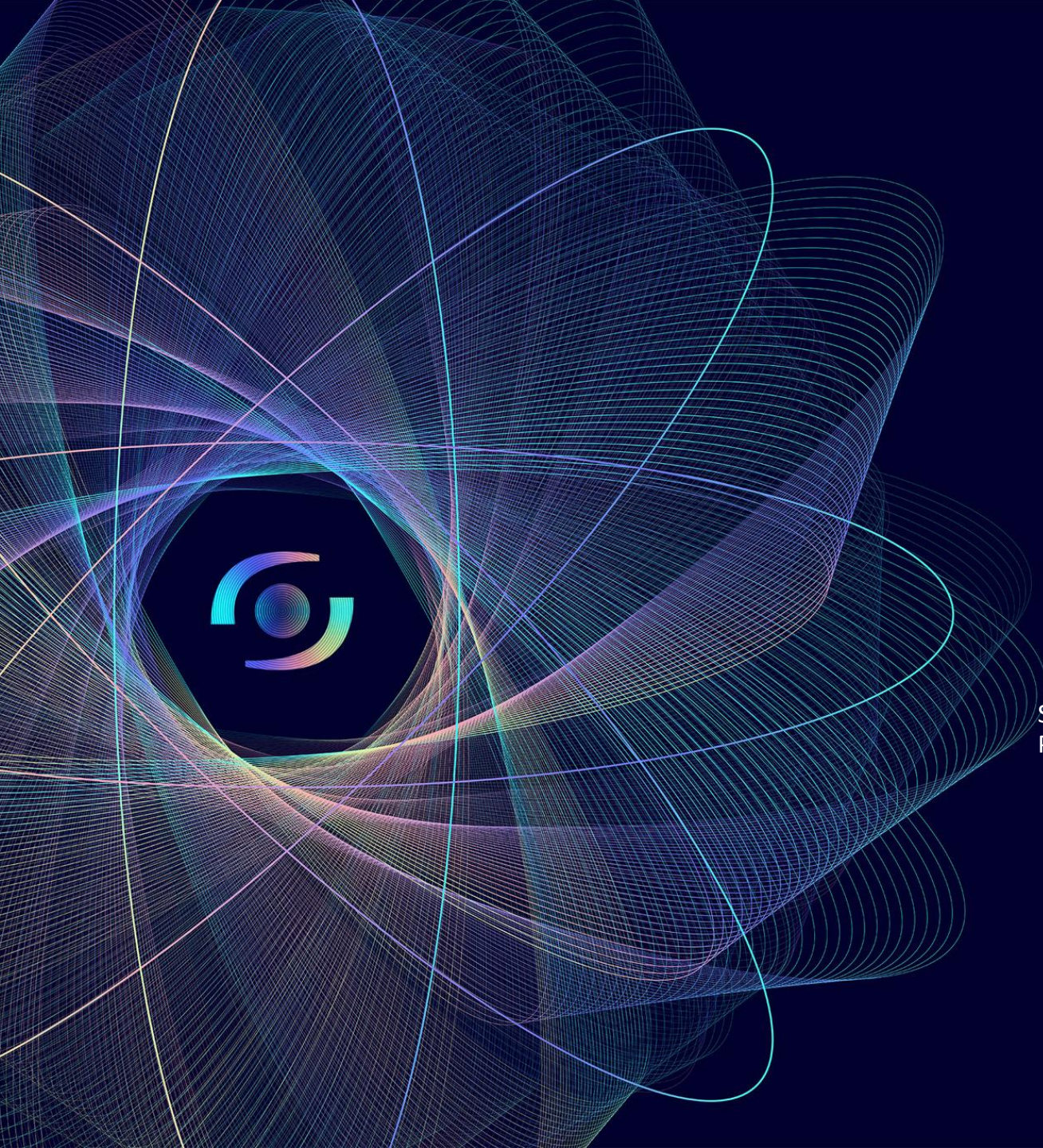


# NetEye User Group 2024

## Live Adversary Simulation

Simone Ragonesi & Simone Cagol, Würth Phoenix

WÜRTHPHOENIX

# WHAT IS THE CLOUD?

**Definition:**
Cloud computing refers to the delivery of computing services (servers, storage, databases, networking, software) over the internet (the cloud).
It offers flexible resources, faster innovation, and economies of scale.


