SentinelOne®

Embrace the Attacker's Mindset:

Protecting Australian Organisations with an Offensive Cloud security strategy

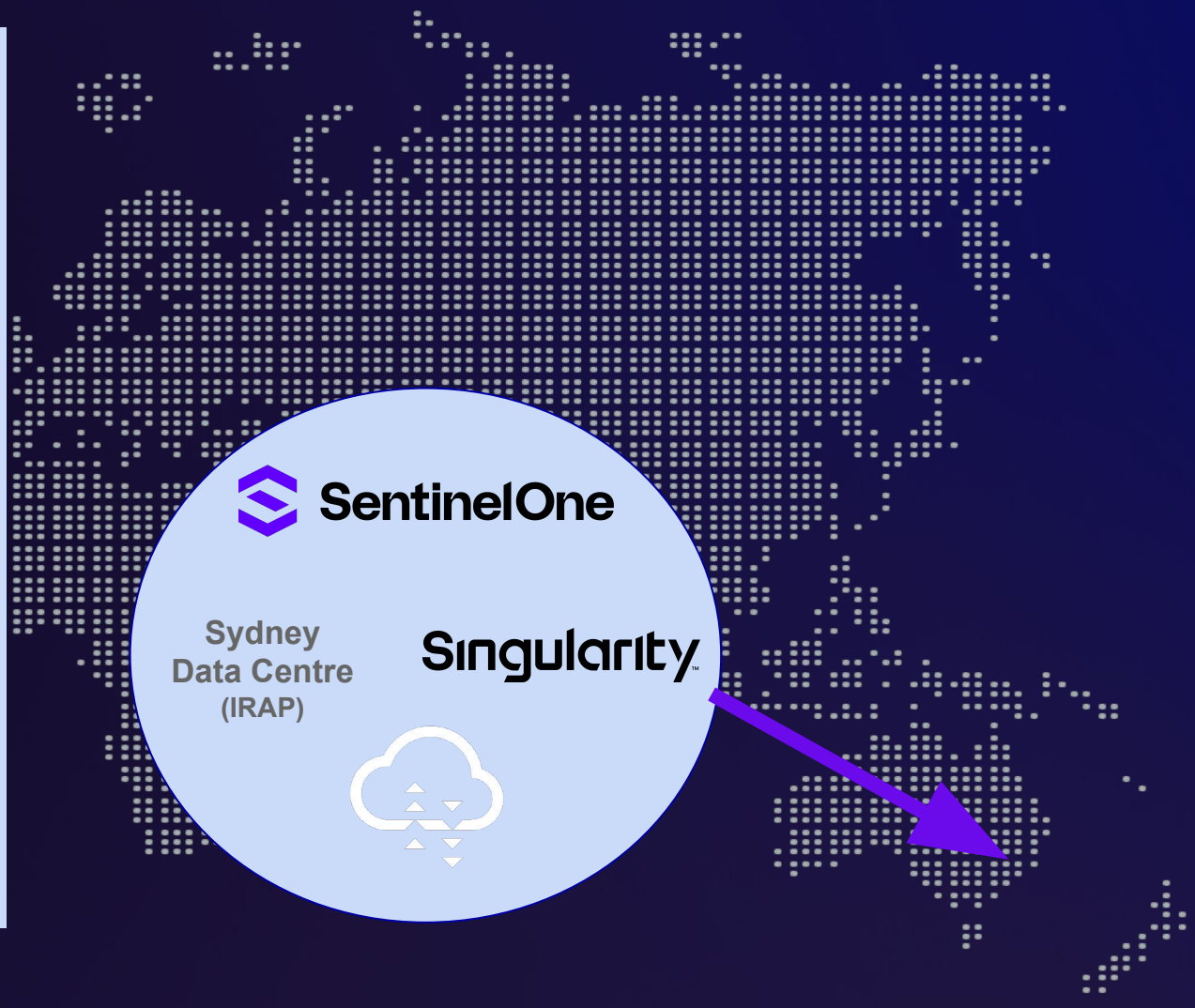
SentinelOne is a Platform company.
The world's most advanced cybersecurity platform.

Security is a Data problem.
Real-time visibility and automation are key.

Securing the Cloud.
From build time to runtime.

