



Using AI to create more secure IAM policies



Today's Session

- Introductions
- IAM Privilege Escalation attacks
- Using AI for generating secure IAM policies
- Tools for detecting insecure IAM policies
- How to implement them in your CI/CD pipelines








About Us





About Ihor Sasovets

-  Lead Security Engineer at TechMagic
-  4+ years of AWS experience
-  Background in security testing automation
-  CTF player, booklover, play chess, love travelling
-  I live in Lviv, Ukraine



Ihor Sasovets

linkedin.com/in/ihor-sasovets/



@IgorSasovets

github.com/IgorSasovets





About Christophe Limpalair

- 🎬 Founder and Trainer at Cybr
- 🧑‍💻 8+ years of AWS experience
- ⏪ Background primarily in web dev and AWS cloud
- 🥾 I live in Colorado and love hiking & skiing



[Cybr.com/discord](https://cybr.com/discord)



Christophe Limpalair

<https://linkedin.com/in/christophelimpalair>



@ChristopheLimp

<https://twitter.com/christophelimp>

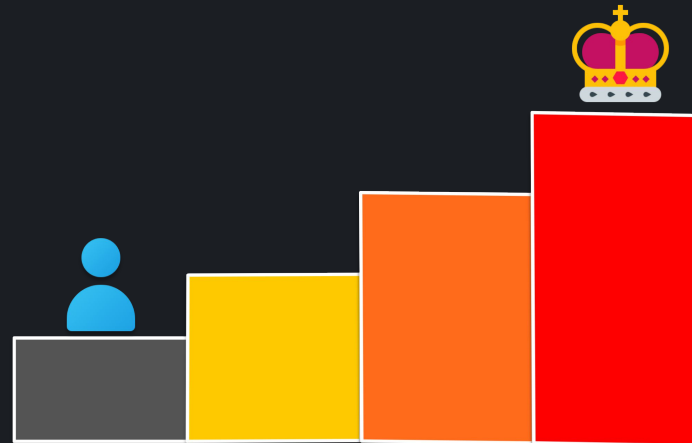




What are Privilege Escalations?

In simple terms:

An attacker going from lower to higher privileges

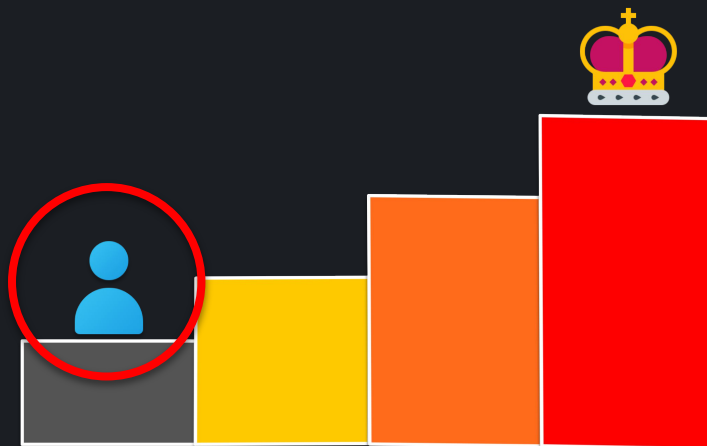




What are Privilege Escalations?

In terms of AWS PrivEscs:

An attacker found a way in through a user, role, or resource, but their access is limited

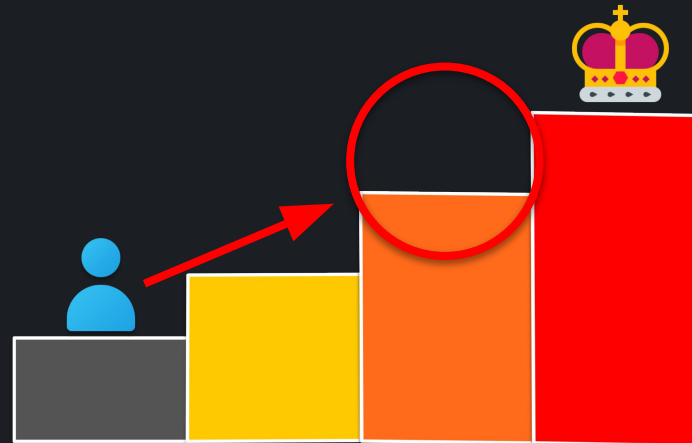




What are Privilege Escalations?

