





AWS IAM PrivEsc
Attacks & Defenses

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



FAQ

- This will be recorded and sent out in about 24 hours to the email you registered with
- These slides will also be available for download
- You can ask questions at any time and we will answer throughout the presentation or at the end

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Today's Session

- Introductions
- What are privilege escalations?
- Real-world attack that involved PrivEscs in AWS
- Demo attack (with Hands-On Lab)
- Demo defense
- About CodeShield & Cybr
- Q&A

code_shield

CYBR

About Us











About Manuel Benz

- Founder and CTO of CodeShield
- ☁️ 5+ years of AWS experience
- 🔬 Research background in SAST/DAST
- 🥁 Drummer and house owner
- ✈️ I live next to Frankfurt, Germany

Manuel Benz
linkedin.com/in/manuel-benz/

code_shield

CYBR

AWS IAM PrivEsc Attacks & Defenses

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield





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

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

@ChristopheLimp
https://twitter.com/christophelimp

code_shield

CYBR

Christophe Limpalair
Founder & Trainer
at Cybr



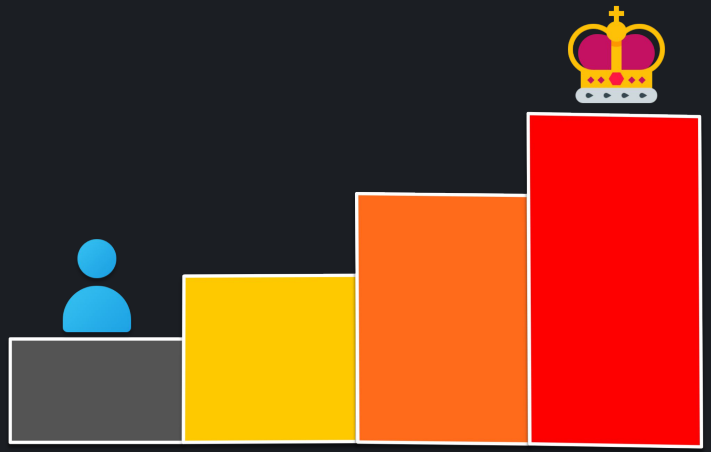
Manuel Benz
CTO and Co-Founder of
CodeShield



What are Privilege Escalations?

In simple terms:

An attacker going from lower privileges to higher privileges



Christophe Limpalair
Founder & Trainer
at Cybr



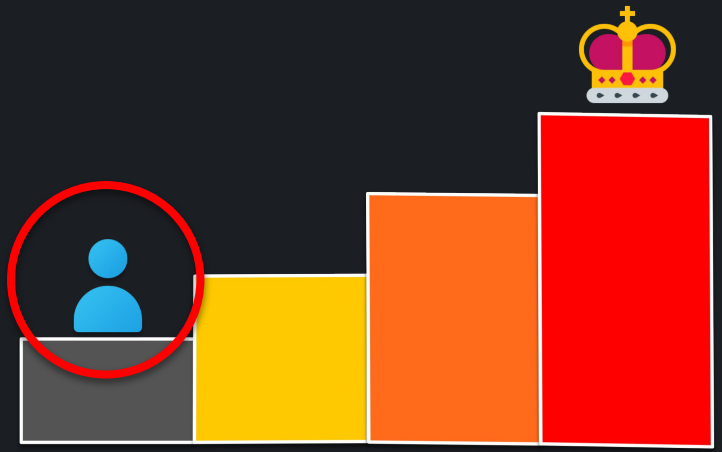
Manuel Benz
CTO and Co-Founder of
CodeShield



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



Christophe Limpalair
Founder & Trainer
at Cybr



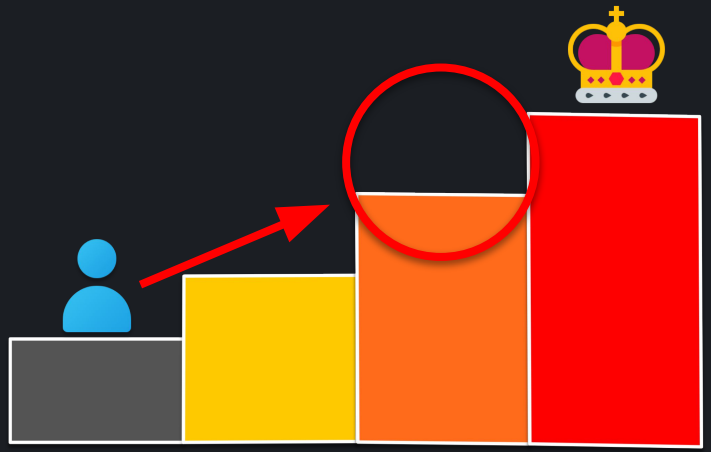
Manuel Benz
CTO and Co-Founder of
CodeShield



What are Privilege Escalations?

