and a variety of trigger payloads

Performers will receive SUT and static evidence of flaw/crash dump, and will

(1) Determine if the flaw is reachable
(2) For reachable flaws will recover
    (a) the flow to the flaw from the attack surface and
    (b) the trigger for the flaw at the attack surface
(3) Remediate by blocking flows/triggers

	Capability at Month 15
Rapid Triage:	
Time to recover trigger	1 week
Remedition:	
Time to deploy fix*	3 days
Overhead:	
Compile time	10%
Runtime	10%
Experimental Setting:	
Target	Enterprise application scale / 1-1.5M LoC
Platforms	1 CPU / ABI + 1 virtual machine runtime / FFI
Distributed	10-50K network nodes

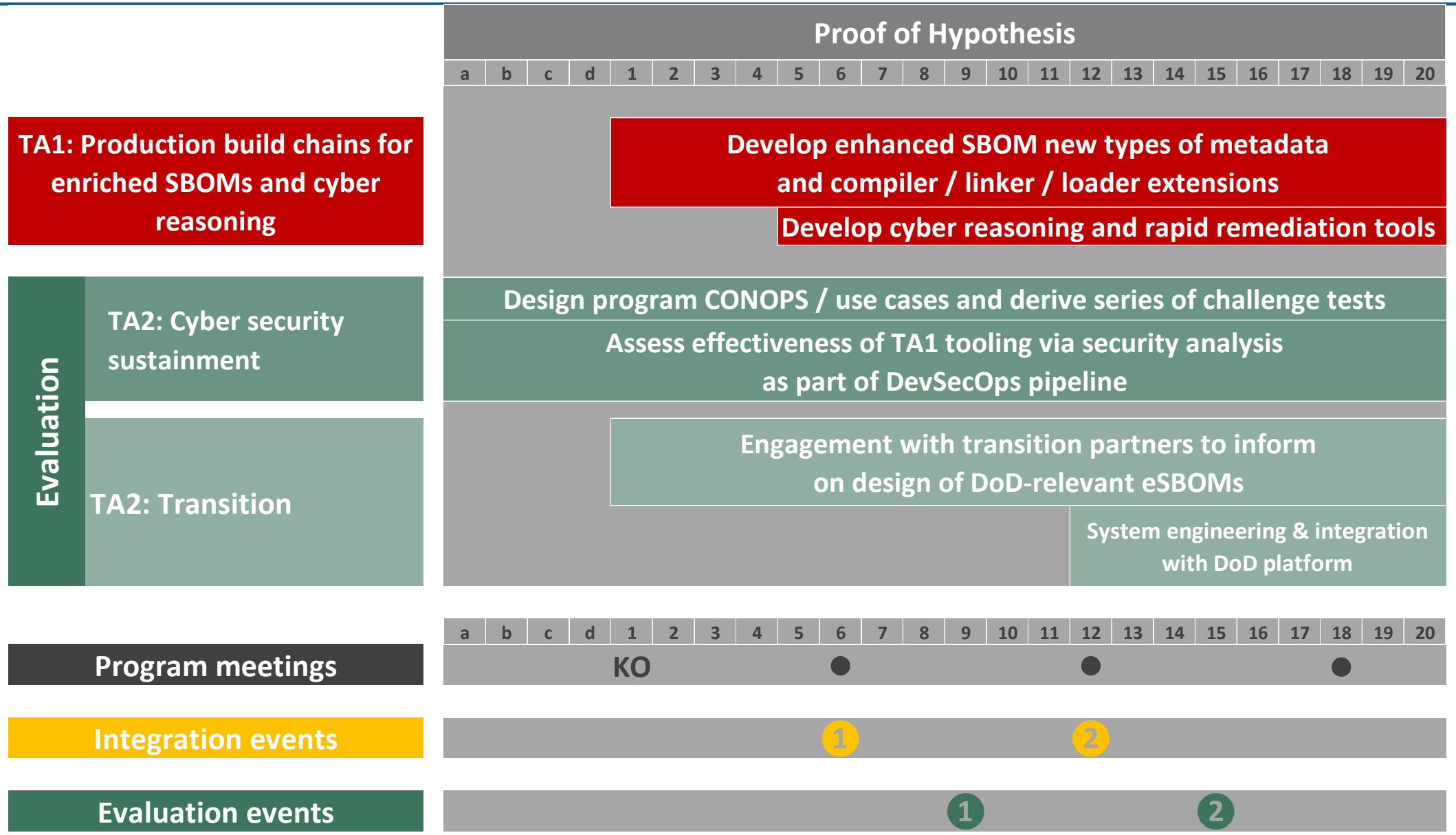
*fix = denial of exploitation

ABI = application binary interface
CPU = central processing unit
FFI = foreign function interface
LoC = lines of code

Potential transition partners

Software Factories	Areas of Interest
Air Force 309th Software Engineering Group (SWEG)	Sustainment for USAF and USSF weapon system software
Naval Sea Systems Command (NAVSEA)	Engage with E-BOSS tools on relevant projects for building trusted Linux distributions
Standards & Best Practices	**Areas Interest**
Cybersecurity and Infrastructure Security Agency (CISA)	Scaling and operationalization of eSBOM, as well as tools, new technologies, and new use cases
National Institute of Standards and Technology (NIST)	Establish guidelines per EO 14028, which sets SBOM requirement when contracting with the govt
Community Engagement	**Areas of Interest**
Open Source Security Foundation (OpenSSF)	Cross-industry collaboration and assessment of open source software security risk via automated checks
Linux Foundation	Improving security of Linux with compiler and linker based techniques

Program Schedule



Funding and programmatic details

- **Proposals due: Tuesday, January 30, 2024 at 12:00 noon (ET)**

- Government anticipates multiple awards for TA1 and a single award for TA2
  - **Most individual awards are anticipated to be under $4M to reflect the minimum viable program structure**
  - Procurement contracts or Other Transactions (OT)

- Proposers may submit separate proposals to both TA1 & TA2
  - Each proposal may address only a single TA
  - Although proposers may submit proposals for both TAs, proposers selected for one TA cannot be selected for another TA
  - Which to consider for award (if any) is at the discretion of the Government

Questions

- Questions for the Q&A session today can be submitted until 12:00 PM ET via E-BOSS@darpa.mil. Please do not post questions in Zoom.

- Questions not answered verbally during today's Q&A session will be addressed through the FAQ. This will get regularly updated and posted on https://www.darpa.mil/work-with-us/opportunities.

Information precedence

- If anything said or addressed during this presentation or in the FAQ conflicts with the published solicitation, **the BAA takes precedence**. The Government may issue amendments to the BAA to effect any changes deemed necessary in response to the FAQ. Such amendments would be posted to Contract Opportunities (https://sam.gov) prior to the solicitation closing date and would supersede previous versions of the solicitation.

www.darpa.mil