
cybr.com
What hackers know about your AWS accounts
Hint: it’s not nothing
CYBR

What hackers know about your AWS accounts

Today's agenda

- About us
- What can threat actors see inside of your accounts?
- How to use this information
- AWS security challenges orgs struggle with

CYBR

About Us



Christophe Limpalair

- 📽️ Founder and Trainer at Cybr
- 👨‍💻 8+ years of AWS production experience
- 🥾 Originally from France, but currently live in Colorado and love hiking & skiing
- 🍻 I'm also a professional hobbyist *(current: flying, home brewing, and prior: growing mushrooms)*

Cybr.com/discord

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

CYBR

About Us



Daniel Grzelak
https://linkedin.com/in/danielgrzelak/

Daniel Grzelak

- Super Serious Internet Guy
- Milo Enthusiast
- AWS hackerer
- Chief Innovation Officer at Plerion (plerion.com)



CYBR

Why does it matter?
&
The lies of omission we tell...

What hackers know about your AWS accounts

1. Hacking before cloud
2. Hacking after cloud

CYBR

Cloud hacking example 1: SQS

https://sqs.{region}.amazonaws.com/{account_id}/{queue_name}

Cloud hacking example 2: S3 CDK shadow resources

cdk-{hnb659fds}-cfn-exec-role-{account_id}-{region}

What identifiers do hackers need?

Account IDs
IAM keys
Amazon hostnames
Resource IDs
Resource Names
ARNs

How can they get them?

Github (Sourcegraph demo)
PyPi, Nuget, NPM etc.
“Threat intel”

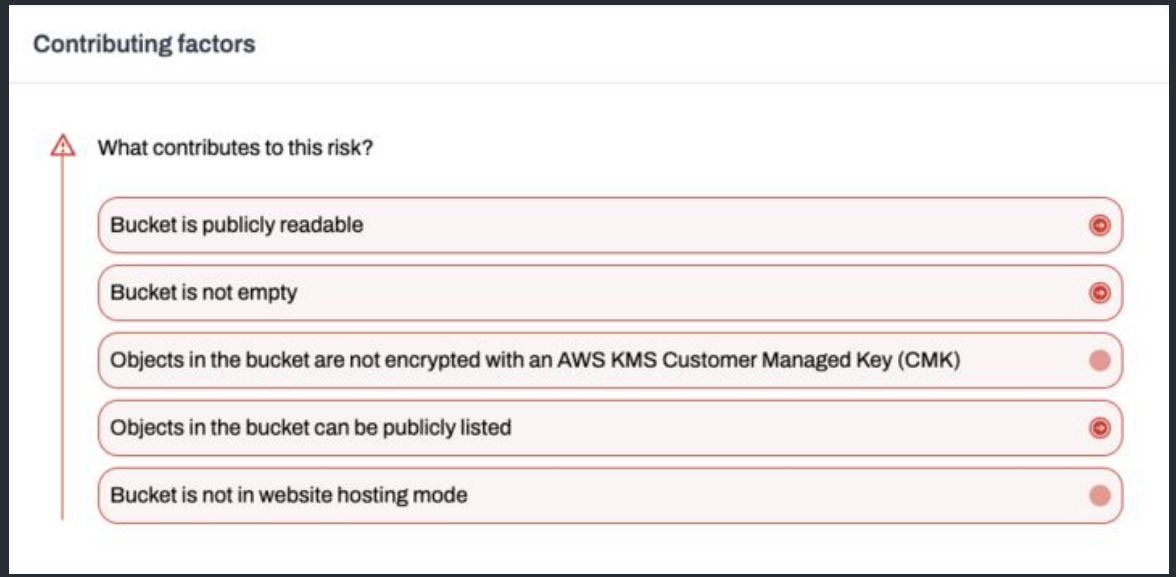
Awseye.com

All that stuff and more...
Let's try it.

But what does it all mean?

You aren’t hacked but you might have some sleuthing to do.

How we (Plerion) are using that information?



CYBR

AWS security challenges

1. Knowing what they have
2. Understanding what it means
3. Prioritising the work
4. All the usual - budgets, org structure, demonstrating progress, communication





Thank you for attending!

Any questions?

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

Daniel Grzelak
https://llinkedin.com/in/danielgrzelak/

Live training webinars
https://cybr.com/webinars