In terms of AWS PrivEscs:

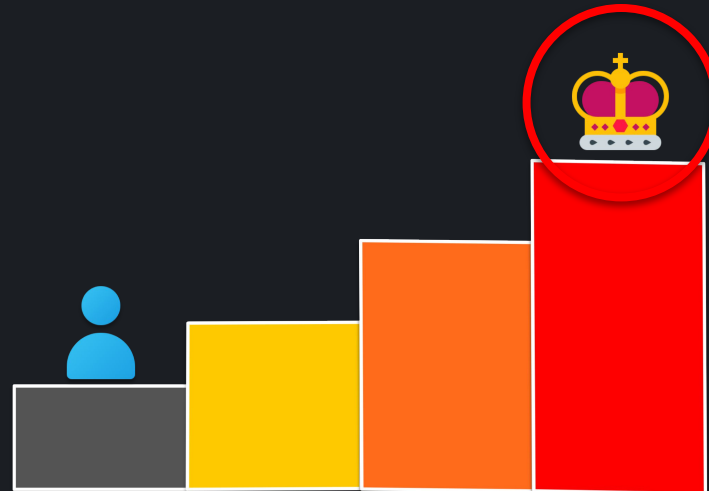
They will want to look for a privilege escalation path to elevate their permissions





What are Privilege Escalations?

Ideally, they would grant themselves admin rights...but realistically that's often not needed...





What are Privilege Escalations?

Even without admin rights, they could:

- Launch big EC2 instances for crypto mining
- Exfiltrate sensitive data
- Access secret values (ie: from Secrets Manager)
- Etc...



