

# Beyond Manual: Enhancing and Scaling Security Activities with Automation

Christian Bauer  
[contact@christianb.net](mailto:contact@christianb.net)  
BSides Munich  
11th Nov 2024



# Motivation

Security teams might be busy repetitive tasks or those requiring significant human effort.

Solution: let automation perform routine and repetitive manual tasks, or those requiring significant effort



# Part 1

An Automation Example:  
External Attack Surface  
Monitoring/Management (EASM)



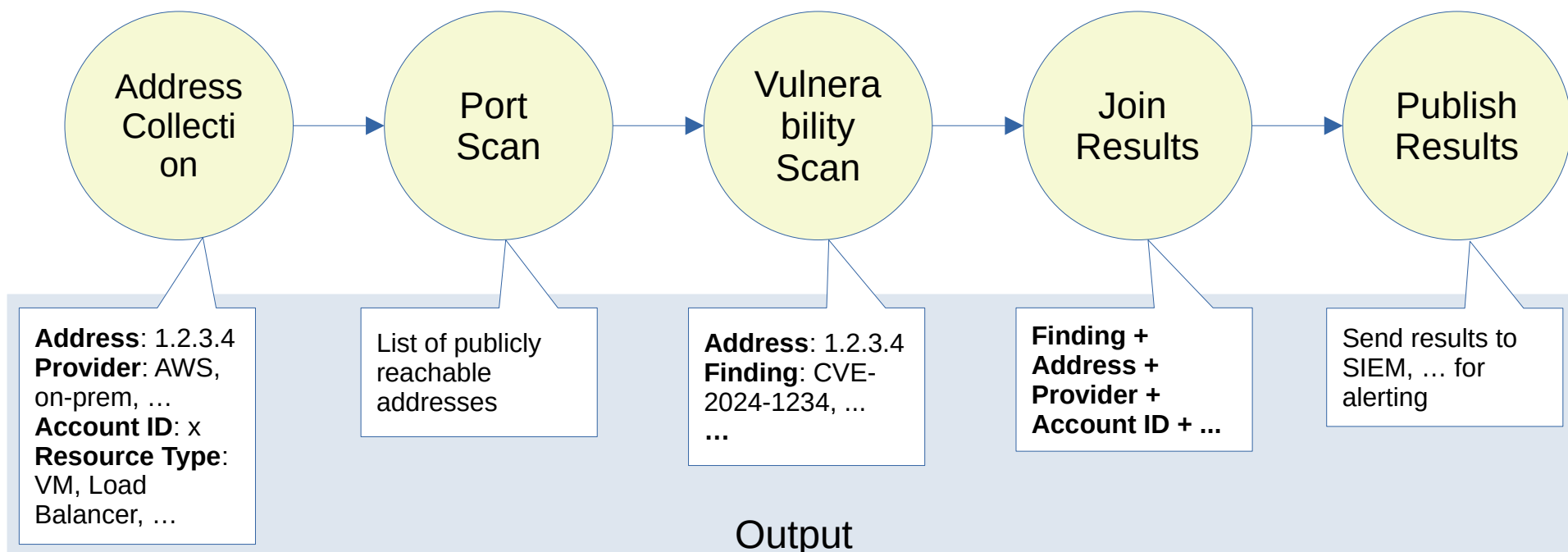
# Definition

## What is EASM?

- An organization has assets; some of these assets are exposed to the Internet.  
E.g. web application servers, load balancers, VPN Gateways, ...
- These assets might have
  - Known vulnerabilities (CVEs)
  - Misconfigurations: e.g. anonymous access or default username/password
- We want to be able to detect these things across the entire organization

# EASM - Stages

EASM can be modeled as a workflow



# EASM - Implementation

EASM is a workflow consisting of different stages.  
So use a workflow orchestration engine to implement it:



**Argo  
Workflows**

Kubernetes-native workflow engine supporting  
DAG and step-based workflows.

