

Ethan
Troy

GRC Engineering in the Cloud



The Problems with GRC (Governance, Risk, and Compliance)

“The Players are Not Mature Enough”

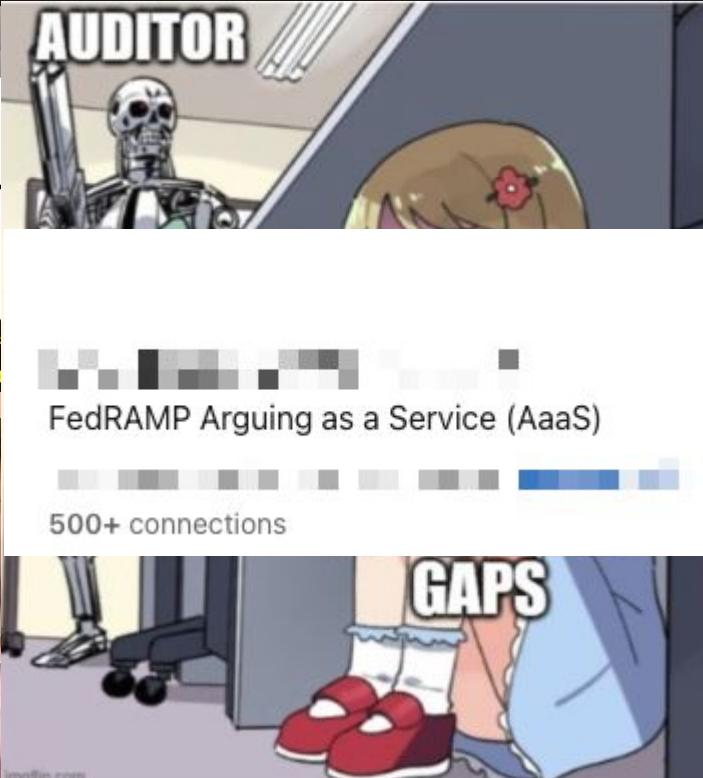
The Problem with Auditors



EVERYWHERE THE LIGHT TOUCHES IS "GRC BRO LAND"
WHERE PEOPLE MEMORIZE THE NIST 800-53
AND LIE ABOUT READING DOCUMENTATION FOR FUN



