SANS | DFIR

The Good, Bad and Ugly of Cloud Incident Response

London @Night Talk

KORSTIAAN STAM

Incident Response in the cloud is easier

Incident Response in the cloud is more difficult

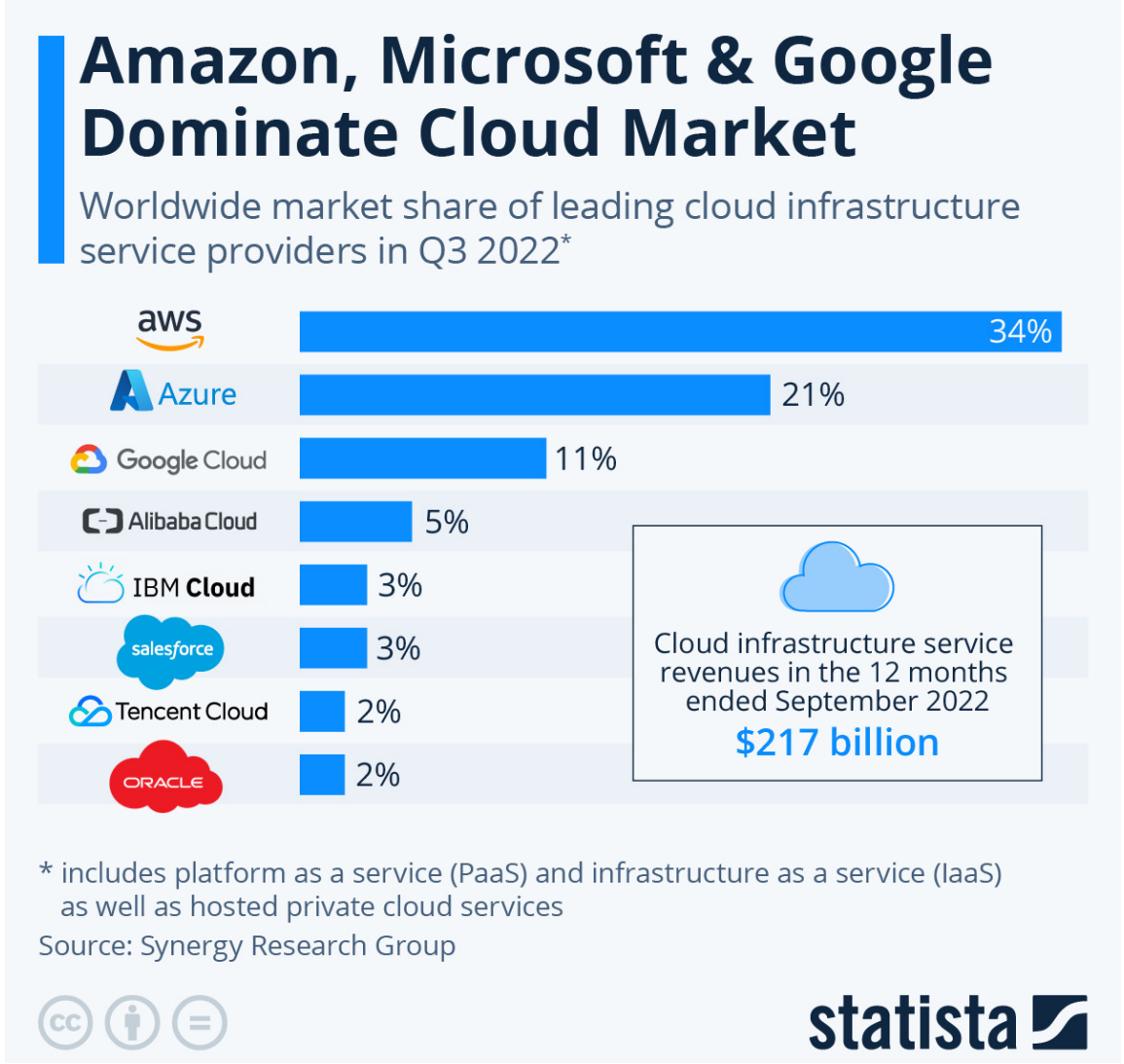
The cloud is more secure by default compared to on-premise

I know the forensic artefacts available in the cloud

About me

- SANS Instructor FOR509: Enterprise Cloud Forensics and Incident Response
- Founder & CEO Invictus Incident Response B.V.
- Previous IR positions at PwC and Northwave Cybersecurity
- Open-source developer
- Parttime teacher at Amsterdam University of Applied s
- Most importantly cloud incident response enthusiast!