Supporting Australian Organisations Regional Data Sovereignty and Management

- Australia Data Centre
- Data remains within Data Centre
- IRAP Assessed
- Options for dedicated instances (Platform Pro)
- Deploy on Private AWS



Securing your cloud: Competing tensions

External challenges
Evolving cloud threat landscape
and motivated threat actors (APTs)

Internal challenges
People, processes,
and technology
innovation drive

SentinelOne

Cloud threats are on the rise

Increase in number of cloud security events
Targeting business-critical applications in cloud and 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, and stuffing

The knock on the door

Fileless attacks
running in memory, steadily rising

Wipers and ransomware
now have Linux variants

Container-specific attacks
(container escape, mounting filesystems)

Cryptojacking

OS- and app-level vulnerabilities
found via automated tooling
and exploited via automated tooling

Malware polymorphism
is potentially improving with AI

SentinelOne

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 pipeline 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

SentinelOne

Cloud misconfigurations

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

Often **targeting and involving cloud identity**

Additionally, threat actors are now being seen **causing cloud misconfigurations**

There is a new requirement to differentiate between mess/noise and which misconfigurations are compromise artifacts

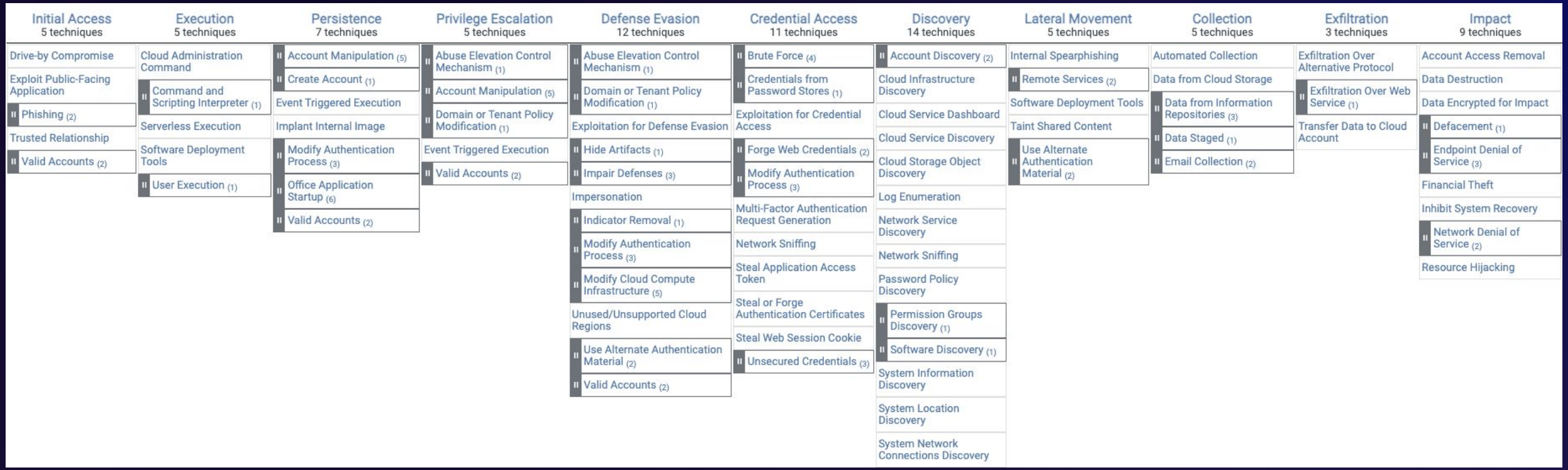
SentinelOne

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

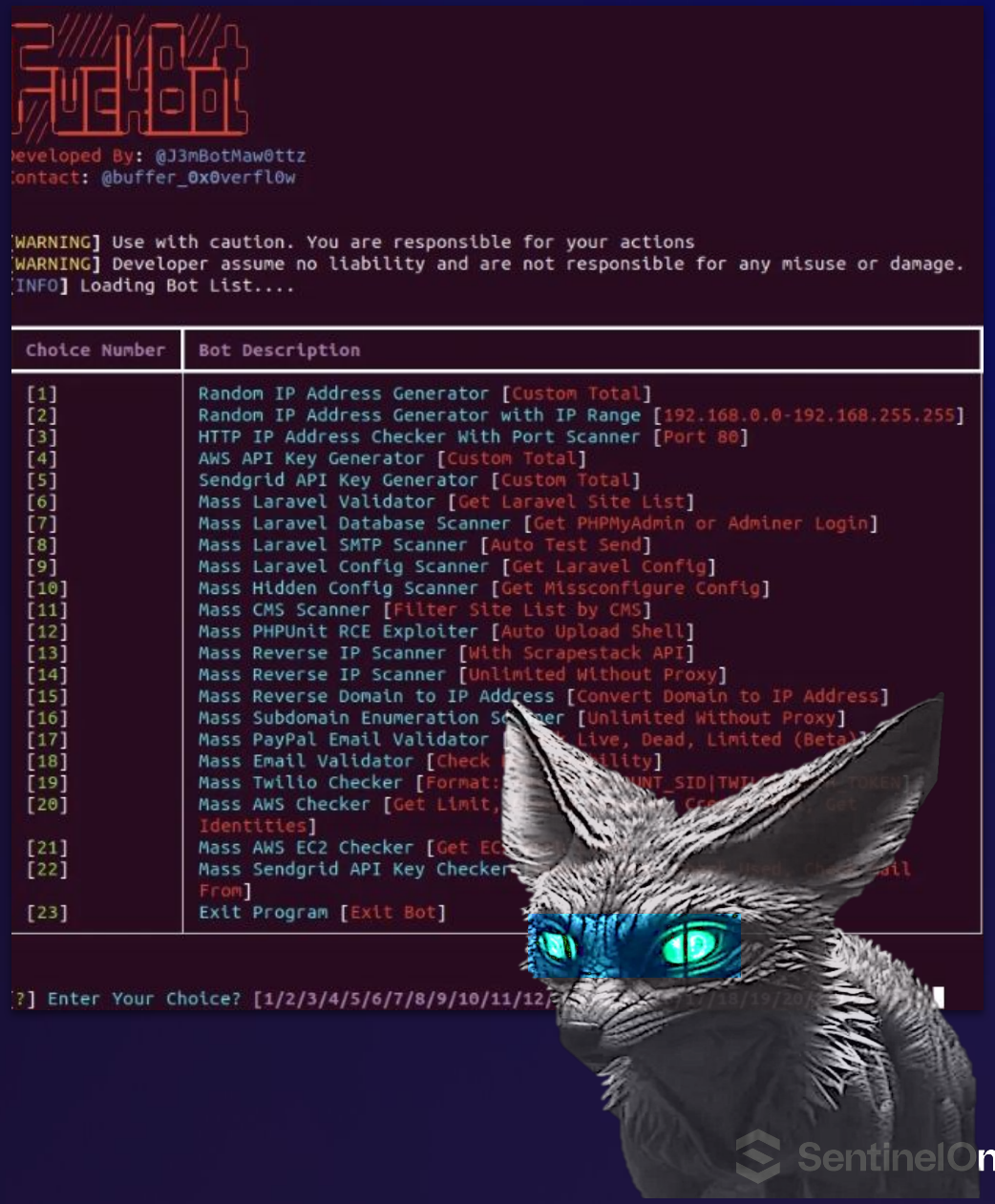
Cloud compute Cloud identity Cloud services



SentinelOne

Open source tooling readily available: FBot and AlienFox

Dumps configuration files from misconfigured servers	Initial access
Discovery and extraction of sensitive information	Discovery
Imports boto3 locally and uses the stolen AWS access key	Credential access
New login profile created with a hardcoded password	Persistence
AdministratorAccess privileges attached	Privilege escalation



Need to identify cloud security gaps

SentinelOne

Tools, consoles, plug-ins

Build lifecycle

Visibility and policies designed to shift security left

Cloud services

Radically reduce your largest attack surface

Cloud compute and container

Secure business critical cloud infrastructure

SentinelOne

Cloud pain due to tooling

Right now, it's often a combination of tools, which can be disparate, disconnected, and lacking context and correlation

Tool Sets can be incredibly noisy

Often without any prioritization

Mostly built on prevention alone

Often lacking machine speed security

SentinelOne

Singularity Cloud Security

BLOCK ATTACKS WITH OUR AI-POWERED CNAPP

Cloud Native Security

Agentless cloud security with a unique offensive engine

+

Cloud Workload Security

Agent-based threat protection for cloud compute and container (including AWS Fargate)