The Problem with GRC Pros



The Problem with Leaders

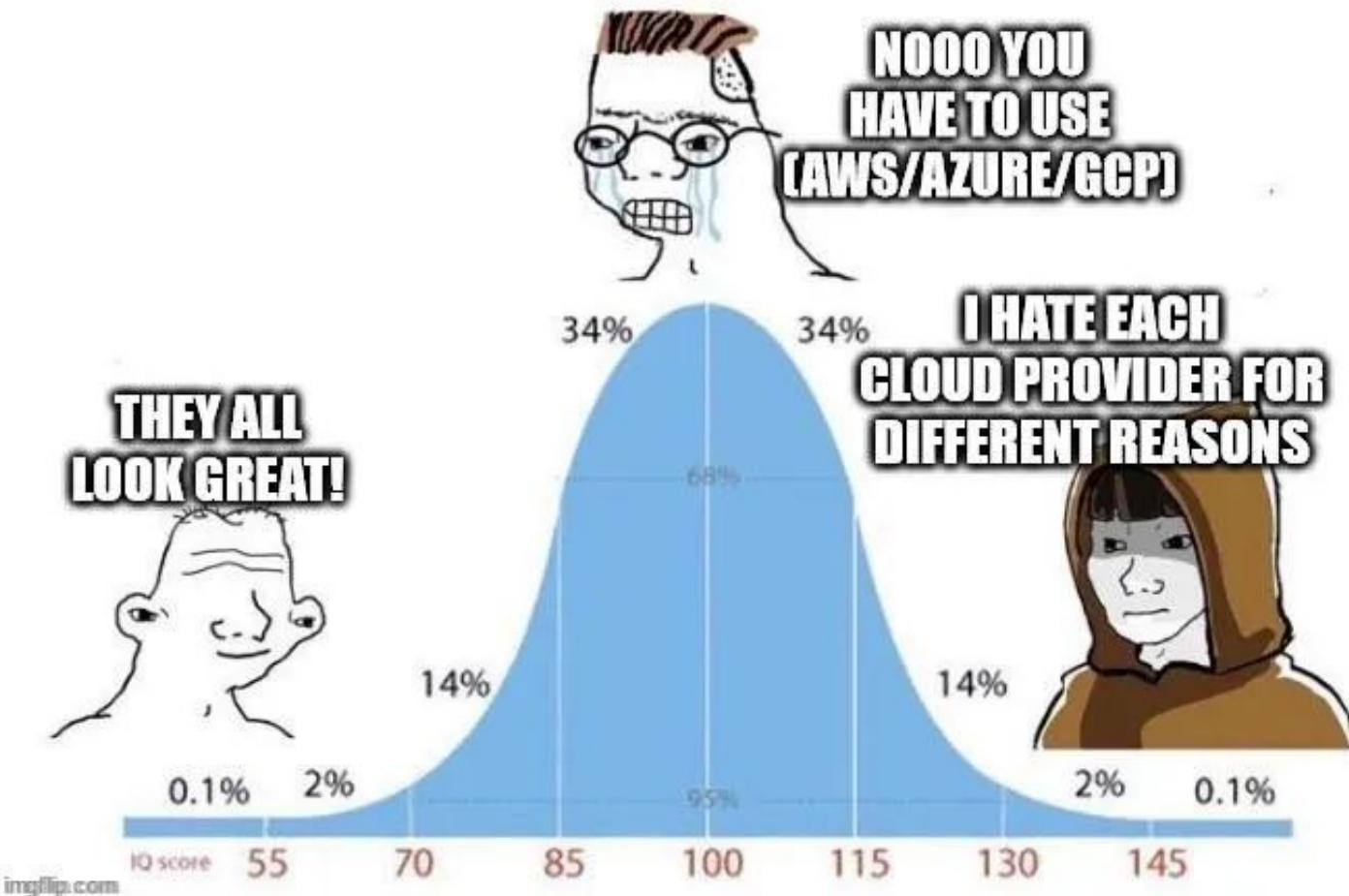
“You need to be able to translate this to your leadership”





The Solution -
Creativity

CHOOSING A CLOUD PROVIDER



Major Clouds



Azure

A favorite among those that come from classical on-prem AD environments



GCP

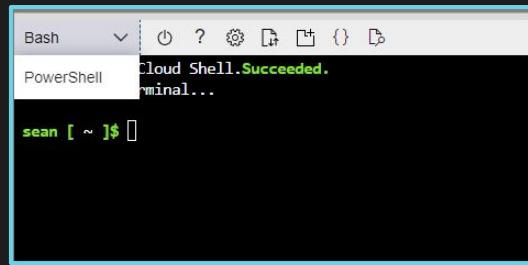
Smallest Market Share but rapidly growing



AWS

The Market Leader
Many developer services are actually just AWS Wrappers

Cloud Shell



```
ethanolivertroy@cloudshell:~$ pwd
/home/ethanolivertroy
ethanolivertroy@cloudshell:~$ ls
README-cloudshell.txt
ethanolivertroy@cloudshell:~$ python
Python 3.12.3 (main, Aug 14 2025, 17:47:21) [GCC 13.3.0] on
linux
Type "help", "copyright", "credits" or "license" for more in
formation.
>>> 
```

```
[cloudshell-user@ip-10-140-114-209 ~]$ zsh
[cloudshell-user@ip-10-140-114-209]~% pwsh
PowerShell 7.4.2
PS /home/cloudshell-user> bash
[cloudshell-user@ip-10-140-114-209 ~]$ 
```

Azure

Released in September 2017

GCP

Released in 2016

AWS

Released in December 2020

There is a CMD for that

```
# List users without MFA
aws iam list-users --query "Users[?PasswordLastUsed!=null].UserName" | xargs -I {} aws iam list-mfa-devices --user-name {} --query "MFADevices[0].UserName" | grep null

# Find overly permissive policies (Admin access)
aws iam list-policies --query "Policies[?contains(PolicyName, 'Admin')].Arn"

# Check root account last login
aws iam get-account-summary --query "SummaryMap.AccountAccessKeysPresent"
```