IAM PrivEsc Attack Example

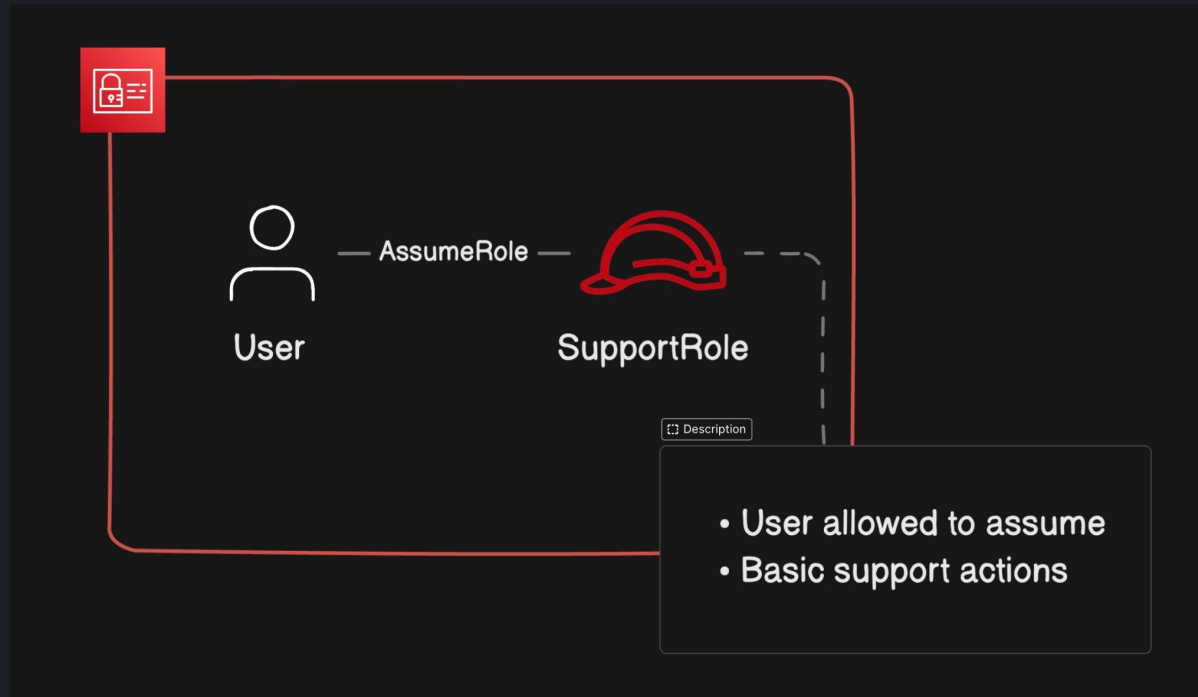
iam:AttachRolePolicy

One of our Hands-On Labs:

<https://cybr.com/courses/iam-privilege-escalation-labs/lessons/lab-ctf-iamattachrolepolicy-privesc/>