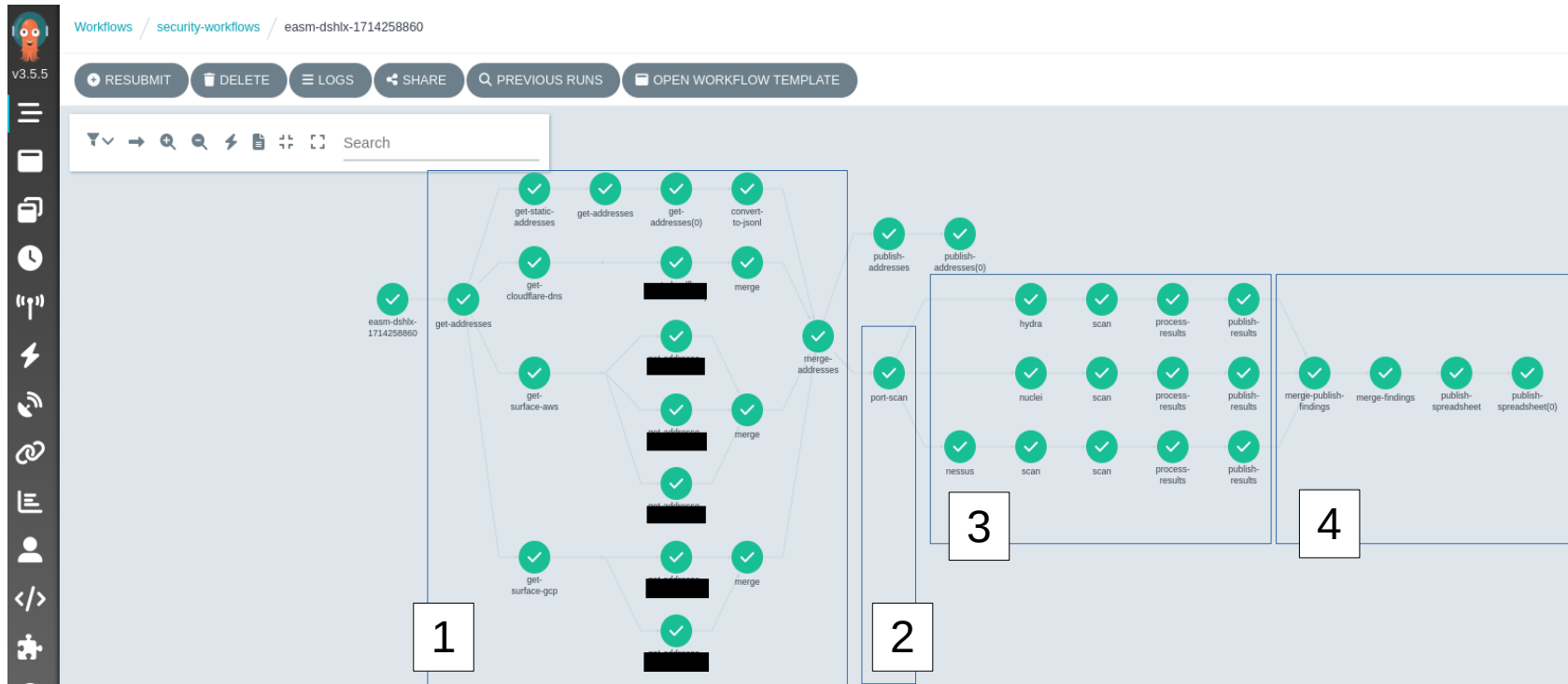
[Documentation](#)



# EASM - Implementation /2

Demo / Video

# EASM - Implementation /3



(1) Address Collection, (2) Port scan, (3) Vulnerability Scans, (4) Merge/publish results



# EASM - Vulnerability Scan

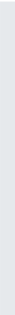
Argo Workflow template using Nuclei for scan stage:

```
name: scan
inputs:
  artifacts:
    - name: host-port-list
      path: /tmp/host-port-list.txt
outputs:
  artifacts:
    - name: results
      path: /tmp/nuclei-results.json
script:
  image: container-repo/my-nuclei-image:1.2.3
  command: [bash]
  source: |
    set -e
    echo "Fetching latest Nuclei templates"
    nuclei -ut -silent
    echo "Performing scan over $(cat /tmp/host-port-list.txt | wc -l) entries"
    touch /tmp/nuclei-results.json
    nuclei -duc -silent -jsonl -dut \
      -s medium,high,critical,unknown \
      -ss host-spray \
      -l /tmp/host-port-list.txt \
      >> /tmp/nuclei-results.json
    echo "Done"
```



# EASM - Reporting

Results can be pushed to alerting/notification system, e.g. to Slack:



New finding: CVE-2024-6387 (tool: Nuclei)  
Severity: High  
Address: 1.2.3.4  
Resource type: EC2 instance, resource ID: X  
Environment: AWS o-1234, account ID 1234567890  
Details: ...