There is a CMD for that

```
# Check if audit logs are enabled  
gcloud logging sinks list --format="table(name,destination)"  
  
# Verify Cloud Storage bucket logging  
gsutil ls | xargs -I {} gsutil logging get {}  
  
# Check VPC Flow Logs  
gcloud compute networks subnets list --format="table(name,enableFlowLogs)"
```

There is a CMD for that

```
# Find storage accounts without encryption
az storage account list --query "[?encryption.services.blob.enabled!=\`true\`].name"

# Check VMs without disk encryption
az vm list --query "[].{Name:name, DiskEncryption:storageProfile.osDisk.encryptionSettings.enabled}"

# Find Key Vaults without soft delete
az keyvault list --query "[?properties.enableSoftDelete!=\`true\`].name"
```

#AbolishScreenshots

IAM Identity Center > AWS Organizations: AWS accounts > [REDACTED]

Overview

Account name: [REDACTED]

Account ID: [REDACTED]

Email: [REDACTED]

[Users and groups \(159\)](#) [Permission sets \(36\)](#)

Assigned users and groups (159)

The following users and groups in IAM Identity Center can select this AWS

Find users by username, find groups by group name

Username / group name

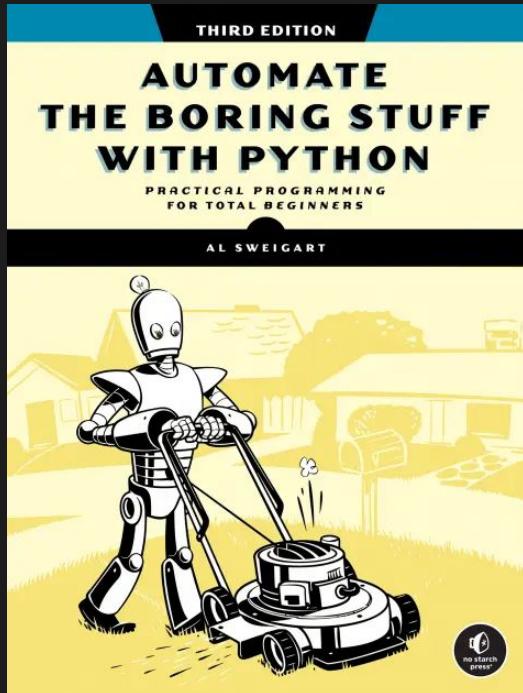
- [REDACTED]

[Give access](#) [Assign users or groups](#)

6 7 ... 16 >

aws organizations list-accounts

Automation



```
~/.ssh/Fo/2/Fortreum-FedRAMP-20x-GCP-Evaluation on main ?11
> python gcp_fedramp_collector.py
```

```
# Only checks bucket ACL - misses critical security settings  
aws s3api get-bucket-acl --bucket my-bucket
```

Just because
you've
programtically
pulled something,
doesn't mean that
is the whole
picture



```
# Comprehensive S3 security audit  
aws s3api get-bucket-acl --bucket my-bucket  
aws s3api get-bucket-policy --bucket my-bucket  
aws s3api get-bucket-encryption --bucket my-bucket  
aws s3api get-bucket-versioning --bucket my-bucket  
aws s3api get-bucket-logging --bucket my-bucket  
aws s3api get-public-access-block --bucket my-bucket  
aws s3api get-bucket-policy-status --bucket my-bucket  
  
# Check for publicly accessible objects  
aws s3api list-objects-v2 --bucket my-bucket \  
--query "Contents[?contains(Grants[],Permission,  
'READ')]"
```

```
import json
import boto3
from datetime import datetime
from pathlib import Path

class ComplianceEvidenceCollector:
    def __init__(self, framework="NIST-800-53"):
        self.framework = framework
        self.s3 = boto3.client('s3')
        self.evidence_bucket = 'compliance-evidence'

    def collect_and_store(self, control_id, evidence_data):
        # Structure evidence
        evidence = {
            'control_id': control_id,
            'framework': self.framework,
            'timestamp': datetime.now().isoformat(),
            'automated_check': True,
            'evidence': evidence_data,
            'status': self.evaluate_compliance(evidence_data)
        }

        # Store to S3 with proper structure
        key = f"{self.framework}/{control_id}/{datetime.now().strftime('%Y%m%d_%H%M%S')}.json"

        self.s3.put_object(
            Bucket=self.evidence_bucket,
            Key=key,
            Body=json.dumps(evidence, indent=2),
            ServerSideEncryption='AES256',
            Metadata={
                'control-id': control_id,
                'framework': self.framework,
                'automated': 'true'
            }
        )

        return key

    def evaluate_compliance(self, data):
        # Logic to determine pass/fail
        if data.get('non_compliant_resources'):
            return 'FAIL'
        return 'PASS'
```

