Compromising AWS® for fun and profit

Simon Whittaker

Cyber Security Director - Vertical Structure Ltd

Simon Whittaker - Lukasz Mrozowski

Simon.whittaker@verticalstructure.com

Prepare, Protect, Persist®

- **Prepare**
- We help you and your partners to understand how to identify and resolve potential security issues at the earliest stages with hands on 'hack yourself first', threat modelling and GDPR compliance workshops as well as security training for non-technical colleagues.
- **Protect**
- Using automated and manual penetration testing techniques, we provide a comprehensive security report for your Web and mobile applications, including API testing, and networks. The report highlights potential issues and their resolutions.
- **Persist**
- We ensure that your organisation benefits from continual improvements in security levels through information assurance processes, auditing and certification including ISO27001:2013 and Cyber Essentials.

simon.whittaker@verticalstructure.com

Bingo

Bingo Caller's Card		
Brexit	Blockchain	AI
Machine Learning	AWS	Cloud
Cyber	Computer Misuse Act	Privileges

https://vsltd.co/bsBingo

simon.whittaker@verticalstructure.com

Qualifications

Simon.whittaker@verticalstructure.com

Shared Responsibility Model

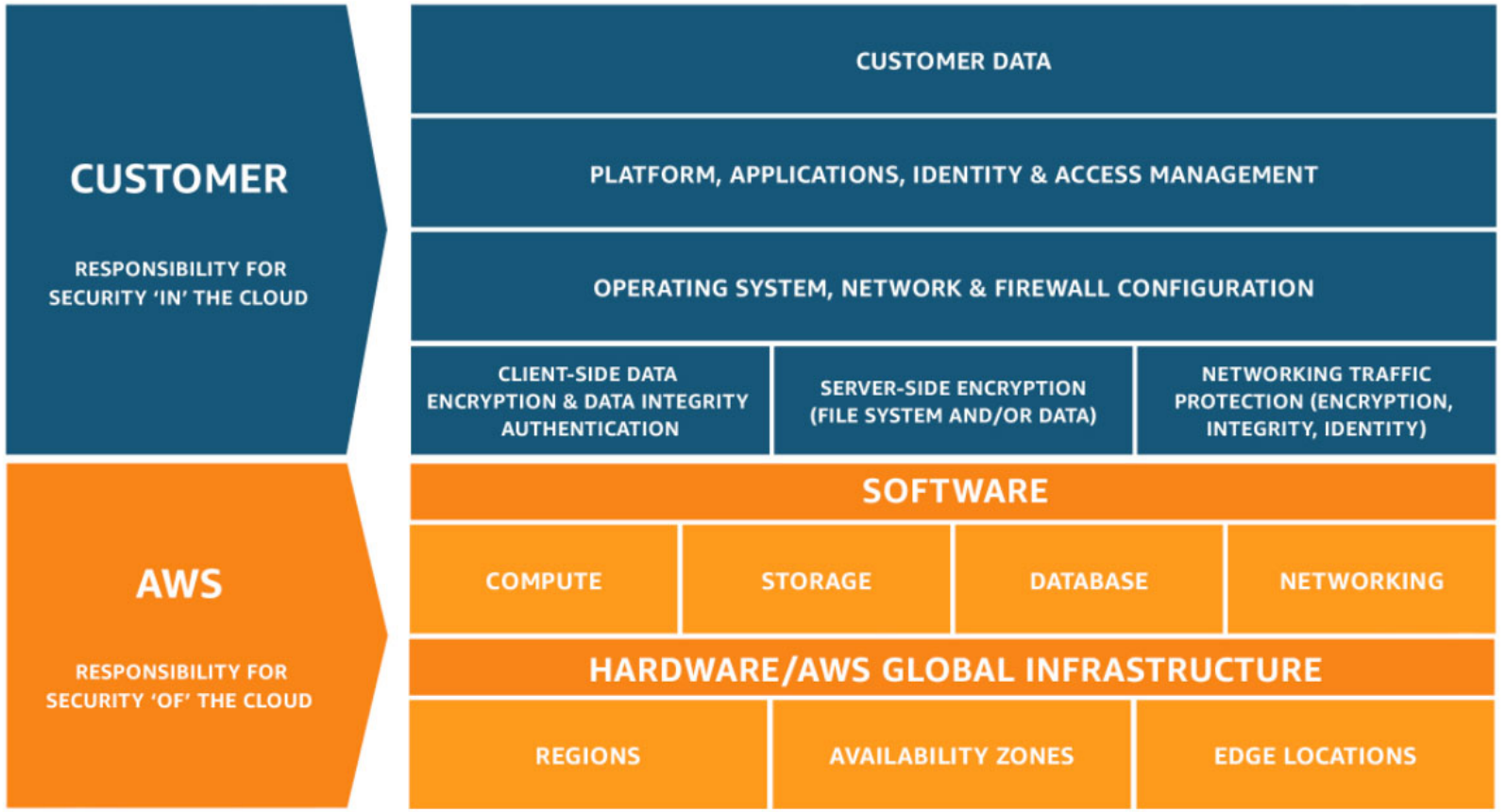


Image from: https://aws.amazon.com/compliance/shared-responsibility-model/

simon.whittaker@verticalstructure.com

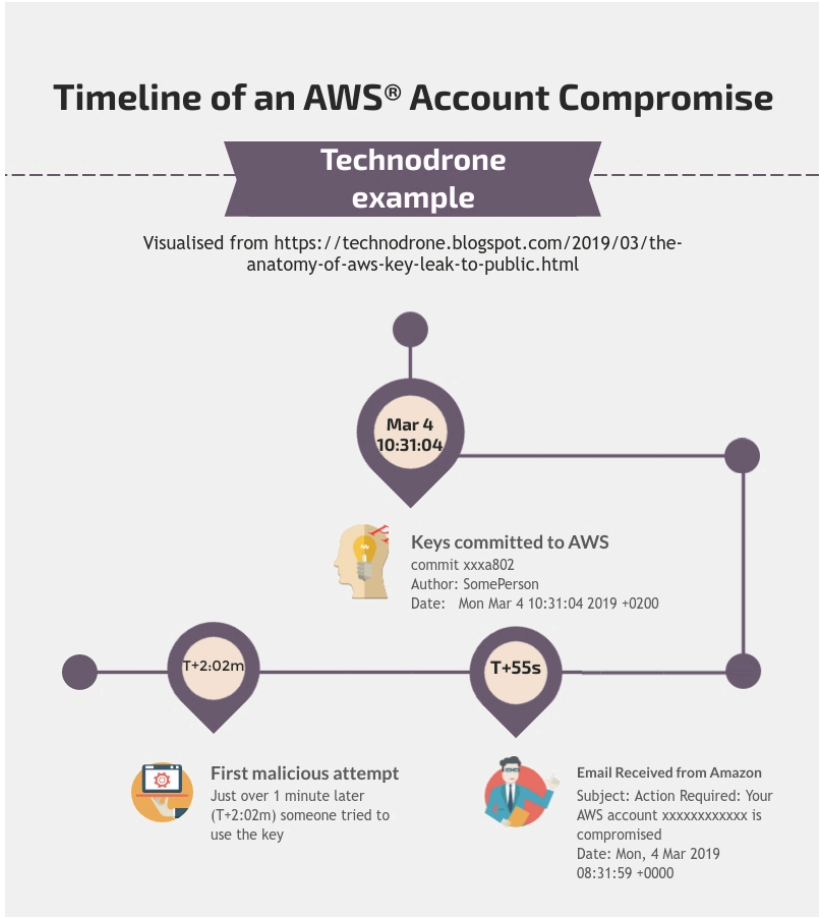
What do attackers want?

