CSA | AI Summit at RSAC 2024

May 6, 2024 | *Welcome!*

CSA | AI Summit at RSAC 2024

Securing The Cloud: Taking Back The Attacker's Mindset

PRESENTED BY

SentinelOne

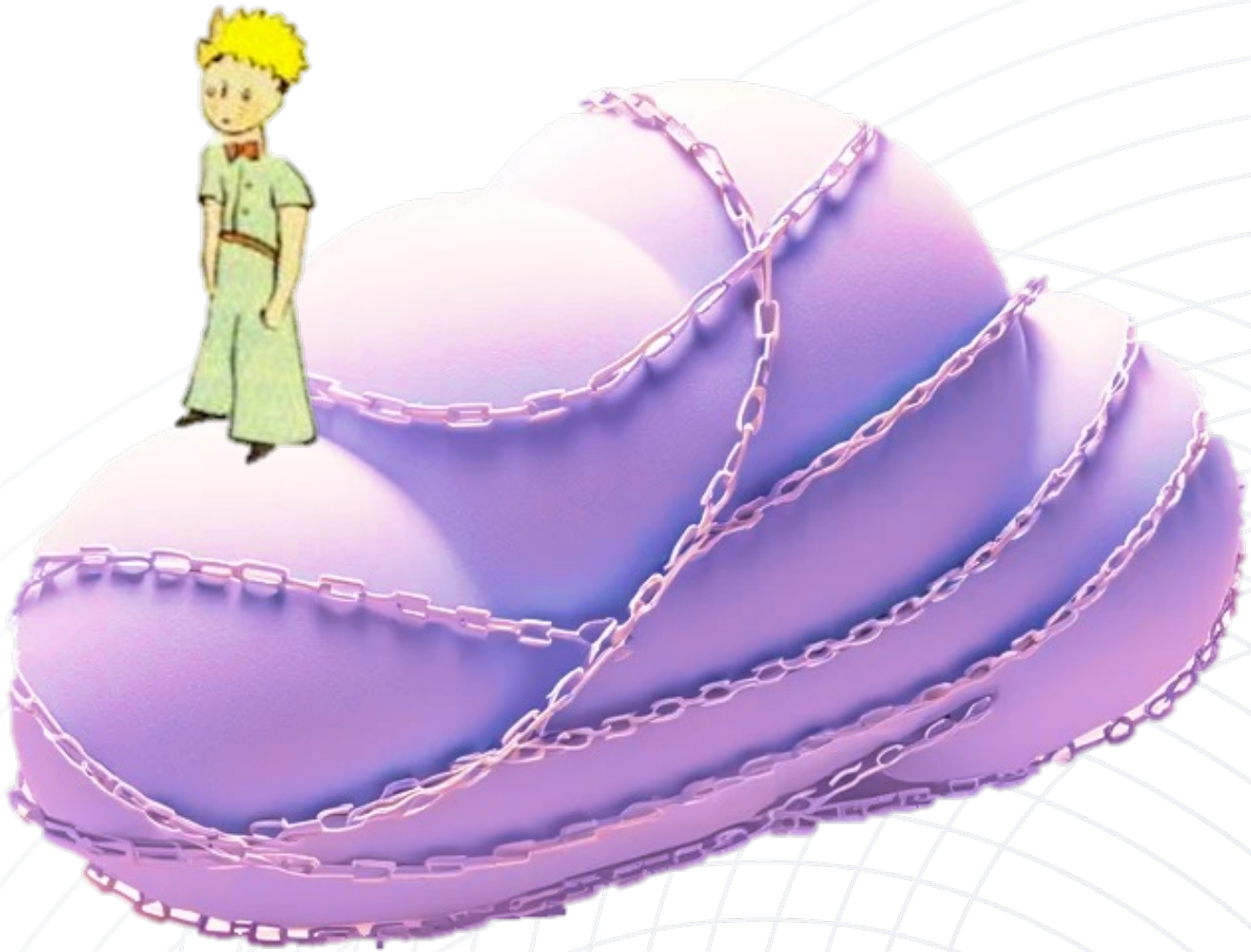
Chris Hosking
Cloud Security Evangelist

Agenda

1. AI Within the Cloud Security Challenge
2. Cloud Threat Landscape
3. AI to Secure the Cloud
4. Taking Back the Attacker's Mindset

Antoine de Saint Exupéry

"The machine does not isolate man from the great problems of nature but plunges him more deeply into them."



