The Evolution Of Cloud Attacks

John Pease - CISSP, CEH
Strategic Cloud SE - EMEA

SentinelOne

Agenda

- Cloud Attacks - Where We Were
- Cloud Attacks - Where We Are Now
- Real World Breaches
- Traditional Cloud Security
- Lessons Learned &
  The Defense Required

Threat Actors Targeting Cloud and Containers On The Rise

Increase in # of cloud breaches:
Targeting business critical applications in cloud & the increasing amount of data stored in public cloud

Increase in cloud attack sophistication:
Novel techniques continue to be seen, across more threat actors, and in new combinations

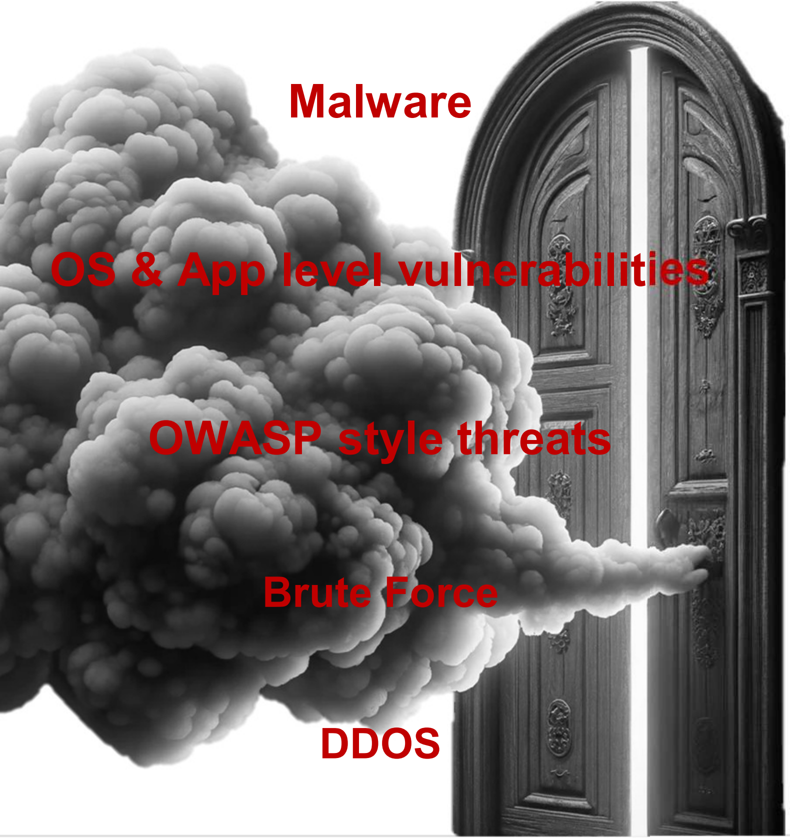
Increase in automation in cloud attacks:
Worm GPT, & bots, bots, bots including crypto-miners, scrapers, phishing, credential harvesting & stuffing

The 6 Phases of a Targeted Attack

Recon	Technical Reconnaissance Non-Technical Reconnaissance
Initial Access	Mis-Configuration Phishing, Credential Leakage and Exploitation
Lateral Movement	Credential Access On-Prem ⟺ Cloud
Discovery	Built in Tools - Living off the Land Download and install tools
Exfiltration	Establish C2 connections (DNS) Data gathering
Impact	Data destruction, Data Encryption Extortion