**Key Features:**
- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Seamless Scaling

# WHAT IS GITHUB?

**Definition:**
GitHub is a web-based platform for version control and collaboration, built on top of Git. It allows multiple developers to work on projects simultaneously, manage source code, and track changes.

**Key Features:**

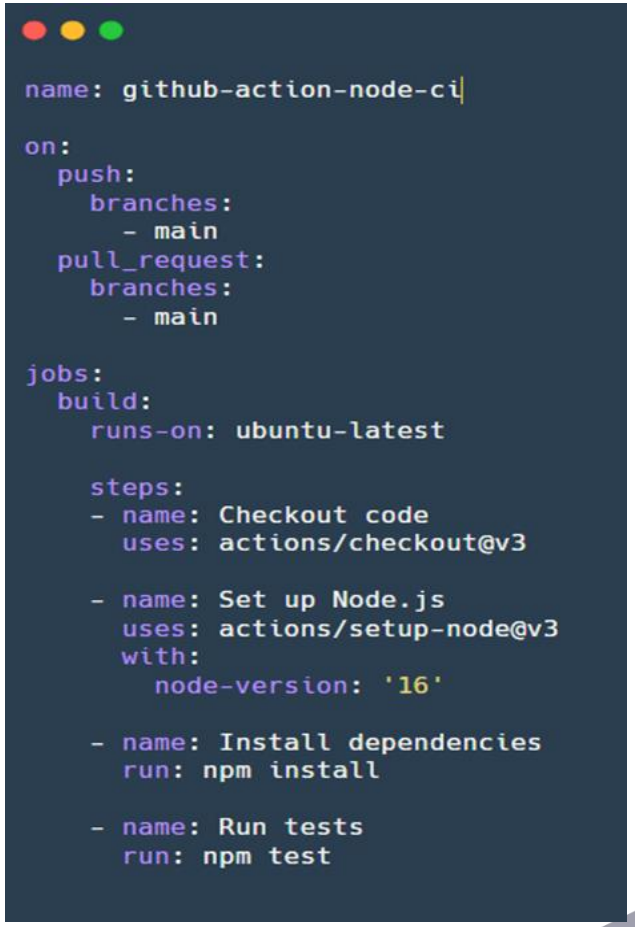
- Repository Management (public/private)
- Version Control with Git
- Collaboration Tools (Pull Requests, Issues, Wikis)
- GitHub Actions (CI/CD integration)

# WHAT IS GITHUB ACTIONS?

**Definition:**
GitHub Actions is an automation tool provided by GitHub, which enables continuous integration and continuous delivery (CI/CD) directly from your GitHub repositories.
It allows developers to automate the build, test, and deployment pipeline.

**Key Features:**

- Workflow Automation (YAML configuration)
- Integration with GitHub Repositories
- Multi-Platform Build (Linux, macOS, Windows)
- Customizable Action Marketplace
- Event-Driven Triggers (push, pull request, etc.)



```yaml
name: github-action-node-ci

on:
  push:
    branches:
      - main
  pull_request:
    branches:
      - main

jobs:
  build:
    runs-on: ubuntu-latest

    steps:
    - name: Checkout code
      uses: actions/checkout@v3

    - name: Set up Node.js
      uses: actions/setup-node@v3
      with:
        node-version: '16'

    - name: Install dependencies
      run: npm install

    - name: Run tests
      run: npm test
```

