



Compromising AWS® for fun and profit

Simon Whittaker

Cyber Security Director - Vertical Structure Ltd

Simon Whittaker - Lukasz Mrozowski





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.

Bingo



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

<https://vs ltd.co/bsBingo>

Qualifications



Select

Consulting
Partner



Security - Specialty

Shared Responsibility Model

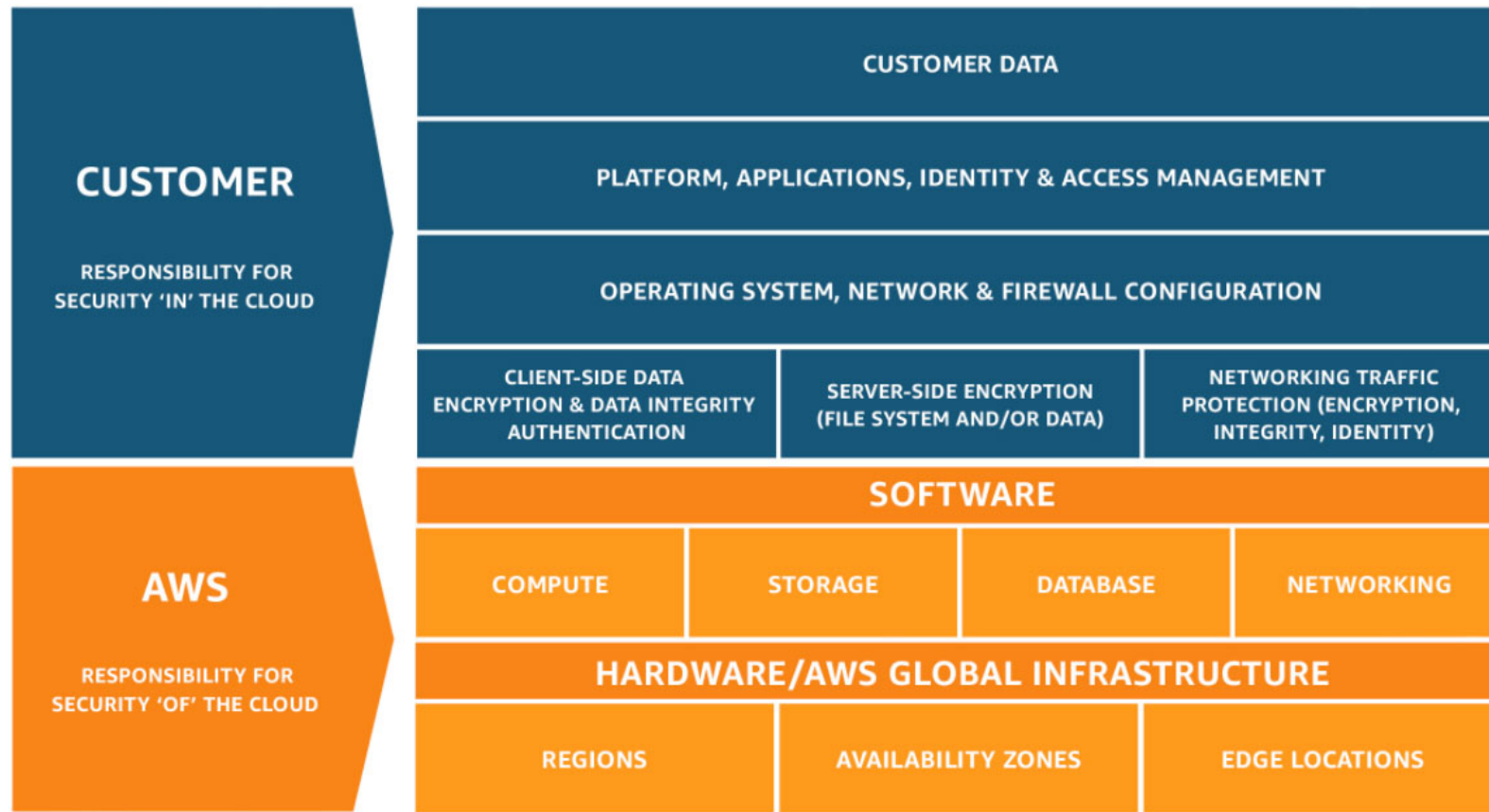


Image from: <https://aws.amazon.com/compliance/shared-responsibility-model/>

What do attackers want?