AI within the Cloud Security challenge

AI-fueled External Challenges:
Evolving Cloud Threat Landscape
& Motivated Threat Actors (APTs)

Internal AI opportunities:
People, Processes
& Technology

Cloud Threats 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 AI & automation in cloud attacks:
Chat & WormGPT, & bots including crypto-miners, scrapers, phishing, credential harvesting & stuffing

Previous Examples of AI-Powered Attacks

PassGan & PCFG Crackers
AI & ML powered password crackers

MalGan
Feed-forward neural networks designed to evade ML detection engines

DeepLocker
IBM POC with deep neural network capabilities & stays hidden until hitting pre-defined context

Cloud Attacks: 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

AI-Malware polymorphism
Black Mamba recent example

Cloud Attacks: 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

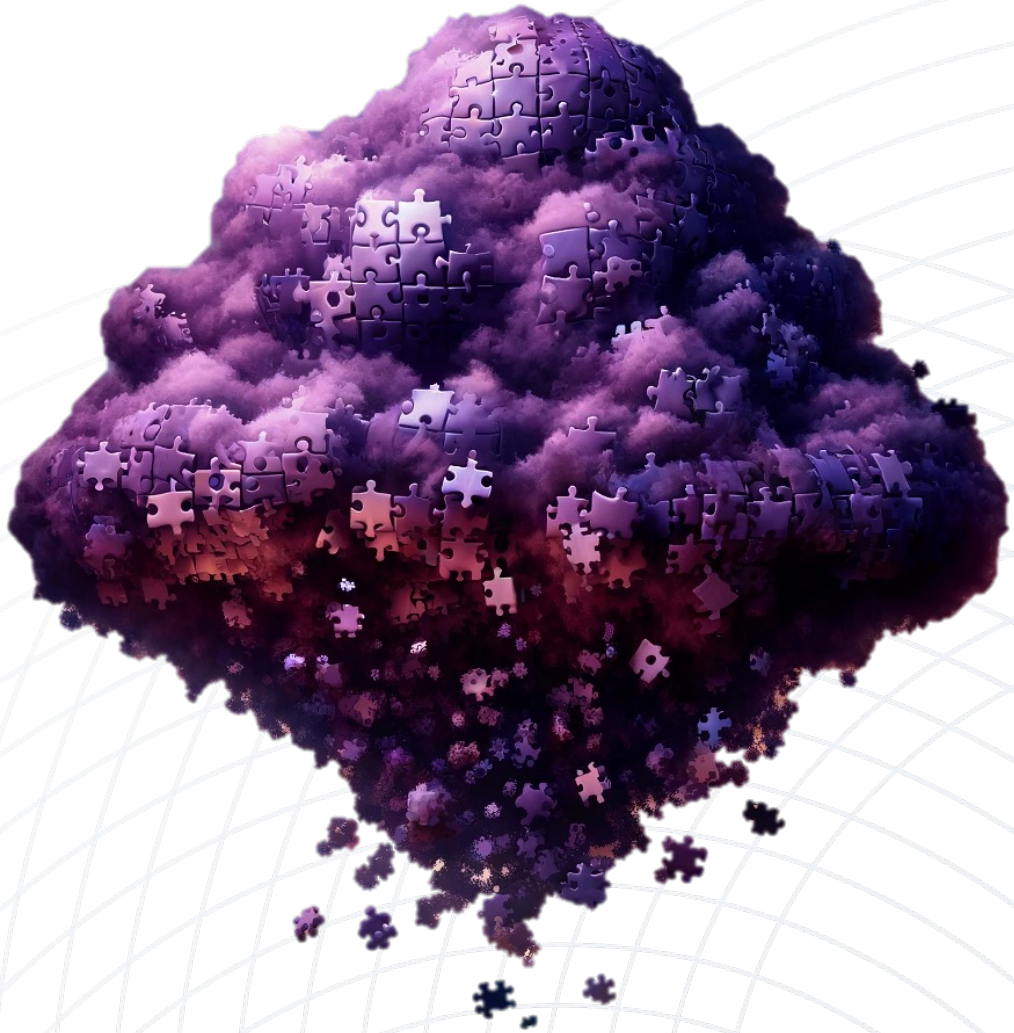
Cloud Attacks: Cloud Misconfigurations…

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**

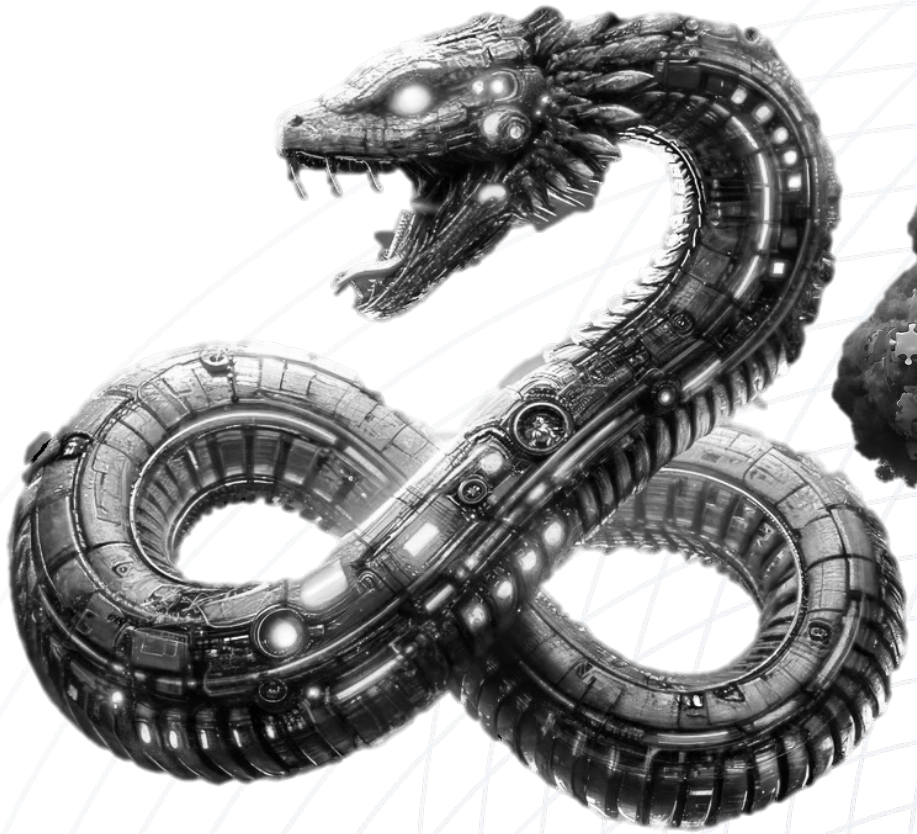
A new requirement to differentiate between mess and noise & what misconfigurations are compromise artifacts…
How do you hunt for Cloud LoLBins?