Cloud Attacks – Where We Were…

The Knock On The Door



Malware

OS & App level vulnerabilities

OWASP style threats

Brute Force

DDOS

DevOps Pipeline Threats

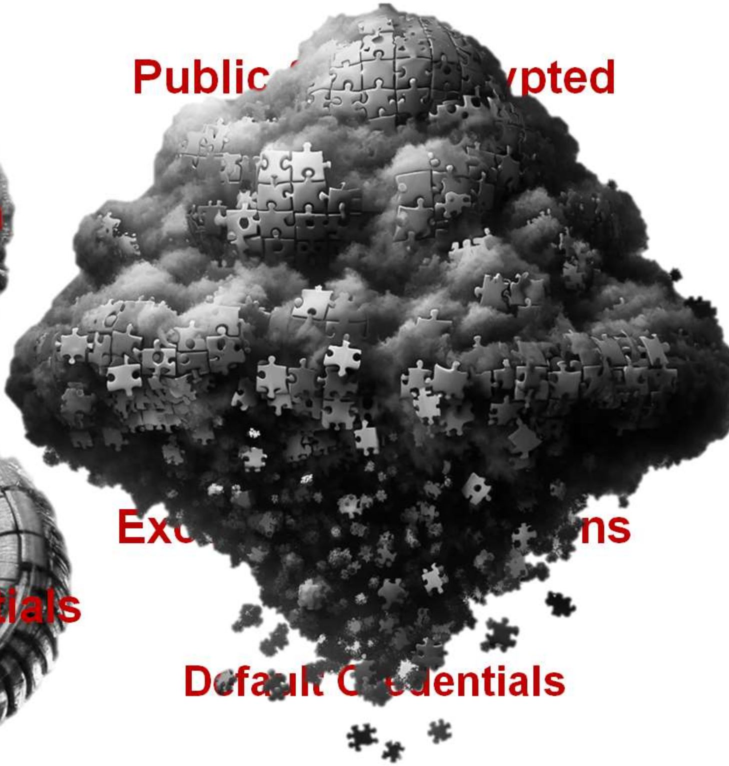
Open Source packages with dangerous contents:

Malicious

Unintentional

Credential Abuse via Leaked / Compromised Credentials

Cloud Misconfigurations



Public [illegible]ypted

Exc[illegible]ns

Default C[illegible]edentials

The Knock On The Door…

Fileless attacks
running in memory steadily rising

Wipers & Ransomware
now have Linux variants

Container specific attacks
(container escape, mounting filesystems)

Cryptojacking

OS & App level vulnerabilities
found via automated tooling
& **exploited** via automated tooling

***Malware polymorphism**
is potentially improving with AI*

DevOps Pipeline Threats…

Targeted Supply Chain campaigns are being observed for the first time

Use of non-standard languages for threat actors to hide in open-source packages

Code Repositories are being targeted – for credential harvesting and supply-chain threat opportunities

CI/CD Pipelines Abuse to deploy malware, exfiltrate data, and/or execute unauthorized commands within DevOps workflows

Account Take Over enables popular libraries to be poisoned

Certain Threat Actors are targeting developers to understand business logic and weaknesses of web apps