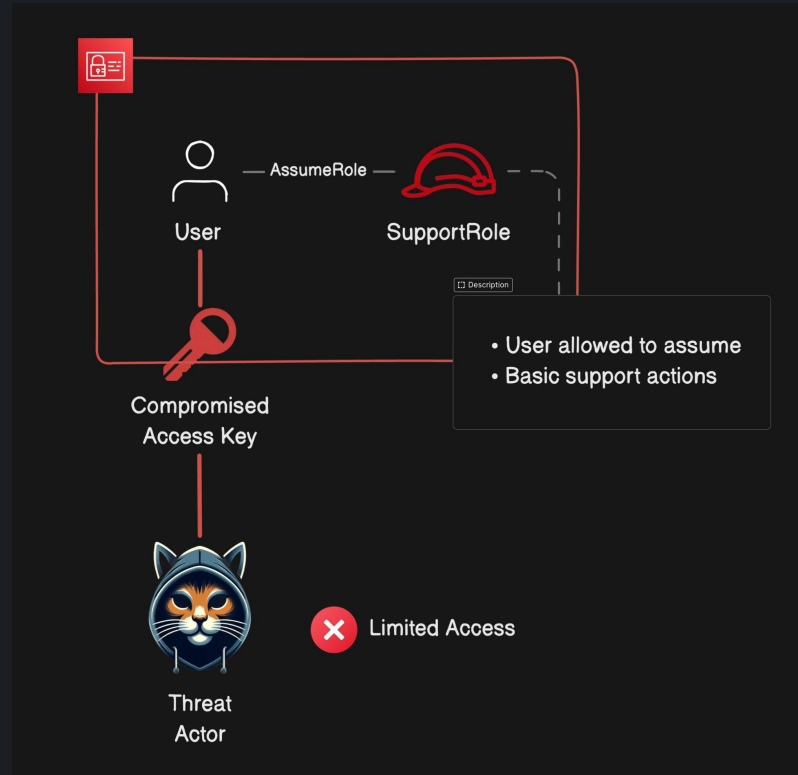


iam:AttachRolePolicy Lab



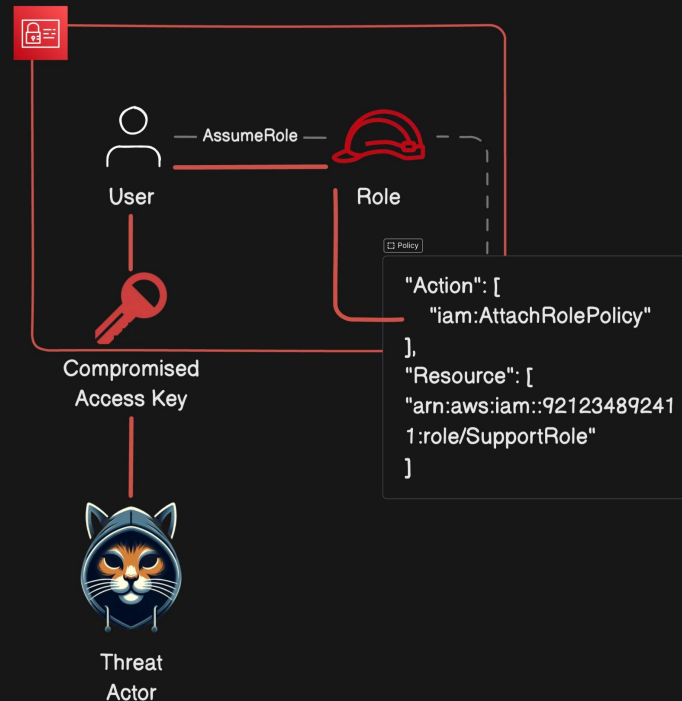


iam:AttachRolePolicy Lab



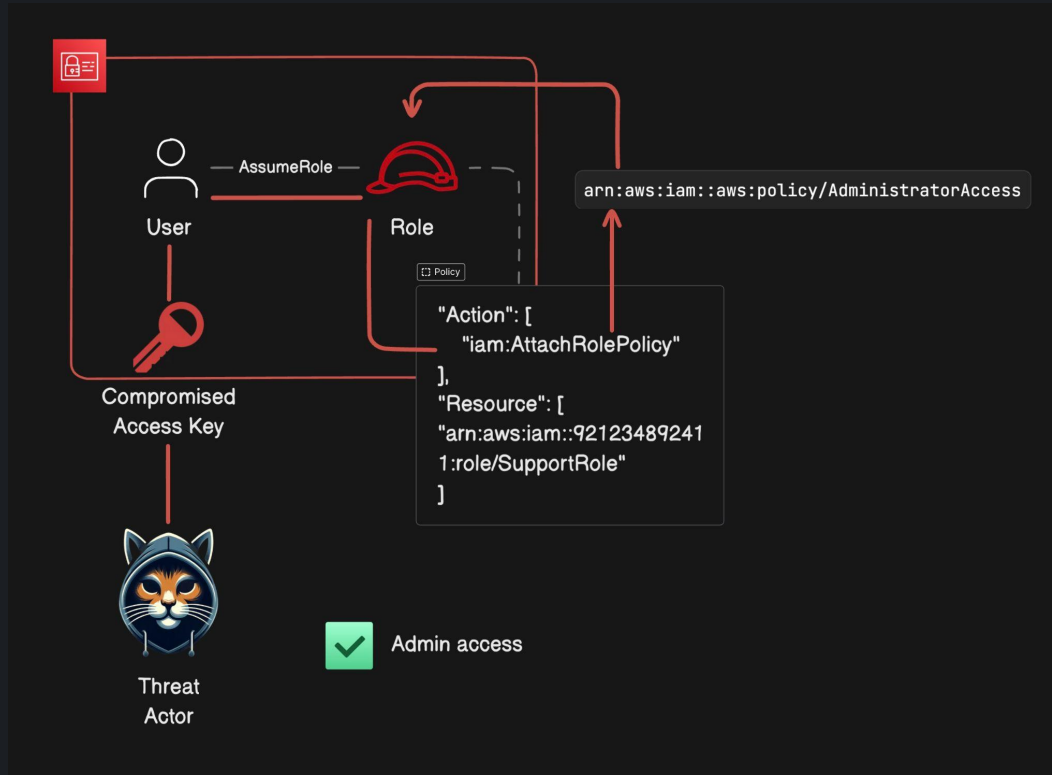


iam:AttachRolePolicy Lab





iam:AttachRolePolicy Lab





Using AI for writing secure IAM policies



How to use AI for writing secure IAM policies?

1. Do not use real account/resource ids, names, regions, etc. in order to not disclose any sensitive data by accident.
2. Be more specific when defining policy requirements.
3. Create a dedicated chat for writing policies.
4. Experiment with different AI systems.
5. Validate generated policies.



How to use AI for writing secure IAM policies?

Sample prompt that can be used to generate an IAM policy:

- *Act as experienced Cloud Security Engineer. Create an IAM policy that satisfies the following requirements:*
 - *follows the principle of least privilege*
 - *contains only the defined below permissions*
 - *AWS account ID - 012345678911*
 - *allows to read and write objects to the S3 bucket called "sample-test-bucket"*
 - *allows to start and stop EC2 instances with these ids: "i-0123456789abcdf01", "i-0123456789abcdf02" in "us-east-1" region*
 - *allows to read data from DynamoDB table called SampleTable in "us-east-1" region*



How to use AI for writing secure IAM policies?

