



Novel Bedrock Attack Techniques

Maya Parizer and Tal Peleg

Varonis Threat Labs

Troopers 26 Conference



MAYA PARIZER



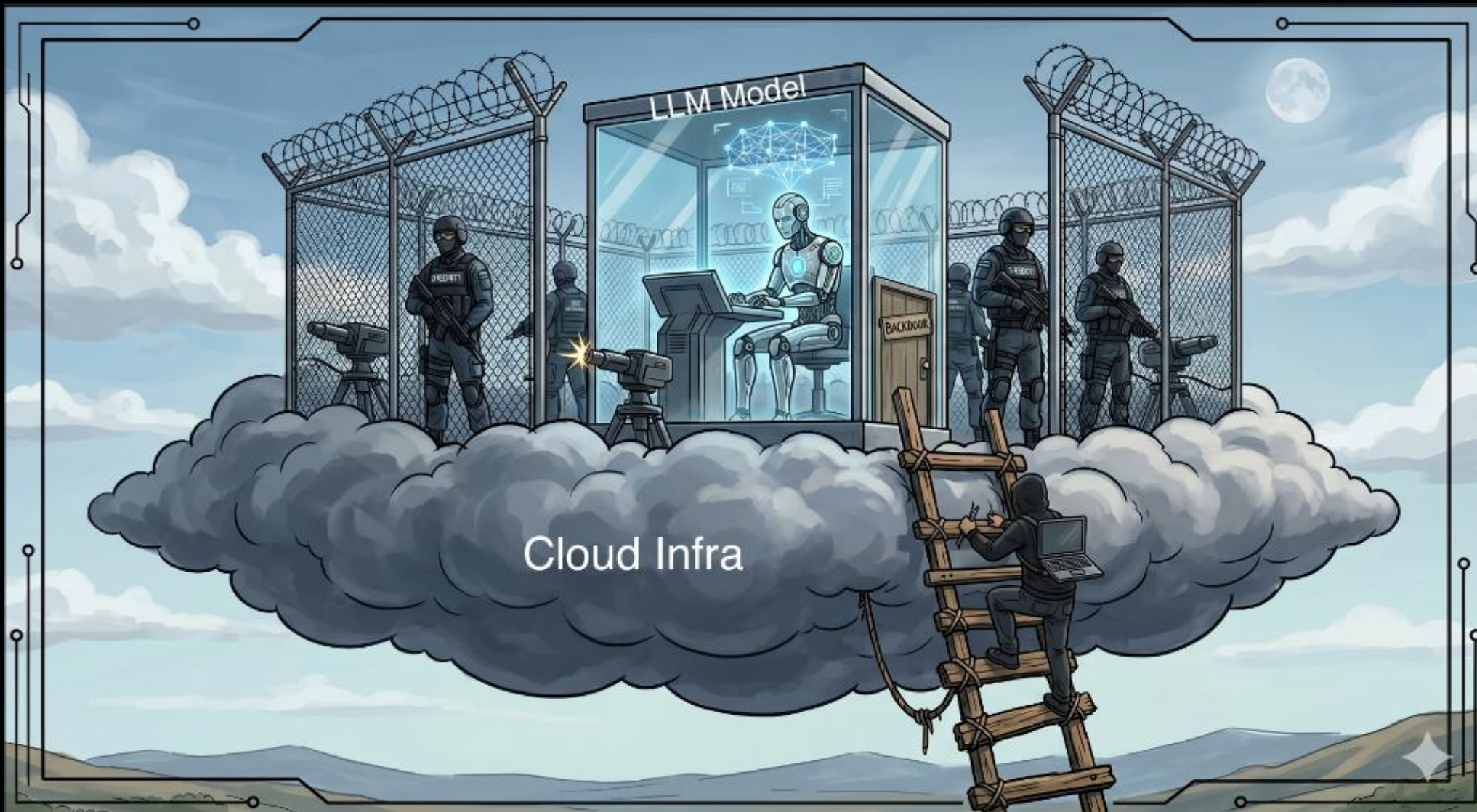
TAL PELEG

AI may be black magic; Bedrock isn't.
Be mindful of where data travels, who sees it, and
always remember:
Less is more.