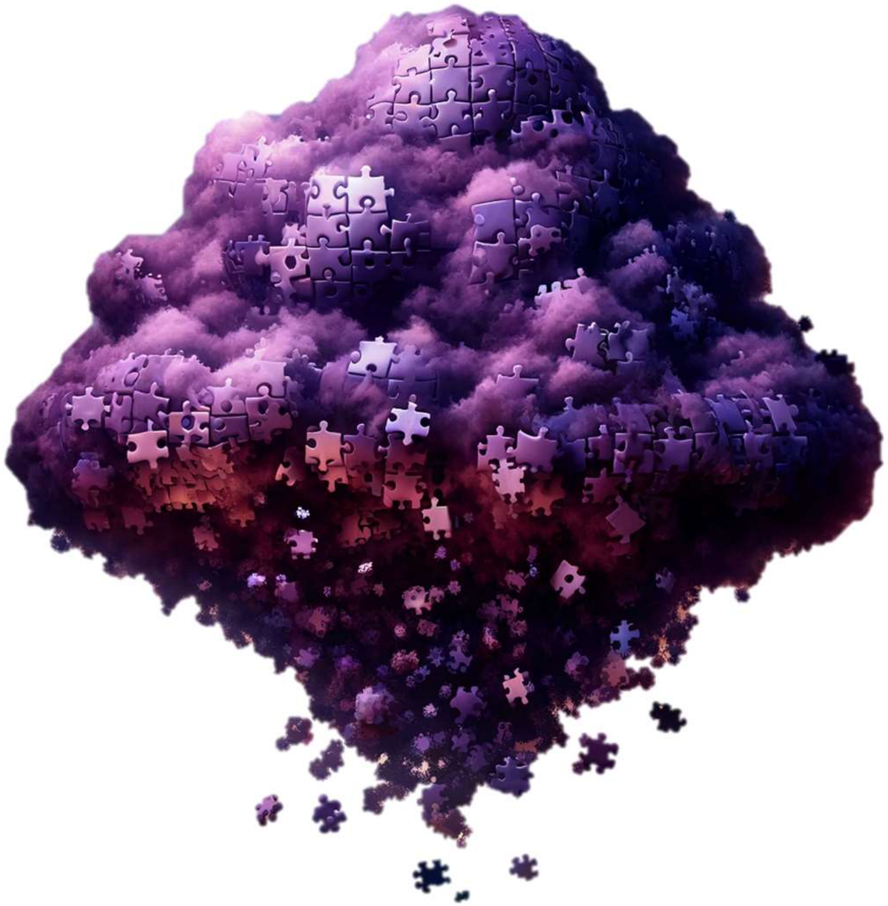
Cloud Misconfigurations…

Threat actors often **combine misconfigurations** into a more complex attack chain

Often **targeting and involving Cloud Identity** (AWS IAM & Azure AD)

Additionally, threat actors are now being seen **causing Cloud Misconfigurations**

A new requirement to differentiate between mess and noise & what misconfigurations are compromise artifacts!

