

PROWLER

Securing the Cloud
with Open Source

\$ aws sts get-caller-identity



Cloud Security Engineer at Prowler

 /andoniaf

 andoniaf

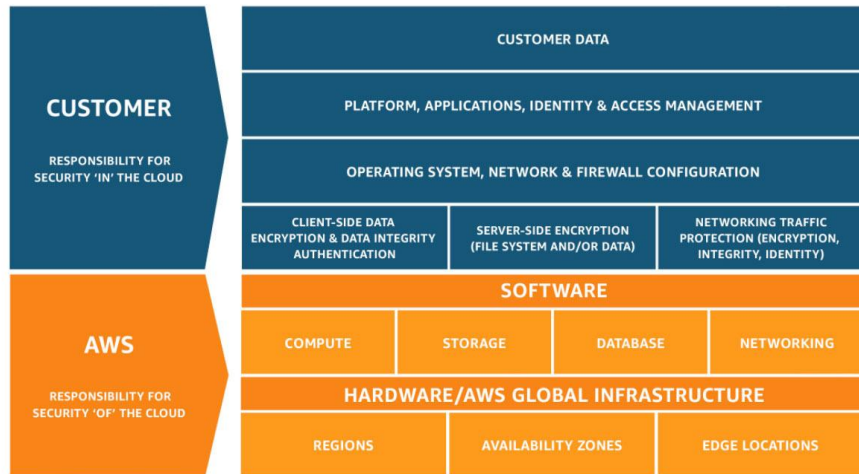


Agenda

- 01 Incidents review + Shared responsibility model
- 02 What is Prowler
- 03 Demo
- 04 How to contribute
- 05 Q&A

There is **no cloud**, it's just some else's computer

- What does that means for us?
 - Security “**of**” the cloud
 - Security “**in**” the cloud



From <https://aws.amazon.com/es/compliance/shared-responsibility-model/>

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	●	●	●	●	●
Client and end-point protection	●	●	●	●	●
Identity and access management	●	●	●	●	●
Application-level controls	●	●	●	●	●
Network controls	●	●	●	●	●
Host infrastructure	●	●	●	●	●
Physical security	●	●	●	●	●

● Cloud Customer ● Cloud Provider

From <https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know>

Top 5 Cloud Security Threats & Common Attacks

1. Misconfigurations

- Public exposed resources, weak IAM policies, unrestricted security groups

2. IAM vulnerabilities

- Credential theft, privilege escalation, brute force attacks

3. Insecure APIs and Interfaces

- API key leaks, MITM attacks, rate-limiting bypass

4. Data Breaches and Exfiltration

- Unencrypted data exposure, insider threats, SQL injection attacks.

5. Inadequate Monitoring and Logging

- Log tampering, cryptojacking, lack of real-time alerts

Act on cloud predictions

Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.

Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks.

Through 2025, 99% of cloud security failures will be the customer's fault.

<https://www.gartner.com/smarterwithgartner/is-the-cloud-secure>

Misconfiguration

Prevalence: widespread; Attacker Sophistication: low

While CSPs often provide tools to help manage cloud configuration, misconfiguration of cloud resources remains the most prevalent cloud vulnerability and can be exploited to access cloud data and services. Often arising from cloud service policy¹ mistakes or misunderstanding shared responsibility, misconfiguration has an impact that varies from denial of service susceptibility to account compromise. The rapid pace of CSP innovation creates new functionality but also adds complexity to securely configuring an organization's cloud resources.

Examples of abused misconfigurations:

- In May 2017, a large defense contractor exposed sensitive NGA data and authentication credentials in publicly accessible cloud storage [1];
- In September 2017, a security researcher discovered CENTCOM data accessible to all public cloud users [2];
- In September 2019, a research team discovered sensitive travel details of DoD personnel exposed in a publicly accessible Elasticsearch database [3].