# **EASM - Special Note**

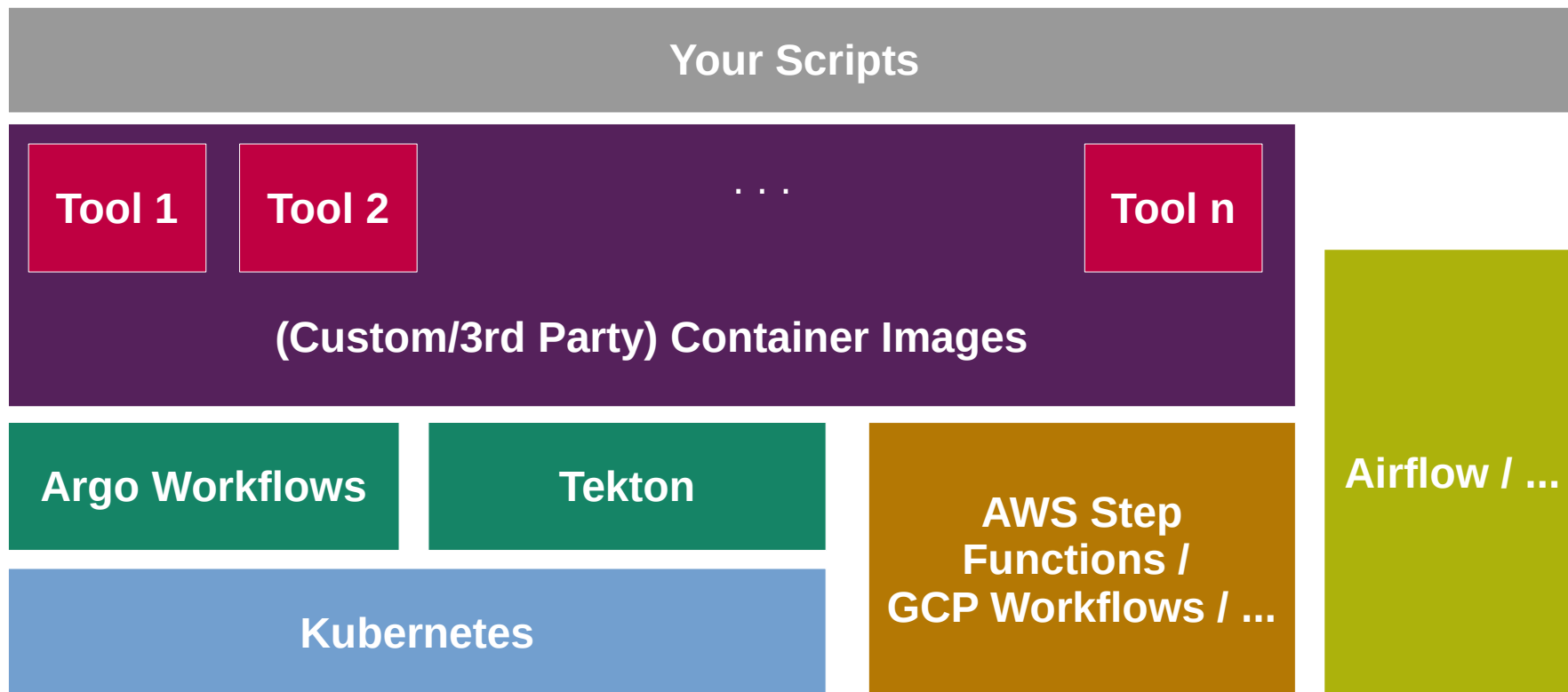
Before you implement this: contact your data center provider and ask them whether you are allowed to scan your assets hosted in their environment!



# Part 2

## Building a Generic Security Automation Platform

# Software Stack





# Workflow Triggers



## Time

Workflow is triggered by cron schedule. E.g. 1x/week, once every 2 days, ...