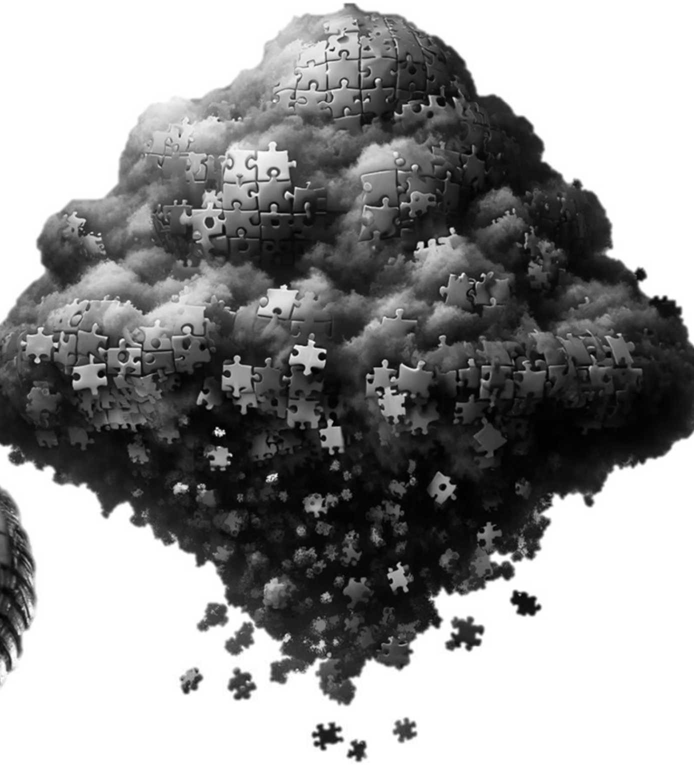


Cloud Attacks – Where We Are Now…

The Knock
On The Door

DevOps
Pipeline Threats

Cloud
Misconfigurations



Cloud Attacks – Where We Are Now…

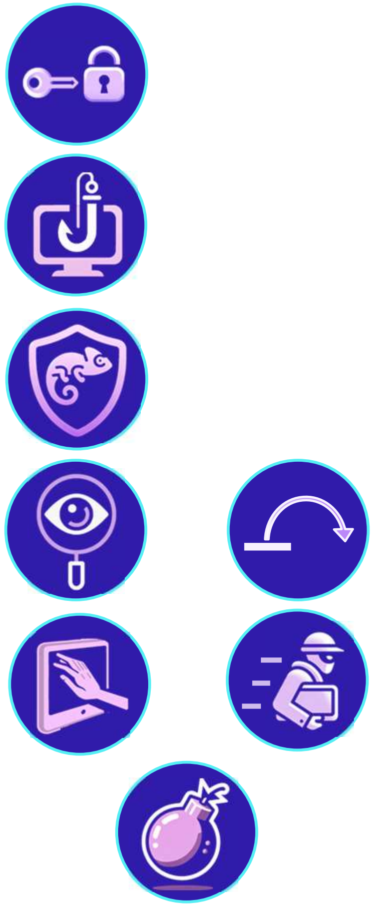
Modern Cloud Attacks
are combining
tactics and techniques
across the
cloud threat landscape

Mapping Cloud Attacks to MITRE ATT&CK

Cloud Infrastructure

Cloud Identity

Cloud Services



Real World Cloud Breaches

A Sliver Of Cloud: Targeting Cloud Credentials

Vulnerable public facing web app (PHP) allows RCE	Initial Access
Enumerate IAM roles via instance metadata API	Discovery
Cron job to download & run a Sliver implant upon reboot	Persistence
Actor attempted to harvest cloud credentials via instance metadata	Credential Access
Curl used to download the same Sliver implant	Command & Control

Chinese Threat Actor Moves With Stealth

CVE-2022-29464 leveraged to allow RCE

Initial Access

wget and curl used to access malicious tooling

Command & Control

Anti-forensic efforts seen: timestomping webshell files

Defense Evasion

AWS CLI installed to perform reconnaissance: network service discovery

Discovery

Adversary began enumerating AWS credentials and hunted in sensitive files incl. /etc/shadow

Credential Access

Attempted lateral movement to internal hosts via SSH

Lateral Movement

Roasted 0ktapus (with BlackCat!)

Accessed AzureAD creds via smishing campaign

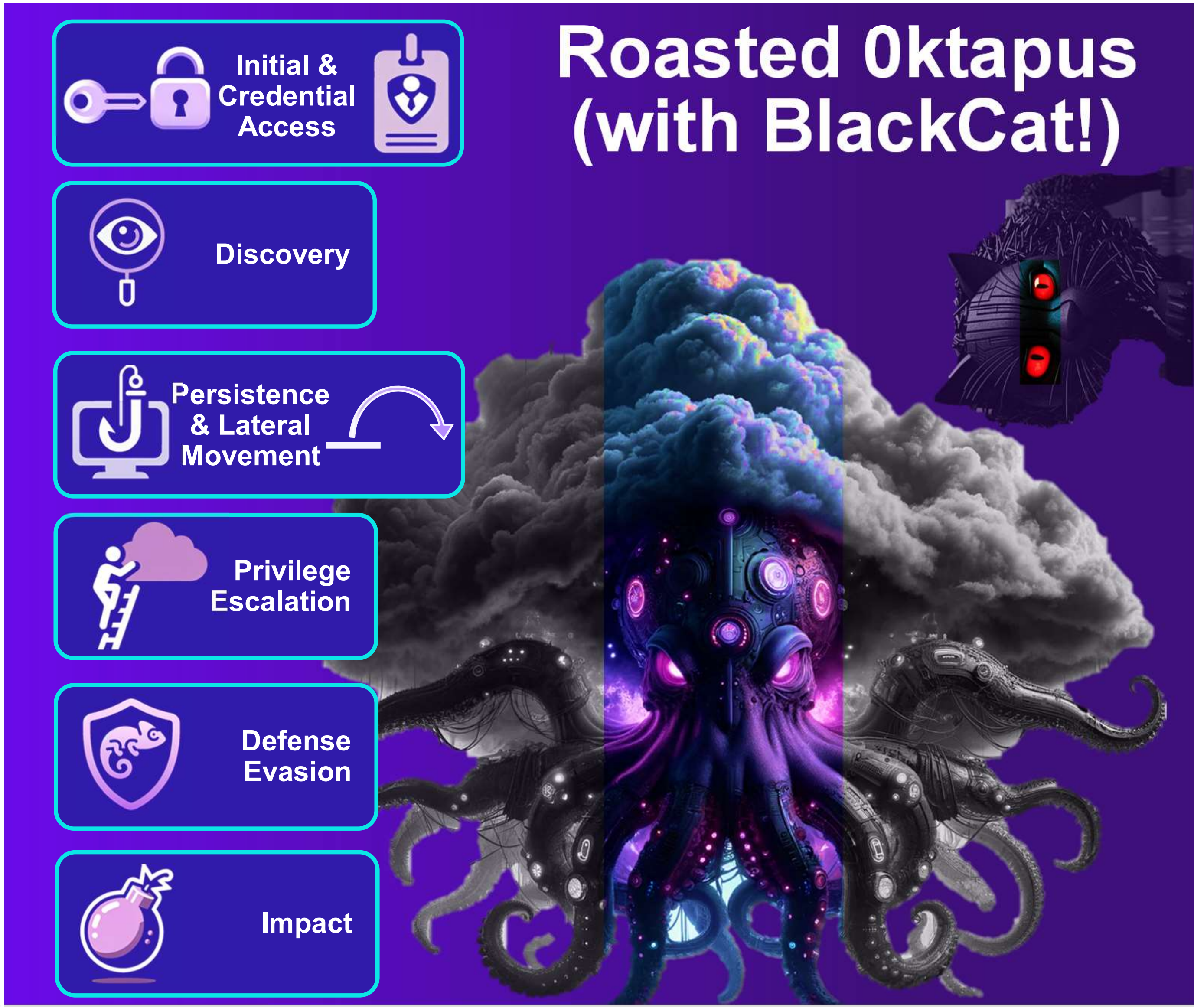
Listed cloud assets and activated AWS Systems Manager Inventory