Real World Examples: Capital One



Name	Date	Root Cause	Escalation Vector(s)	Impact
Capital One	2019, April	"Misconfigured WAF" that allowed for a SSRF attack	Over-privileged EC2 Role	100 million credit applications

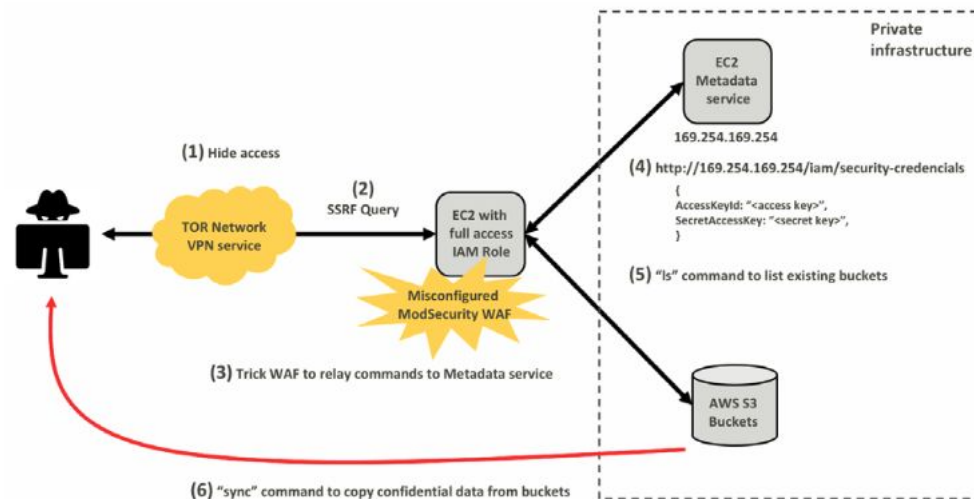
<https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach>
<https://www.capitalone.com/digital/facts2019/>

What Happened?

- An outside individual gained access through a **misconfigured WAF** and a **SSRF** vulnerability.
- Then used the **instance IAM role** to **steal** data from Capital One S3 buckets.
- **100 million+ customer records** were exposed, including Social Security numbers and credit applications.

Lesson:

- **Least privilege IAM policies** are critical, don't allow unnecessary permissions.
- Always **monitor** and **audit** IAM roles and access logs.



Real World Examples: Tesla



Name	Date	Root Cause	Escalation Vector(s)	Impact
Tesla	2018, February	Globally exposed Kubernetes console, Pod with AWS credentials	N/A	Cryptojacking

<https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/>

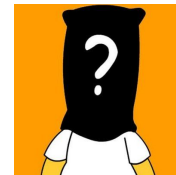
What Happened?

- Attackers found Tesla's **Kubernetes dashboard exposed to the internet without authentication**.
- They deployed **cryptocurrency miners** inside Tesla's cloud environment, stealing compute resources.

Lesson:

- **Never expose internal dashboards/APIs to the public.**
- Use IAM roles, **MFA**, and firewalls to restrict access.
- **Monitor cloud resource usage**— unexpected spikes may indicate hijacking.

Real World Examples: ??



Date	Root Cause	Escalation Vector(s)	Impact
2023, April	SSRF via known CVE and IMDSv1	Backdoored IAM role	Cryptojacking, outbound DDOS

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/unit42-cloud-threat-report-volume7.pdf

What Happened?

- Internal web server was accidentally made public due to a **misconfigured security group** setting during a migration process.
- Server was vulnerable to Server Side Request Forgery (**SSRF**) allowing attackers to send HTTP requests to hosts behind the firewall.
- Usage of outdated **IMDSv1** allowed the threat actor to exfiltrate temporary credentials associated with the VM instance.
- **Cryptomining** and **DDoS attacks** using their infrastructure.

Lesson:

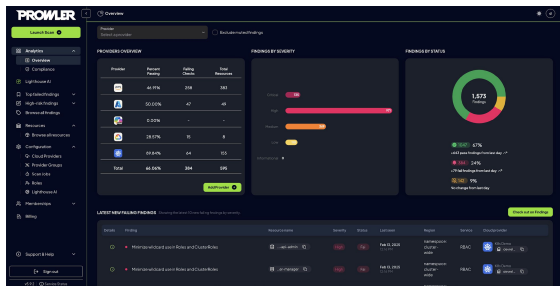
- Same as previous slides. 😅



What's Prowler?