Maya Parizer

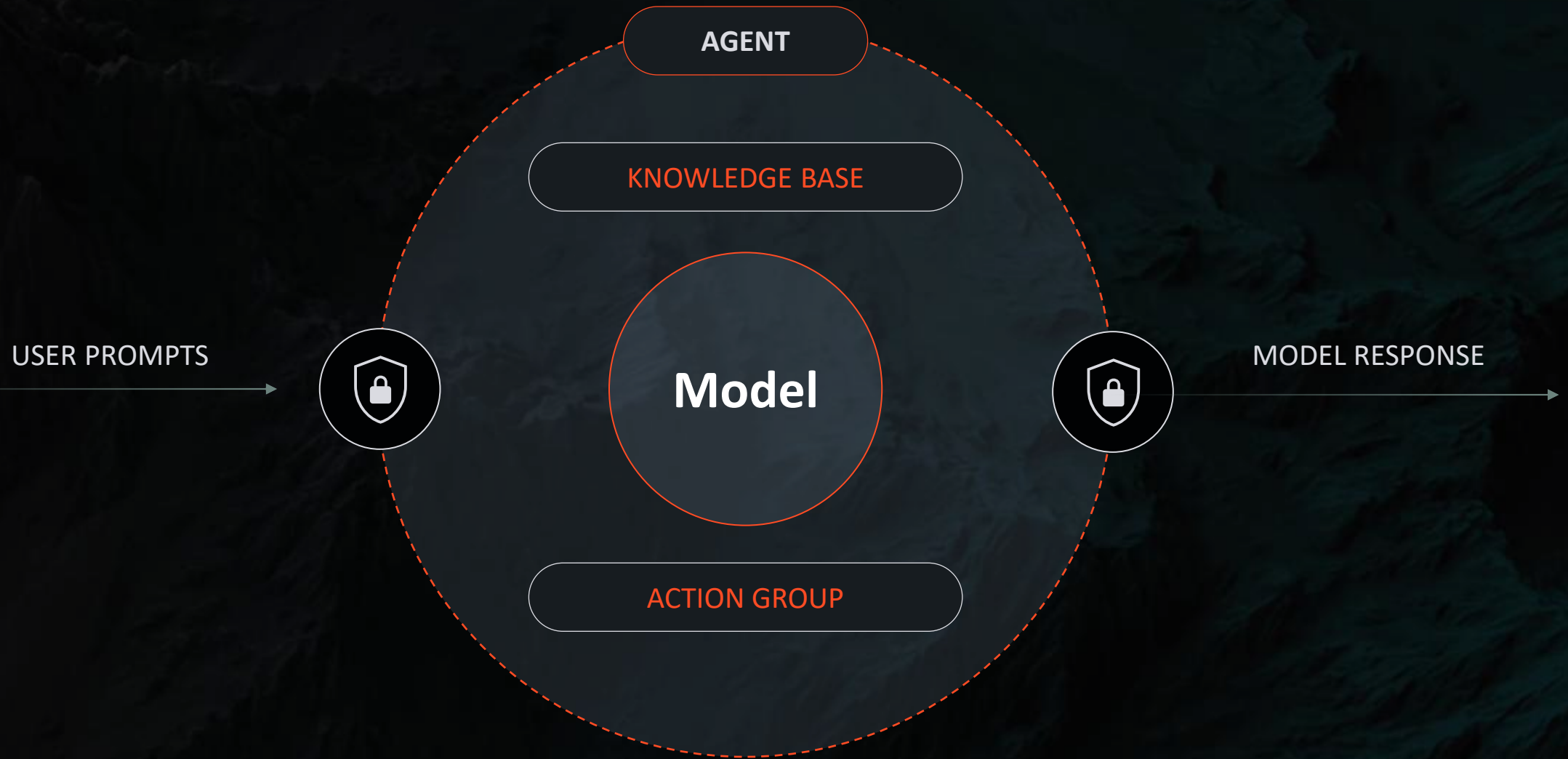
AGENDA

- 01 Bedrock Introduction
- 02 Abusing Guardrails
- 03 Leaking Knowledge Base Secrets
- 04 AgentCore Privilege Escalation
- 05 Conclusions