In terms of AWS PrivEscs:

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



Christophe Limpalair
Founder & Trainer
at Cybr

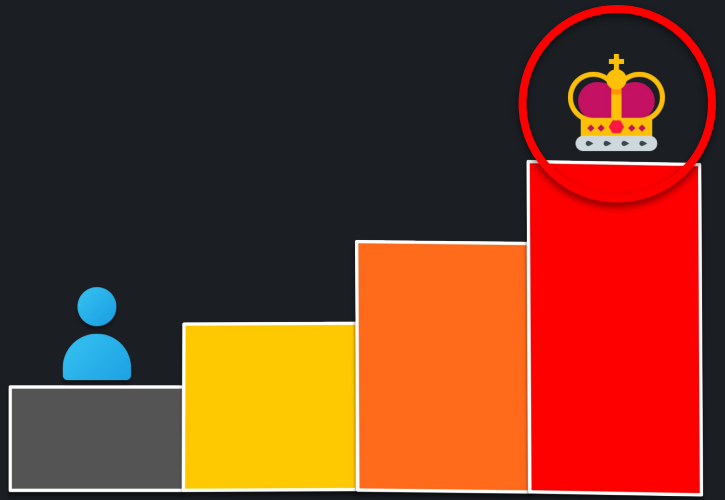


Manuel Benz
CTO and Co-Founder of
CodeShield



What are Privilege Escalations?

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



Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



What are Privilege Escalations?

Even without admin rights, they could:

- Launch big EC2 instances for crypto mining ($$$)
- Exfiltrate sensitive data (S3, database, code, etc…)
- Access secret values in Secrets Manager *<- What we'll demo today*
- Etc…

code_shield

CYBR

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



What are Privilege Escalations?

In fact, Manuel brought a real-world example of impact…

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Hacker Puts Hosting Service Code Spaces Out of Business



"Within 12 hours, Code Spaces went from a viable business to devastation. The company reported that all of its svn repositories—backups and snapshots—were deleted. All EBS volumes containing database files were also deleted. A few old svn nodes and one git node were left untouched, the company said."

Code Spaces hack 2014
https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/

code_shield

CYBR

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces
5. Code Spaces changed keys for EC2

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces
5. Code Spaces changed keys for EC2
6. Attackers deleted all business data and backups

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



IAM PrivEsc Attack Demo

iam:PutRolePolicy

If you want to follow along:
https://cybr.com/webinar-privesc

code_shield

CYBR

AWS IAM PrivEsc Attacks & Defenses

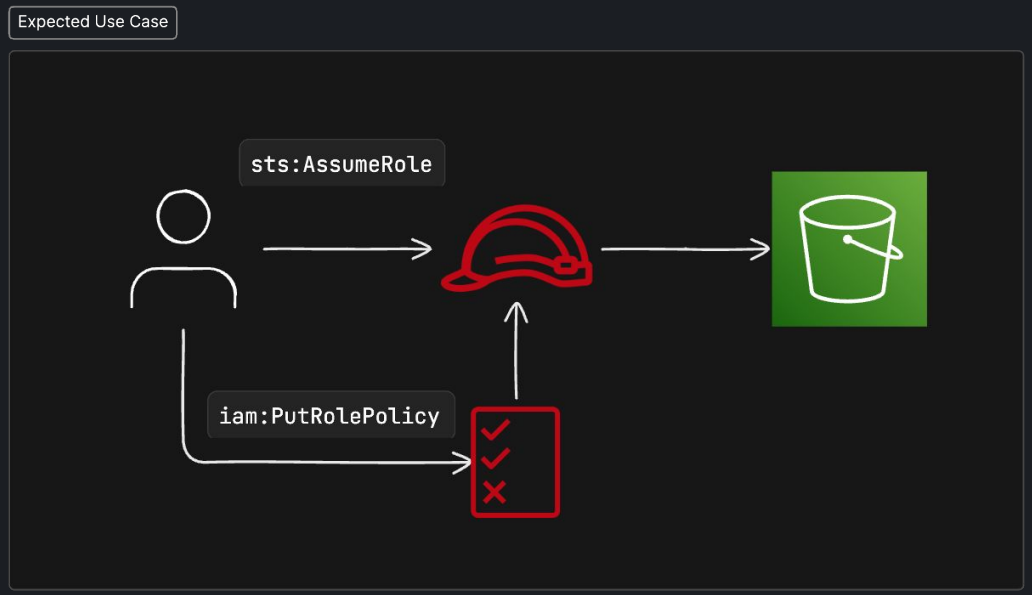
Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Scenario: You're a developer working on a team with access to S3 through an IAM role. Since you need to be able to create more buckets and change settings on those buckets without constantly requesting permission, your manager gave you the ability to update your role policy. Unfortunately, the policy granted was misconfigured and made you able to escalate your privileges.