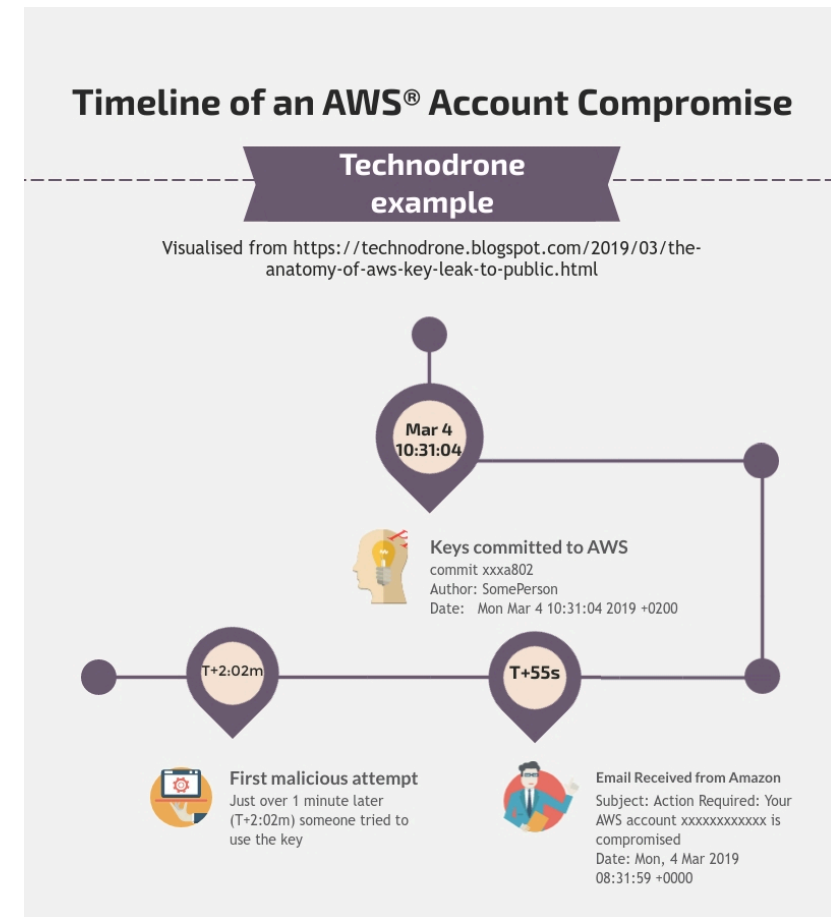
Tesla Hackers Hijacked Amazon Cloud Account to Mine Cryptocurrency