Added own MFA, created a public EC2 in a new Security Group

Created new access key for an IAM user & attached an admin access policy

Disabled GuardDuty and attempted to delete existing CloudTrail

Used cloud orchestration tool to deploy BlackCat's AlphV ransomware



Initial & Credential Access

Discovery

Persistence & Lateral Movement

Privilege Escalation

Defense Evasion

Impact

Cloud Attack Trends Observed

Threat actors are infiltrating cloud and container environments, with relative **confidence in defense evasion**

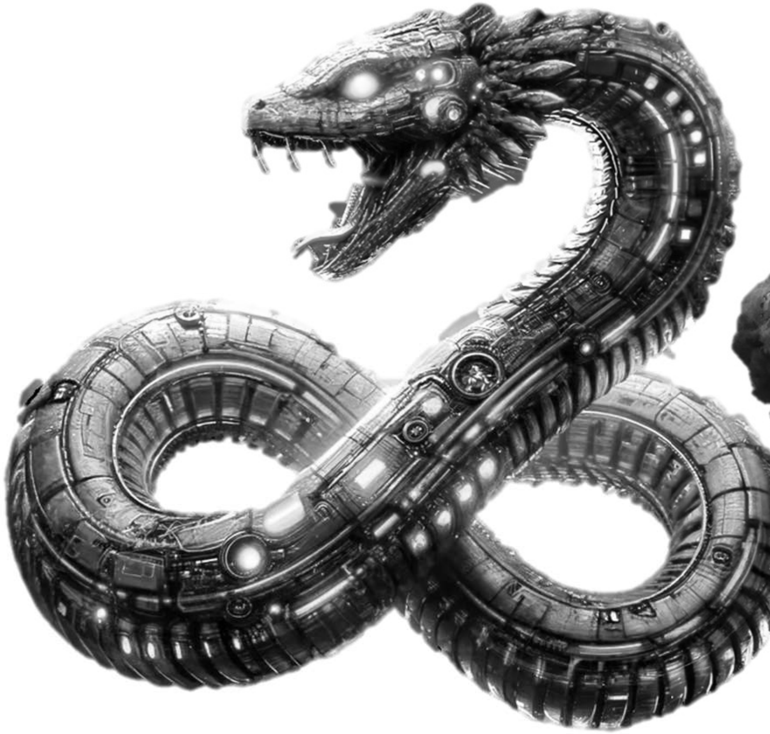
Observed methodology & TTPs notably includes: **Leveraging, Modifying and Disabling Cloud Services & Abusing Cloud Identity**

