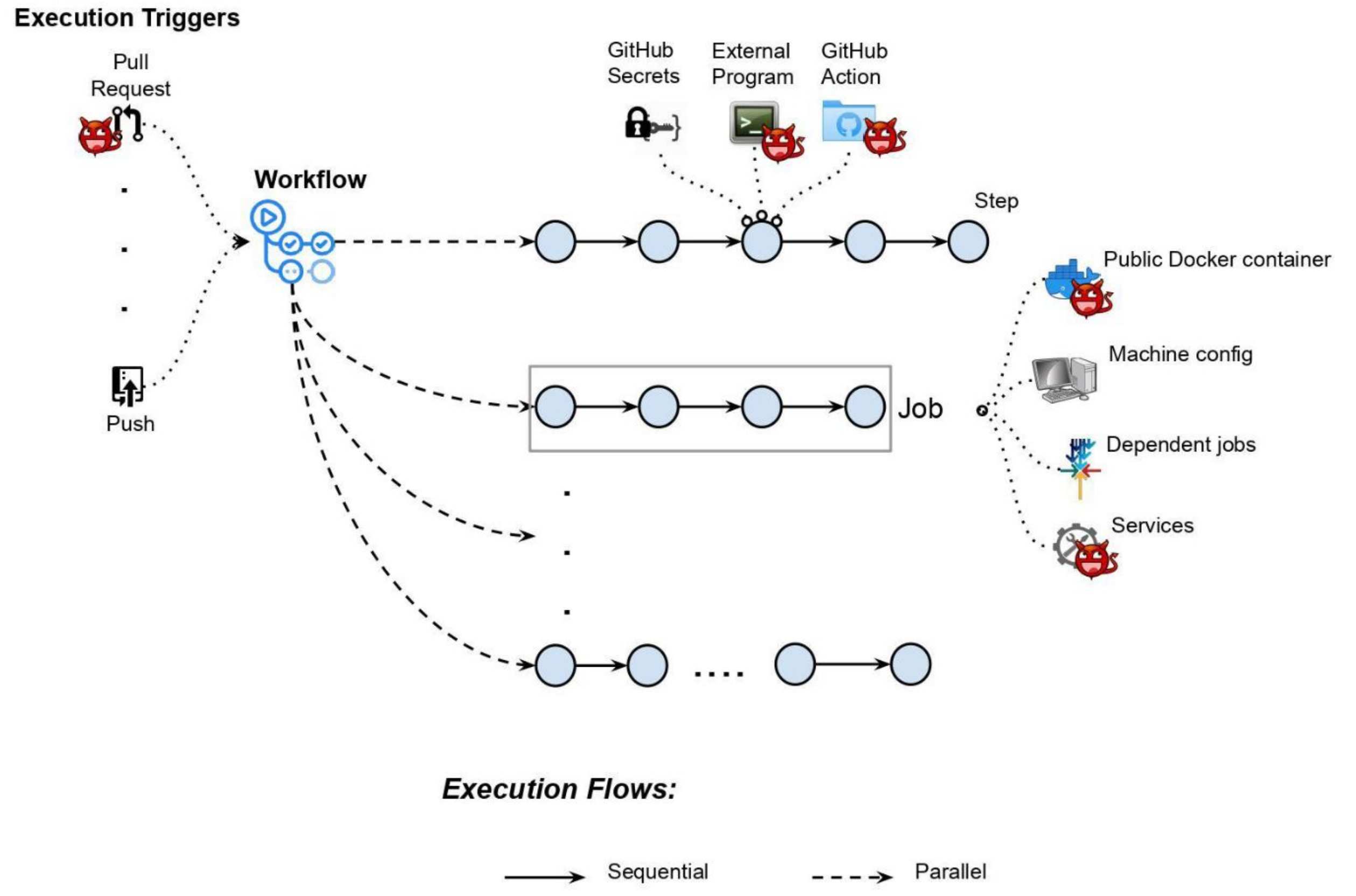
ARGUS: A Framework for Staged Static Taint Analysis of GitHub Workflows and Actions