Background



- The cloud is here to stay and it's still growing
- The focus for cloud incident response and this talk will be on the big 3
- The fastest growing cloud is Google Cloud followed by Oracle and Microsoft
- You might encounter other clouds

Sources (statista.com, datamation.com, financialmirror.com)

Cloud incidents

1. Data breaches
2. Denial-of-service (DoS) attacks:
3. Insider threats
4. Malware and ransomware
5. Account hijacking
6. API attacks
7. Man-in-the-middle (MitM) attacks
8. Cryptojacking
9. Advanced persistent threats (APTs)

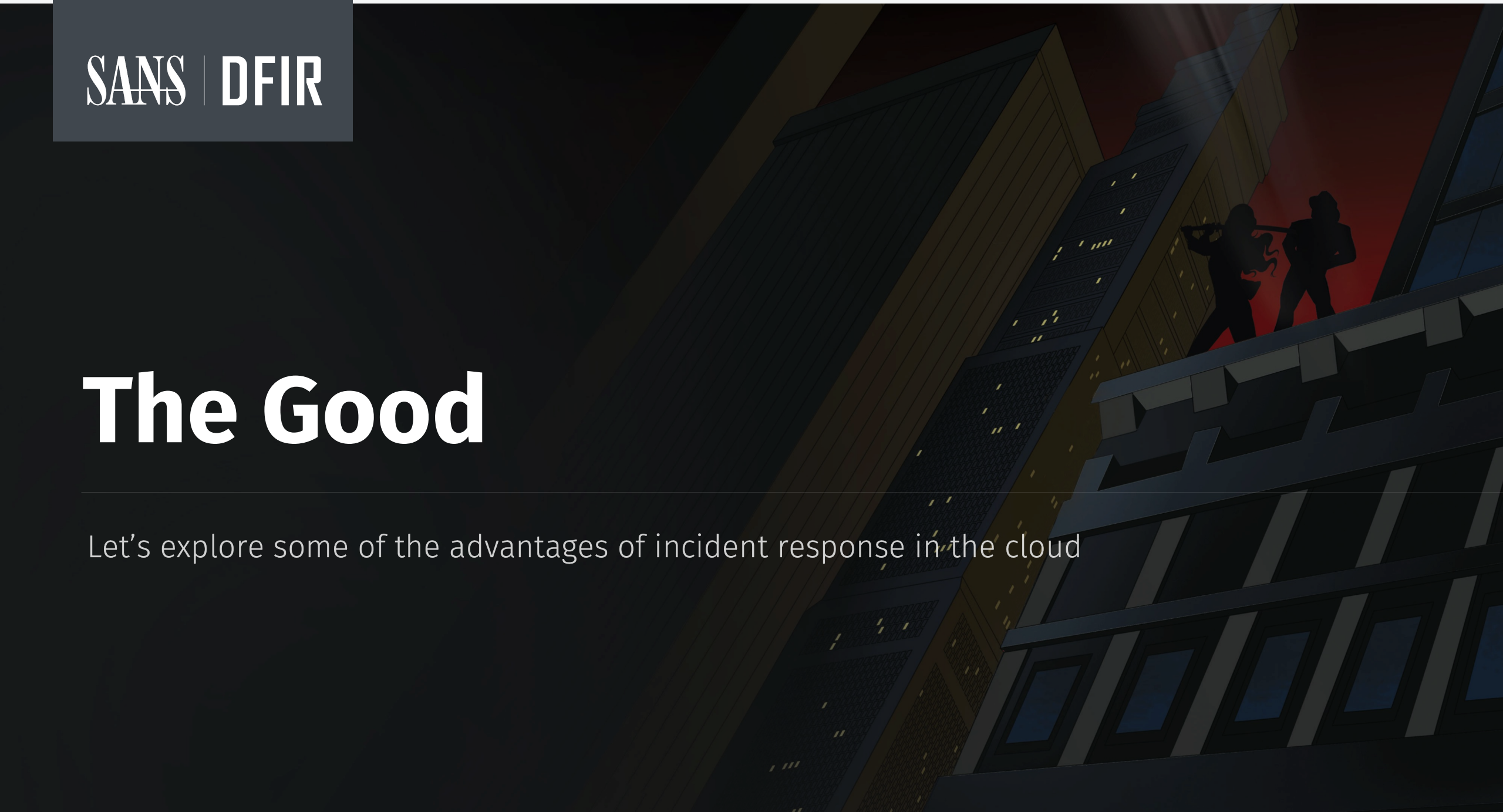
What happens after initial access?