ChatGPT 4

VS

Gemini

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::sample-test-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:012345678911:instance/i-0123456789abcdef01",
        "arn:aws:ec2:us-east-1:012345678911:instance/i-0123456789abcdef02"
      ]
    }
  ],
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ReadWriteBucket",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject" // Optional, for deleting objects if needed
      ],
      "Resource": [
        "arn:aws:s3:::sample-test-bucket/*"
      ]
    },
    {
      "Sid": "EC2StartStopSpecificInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:012345678911:instance/i-0123456789abcdef01",
        "arn:aws:ec2:us-east-1:012345678911:instance/i-0123456789abcdef02"
      ]
    }
  ],
}
```



How to use AI for analyzing IAM policies?

Sample prompt that can be used to analyze an IAM policy. **IMPORTANT:** delete/replace all sensitive information from policy before sending it to AI:

- *Act as experienced Cloud Security Engineer. Analyse the following AWS IAM policy and do the following:*
 - *check if it follows the principle of least privilege*
 - *highlight overly permissive actions*
 - *describe suggested fixes that can be used to fix the detected issues*
 - *provide a new secure version of the policy with all the suggested fixes included**<policy> insert your policy without sensitive data here... <policy>*



How to use AI for analyzing IAM policies?

Original

ChatGPT 4

Modified

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "codebuild:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "lambda:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ],
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::example-bucket/*",
        "arn:aws:s3:::example-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "codebuild:StartBuild",
        "codebuild:ListBuilds"
      ],
      "Resource": "arn:aws:codebuild:region:account-id:project/example-project"
    }
  ],
}
```



How to use AI for analyzing IAM policies?

Original

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "codebuild:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "lambda:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ],
}
```

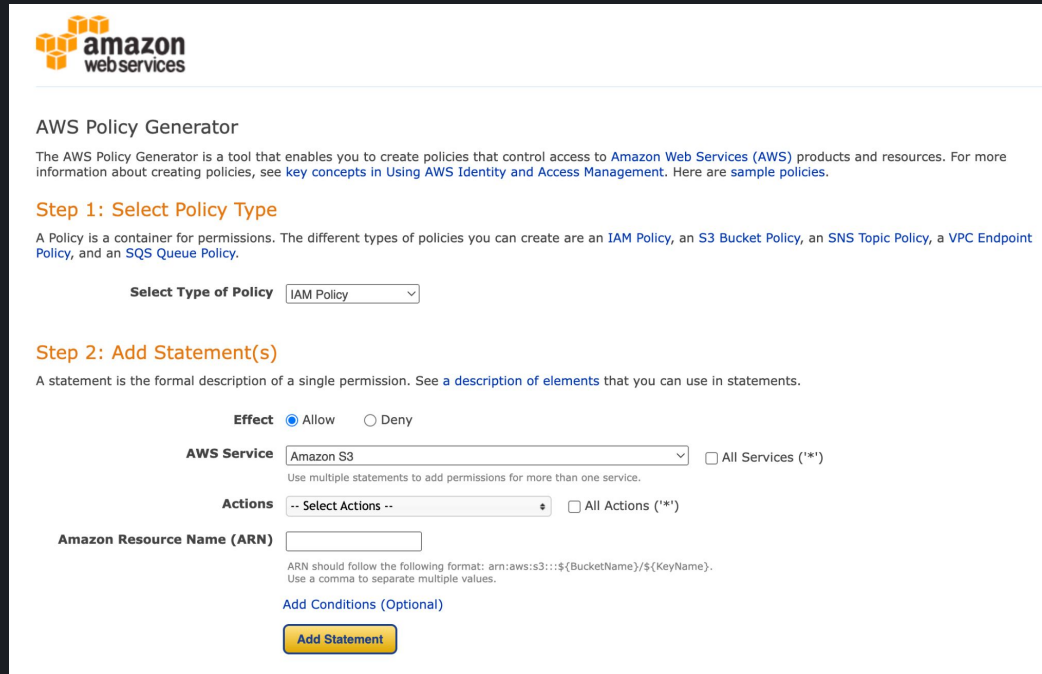
Gemini

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::my-secure-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "codebuild:StartBuild",
        "codebuild:GetBuild"
      ],
      "Resource": [
        "arn:aws:codebuild:REGION:ACCOUNT-ID:project/my-project"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:REGION:ACCOUNT-ID:function:my-lambda-function"
      ]
    }
  ],
}
```