Tesla Hackers Hijacked Amazon Cloud Account to Mine Cryptocurrency

simon.whittaker@verticalstructure.com

Working fast

- IAM is confusing
- Use principle of least privilege
- Never commit credentials



https://technodrone.blogspot.com/2019/03/the-anatomy-of-aws-key-leak-to-public.html

Simon.whittaker@verticalstructure.com

IAM

simon.whittaker@verticalstructure.com

Let’s have a play

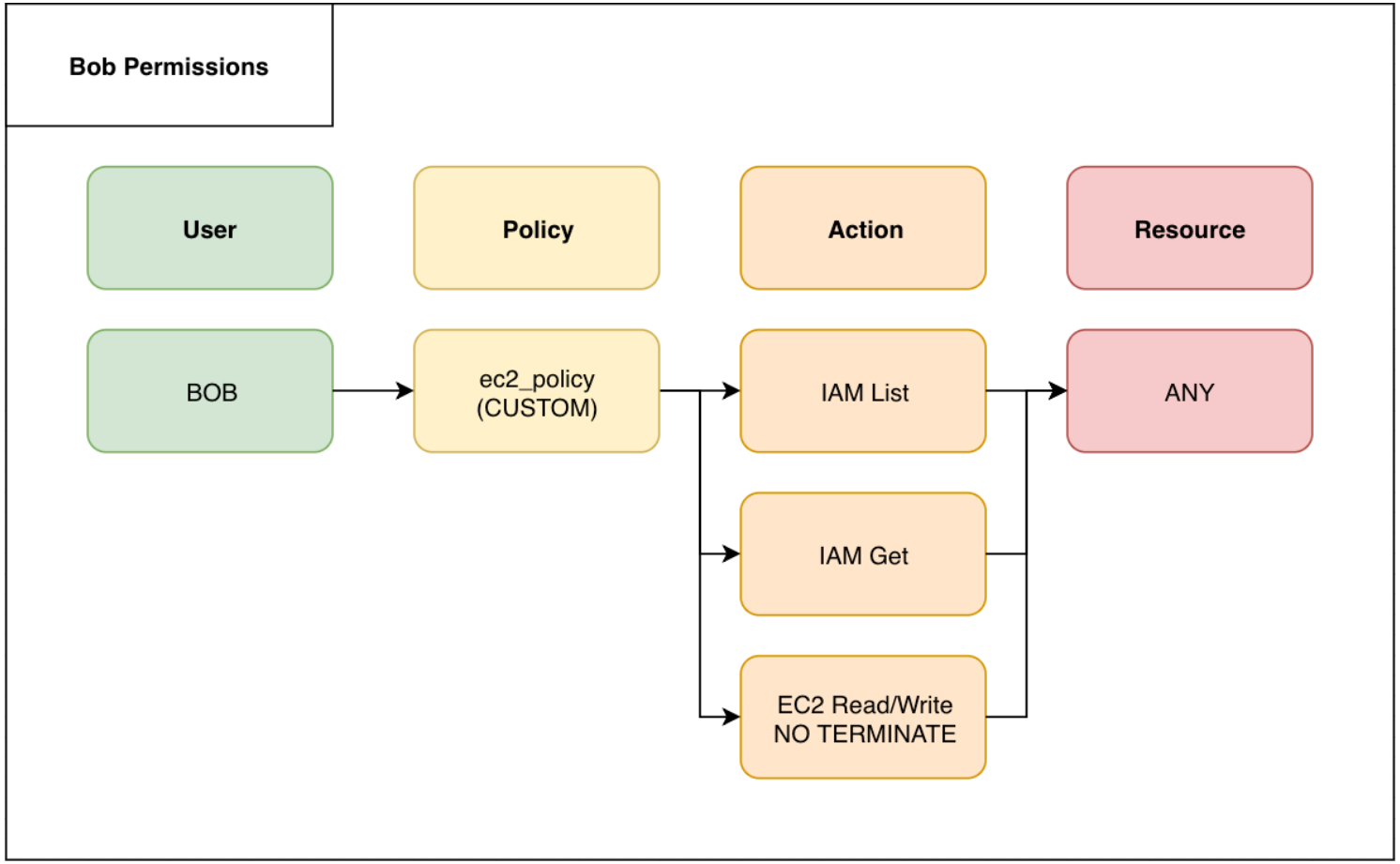
All exploits are being performed in a safe environment