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>



IAM



Let's have a play

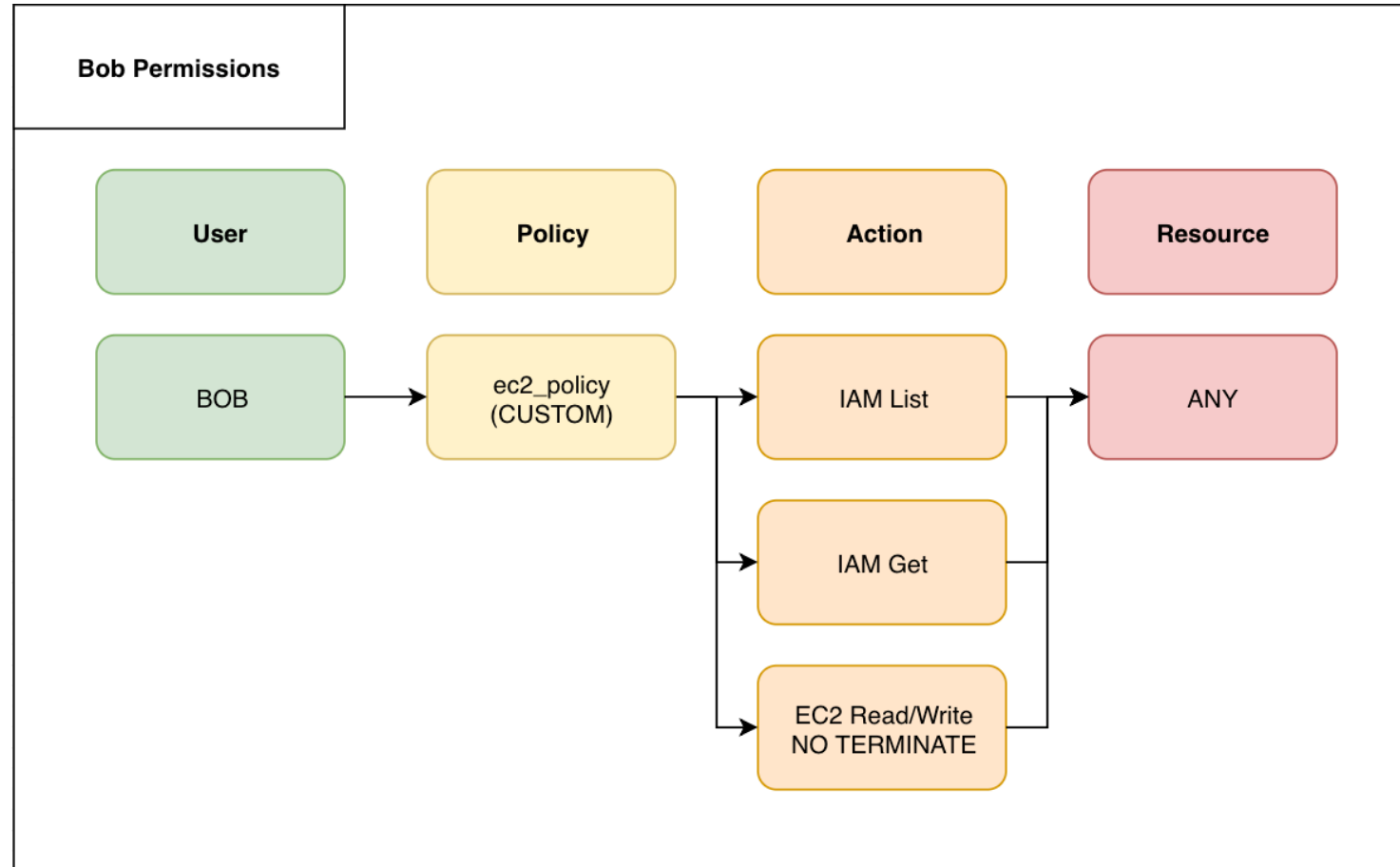


All exploits are being performed in a safe environment

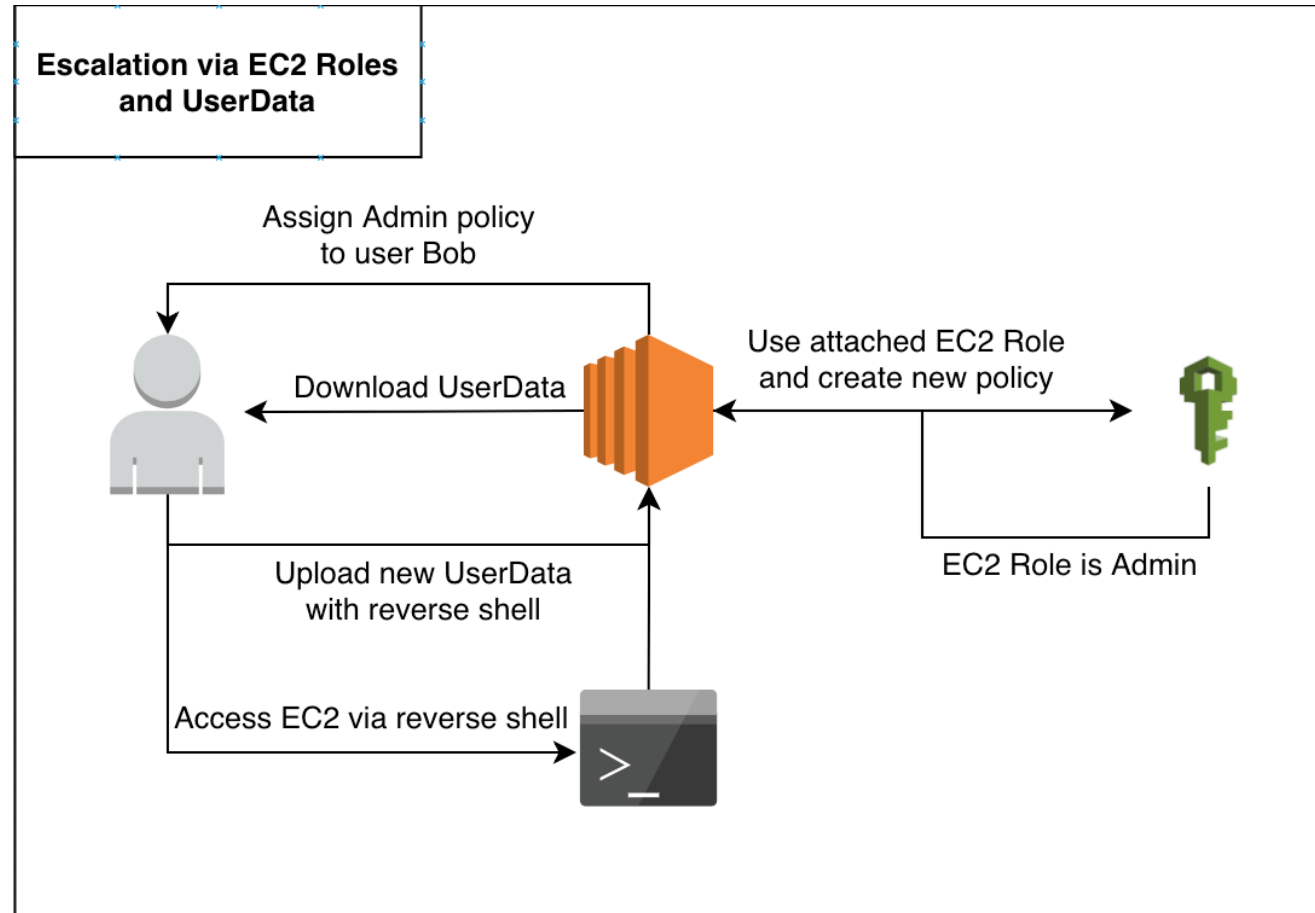


Example 1 – EC2 escalation

Bob's permissions



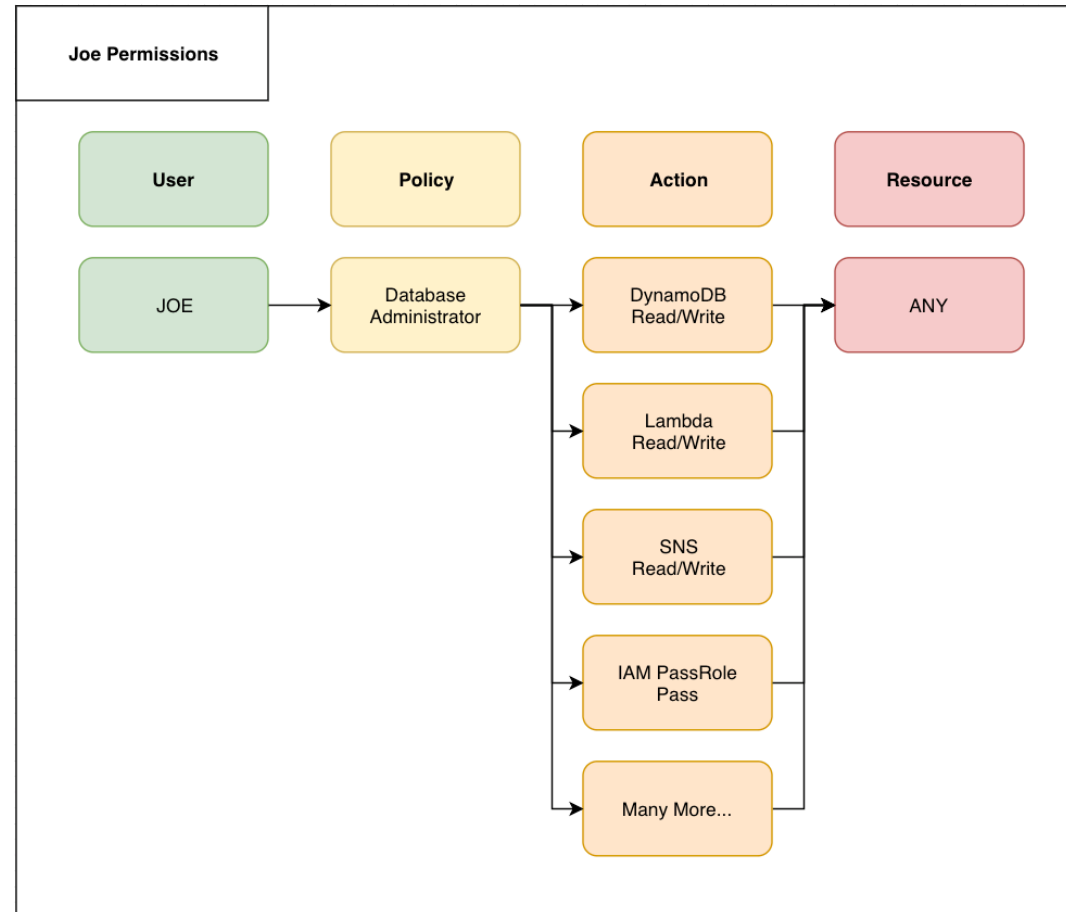
The process



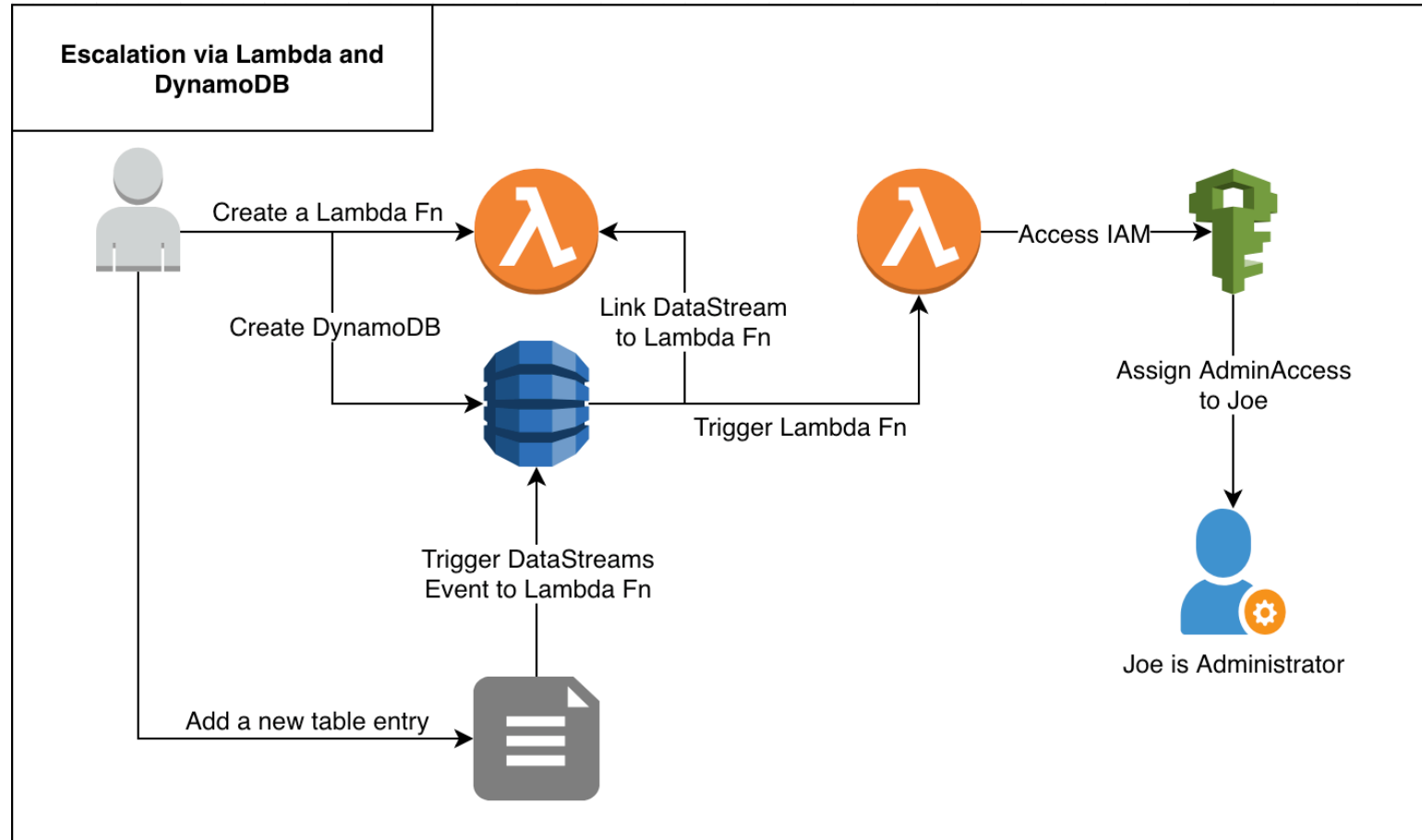


Example 2 - Escalation to IAM Administrator

Joe's permissions



The process



Consequences



GitHub, Inc. [US] | <https://github.com/rebuy-de/aws-nuke>

jump to... / Pull requests Issues Marketplace Explore

rebuy-de / aws-nuke

Watch 37 Star 528 Fork 77

Code Issues 30 Pull requests 8 Security Insights

Nuke a whole AWS account and delete all its resources.

aws golang cli

597 commits 6 branches 25 releases 28 contributors MIT

Branch: master New pull request Create new file Upload files Find File Clone or download

svenwltr Merge pull request #372 from Technofy/feature/vpn-conn-tags Latest commit f83e18d 14 days ago

.github	Add prp-team to CODEOWNERS	3 months ago
cmd	return error when max wait threshold is reached	a month ago
config	Register MSK service	a month ago
pkg	improve error reporting	3 months ago
resources	Added tags list for vpn connections	14 days ago

Fun and Profit





Try for yourself

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





Protection Measures

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



Bingo results



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



Questions?

Simon.Whittaker@verticalstructure.com

@szlwzl

<https://vs ltd.co/NIDevConf19>