Resultant actions after compromise	Percentage
Conduct cryptocurrency mining	86%
Conduct port scanning of other targets on the Internet	10%
Launch attacks against other targets on the Internet	8%
Host malware	6%
Host unauthorized content on the Internet	4%
Launch DDoS bot	2%
Send spam	2%

What will you learn today?

1. **The Good**
   Let's explore some of the advantages of incident response in the cloud
2. **The Bad**
   Although the sun might be shining in the cloud you might encounter some heavy weather
3. **The Ugly**
   Let's explore some real-life cloud incidents
4. **Takeaways**
   What can you do today to be prepared!
5. **Resources**
   Some helpful tools to increase your cloud incident response capabilities
6. **Q&A**

SANS | DFIR



The Good

Let’s explore some of the advantages of incident response in the cloud

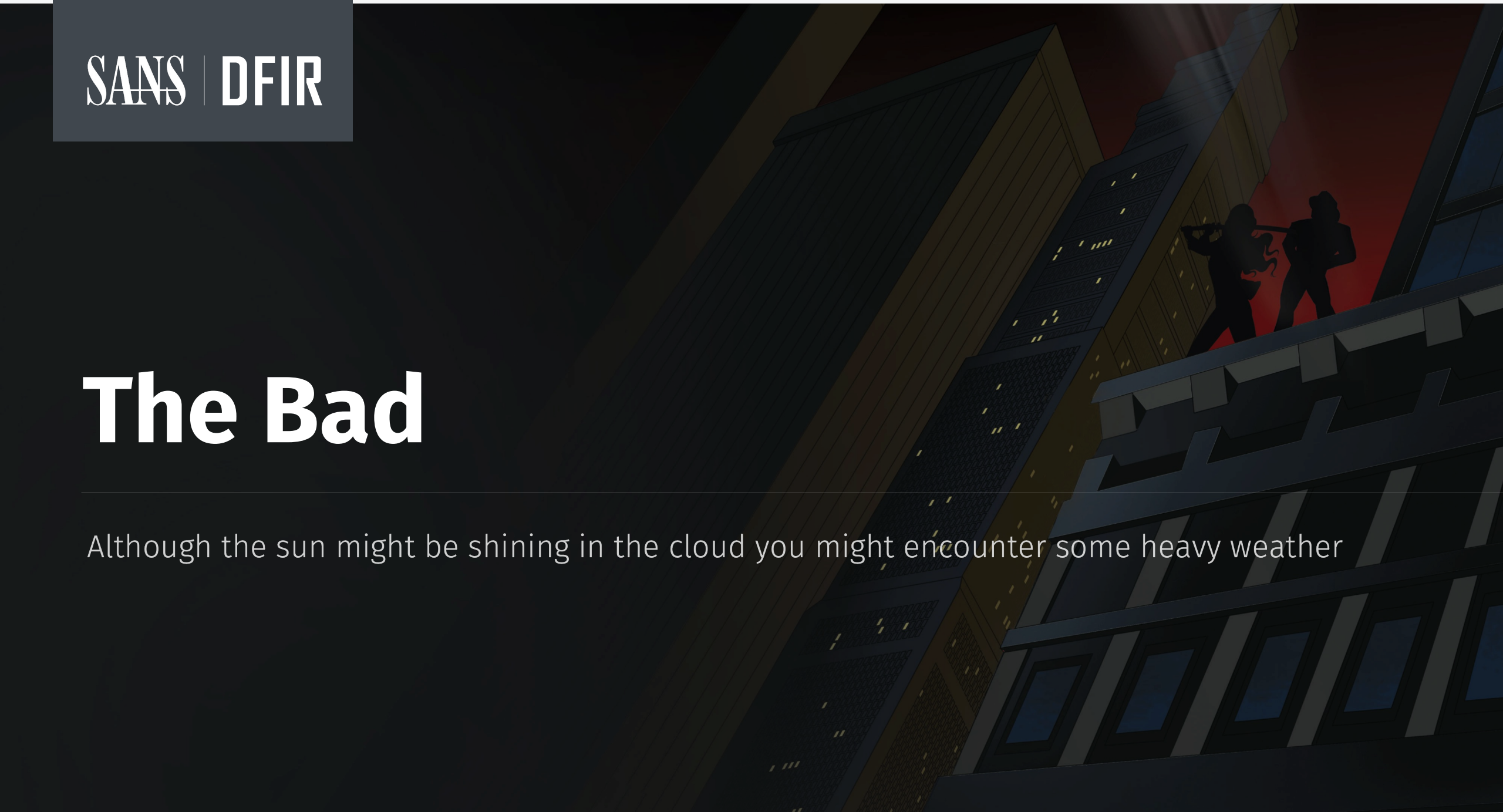
What do we like

- **Centralized logging available in all cloud platforms**
  - All cloud platforms have default platform logging enabled and available

Microsoft 365/Azure	AWS	Google Cloud
Azure AD Sign-in logs/Audit logs	CloudTrail	Cloud Audit Logs
Retention: 7-30 days	Retention: 90 days	Retention: 400 days

- **Premium logging can be enabled on the go**
  - NetFlow logging (e.g. active beaconing activity)
  - Data access logging (e.g. who is accessing my data?)
- **Good remediation and recovery options available**
  - Easily create a segmented network with auditing enabled
  - Setup a new subscription/account/project in the same Organization to move resources
  - Rotating credentials and keys can be done with the click of a button

SANS | DFIR



The Bad

Although the sun might be shining in the cloud you might encounter some heavy weather