simon.whittaker@verticalstructure.com

Example 1 – EC2 escalation

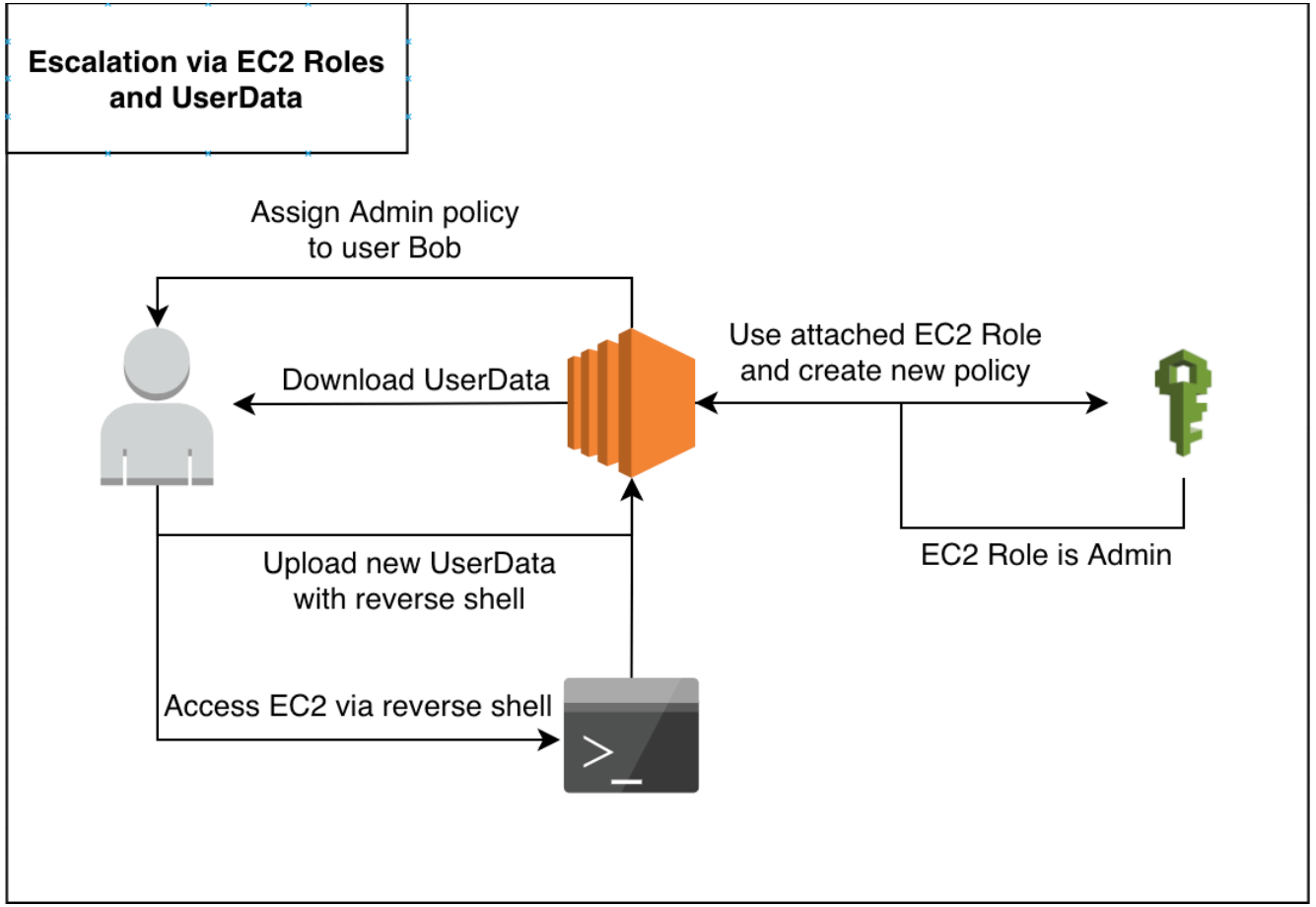
Simon.whittaker@verticalstructure.com

Bob's permissions



simon.whittaker@verticalstructure.com

The process

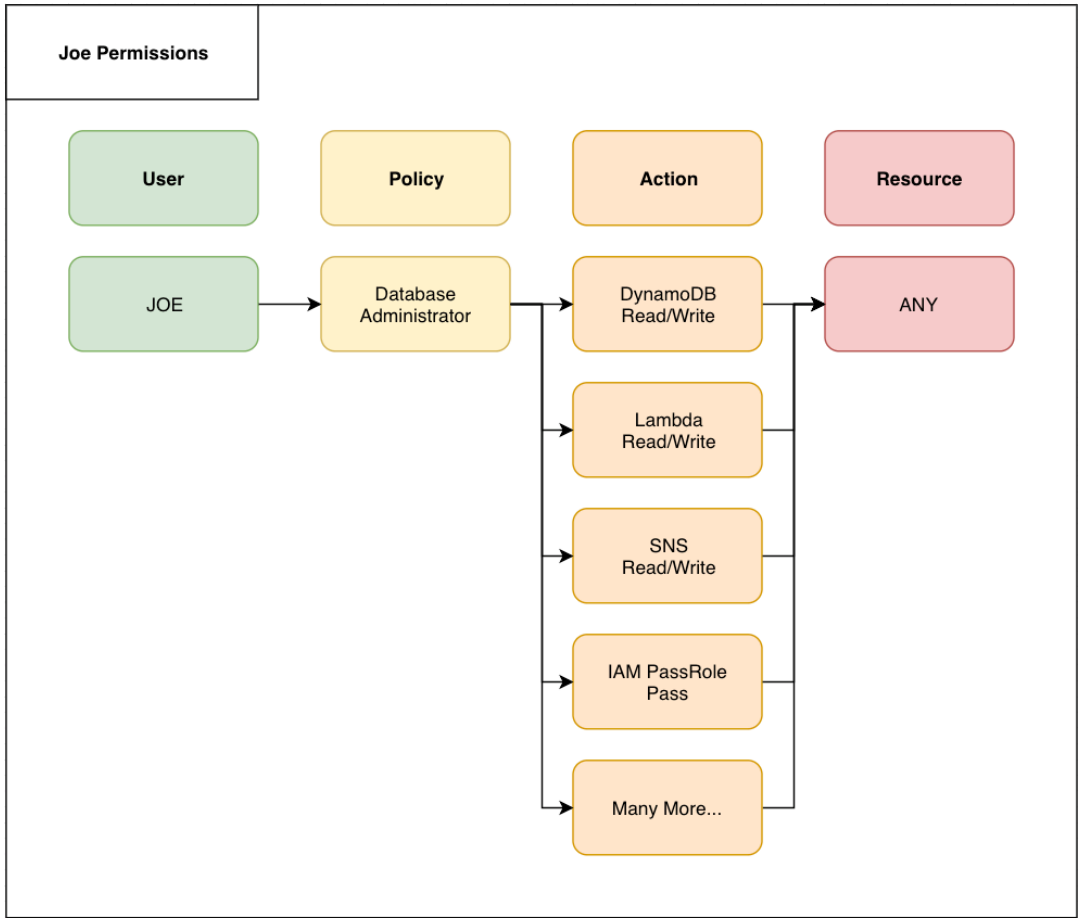