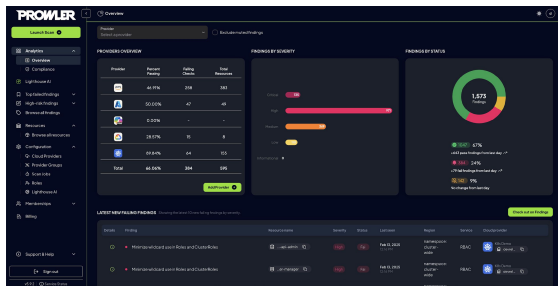
What's Prowler ?

Prowler es la plataforma de **Seguridad** en la Nube Abierta para automatizar la seguridad y el cumplimiento en cualquier entorno cloud (**AWS, Azure, GCP, K8s, M365, GitHub, OCI, Infrastructure as Code, LLMs y más**).



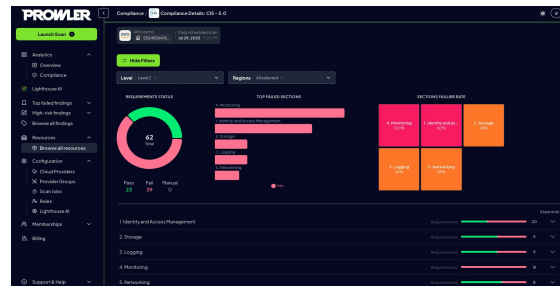
Security Monitoring

Address security risks before they become incidents



IaC monitoring

Static code analysis for Infrastructure as Code (Terraform, Cloudformation, Kubernetes YAML)



Compliance

Audit & Compliance Assessments (including CIS, SOC2, HIPAA, PCI, CISA, NIST, ISO27001, etc.)

What's Prowler ?

Prowler **Project**

- Open source + soporte de AWS, Azure, GCP, K8s, GitHub y más.
- Ofrece **monitorización continua**, evaluaciones y auditorías de seguridad, respuesta a incidentes, cumplimiento normativo, endurecimiento y preparación forense.
- Funciona tanto on-premises como en la nube.
- Incluye **CLI**, **SDK**, **API** y una interfaz gráfica (**UI**) para mayor versatilidad.

Prowler Cloud

- El Servicio Gestionado de Prowler se encarga del alojamiento de Prowler con registro de clientes.
- Admite pagos a través de Marketplaces y Stripe.
- Monitoreo proactivo 24x7 por ProwlerPro, Inc.
- Incluye actualizaciones automáticas, parches y nuevas versiones, con copias de seguridad y configuración de alta disponibilidad.
- cloud.prowler.com

Prowler Hub



- Base de conocimiento sobre todos los proveedores, checks, frameworks de cumplimiento...
- Toda esta información está expuesta vía API y UI lo que permite integraciones con Prowler y Prowler Studio
- hub.prowler.com

Prowler **MCP**

- Crea, comparte y ejecuta chequeos de detección, remediaciones y marcos de cumplimiento utilizando nuestro SDK en línea y tecnología de IA.



Prowler breaths opensource

Prowler es la herramienta de seguridad en la nube de código abierto (ALv2) más utilizada del mundo.*

40M+
descargas

1M+
descargas/week

12K+
GitHub stars

300+
contributors


recomendado por
AWS Prescriptive Guidance

1000+
detections,
remediations, &
compliance frameworks



prowler-cloud / prowler

Qué se puede hacer con Prowler

Demo Time!

Demo failed?



How to **contribute** ?

Developer Guide

goto.prowler.com/devguide

Our Slack

goto.prowler.com/slack



prowler-cloud / prowler

Thanks!

Any question?



Deep dive **workshop!**



unicrons.cloud



andoniaf



andoniaf.unicrons.cloud