Siddharth Muralee, Igibek Koishybayev, Aleksandr Nahapetyan, Greg Tystahl,
Brad Reaves, Antonio Bianchi, William Enck, Alexandros Kapravelos, Aravind Machiry



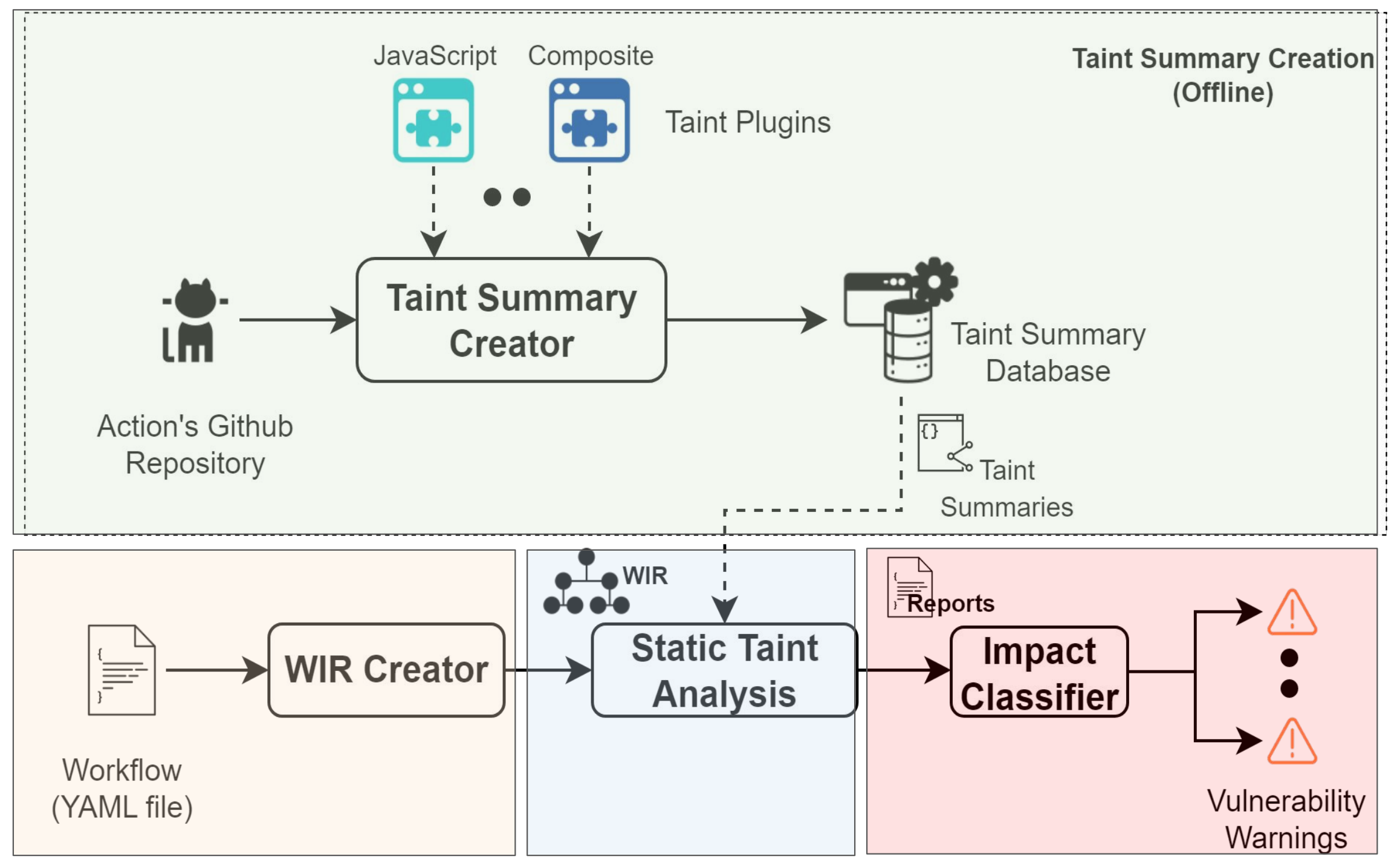
Threat Model

- Execute **Arbitrary Commands** without code changes
- Gain **Unauthorized Read/Write** access to repository
- Exfiltrate **Confidential Secrets** present in the pipeline