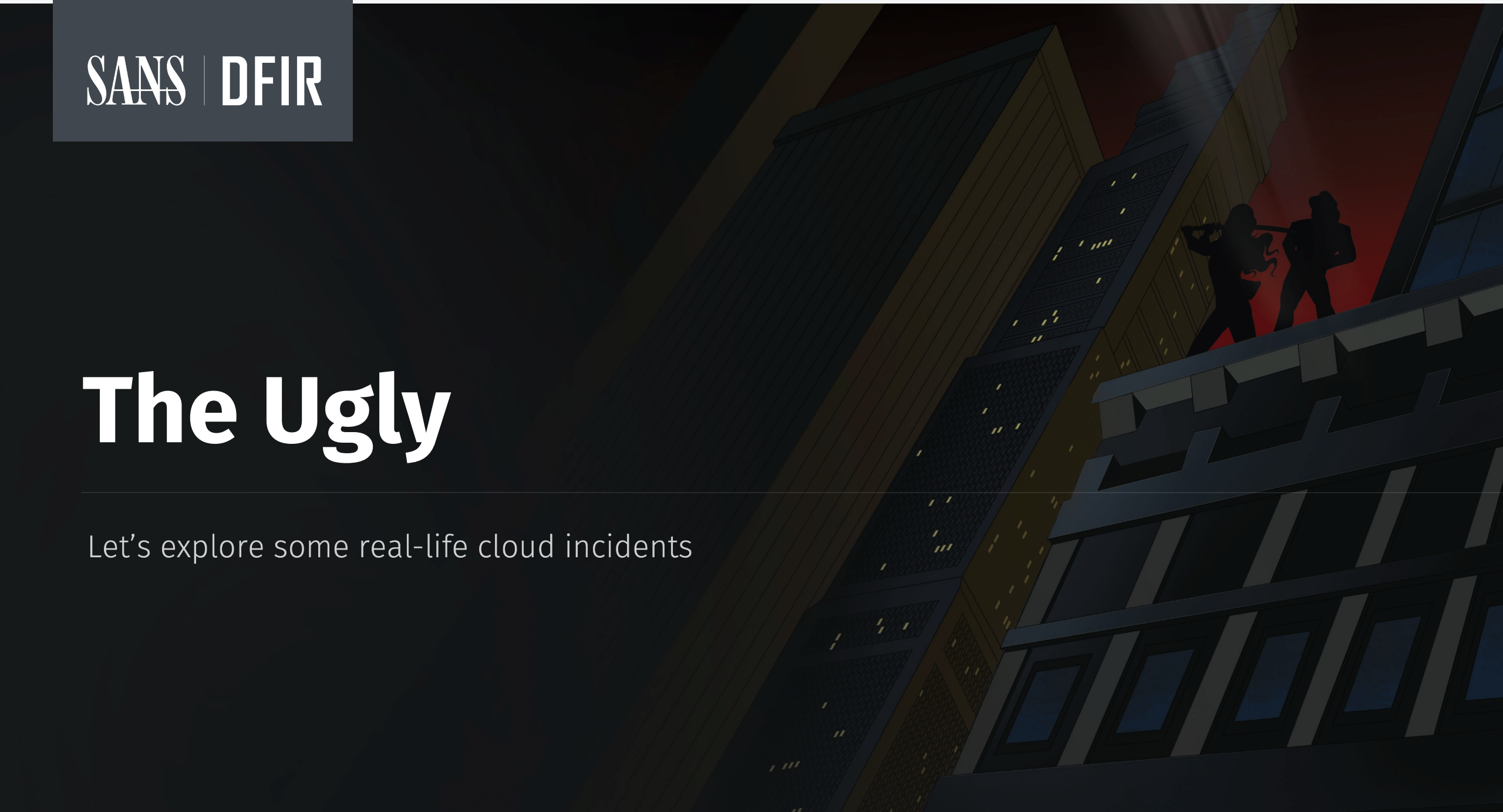
Challenges with the cloud

- **Centralized environment may not be available**
  - Everyone with a credit card can setup their own environment in the cloud
- **Licensing**
  - You may need additional licenses to get all the relevant logging (e.g. Microsoft E5)
- **The 'Security lag' problem**
  - New technology and features advance faster than security measures (e.g. Kubernetes)
- **Costs**
  - Each investigation will cost you money
  - Exporting data out of the cloud or sometimes between regions incurs costs
- **Multi-cloud approach**
  - Having knowledge of one cloud is already a challenge, imagine having 3 separate cloud platforms to maintain and secure

SANS | DFIR

The Ugly

Let’s explore some real-life cloud incidents



Case study 1 – Crypto mining

The Case

The threat actor used leaked credentials to access an environment and spin up Microsoft VM's at nighttime. Damage in Microsoft bills $26k, the gains of the threat actor.....

What did we do?

- Forensic investigation into the root cause of the incident through acquisition and analysis of cloud platform logging
- Remediate and Recover using a new resource group and washing and moving 'clean' systems to the new resource group.
- Working with Microsoft to prove that this was indeed an attack

What can you do?

- Setup spending quotas/limits to avoid surprises
- Prevent the creation of 'expensive' machines using policies in your Organization/Subscription

Case study 2 – Spearphishing through Google Workspace

The Case

Threat actor was able to gain access to a Google Workspace account. Used the internal search functions to identify interesting emails and targets. Downloaded address book for further phishing/spamming.

What did we do?

- Acquired Google Workspace logging
- Identified address book downloads which is logged as part of administrative actions
- Analysis of logging to identify what data was accessed by the threat actor to support with notification to authorities and victims

What can you do?

- Enable MFA ☺
- Enable MFA everywhere..

Case study 3 – Ransomware

The Case

Ransomware actors follow their targets and since companies are moving to the cloud, ransomware is coming to the cloud. In this example a companies cloud buckets got deleted and a ransomware note was left.