Modified



Writing secure IAM policies using AWS Policy generator ([link](#))



The screenshot shows the AWS Policy Generator web interface. At the top left is the Amazon Web Services logo. Below it, the title "AWS Policy Generator" is followed by a brief description of the tool. The interface is divided into two main steps:

- Step 1: Select Policy Type**: A dropdown menu labeled "Select Type of Policy" is set to "IAM Policy".
- Step 2: Add Statement(s)**: This section includes:
 - Effect**: Radio buttons for "Allow" (selected) and "Deny".
 - AWS Service**: A dropdown menu set to "Amazon S3", with a checkbox for "All Services (**)".
 - Actions**: A dropdown menu set to "-- Select Actions --", with a checkbox for "All Actions (**)".
 - Amazon Resource Name (ARN)**: An empty text input field.
 - ARN format**: A note stating "ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}. Use a comma to separate multiple values."
 - Add Conditions (Optional)**: A section with an "Add Statement" button.



Tools for validating IAM policies

1. AWS IAM Policy Validator ([link](#))
2. AWS IAM Policy Simulator ([link](#))
3. Parliament ([link](#))



AWS Tools for detecting insecure/unused IAM policies

- IAM Access Analyzer ([link](#))



Tools for detecting issues IAM policies inside IaC templates

- trivy ([link](#))
- Checkov ([link](#))
- Cfn-nag ([link](#))
- Snyk IaC ([link](#))



CI/CD Tools Demo ([link](#))



About TechMagic



- Penetration testing services: Web and Mobile Application, Cloud infrastructure pentest
- Managed security services: embedding security practices into SDLC
- Security awareness team training on identification and mitigation of common security risks
- Compliance guidance: ISO, SOC2 certification preparation

We trusted by



[Book a Call](#)


or drop me an email @ igor.sasovets@techmagic.co





About Cybr.com

Learn **AWS cloud security** hands-on

Access training Courses,  Hands-On Labs,
and Ebooks on AWS Cloud Security



 <p>RED TEAM</p> <p>FREE</p> <p>Intro to AWS IAM Enumeration</p>	 <p>RED TEAM</p> <p>FREE</p> <p>Intro to Secrets Manager Enumeration</p>	 <p>RED TEAM</p> <p>FREE</p> <p>Intro to S3 Enumeration</p>	 <p>FOUNDATIONAL</p> <p>FREE</p> <p>Getting started with the AWS CLI</p>
 <p>BLUE TEAM</p> <p>Configure Security Groups</p>	 <p>BLUE TEAM</p> <p>Create a VPC with public and private subnets</p>	 <p>BLUE TEAM</p> <p>Deploy AWS WAF ACL for Application Load Balances</p>	 <p>RED TEAM</p> <p>S3 Data Exfiltration via EC2</p>



Resource Links

- GitHub demo project:
 - <https://github.com/IgorSasovets/aws-iam-policy-tools>
- Cybr's Hands-On Labs:
 - <https://cybr.com/hands-on-labs>
- Learn more about TechMagic Cyber Security Services:
 - <https://www.techmagic.co/security-testing-services>



Thank you for attending!

Any questions?



Christophe Limpalair

<https://linkedin.com/in/christophelimpalair>



Ihor Sasovets

<https://linkedin.com/in/ihor-sasovets/>



Upcoming webinars

<https://cybr.com/webinars>