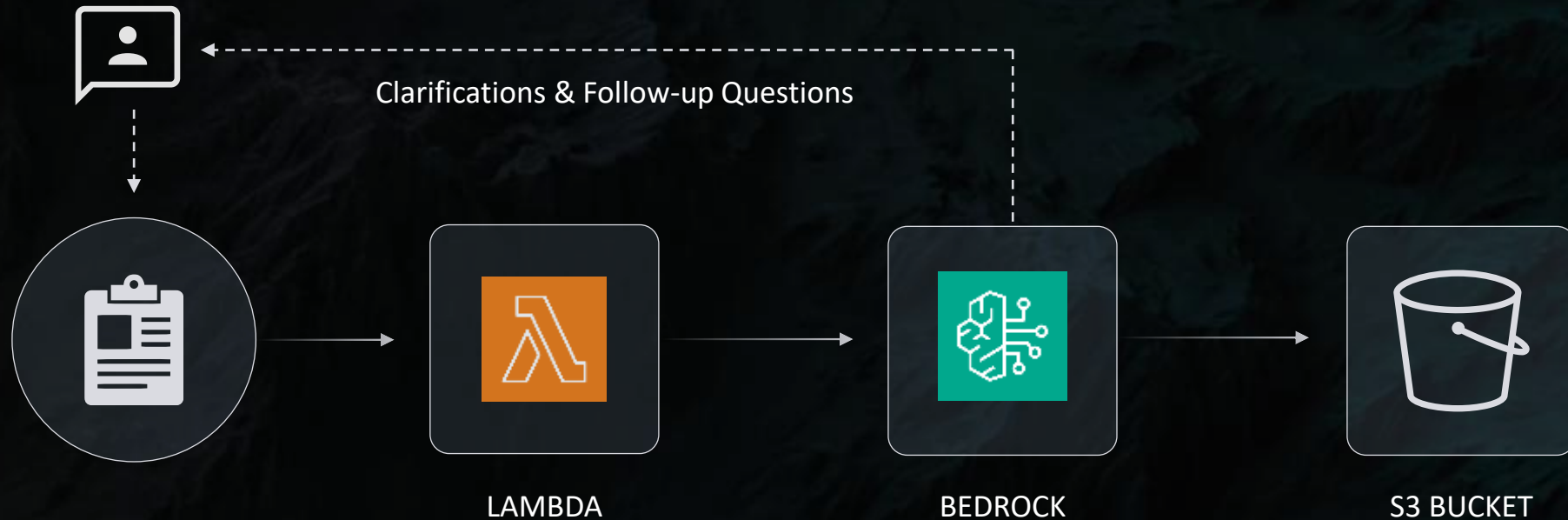




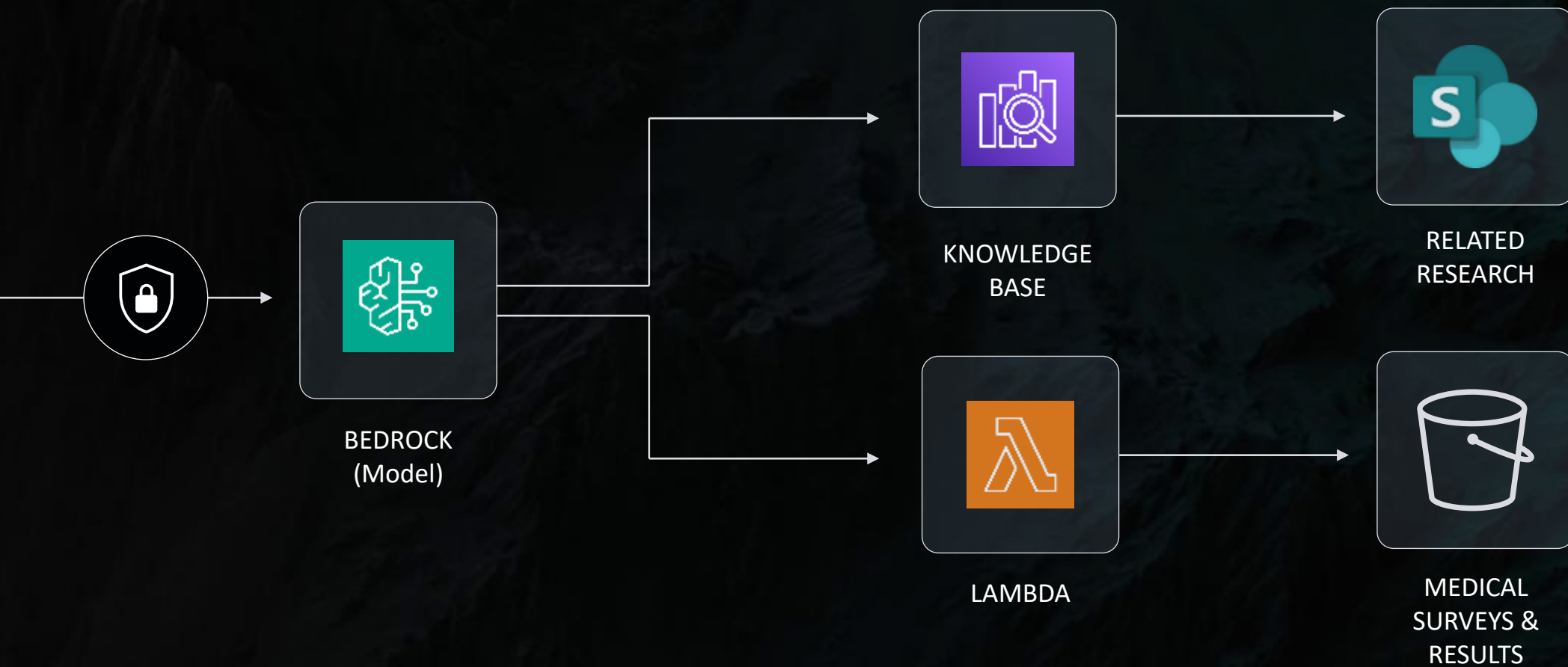
Amazon Bedrock



What is Amazon Bedrock?