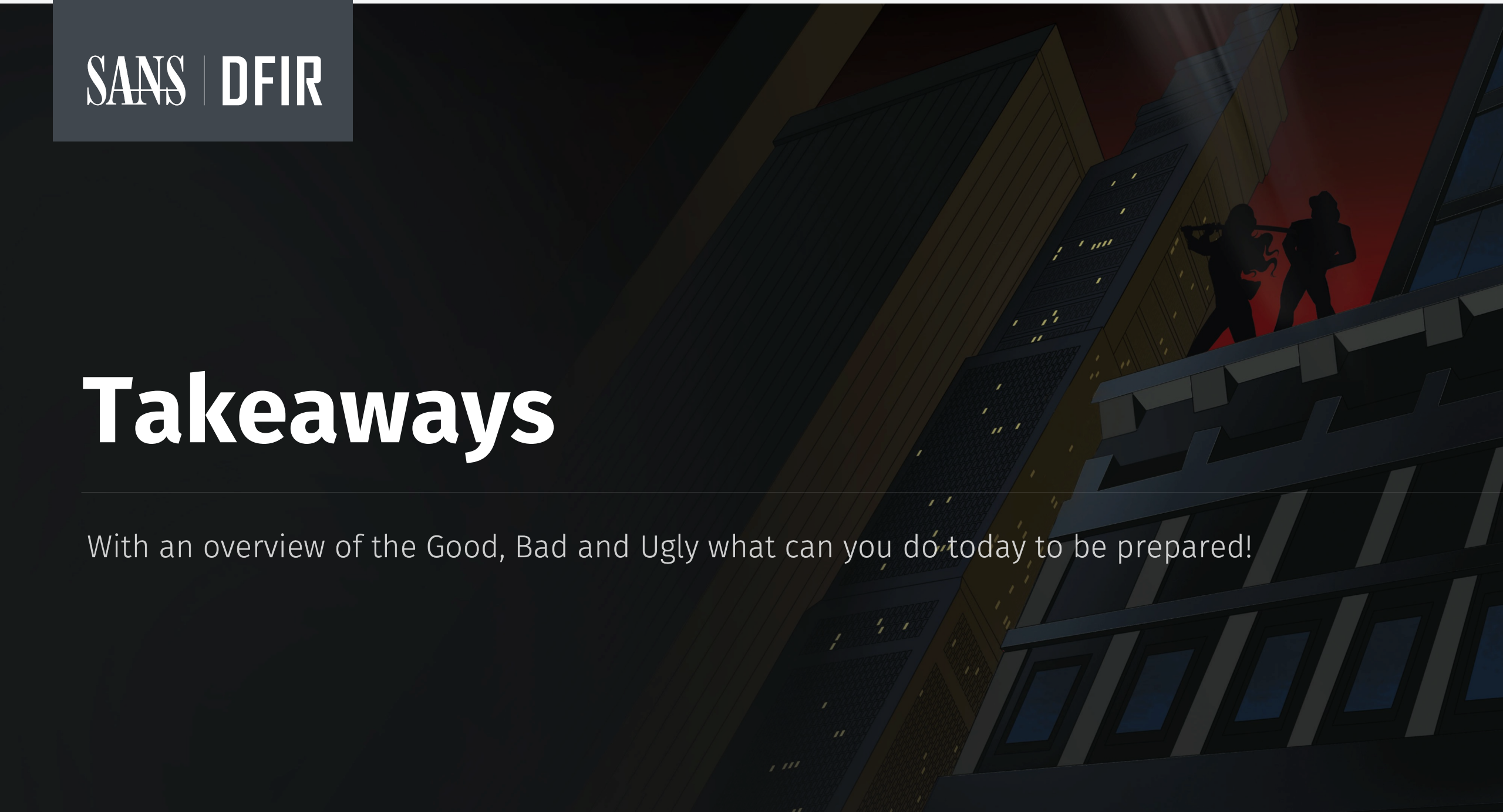
What did we do?

- Identified initial access through analysis of CloudTrail (guess what it was?)
- Confirmed data exfiltration through AWS billing method
- Rotate access keys and monitor CloudTrail logging

What can you do?

- Don’t use access keys, but rather use IAM roles for programmatic access
- Enable bucket versioning with MFA delete
- Use immutable backup (AWS backup)

