Fugue

A Live Simulation of Cloud Misconfiguration Attacks

Josh Stella, Co-Founder & CTO, Fugue

Agenda

1. Overview of cloud misconfiguration risk
2. Live Demo: Cloud misconfiguration exploits in action
3. Actionable steps to secure your customers' cloud environments
4. Q&A

Fugue

Cloud misconfiguration is a major security risk

CONCERNED THEY'VE BEEN HACKED AND DON'T KNOW IT	CONCERNED THEY'RE VULNERABLE TO A CLOUD BREACH	MISCONFIGURATION RISK WILL INCREASE OR STAY THE SAME THIS YEAR
84%	92%	76%

"I'm seeing a lot of cloud configuration errors in the real world—and it's scaring the hell out of me."

– David Linthicum, InfoWorld

Fugue

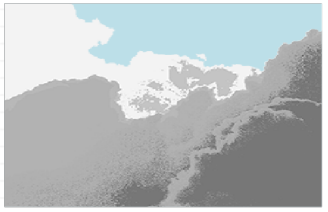
Cloud misconfiguration is a major security risk

66%
IAM

59%
SECURITY GROUP RULES

51%
OBJECT STORAGE ACCESS POLICIES

42%
ENCRYPTION IN TRANSIT DISABLED



Fugue

Cloud misconfiguration is often overlooked

Many dangerous cloud misconfigurations are:

- not recognized as misconfigurations by security teams
- not considered policy violations by compliance frameworks
- exceedingly common in enterprise cloud environments

"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes."

– Neil MacDonald, Gartner

Fugue

How exploit strategy has evolved in the cloud era

Before Cloud

1. Identify your targets
2. Search for vulnerabilities

Cloud

1. Identify vulnerabilities
2. Prioritize your targets

Skilled or well-funded hacker groups are employing automation to discover and exploit misconfigured cloud assets within hours of their deployment."

– John Breeden II, CSO Online

Fugue

Security strategy must evolve too

Before Cloud

1. Network and security teams deliver infrastructure to app teams
2. Network analysis and threat detection tools identify intrusions; human-guided response

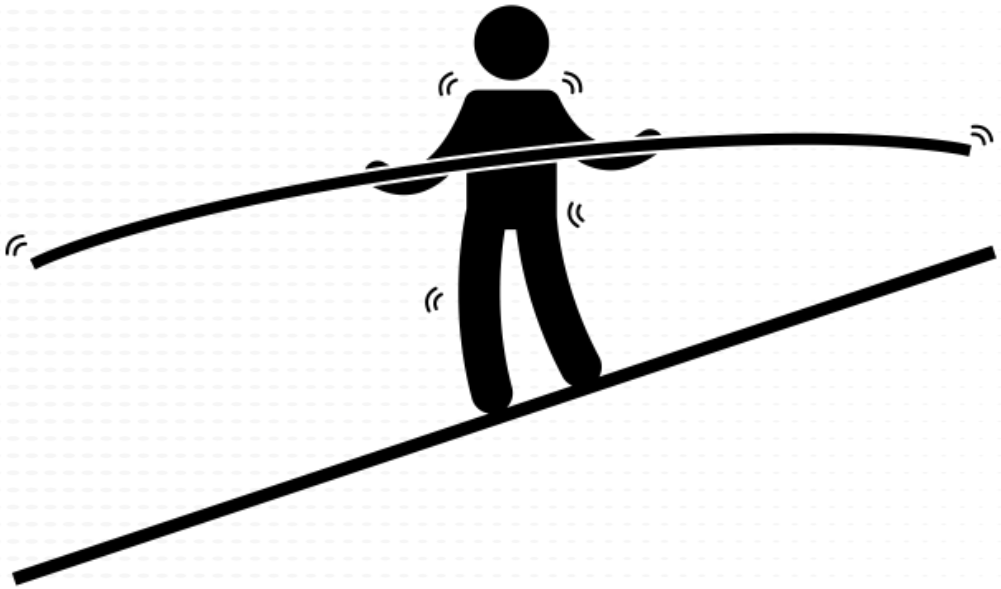
Cloud

1. Developers create their own infrastructure and are empowered to secure it
2. Policy as code validation tools prevent misconfiguration; automated detection and remediation eliminates it

Cloud security is a software engineering problem, not a security analysis problem.

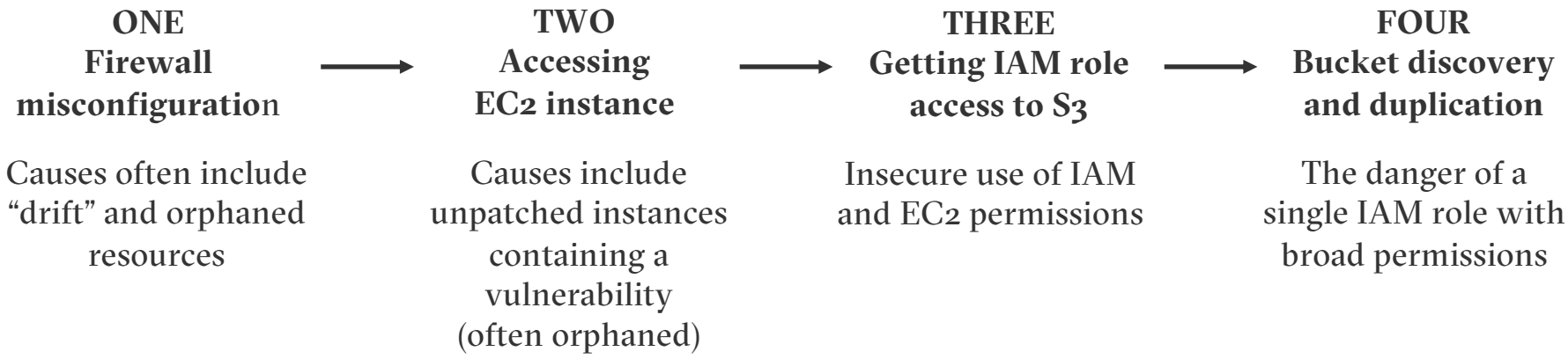
Fugue

A demonstration of a cloud misconfiguration attack



Fugue

This misconfiguration attack in review



Fugue

Key takeaways and recommendations

1: Monitor all access point configurations

- Continuously monitor Security Groups for misconfiguration (e.g. access from 0.0.0.0/0)

2: Apply Principle of Least Permission

- Ruthlessly limit IAM roles to business requirements for the app
- Use different end points for read and write operations
- Eliminate S3 bucket listing in production environments

3: Don't allow EC2 instances to have IAM roles that allow attaching or replacing role policies

Fugue

Key takeaways and recommendations

4. Ruthlessly clean up unused cloud resources (especially EC2 instances and S3 buckets)

- "Orphaned" resources are common and can contain misconfigurations and unpatched OS or application vulnerabilities

5. Include cloud misconfiguration in penetration testing

- Use outside pen testers who understand cloud misconfiguration and how to exploit it.

6. Use automated remediation for security-critical cloud resources

- Focus first on VPCs, S3 buckets, Security Groups, EC2, and IAM)

7. Use an open source policy as code framework for validating compliance

- Open Policy Agent and Rego policy language

Fugue

Questions?

Q&A

www.fugue.co
josh@fugue.co

Fugue