Bedrock knowledge bases & action groups



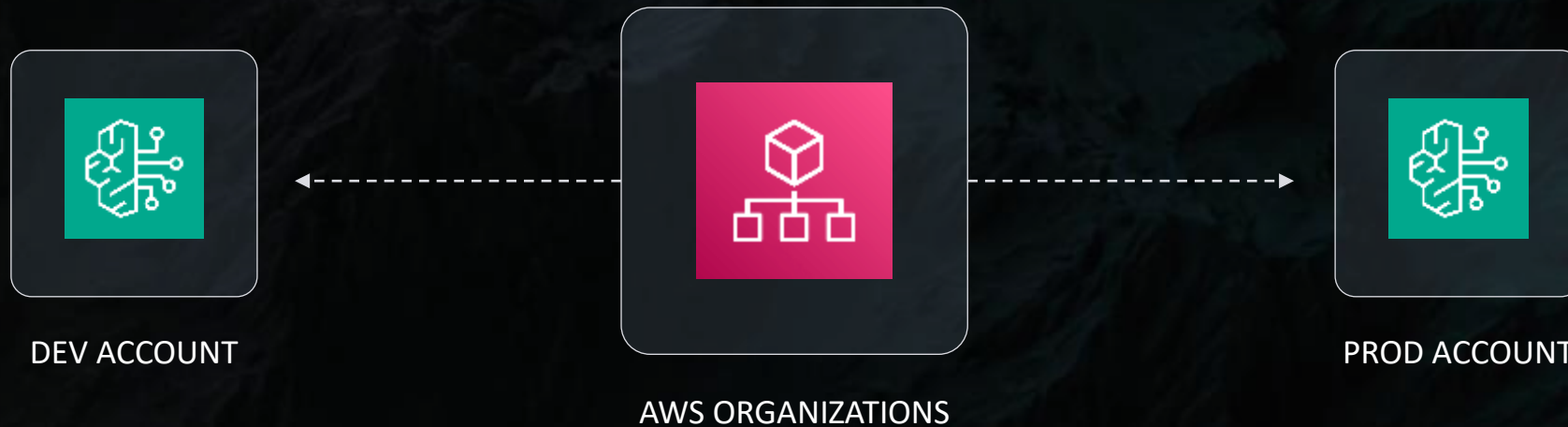


How is Bedrock Being Attacked?