# WHAT IS AWS ?

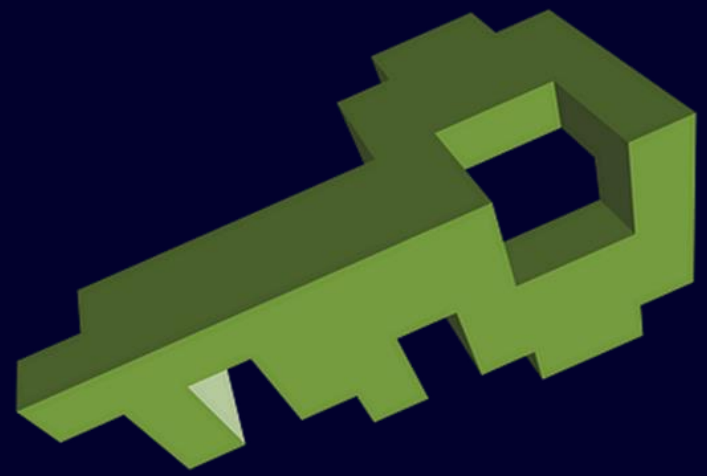
**Definition:**
Amazon Web Services (AWS) is a comprehensive and widely adopted cloud platform,offering over 200 fully featured services from data centers globally.
It provides scalable, reliable, and cost-effective cloud solutions.


**Key Features:**

- Compute Power (EC2, Lambda)
- Storage Solutions (S3, EBS)
- Database Services (RDS, DynamoDB)
- Networking (VPC, Route 53)
- Security and Compliance

# WHAT IS IAM ?

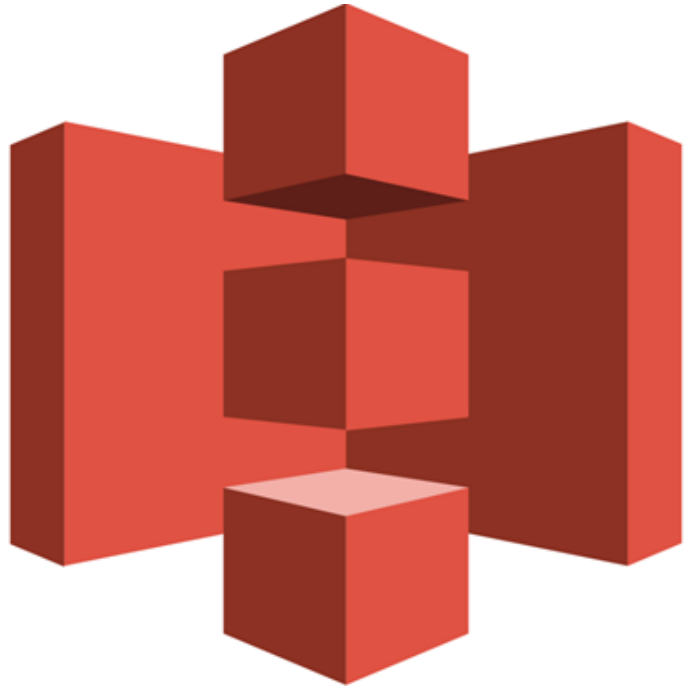
**Definition:**
Identity and Access Management (IAM) in AWS is  a framework of policies that ensure the right individuals access the right resources.
IAM allows you to manage access to AWS services and resources securely.



**Key Features:**
- User Management
- Role-Based Access Control (RBAC)
- Fine-Grained Permissions
- Multi-Factor Authentication (MFA)
- Temporary Security Credentials (STS)

# WHAT IS S3?

**Definition:**
Amazon S3 (Simple Storage Service) is a scalable object storage service offered by AWS.
It is designed for storing and retrieving any amount and type of data from anywhere on the web.