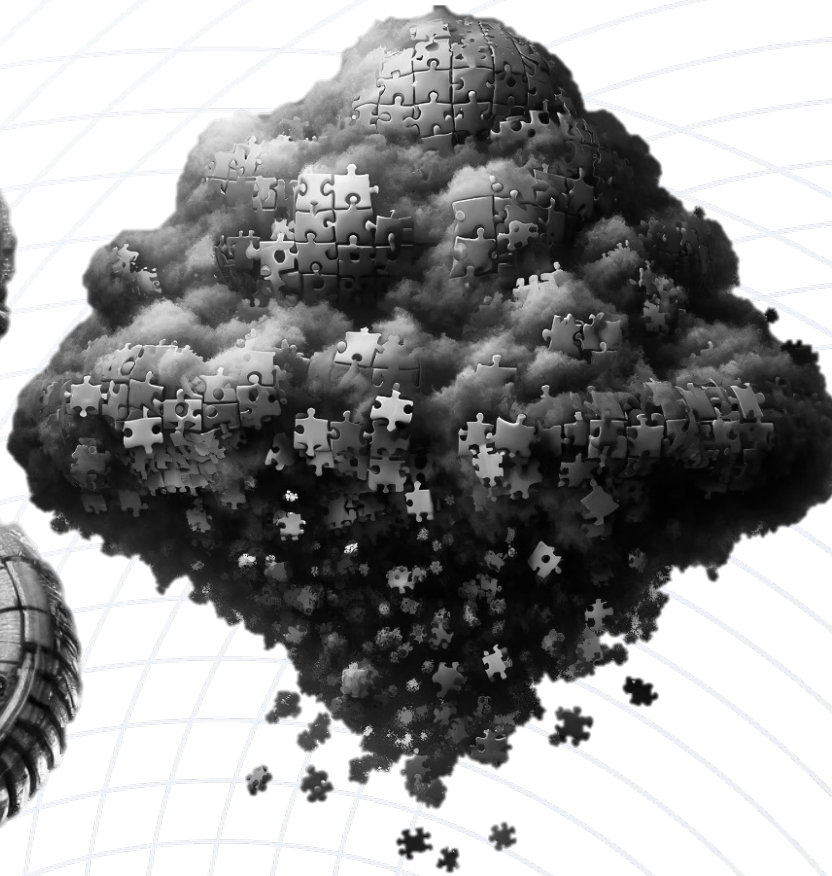
Cloud Attacks: Where We Are Now…

The Knock On The Door

DevOps Pipeline Threats



Cloud Misconfigurations

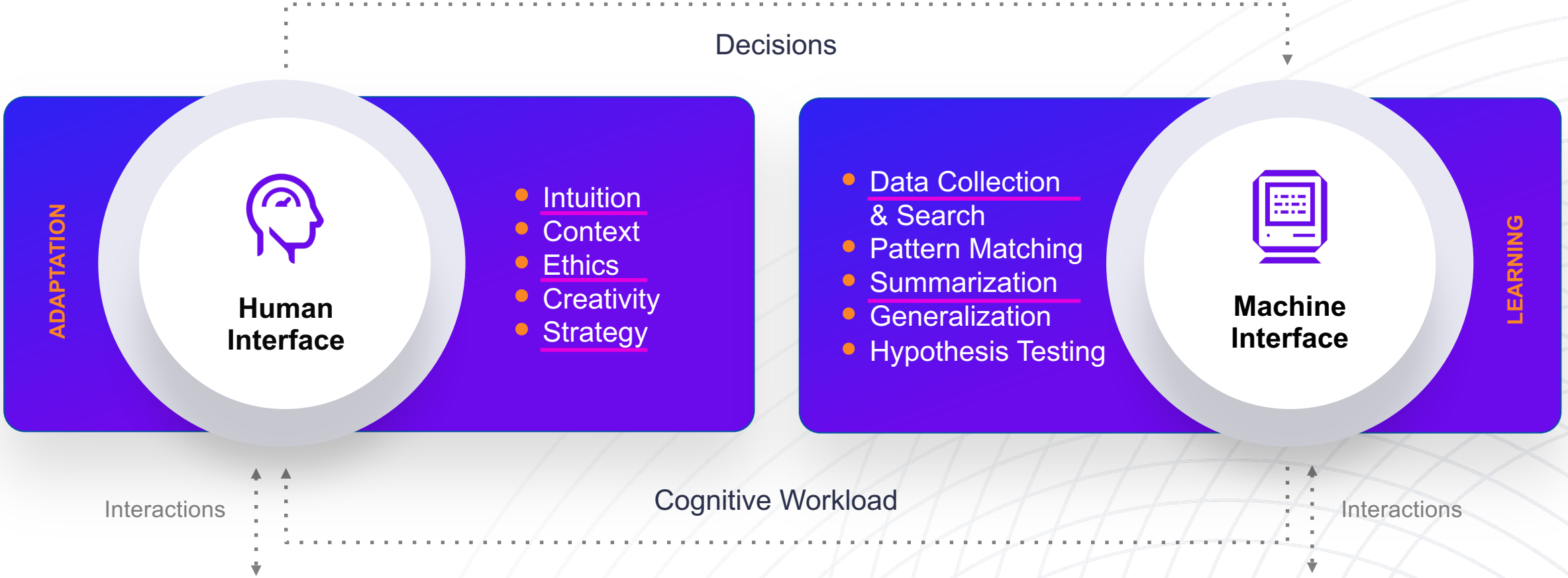


Cloud Attacks: Where We Are Now…

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

& AI-powered defense is required to face this new reality

A Time & Place for Machines



“Real” World

AI Engines for Cloud Runtime Security

Pre-Execution

Static AI/ML

- File inspection
- Parsing file structures
- Entropy
- Opcode histograms

ML algorithms learn good from bad
Unsupervised doesn't require feature labeling

Real-Time

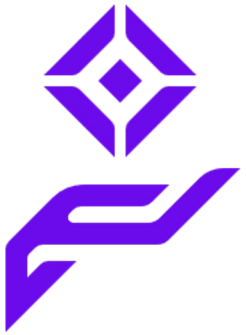
Behavioral AI

- OS process monitoring
- Event linking
- Adds new dimension: Time
- Extensive context

AI learns how programs behave (good & bad)
AI improves over time (observability)

Potential Security Uses of Generative AI

Creation



Creates artefacts of value given a (multimodal) specification

Detection Code
Incident Summaries

Interaction

Supports fluent, context driven dialogue (with knowledge)

Step by Step Guidance
Self-documenting Work

Prediction

Offers a completion, given a sequence and constraints

Attacker Activity
Remedial Action

SentinelOne's Purple AI

Your AI security analyst to help you detect earlier, respond faster and stay ahead of attacks

Empower every analyst

Use natural language to find and respond to critical risk.

Automatically translate conversational inputs to structured PowerQueries leveraging the Singularity Data Lake

Accelerate threat hunting

Guide analysts with Hunting Quickstarts, auto-summaries, and suggested queries.

Reduce hunting cycles times from hours to minutes.