INSECURE GUARDRAIL POLICIES

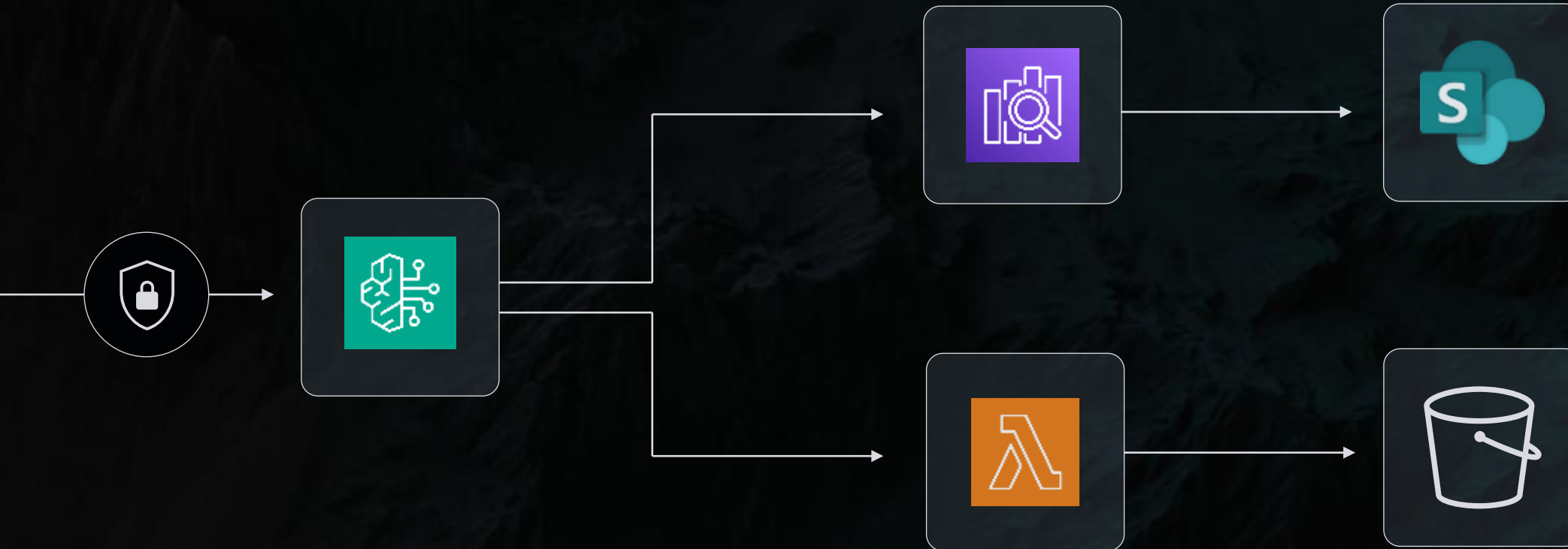
CASE STUDY

Insecure guardrail policies



CASE STUDY

Insecure guardrail policies





CASE STUDY

Insecure guardrail policies: Dev Account

OVERPERMISSIVE

```
"Statement":  
[  
  {  
    "Sid": "Statement1",  
    "Effect": "Allow",  
    "Action":  
    [  
      "bedrock:*"  
    ],  
    "Resource": "*"  
  }  
]
```

CASE STUDY

Insecure guardrail policies: Production Account

OVERPERMISSIVE

```
"Statement":
[
  {
    "Sid": "Statement1",
    "Effect": "Deny",
    "Action":
    [
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream"
    ],
    "Resource": "*",
    "Condition":
    {
      "Null":
      {
        "bedrock:GuardrailIdentifier": "true"
      }
    }
  }
]
```