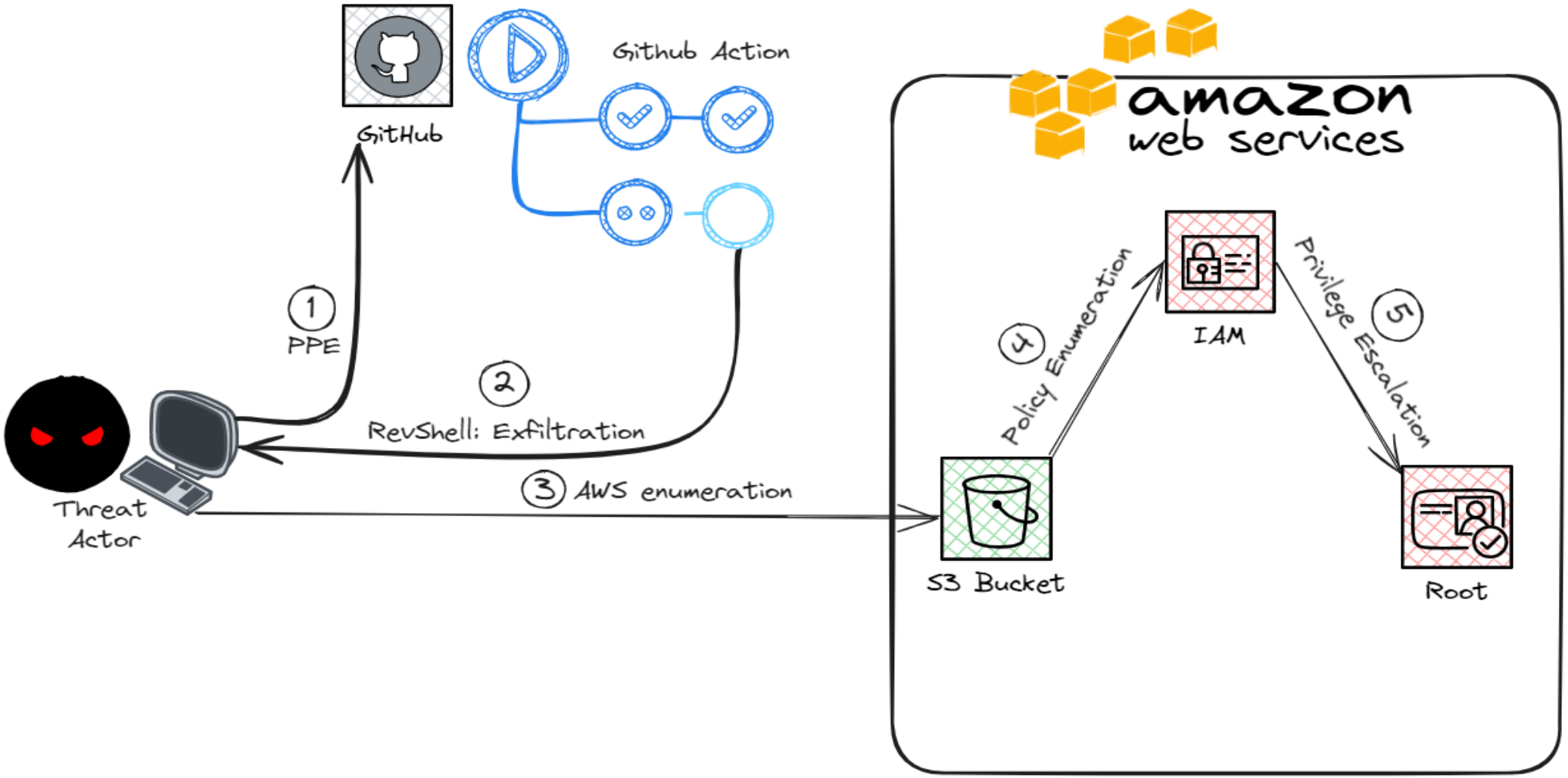
**Key Features:**

- Scalable Storage Capacity
- Data Durability and Availability
- Fine-Grained Access Control (Bucket Policies, ACLs)
- Versioning and Lifecycle Management
- Integration with other AWS Services