+

Cloud Data Security

Configurable policy-based scanning and automated response for cloud object storage

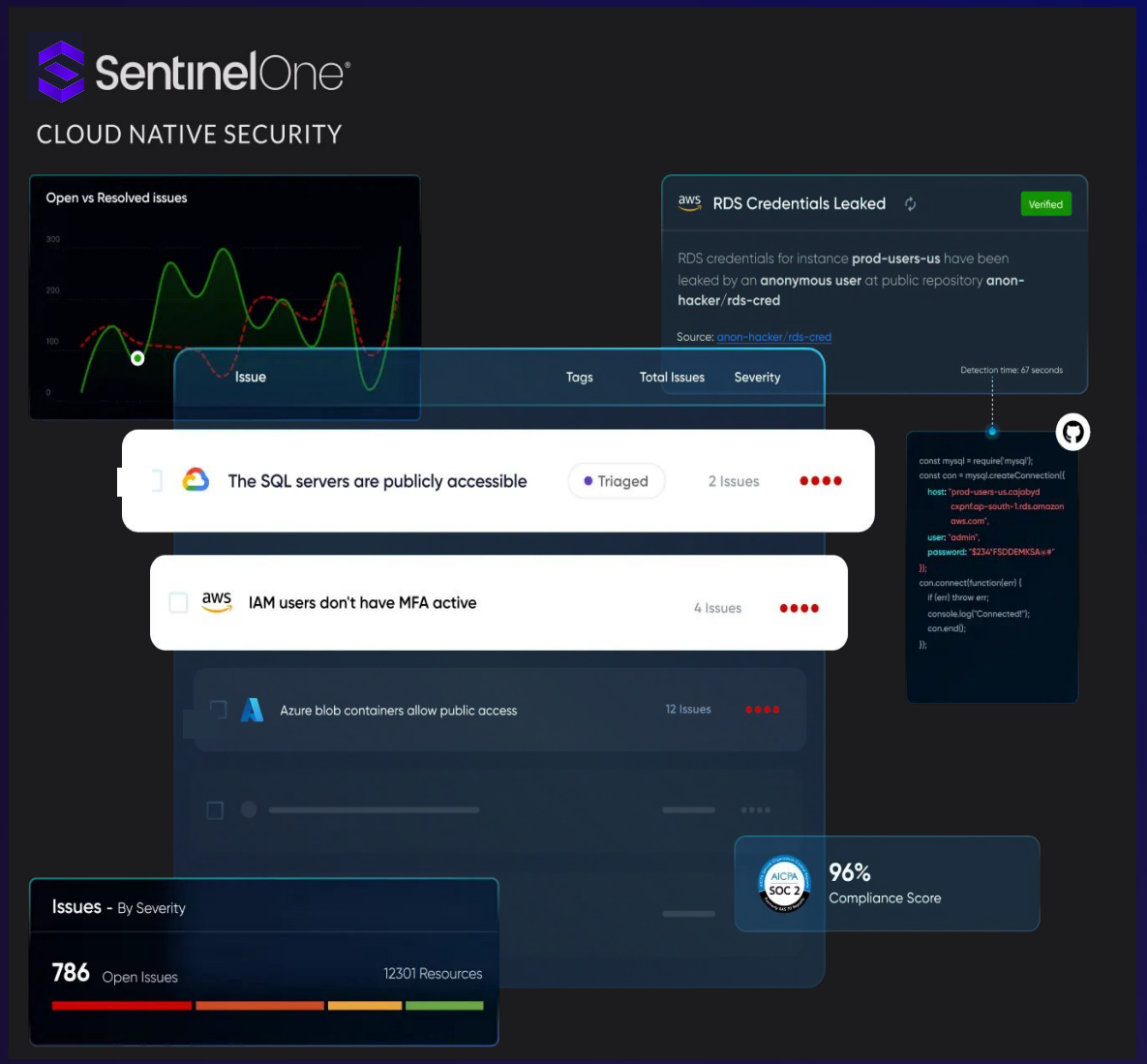
=

Our comprehensive CNAPP

SentinelOne

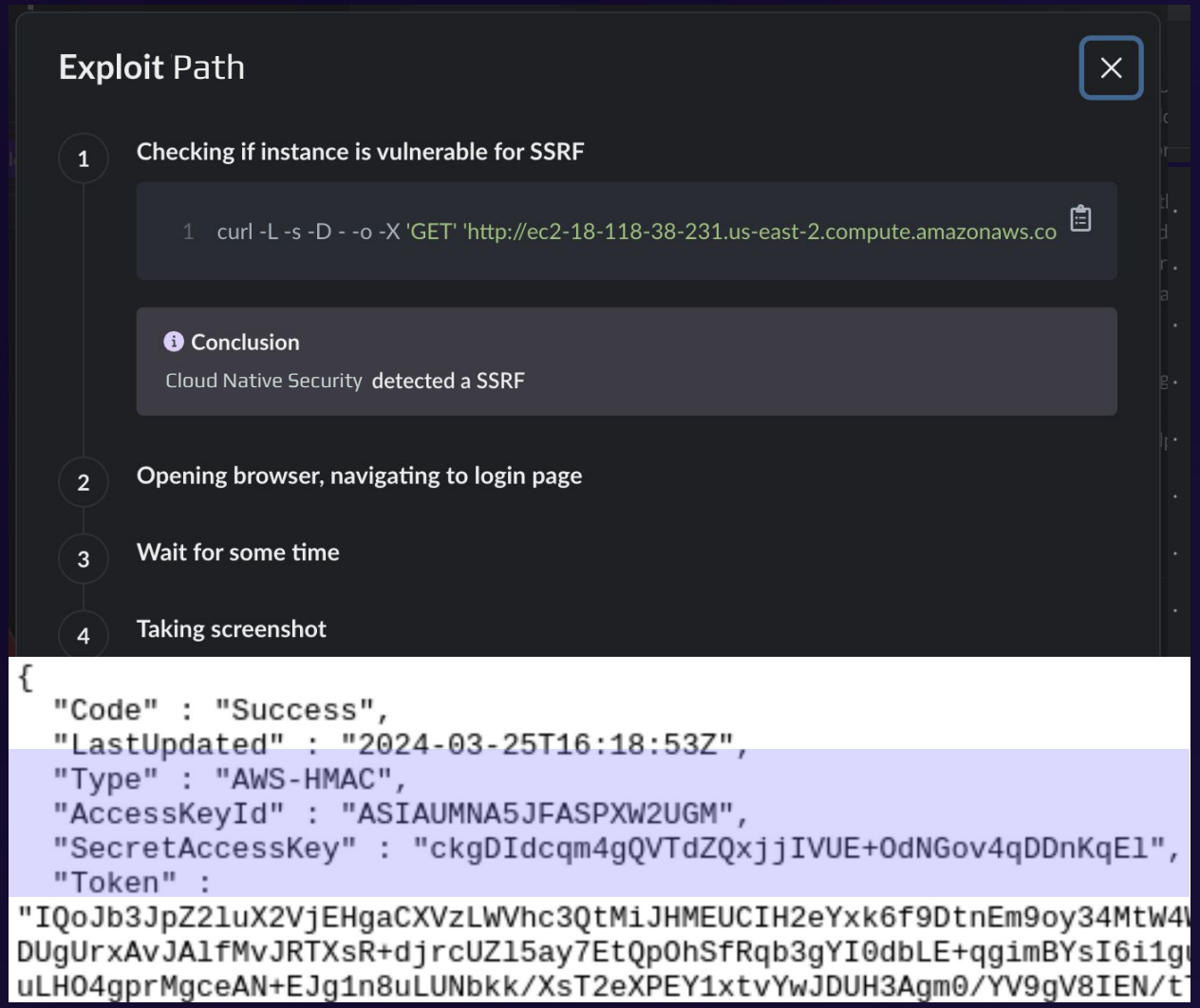
Cloud Native Security

- Vulnerability scanning
- Cloud security posture management (CSPM)
- Infrastructure as code (IaC) scanning
- Container and Kubernetes security
- Secrets scanning



SentinelOne

Offensive Security Engine



- Cloud-native security identifies attack paths; correlates publicly accessible assets with either vulnerable or misconfigured connected resources
- **Offensive security engine** then 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