CASE STUDY

Insecure guardrail policies: Dev Account

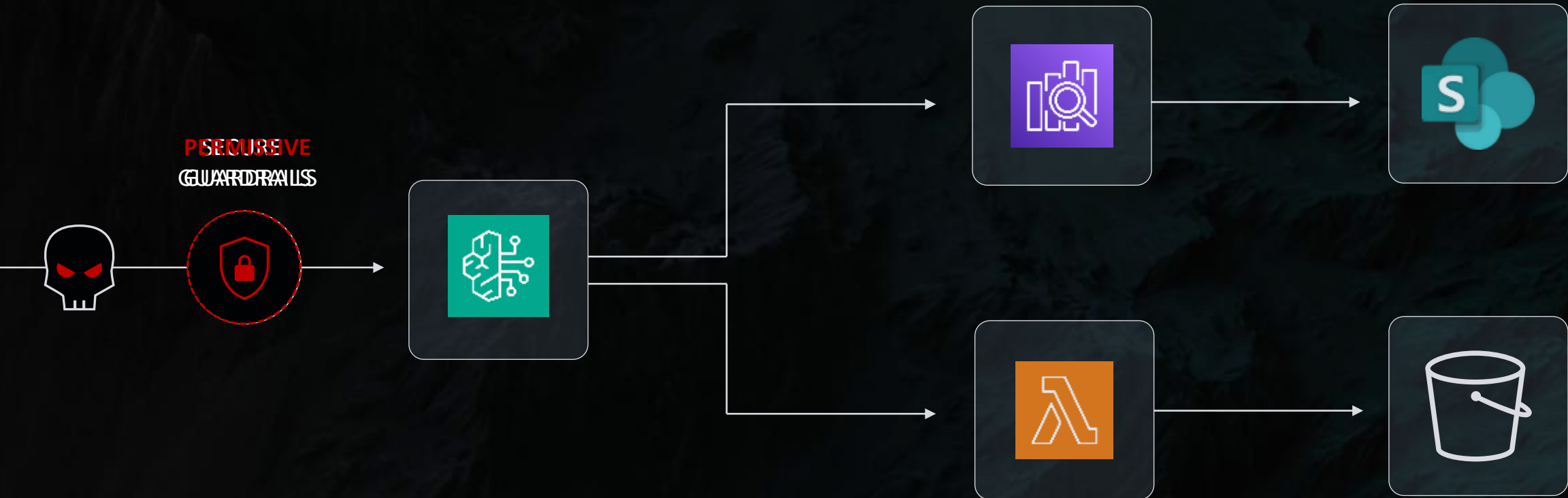


**Guardrails can be added
from **all** accounts
in your organization!**



CASE STUDY

Insecure guardrail policies





How is Bedrock Being Attacked?