Cron Workflow in Argo ecosystem



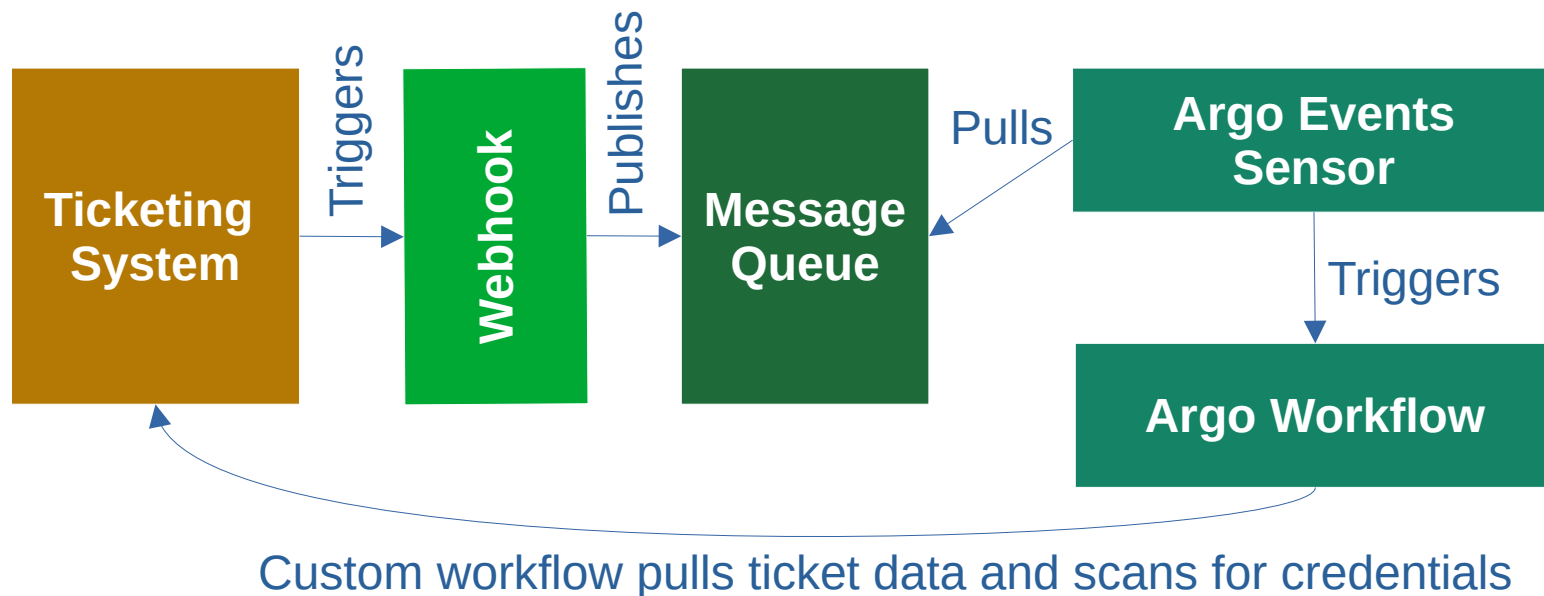
## Event

An event from an external system is triggering a workflow.

Argo Events in Argo ecosystem

# Argo Events Example

Argo Events allows triggering Argo Workflows from a variety of event sources like messaging queues. Example architecture for credential scans in a ticketing system:





# Automation Examples

Asset Data Collection  
(XaaS/public clouds)

*Trigger:* time

*Effort:* low

*Tools:*  
CloudQuery,  
Steampipe, SQL/graph  
database

CSPM Compliance  
Checks

*Trigger:* time

*Effort:* medium

*Tools:*  
Asset database, SQL  
queries

EASM

*Trigger:* time

*Effort:* high

*Tools:*  
Asset database,  
spreadsheets,  
nmap/naabu,  
Nuclei/Nessus,  
dsq/clickhouse-local, ...





# Automation Examples /2

Credential Scans  
(tickets, VCS repos)

*Trigger:* time or event

*Effort:* low-medium

*Tools:*  
Trufflehog, gitleaks, ...

Dangling DNS Records

*Trigger:* time

*Effort:* low

*Tools:*  
Asset database,  
dsq/clickhouse-local, ...

User Audits

*Trigger:* time

*Effort:* low-medium

*Tools:*  
HR records system,  
permission data from  
different systems,  
dsq/clickhouse-local, ...



# Summary

Many security tasks can be automated, resulting in various advantages:

- Automation will continuously run 24/7 and alert on new findings (with further potential for auto-remediation)
- Increase task frequency (hourly, daily, etc.)
- Certain tasks like EASM can not be performed manually, automation is a necessity!

Open source components for building security automation are available and easy to use.