SANS | DFIR



Takeaways

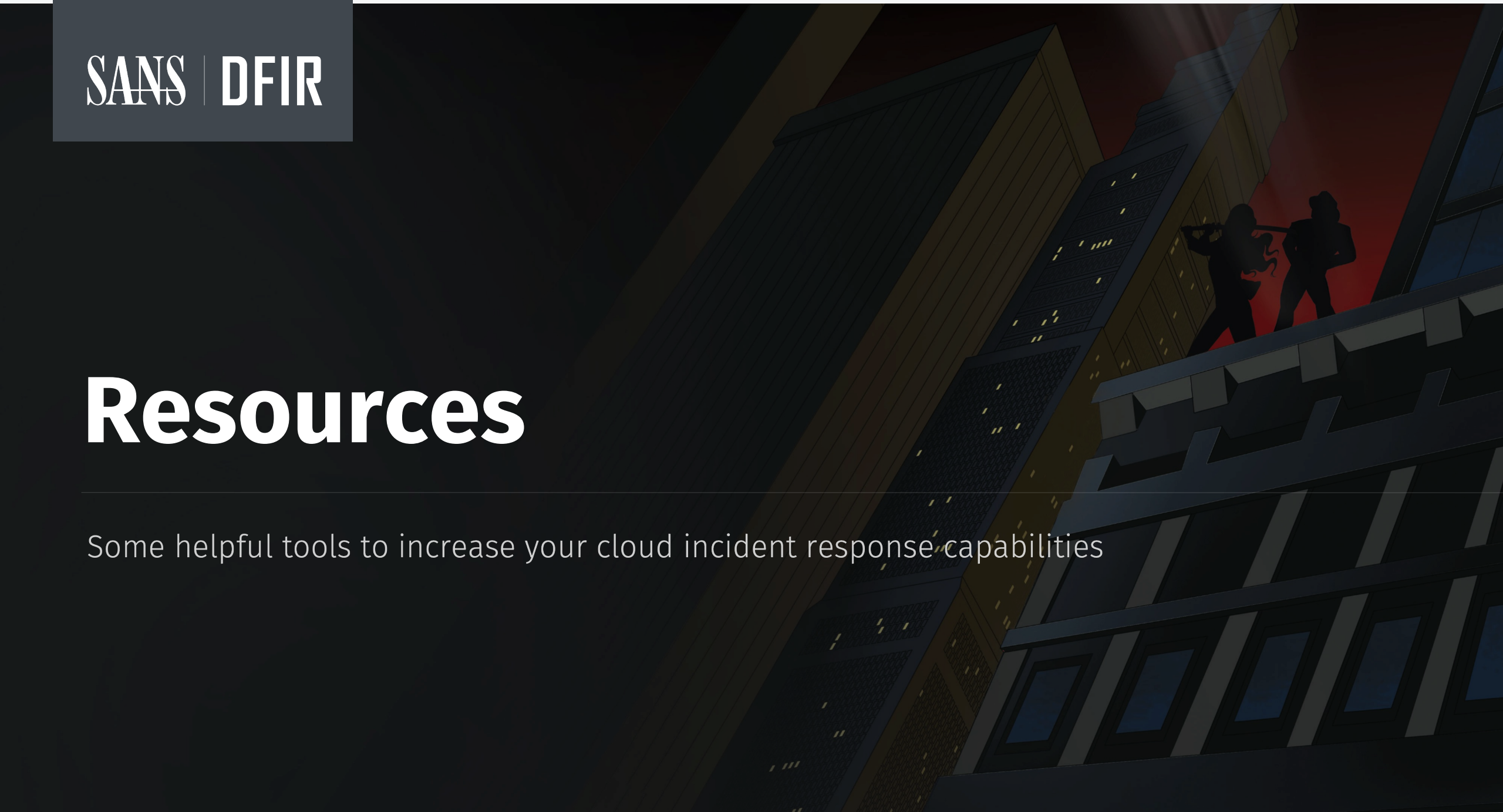
With an overview of the Good, Bad and Ugly what can you do today to be prepared!

What can you do?

- **Incident Preparation**
  - Update playbooks to include cloud resources
    - Microsoft has free IR playbooks
  - Understand & Review the available artefacts
    - Know your retention
    - Know what premium logging is available and enabled
  - Protect your crown jewels with cloud options
    - Just-in time access for administrative users
    - Advanced auditing options
  - Simulate an incident to test your response
    - AWS has five unique IR workshops that simulate an incident and allows you to investigate the logs
    - Use something like Stratus to simulate attack techniques

- **Incident Response**
  - Investigate and understand extent of the breach
    - Identify credentials used by the threat actor (e.g. access keys, user accounts, malicious applications)
    - Assess if any malicious activity with any of the credentials, keep repeating until you're certain of the extent
    - Taking shortcuts will alert the threat actor and prevent recovery
  - Leverage unique cloud capabilities
    - Isolation of resources
    - Enable premium logging for the course of the incident (at least)
    - Where possible automate response activity (e.g. automated snapshot creations)
    - Unlimited storage over the whole world for evidence storage

SANS | DFIR



Resources

Some helpful tools to increase your cloud incident response capabilities

What do we use to make cloud incident response easier?

Acquisition

- Microsoft-365-Extractor
  - https://github.com/invictus-ir/Microsoft-365-Extractor-Suite
- Invictus-AWS
  - https://github.com/invictus-ir/Invictus-AWS
- ALFA
  - https://github.com/invictus-ir/ALFA

Analysis

- Blue Team App for Office 365 and Azure
  - https://github.com/invictus-ir/Blue-team-app-Office-365-and-Azure
- SOF-ELK
  - https://github.com/philhagen/sof-elk


Q&A

SANS | DFIR

Korstiaan Stam

@KorstiaanS

korstiaan@invictus-ir.com