LATERAL MOVEMENT USING
KNOWLEDGE BASE SECRETS

CASE STUDY

Supply chain attacks & lateral movement

01

Want to use **LiteLLM** as a proxy to the Bedrock model

02

LiteLLM provides unified **OpenAI APIs** and cost tracking dashboards

03

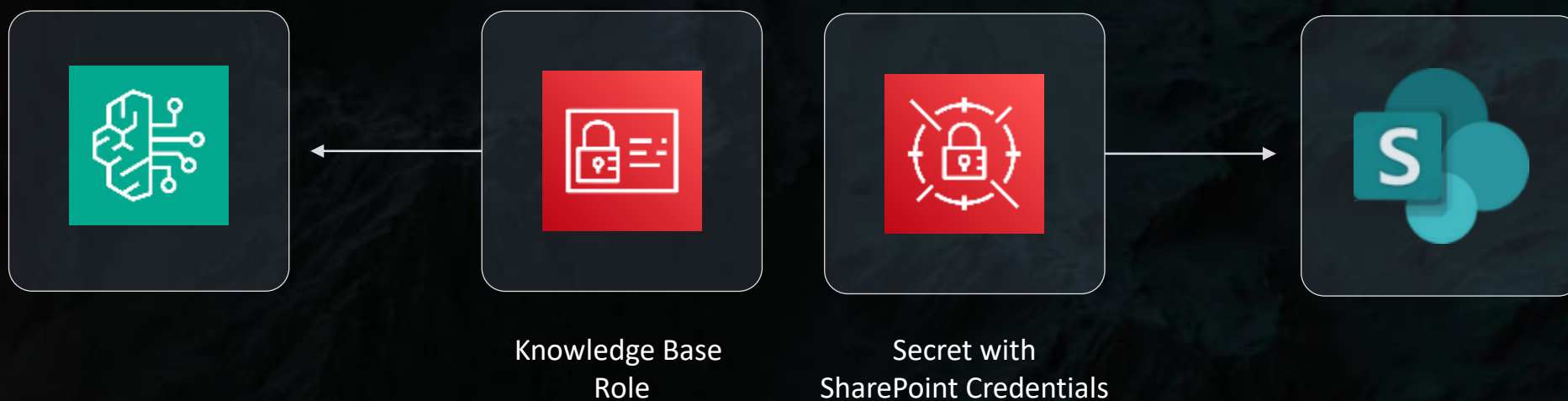
The agent runs on **Kubernetes (EKS)**

04

Runs a RAG task to query relevant **SharePoint** documents



How knowledge bases are configured



Overprivileged IAM policies in supporting services

SCENARIO 1

Overprivileged service account

Overprivileged EKS node role

Overprivileged role exists in AWS account

SCENARIO 2

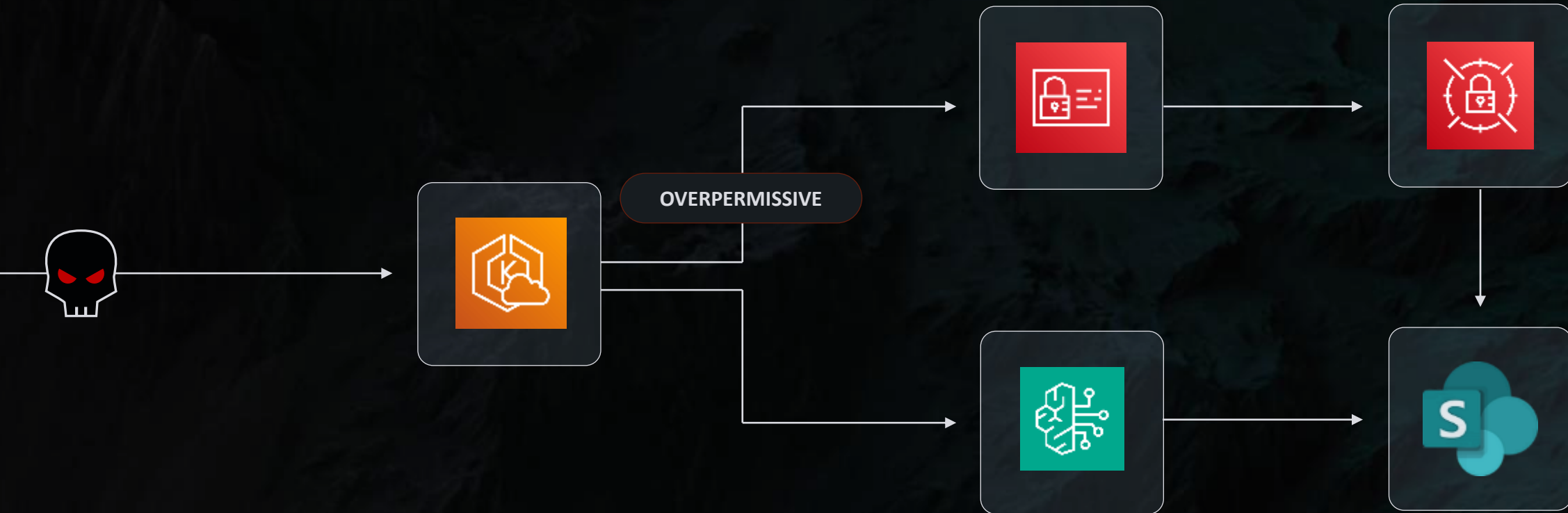
Overprivileged service account role

Overprivileged Entra application

**Protect Bedrock secrets using
least privileges & explicit denies**

CASE STUDY

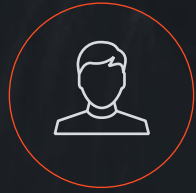
Supply chain attacks & lateral movement





Bedrock AgentCore

Introduction to AgentCore



Identity

Provides agents with identity & credential management



Gateway

Manage connections between users, agents & tools



Runtime

Host agents & MCP servers on a serverless runtime



Code Interpreter

Allows agents to generate & execute code with AWS context



Bedrock AgentCore

EXPLOITING AGENTCORE RUNTIME
FOR ACCOUNT TAKEOVER

CASE STUDY

Exploiting AgentCore runtime for account takeover

HOSPI TROOPERS



CASE STUDY

Exploiting AgentCore runtime for account takeover

GOALS

Exposing Meditroopers APIs as MCP tools so Hospitroopers users can submit medical surveys seamlessly.

Using AgentCore Gateway to handle user authentication between the two applications

CASE STUDY

Exploiting AgentCore runtime for account takeover

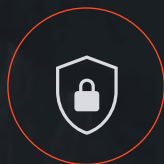


GAME OVER



Tips & Closing Thoughts

Securing your cloud against these attacks



Guardrails

Bypassing guardrail enforcement using cross-account guardrails

TIP

Use IAM to enforce specific guardrails in production environments.



Knowledge Base

Using knowledge base secrets to move laterally to third parties

TIP

Protect knowledge base secrets using explicit denies in resource policies.



AgentCore

Abusing AgentCore for privilege escalation in the AWS account

TIP

Remember to separate the permissions of workload & deployment roles.