simon.whittaker@verticalstructure.com

Example 2 - Escalation to IAM Administrator

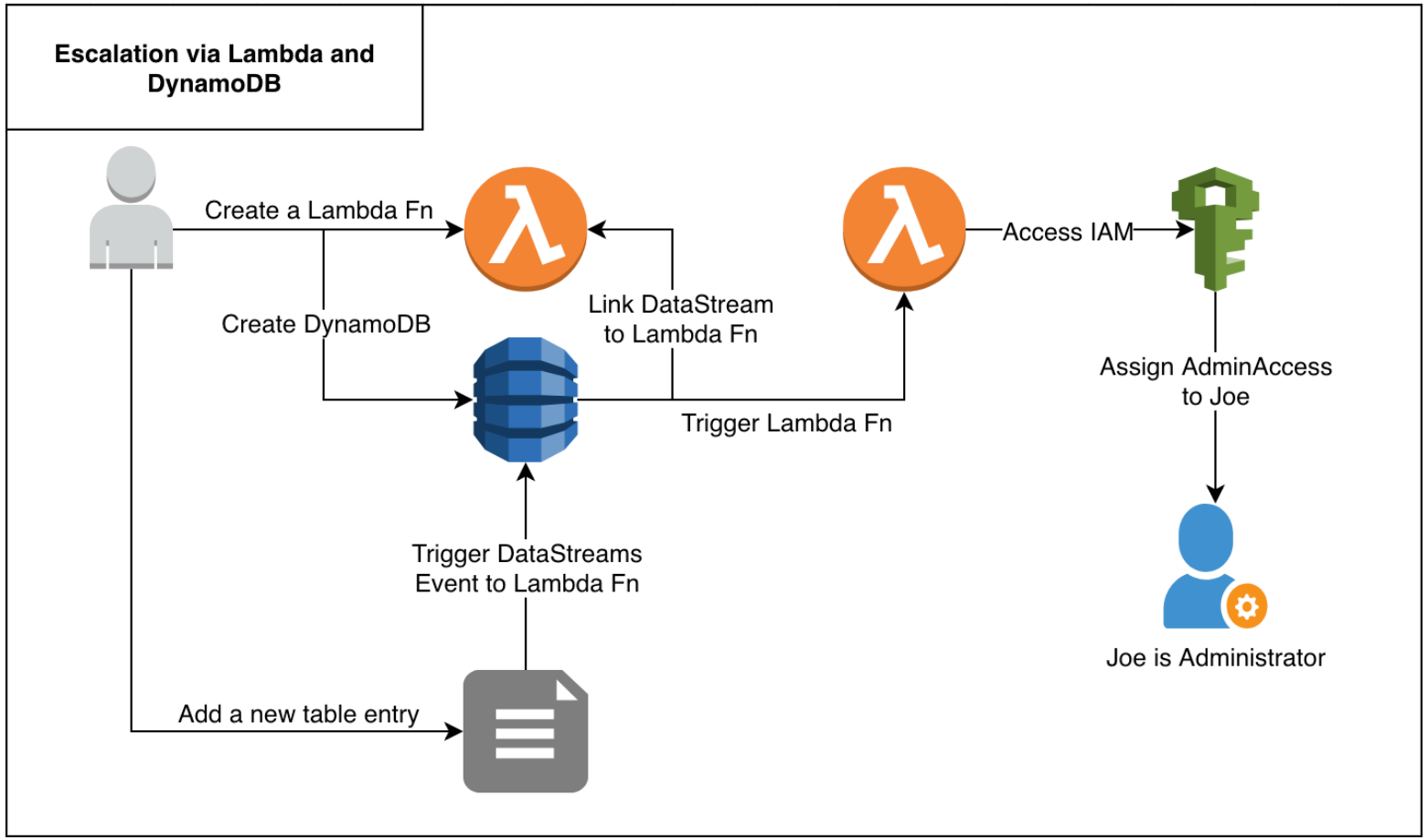
Simon.whittaker@verticalstructure.com

Joe’s permissions



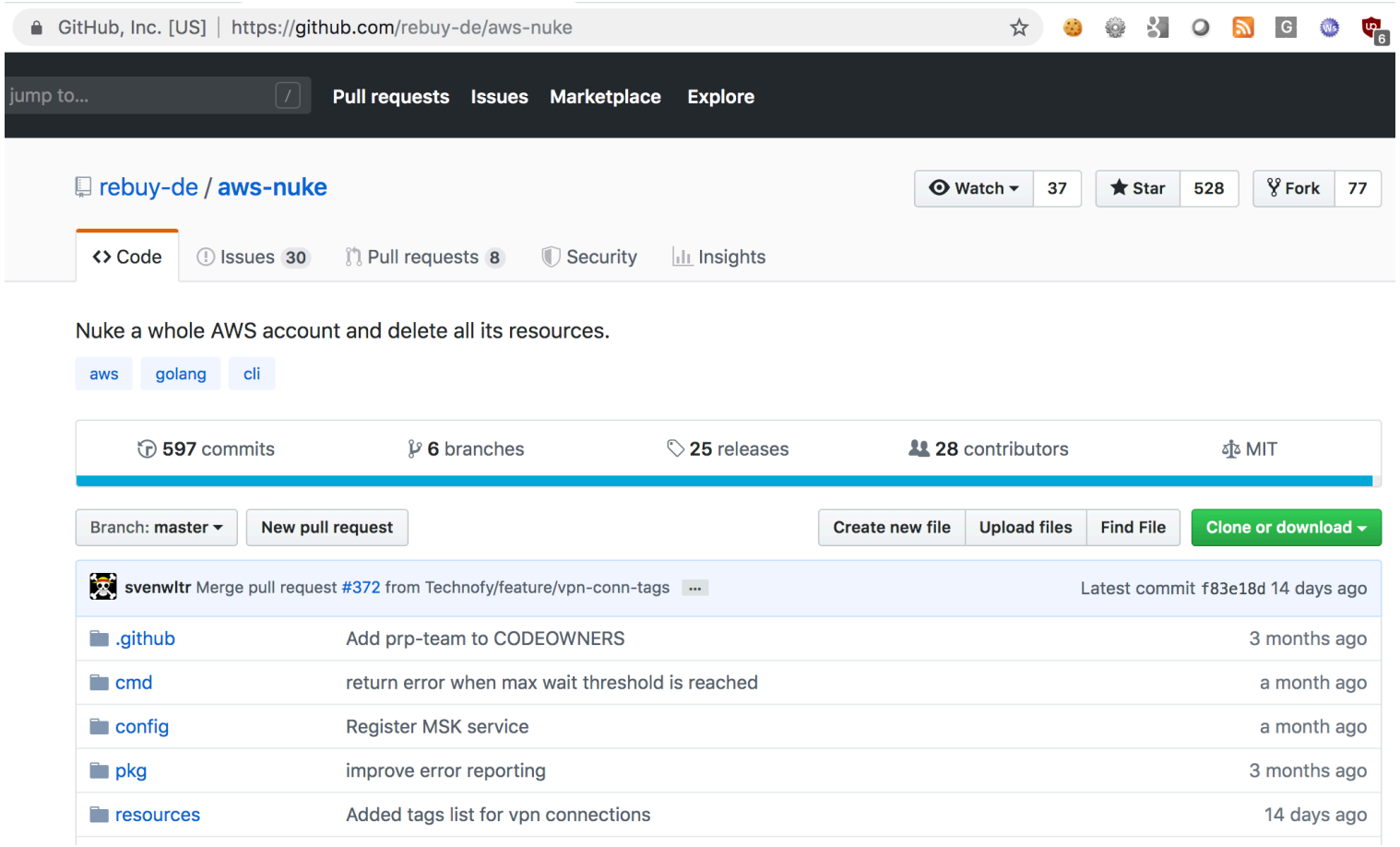
simon.whittaker@verticalstructure.com

The process



simon.whittaker@verticalstructure.com

Consequences



simon.whittaker@verticalstructure.com

Fun and Profit

Simon.whittaker@verticalstructure.com

Try for yourself

- Cloudgoat - https://github.com/RhinoSecurityLabs/cloudgoat

Simon.whittaker@verticalstructure.com

Protection Measures

- Ask questions
  - Some great advice from UK NCSC
- Secure users
- Reduce privileges
- Implement tools to help you

Simon.whittaker@verticalstructure.com

Bingo results

simon.whittaker@verticalstructure.com

Questions?

Simon.Whittaker@verticalstructure.com

@szlwzl

https://vsltd.co/NIDevConf19