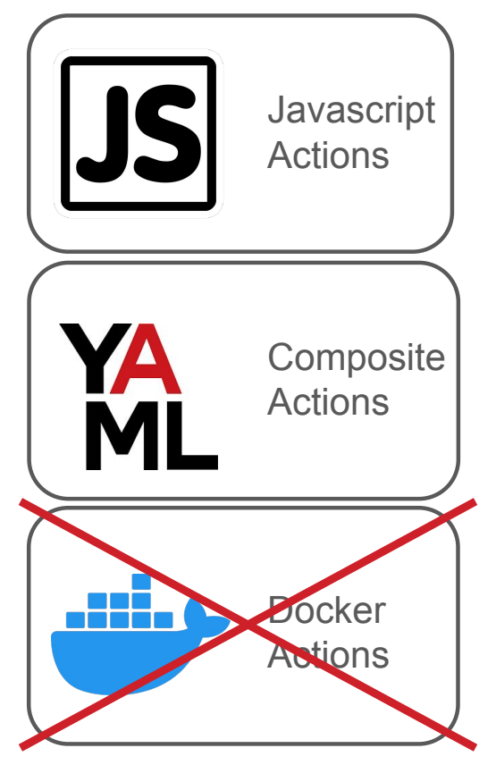
Challenges

- Capture Workflow's **semantics and execution flow**
- Track **dataflow** across workflows and the actions
- Support multiple **programming languages**
- Predict the potential **impact** of identified vulnerabilities