How to secure your org's data

AI security is more than protecting against prompt injection;
it's about keeping a **secure environment**.

01

**Principal of
least privilege**

02

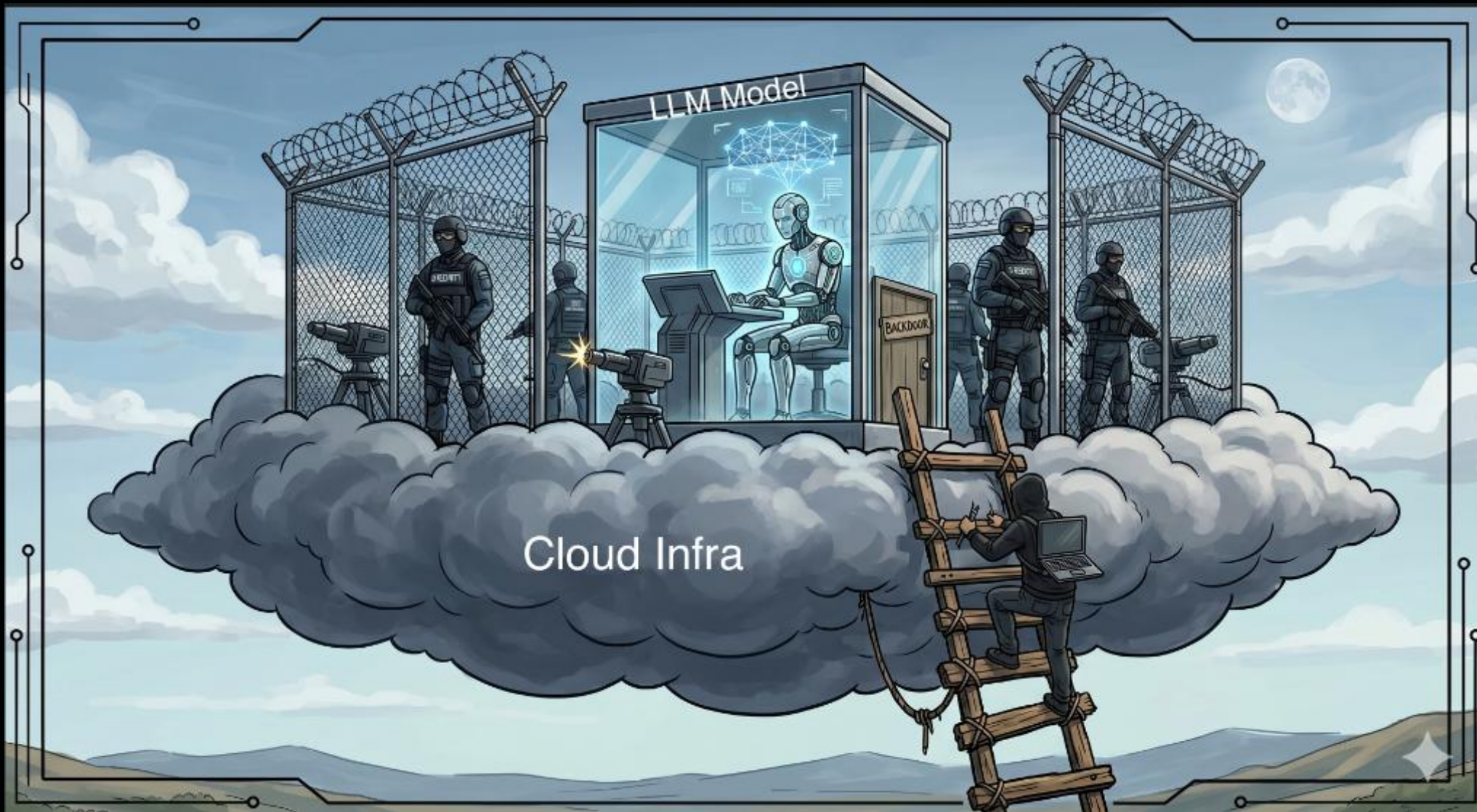
**Defense
in depth**

03

**Track the flow
of sensitive
data**

04

**AI hygiene
education**





THANK YOU

MParizer@Varonis.com

TPeleg@Varonis.com



Follow us on LinkedIn for more content



MAYA PARIZER



 VARONIS



TAL PELEG