SentinelOne

ISM and Essential 8

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government
Information Security Manual

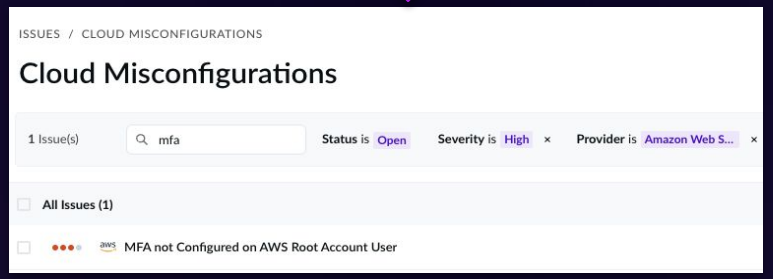
Australian Government
Australian Signals Directorate

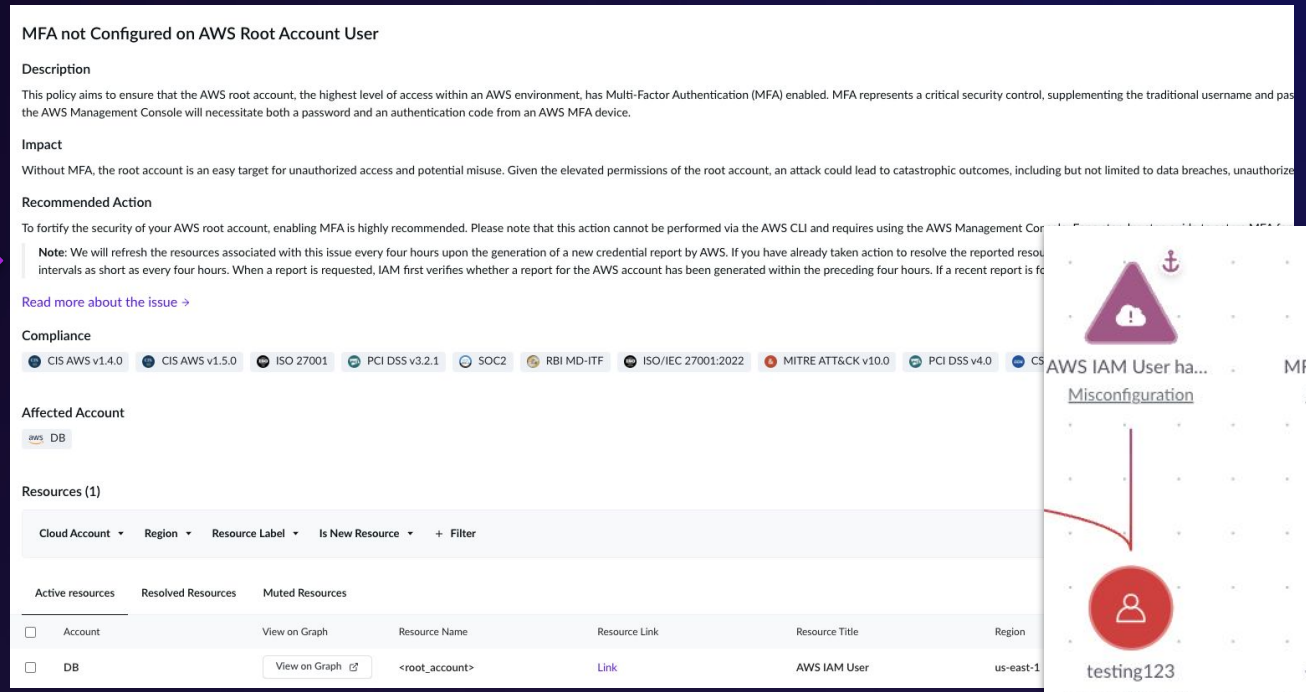
ACSC Australian Cyber Security Centre

Essential 8

Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML1, ML2, ML3
Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Multi-factor_authentication	root-account-mfa-enabled	Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA add an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts.





SentinelOne

Available via demonstration and Proof of Value

- Fast and agentless onboarding
- Discovering cloud inventory
- Context establishment
- Verified Exploit Paths

SentinelOne

Thank You