Mapping to Frameworks



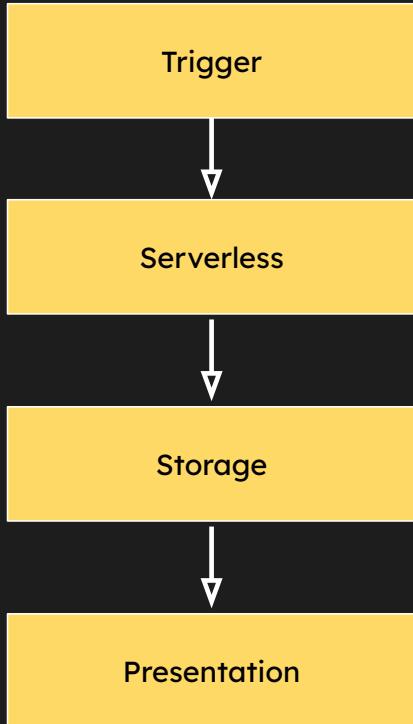
GRC Automation Software



DRATA



Scaling This Yourself



It does not matter what it is called.
They all do the same thing.
Don't get caught up on names.
Get caught up on the function and
result you want to achieve.
Be creative.

Open Source Tools

The screenshot shows the Prowler web application running at `localhost:3000`. The interface has a dark theme with green highlights.

Left Sidebar:

- Launch Scan** button
- Analytics** dropdown
 - Overview** (selected)
 - Compliance
- Lighthouse AI
- Top failed findings
- High-risk findings
- Browse all findings
- Resources** dropdown
 - Browse all resources
- Configuration dropdown
 - Cloud Providers
 - Provider Groups
 - Scan Jobs
 - Roles
 - Lighthouse AI

Header: PROWLER Overview ET

Providers Overview:

Provider	Percent Passing	Failing Checks	Total Resources
AWS	0.00%	-	-
Google Cloud	0.00%	-	-
Microsoft Azure	0.00%	-	-
Cloudflare	48.55%	89	81
Custom	0.00%	-	-
Total	48.55%	89	81

Add Provider button

Findings by Severity:

Severity	Count
Critical	22
High	23
Medium	121
Low	1
Informational	0

Findings by Status:

- 173 Findings**
- 84 pass findings from last day (49%)
- +84 pass findings from last day ↗
- 89 fail findings from last day (51%)
- +89 fail findings from last day ↗
- 0 no change from last day

Latest New Failing Findings: Showing the latest 10 new failing findings by severity.

Details	Finding	Resource name	Severity	Status	Last seen	Region	Service	Cloud provider
...	Ensure That SSH Access Is Restricted From the Internet	...vpn	Critical	Fail	Jul 27, 2025 3:17PM	global	compute	pwnlabsgcpboot

Bottom Buttons:

- Check out on Findings
- Sign out

v5.9.2

Open Source Tools



Offensive Security has some of the
best “GRC” Tools
They simply have to be repurposed

Building Tools with APIs

The screenshot shows a web-based application titled "okta" with a sidebar navigation menu and a central code editor area.