Integrate with your workflows

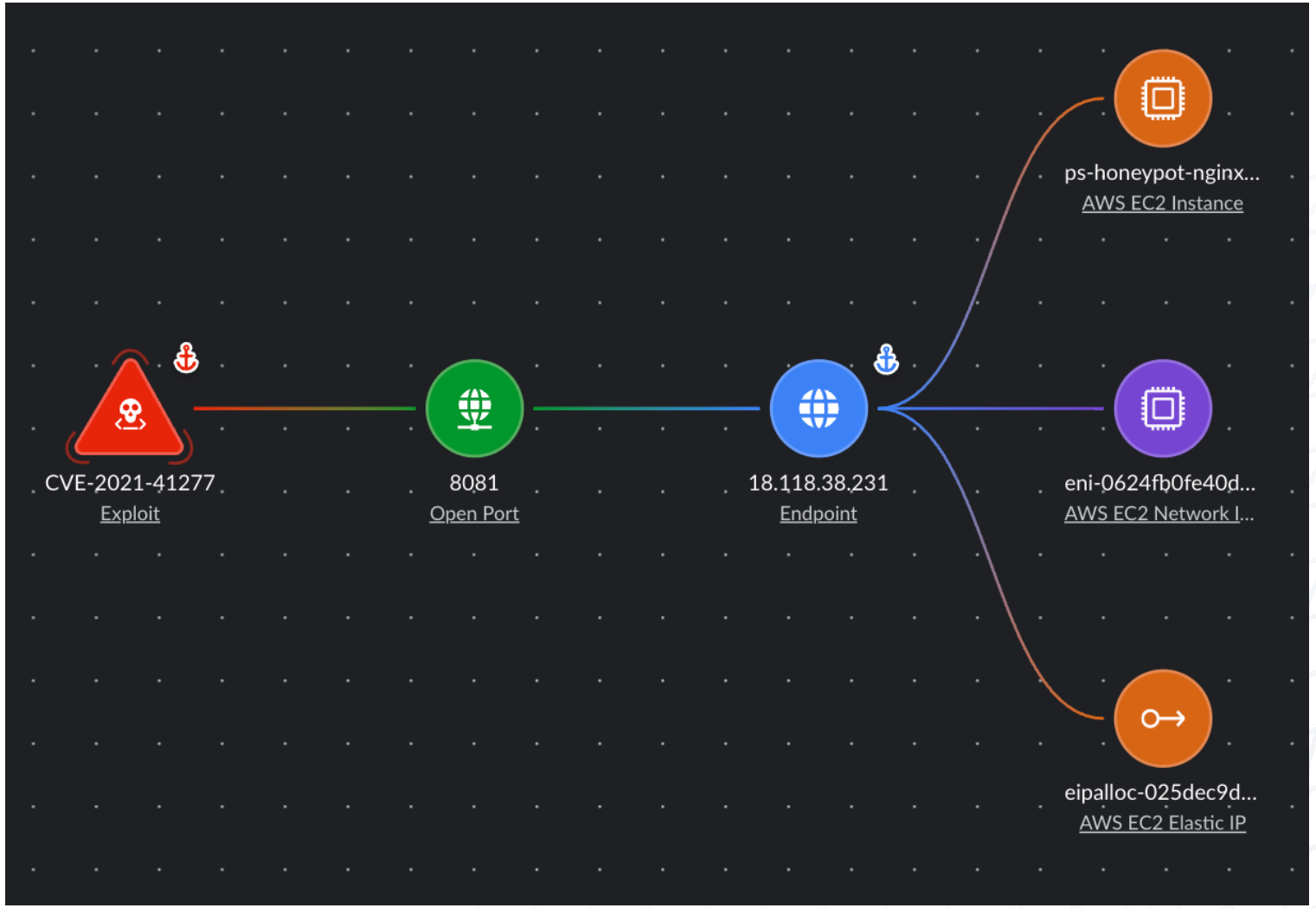
Scale collaboration across teams with saved notebooks.

Streamline threat investigations with unified data access and threat intelligence.

AI & Validation

As we increase AI-reliance within cloud defense, there will be a growing trend of validation, to ensure time isn't wasted chasing AI hallucination