code_shield

CYBR

AWS IAM PrivEsc Attacks & Defenses

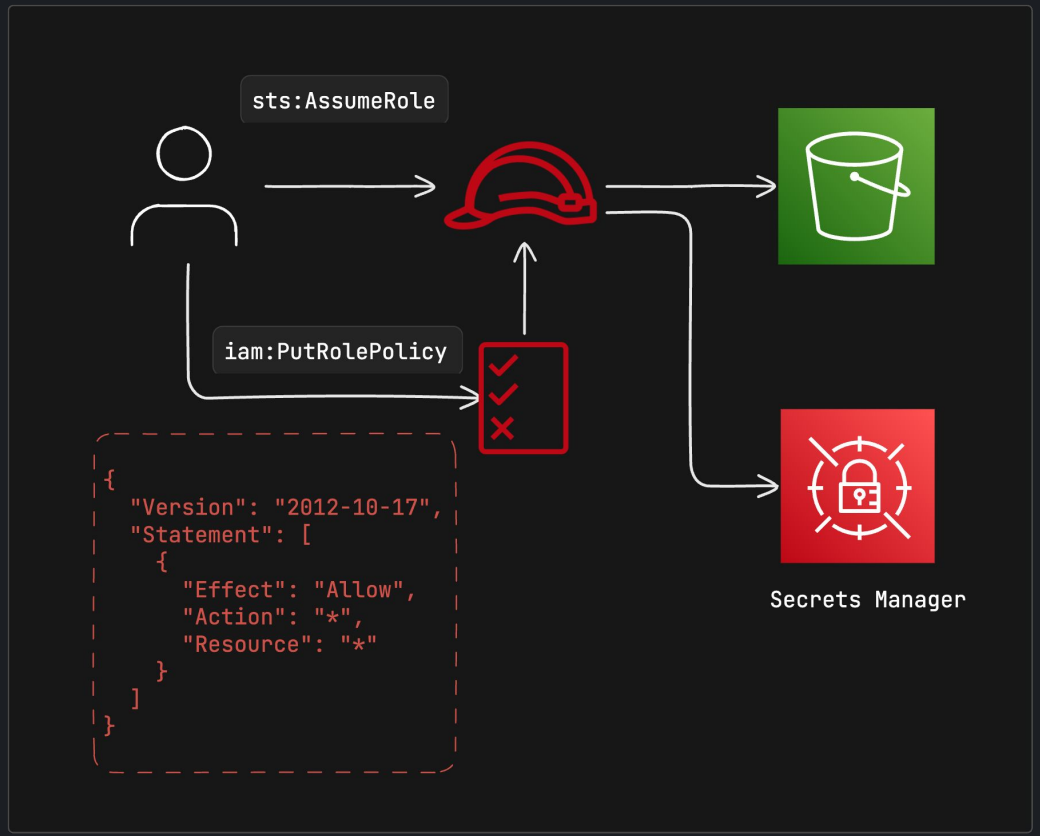
Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Threat Use Case



code_shield

CYBR

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



IAM PrivEsc Defense Demo

code_shield

CYBR

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



About CodeShield.io

- Scan your AWS account for privilege escalation in under 30 minutes
- Gain an overview of all permissions and connectivity of your cloud assets
- Get your first audit including discussion of results for free!
- Learn how to protect against IAM privilege escalation in AWS

Trusted by

DB Systel GmbH · syracom business efficiency engineering · handly · HANKO · northmill bank · TEMPEST Protegendo negócios no mundo digital. · zoph.io

Schedule a Demo

or drop me an email @ manuel.benz@codehield.io

code_shield

CYBR

AWS IAM PrivEsc Attacks & Defenses

Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



🔒 About Cybr.com

Learn AWS cloud security hands-on

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



Christophe Limpalair
Founder & Trainer
at Cybr



Manuel Benz
CTO and Co-Founder of
CodeShield



Resource Links

- Lab used in the demo:
  - https://cybr.com/courses/iam-privilege-escalation-labs/lessons/lab-ctf-iamputrolepolicy-privesc/
- IAM PrivEsc Course:
  - https://cybr.com/courses/iam-privilege-escalation-labs/
- Cybr's Hands-On Labs:
  - https://cybr.com/hands-on-labs
- CodeShield.io:
  - https://codeshield.io

code_shield

CYBR





Thank you for attending!

Any questions?

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

Manuel Benz
https://linkedin.com/in/manuel-benz/

LIVE

Upcoming webinars
https://cybr.com/webinars