Navigation Sidebar:

- Dashboard
- Directory
 - People
 - Groups
- Profile editor
- Directory integrations
- Profile masters
- Applications
- Security
- Workflow
- Reports
- Settings

Code Editor Area:

```
# 2. Authentication and Security
log_info "Retrieving authentication configuration..."
okta_get "https:// ${OKTA_DOMAIN}/api/v1/authenticators" \
"${OUTPUT_DIR}/core_data/authenticators.json"

okta_get "https:// ${OKTA_DOMAIN}/api/v1/authorizationServers" \
"${OUTPUT_DIR}/core_data/authorization_servers.json"

okta_get "https:// ${OKTA_DOMAIN}/api/v1/authorizationServers/default" \
"${OUTPUT_DIR}/core_data/default_auth_server.json"

okta_get "https:// ${OKTA_DOMAIN}/api/v1/authorizationServers/default/credentials/keys" \
"${OUTPUT_DIR}/core_data/auth_server_keys.json"

okta_get "https:// ${OKTA_DOMAIN}/api/v1/authorizationServers/default/claims" \
"${OUTPUT_DIR}/core_data/auth_claims.json"

# 3. Users and Groups
log_info "Retrieving users and groups."
okta_get "https:// ${OKTA_DOMAIN}/api/v1/users?limit=200" \
"${OUTPUT_DIR}/core_data/all_users.json"

okta_get "https:// ${OKTA_DOMAIN}/api/v1/groups?limit=200" \
"${OUTPUT_DIR}/core_data/groups.json"

# 4. Applications
log_info "Retrieving applications..."
okta_get "https:// ${OKTA_DOMAIN}/api/v1/apps?limit=200" \
"${OUTPUT_DIR}/core_data/apps.json"

# 5. Identity Providers
log_info "Retrieving identity providers..."
okta_get "https:// ${OKTA_DOMAIN}/api/v1/idps" \
"${OUTPUT_DIR}/core_data/idp_settings.json"
```

User Interface Elements:

- Search bar at the top right.
- User profile icon and email address "blake.soto@ocorp.c... OCORP" at the top right.
- Right sidebar labeled "Directories" showing 0 items.
- Bottom right corner URL: <https://github.com/ethanolivertroy/okta-inspector>