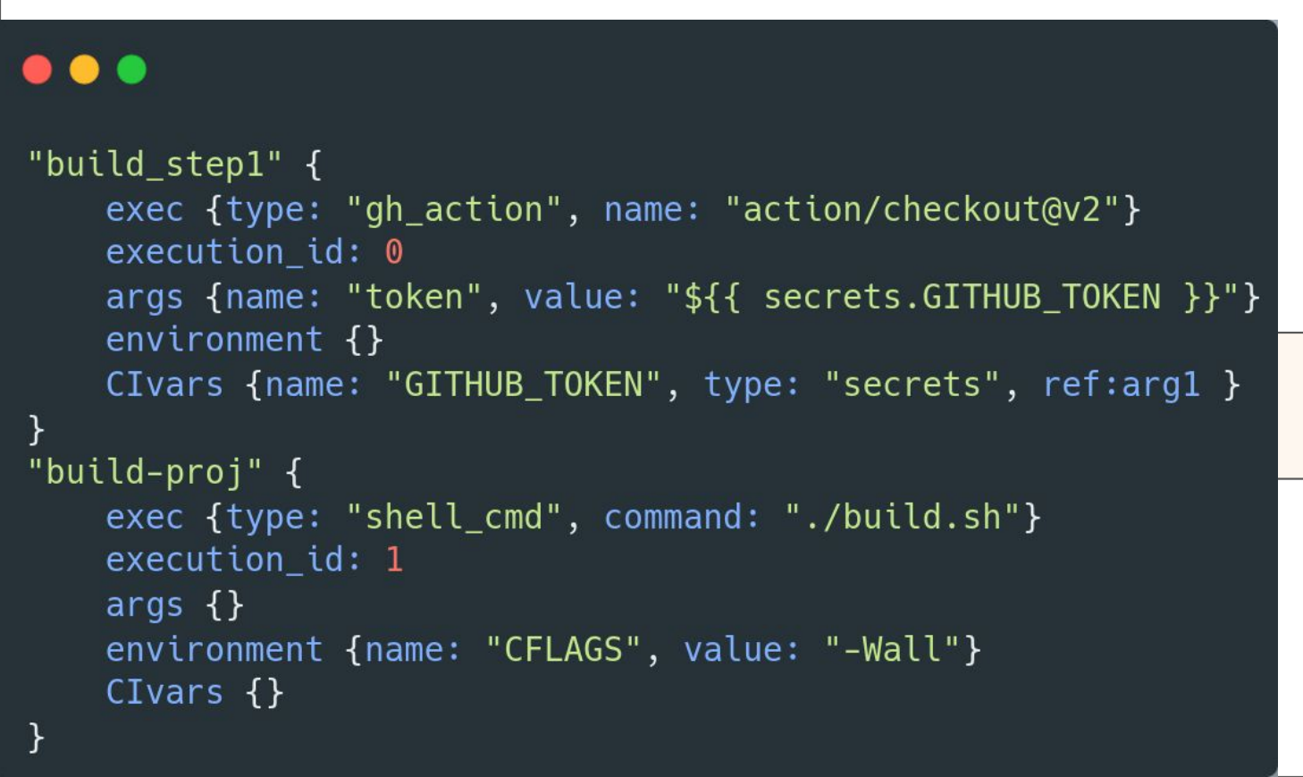
Design



Action Taint Summaries



Workflow IR Generation



```
"build_step1" {
    exec {type: "gh_action", name: "action/checkout@v2"}
    execution_id: 0
    args {name: "token", value: "${{ secrets.GITHUB_TOKEN }}"}
    environment {}
    CIvars {name: "GITHUB_TOKEN", type: "secrets", ref:arg1 }
}
"build-proj" {
    exec {type: "shell_cmd", command: "./build.sh"}
    execution_id: 1
    args {}
    environment {name: "CFLAGS", value: "-Wall"}
    CIvars {}
}
```

ARGUS helps secure GitHub CI pipelines by identifying critical code injection vulnerabilities in GitHub Workflows