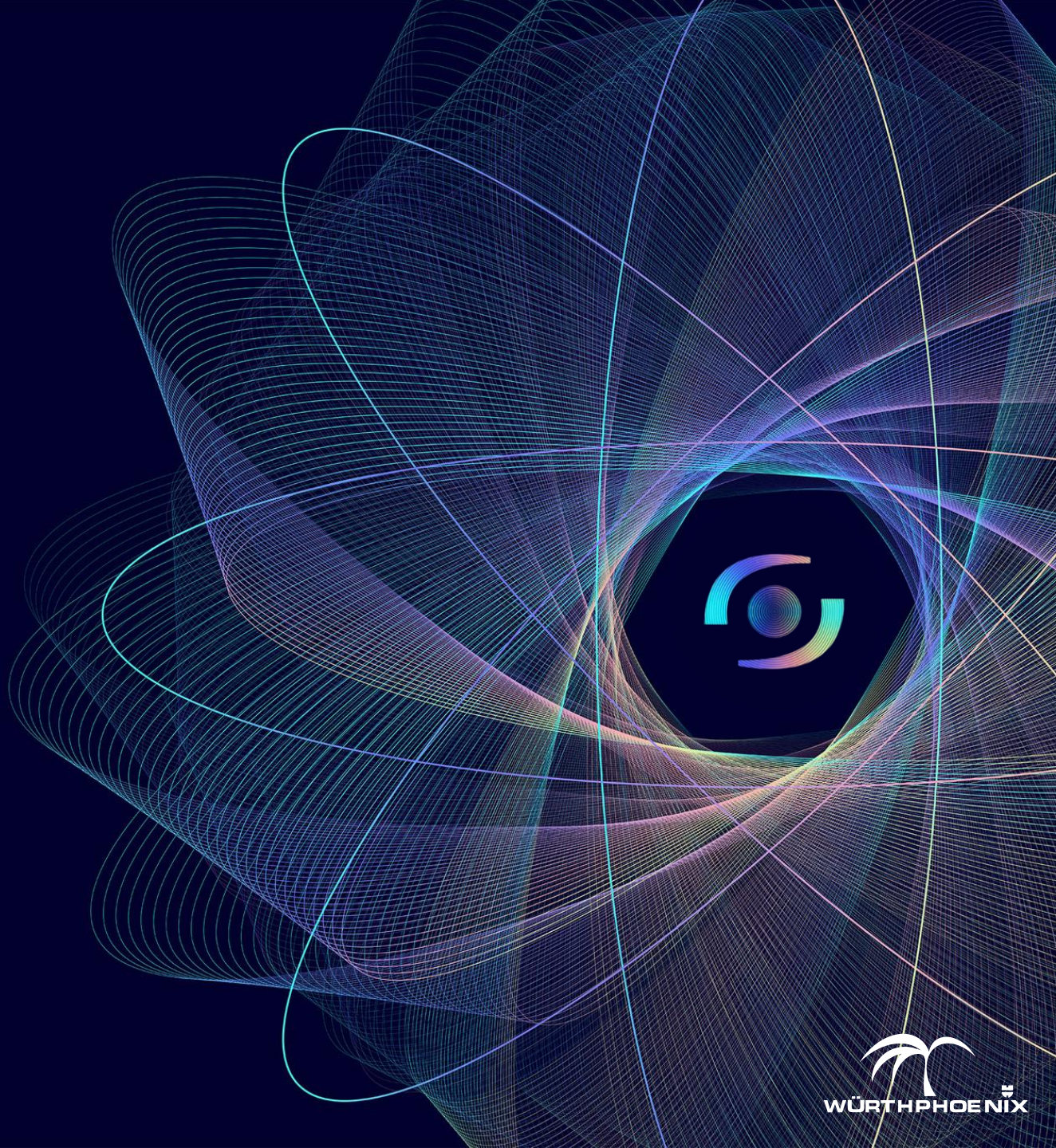
# THE CYBER KILL CHAIN

- Injection of a malicious comment into a GitHub issue to trigger a GitHub Action that initiates a reverse shell **(Poisoned Pipeline Execution).**
- Exfiltration of secrets from the action's runner via reverse shell, uncovering **AWS keys**.
- Enumeration of AWS resources using the previously extracted keys, revealing read access to the contents of an **S3 bucket**.
- The bucket contains some files: the attacker uncover additional **AWS keys**.
- Leveraging these keys, the attacker employ **Pacu** to perform **privilege escalation** and gain **admin access** across the entire AWS account.

# ATTACK PATH


GitHub
Github Action
1
PPE
2
RevShell: Exfiltration
3
AWS enumeration
Threat Actor
amazon web services
IAM
4
Policy Enumeration
5
Privilege Escalation
S3 Bucket
Root

# THANK YOU.



WÜRTHPHOENIX