Building Tools with APIs

```
> python3 bedrock_security_checker.py --expert
Starting AWS Bedrock Security Check (expert mode)
Account: | Region: us-east-1
● Auditing model access permissions...
● No custom models found. Checking IAM policies for foundation model access...
● Checking logging and monitoring configurations...
● Checking network security configurations...
● Checking resource organization...
● Checking for prompt injection vulnerabilities...
● Checking data privacy compliance...
● Checking cost anomaly detection...

AWS BEDROCK SECURITY CONFIGURATION REPORT - EXPERT MODE

Account: [REDACTED]
Region: [REDACTED]
Scan Time: 2025-06-03 21:51:35 UTC
Total Findings: 4
Good Practices: 1

DETAILED FINDINGS

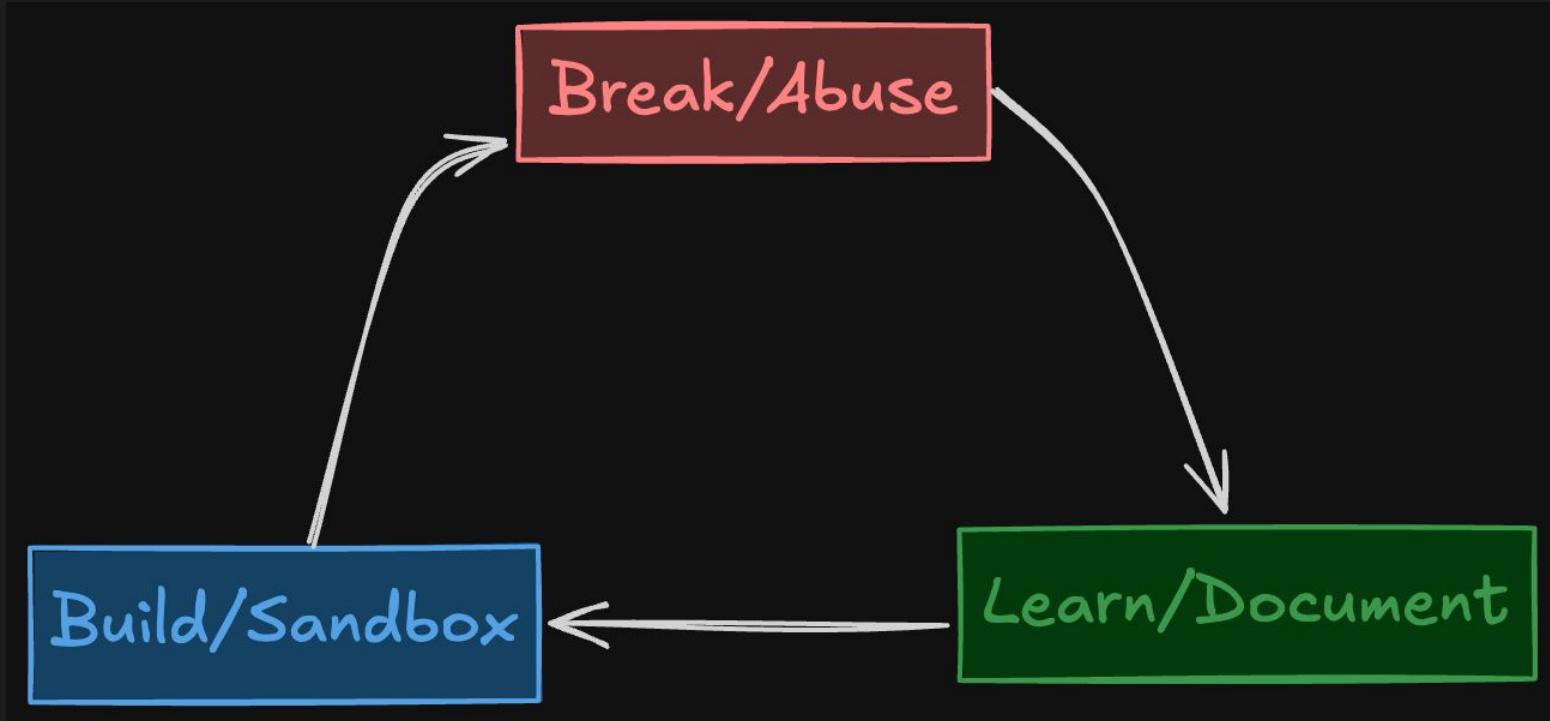
[Audit & Compliance]

Risk Level: HIGH (Score: 8/10)
Resource: Model Invocation Logging
Issue: AI model usage is not being logged
Recommendation: Enable logging to track who uses your models and detect abuse
Technical Details: Model invocation logging is completely disabled
Remediation Command: aws bedrock put-model-invocation-logging-configuration --logging-config file://logging-config.json

[Network Security]
```

<https://github.com/ethanolivertroy/wilma>

Anyone Can Do This

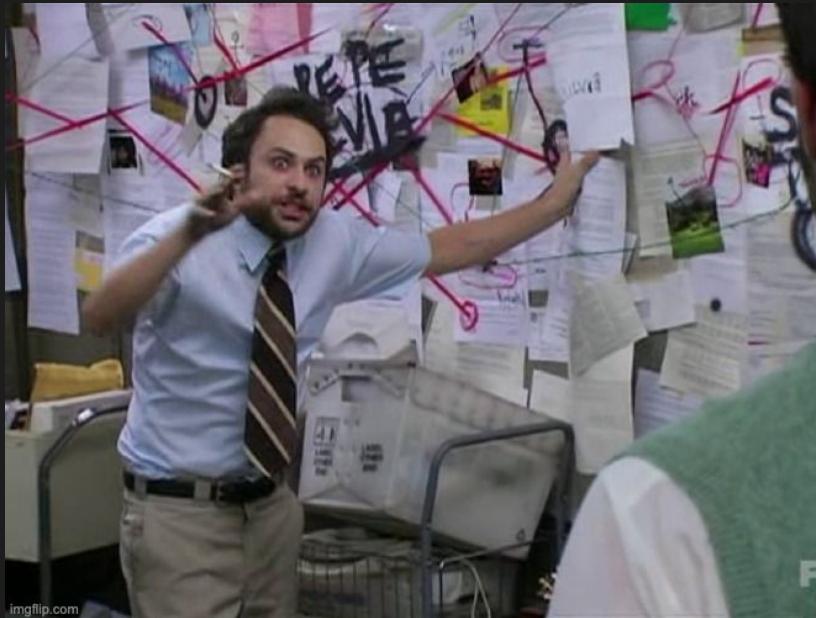


Think Like A . . .