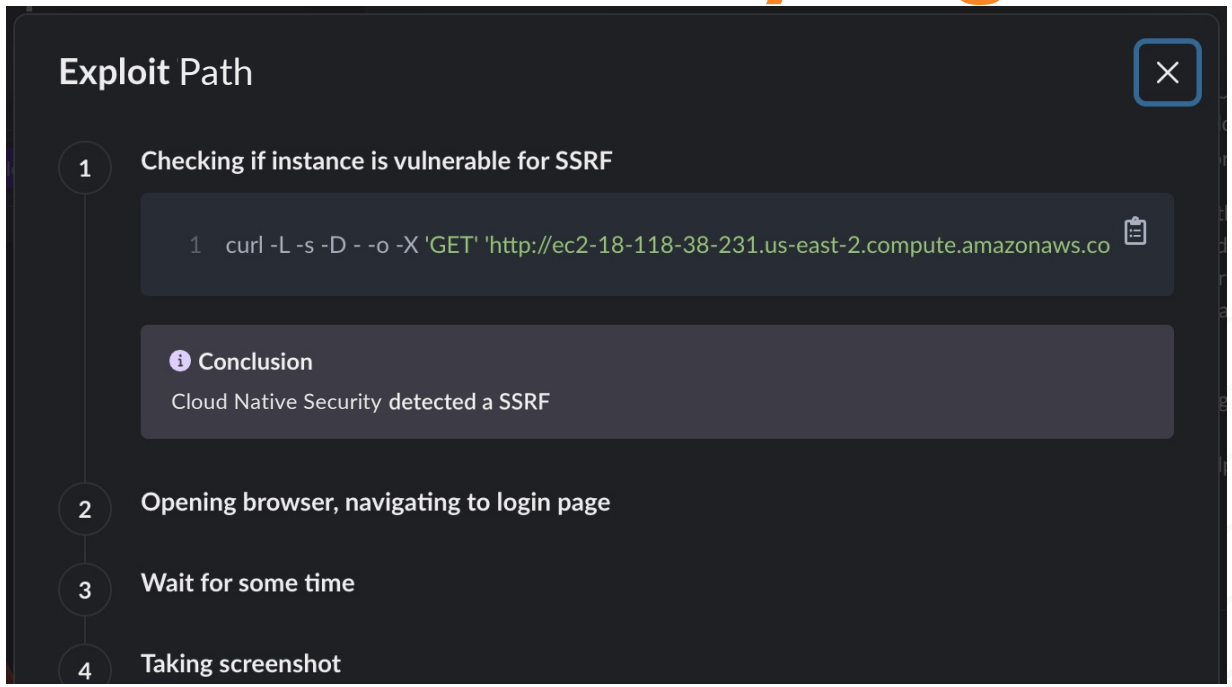
Take back the Attacker's Mindset: Validating Attack Paths

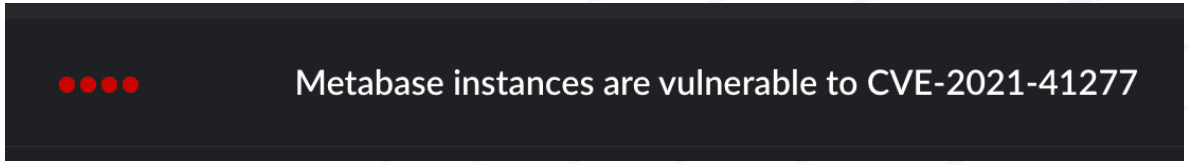


Attack Paths:

The correlation of publicly accessible assets with insecure cloud assets – including misconfigurations and vulnerabilities

Take back the Attacker's Mindset: Offensive Security Engine






```
{
  "Code" : "Success",
  "LastUpdated" : "2024-03-25T16:18:53Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAUMNA5JFASPXW2UGM",
  "SecretAccessKey" : "ckgDIdcqm4gQVTdZQxjjIVUE+OdNGov4qDDnKqEl",
  "Token" :
"IQoJb3JpZ2luX2VjEHgaCXVzLWVhc3QtMiJHMEUCIH2eYxk6f9DtnEm9oy34MtW4\
DUgUrxAvJAlfMvJRTXsR+djrcUZl5ay7EtQpOhSfRqb3gYI0dbLE+qgimBYsI6i1gu\
uLHO4gprMgceAN+EJg1n8uLUNbkk/XsT2eXPEY1xtvYwJDUH3Agm0/YV9gV8IEN/t
```


Offensive Security Engine safely simulates attacker methods and captures the response

Removes false positives by analyzing which theoretical attack paths are actually exploitable

Focus on what matters…
Evidence based prioritization with Verified Exploit Paths®

Take back the Attacker's Mindset: Verified Exploit Paths™

Achieves:

- **What risk is real and requires focus?**
- **What would an exploit look like?**
- **What is the impact? / give me the So What**