Ransomware attacks have pivoted to the cloud, with both Linux variants & cloud focused campaigns

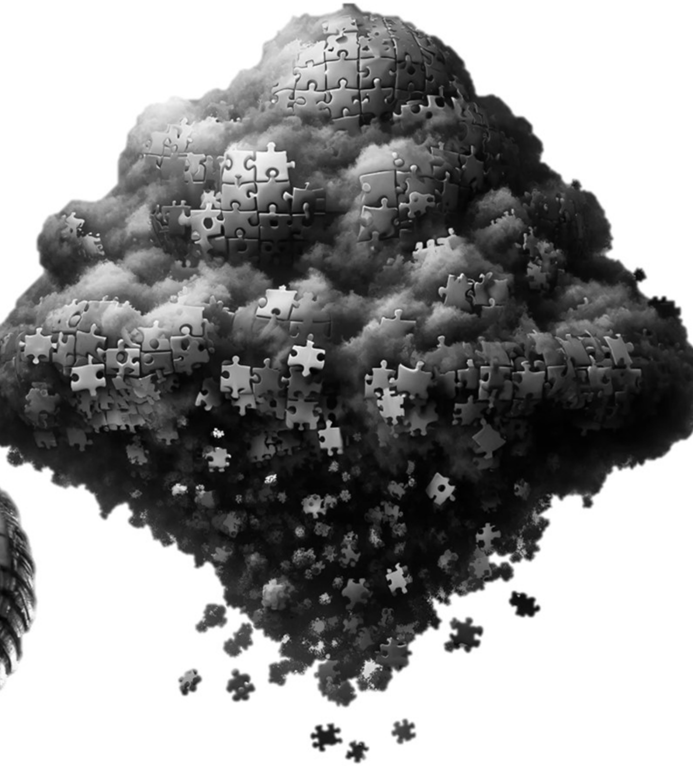
Version One Corresponding Defenses

Endpoint Security
In Cloud

Code Scanning
Owned by DevOps

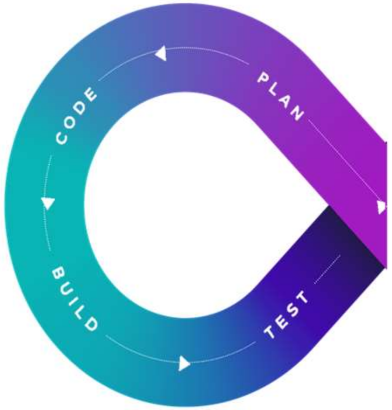


CSPM v1



Tools, consoles, plug-ins…

Build Lifecycle



Cloud Services

Cloud Compute & Container

By 2026, Gartner forecasts that **80%** of companies will have consolidated cloud security tooling to **three or fewer vendors** down from an average of **10 in 2022**

Cloud Pain
Due To Tooling

Right now it’s a combination of tools:

Disparate, Disconnected

Lacking Context, Lacking Correlation

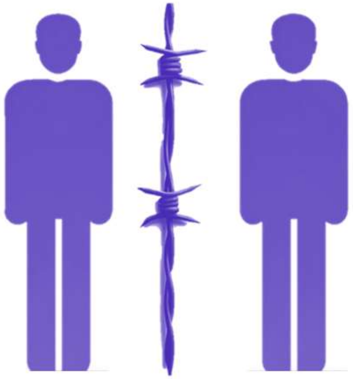
Toolsets are incredible noisy

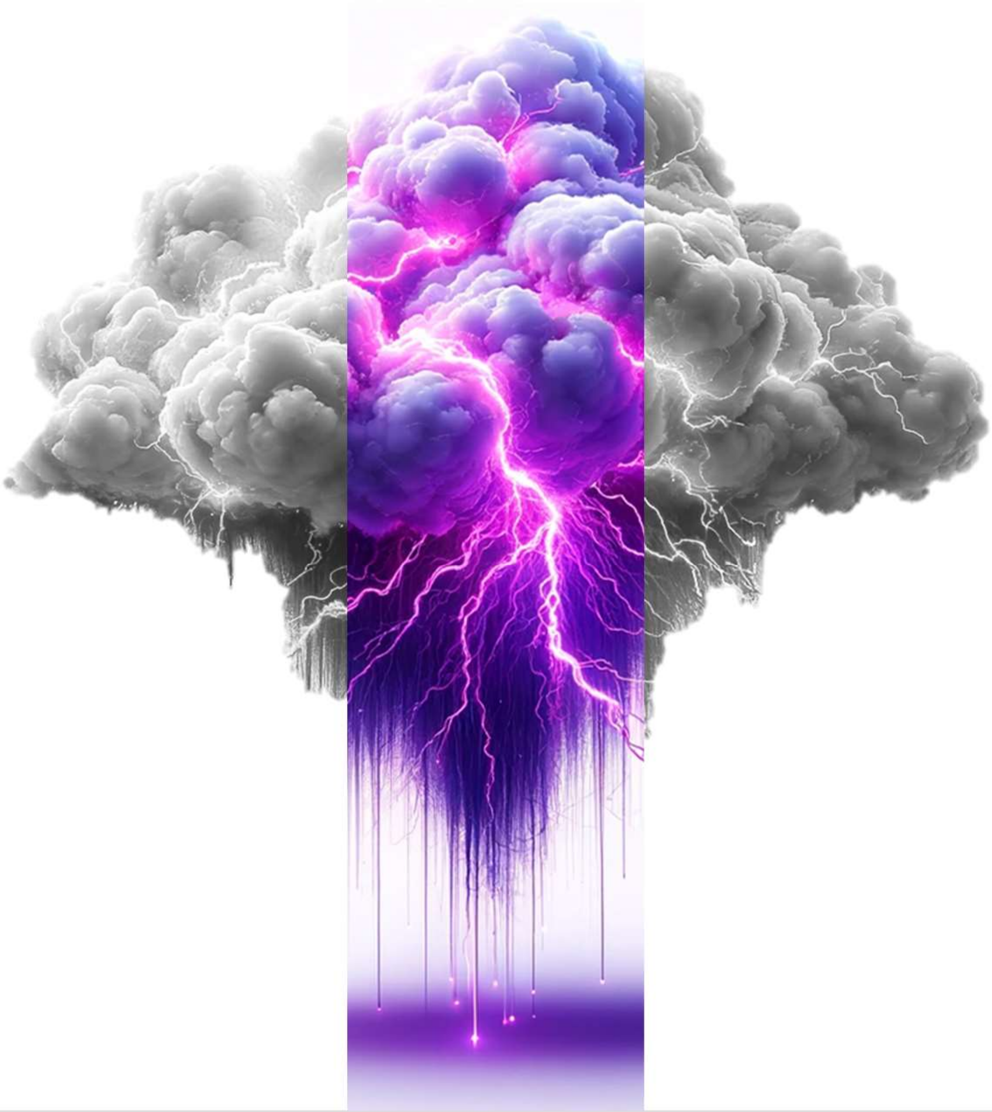
Often without any prioritization

Mostly built on prevention alone

Often lacking machine speed security

Tools have split ownership across: Security, Incident Response, Cloud, Dev(Sec)Ops





Poor Operational Efficiency

& Broken RACI matrices

Lessons Learned & The Defense Required

Cloud Security requires:

Policies, capabilities and visibility through the cloud lifecycle

Context and Correlation

Attacker’s mindset required

Response & Remediation capabilities

Which means:
Agentless &
Agent based
controls combined

Thank You!