Simple But Not Easy

Developers/Builders
Don't Always Think in
the Same Way as
Security Engineers



DVTC Trust Center - Damn Vuln CTF Mode

localhost:3000/ctf

CTF Challenges

Damn Vulnerable Trust Center - Capture The Flag

0 of 12 Challenges Completed

0 / 2150 pts
Your Score 0%

0 Flags Found 12 Remaining 0% Complete

Reset Progress

Cloud Storage 100 pts

Leaky Presigned URL

Find and exploit a long-lived presigned URL to access sensitive documents.

flag{...}

Submit Flag

IAM/Secrets 200 pts

Secrets Manager Loot

Exploit over-permissive IAM roles to read from Secrets Manager.

flag{...}

Submit Flag

Serverless 200 pts

No-Auth Lambda

Call an unauthenticated API Gateway route to execute Lambda functions.

flag{...}

Submit Flag

OSINT/Metadata 150 pts

Machine-Readable Overshare

Find sensitive information in machine-readable compliance feeds.

flag{...}

Frontend Logic 150 pts

Badge Falsification

Manipulate security badges without server-side validation.

flag{...}

Supply Chain 250 pts

CI/CD From Forks

Abuse GitHub Actions to execute code or access secrets from a fork.

flag{...}

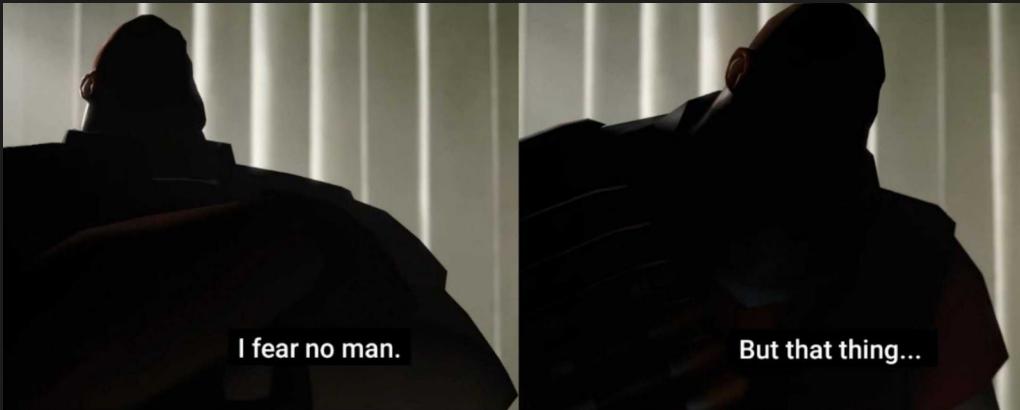
CTF Mode Active
This instance contains intentional vulnerabilities for educational purposes.

Home Tests Reports Compliance Frameworks Controls Policies Documents Audits Trust Center Risk Vendor Assets Personnel Integrations

CTF & UTILITIES

CTF Challenges Admin API Demo

Next Steps



Setting Up Git and GitHub

So programming is 15% coding,
25% debugging and 60% googling?

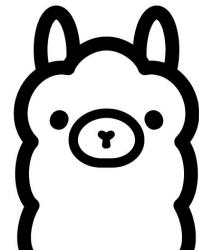
You just insulted my entire race of people.

But yes.