Key Takeaways

Immense Potential for Attacking

Potential

Significantly Enhances Cybersecurity

Enhancements

Humans + AI

Holistic

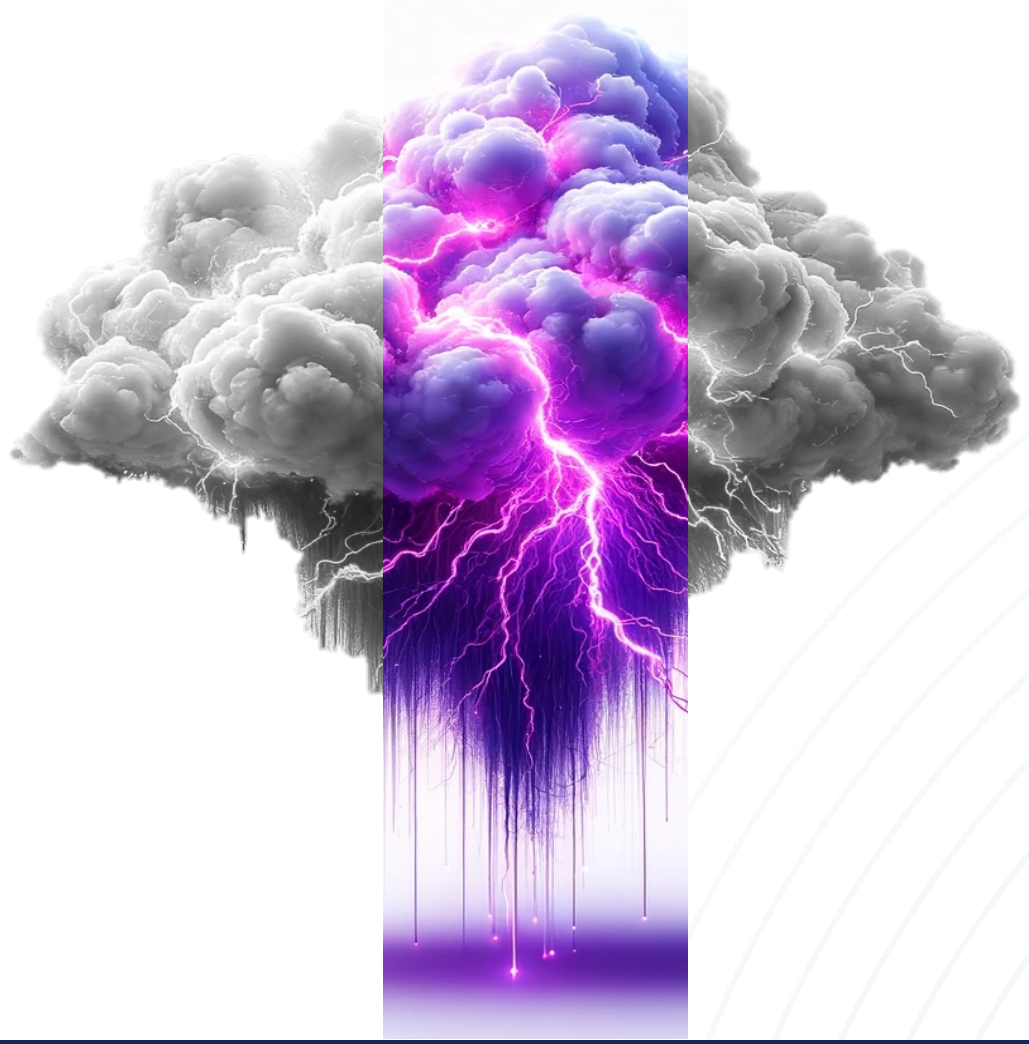
Continually Advance Defensive AI

Defensive

Collaboration is Vital for Effectiveness

Capabilities

Thank You!



SentinelOne®

Chris Hosking

Chris.Hosking@SentinelOne.com