27,489

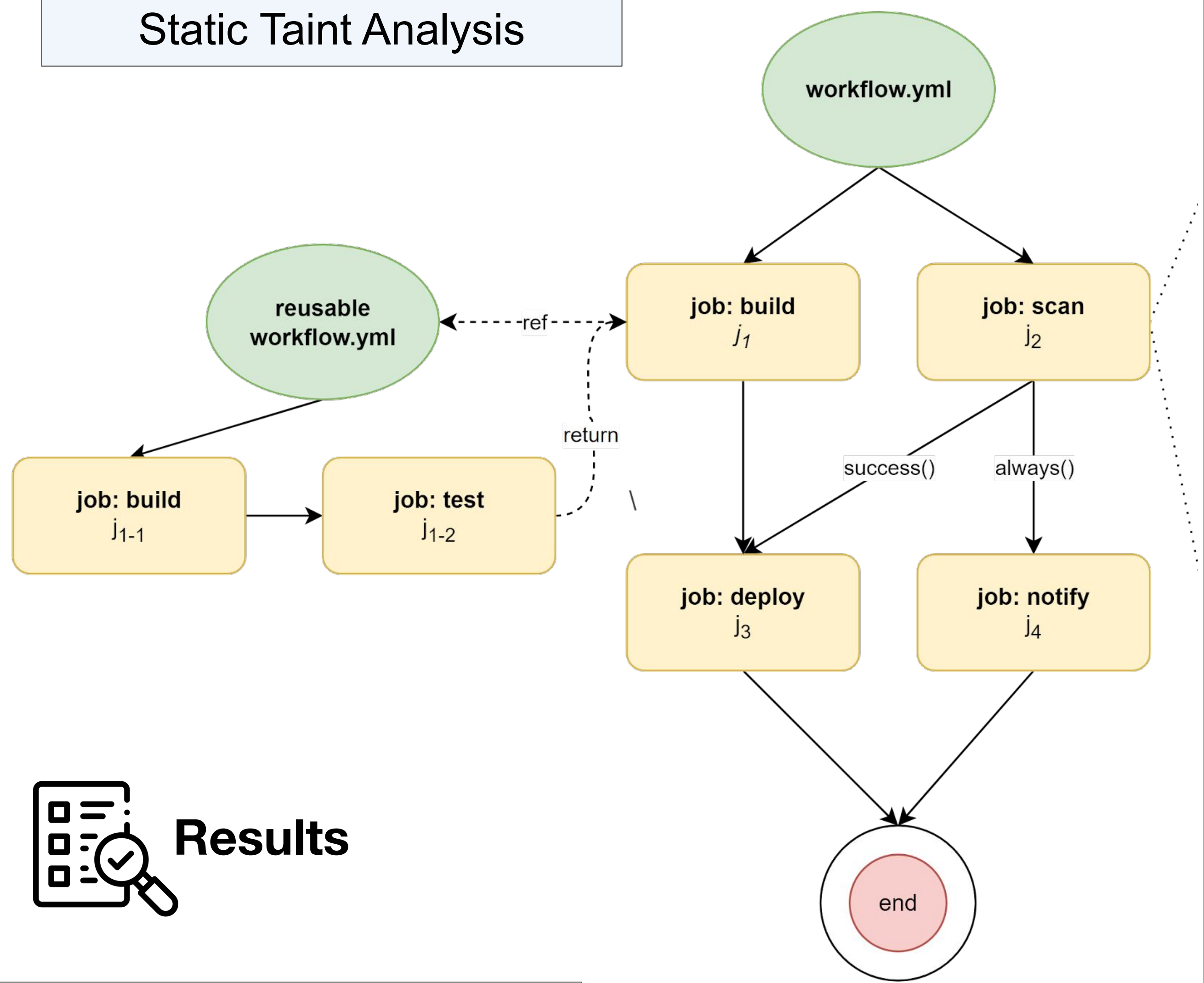
Vulnerable Workflows Identified

3,643

High Impact Vulnerabilities

For more information, visit our website at https://secureci.org or scan the QR code to read our paper!

Static Taint Analysis



Results

Precision of Taint Analysis by ARGUS on Actions

Type	Javascript			Composite		
	True Positives	False Positives	Precision	True Positives	False Positives	Precision
Input Flow	138	10	93.2%	46	1	97.9%
Direct Flow	27	0	100%	109	4	96.4%
Cumulative	175	10	**94.2%**	155	5	**96.8%**

Severity Assignment of Vulnerabilities using the Impact Classifier

Flow Type	No. of Workflows				Num. Repos	Direct Flow Actions		Input Flow Actions	
	High (Total: 3,643)	Medium (Sampled: 1,000)	Low (Sampled: 1,000)	Total (Expected: 5,643)		Unique Root Cause	Unique Actions	Unique Root Cause	Unique Actions
Public Repositories									
Intra-WF	2,875	467	769	4,111	3,226	N/A			
Inter-WF-Ac	787	597	287	1,671	1,257	55	33	34	13
Total	**3,322** (91.18%)	985 (98.5%)	991 (99.1%)	5,298 (93.88%)	4,000	55	33	34	13

Comparative Evaluation of ARGUS with other state-of-the-art works in finding Code Injection Vulnerabilities

Tool	High/Medium				Low			
	TP	FP	FN	P	TP	FP	FN	P
GHAST	744	157	3,563	82.6%	331	363	660	47.7%
GITSEC	1,527	53	2,870	96.6%	204	3	787	98.5%
ARGUS	4,307	336	0	92.8%	991	9	0	99.1%

PURDUE UNIVERSITY
NC STATE UNIVERSITY
S3C2
amazon research awards
DARPA N6600120C4031
NSF CNS-2247686 CNS-2207008