Using AI

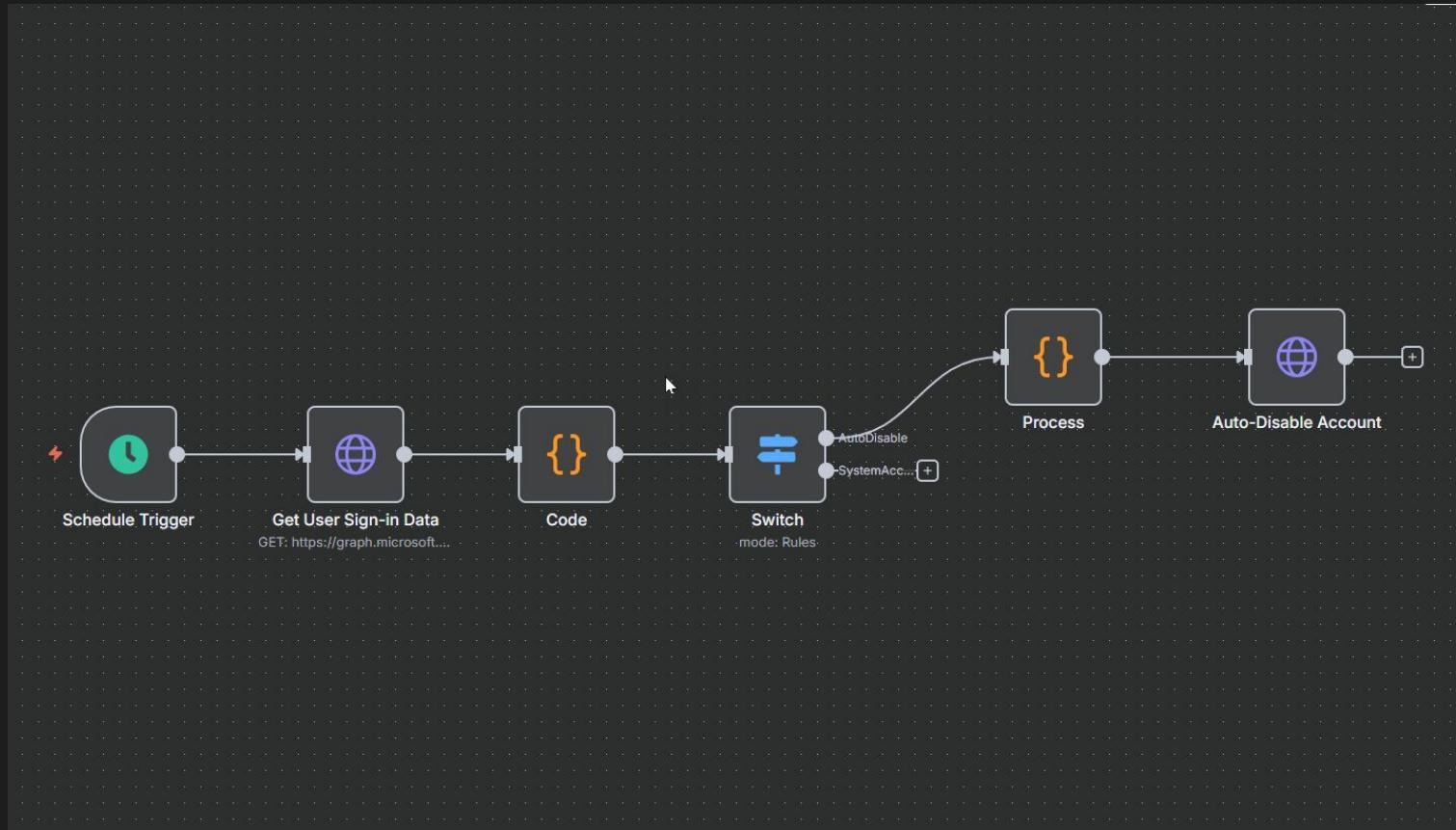


ChatGPT



 Claude

Workflow Automation Ideas





PWNED LABS

Sign in

Sign up

Your security training ground

START FOR FREE!

Experience, **real-world, byte sized cloud security labs** for training cyber warriors. From beginners to pros, our engaging platform allows you to secure your defenses, ignite your career and stay ahead of threats.

Join us at any stage of your journey



PWNED LABS
UNLOCK YOUR CYBER POWER

Subscribe to hackIDLE.com - 3 Memberships for PWNED Labs



Q&A

?