



# SentinelOne®

**Embrace the Attacker's  
Mindset:**

**Protecting Australian  
Organisations with an  
Offensive Cloud security  
strategy**



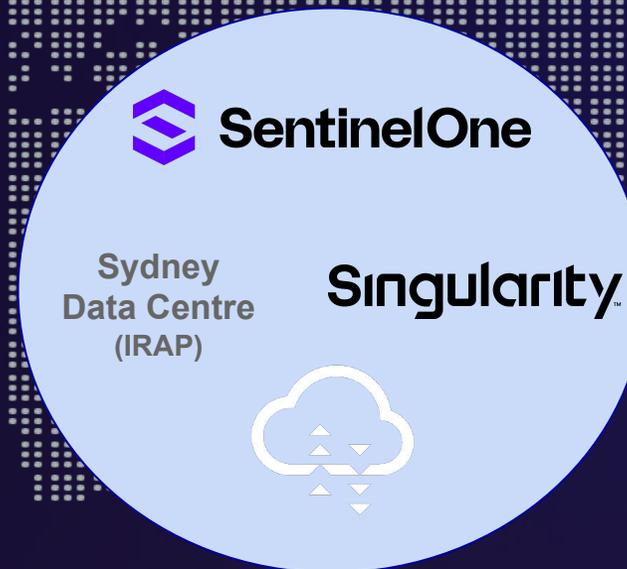
**SentinelOne is a Platform company.**  
**The world's most advanced cybersecurity platform.**

**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



# 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

# 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

# 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**



# 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

Initial Access 5 techniques	Execution 5 techniques	Persistence 7 techniques	Privilege Escalation 5 techniques	Defense Evasion 12 techniques	Credential Access 11 techniques	Discovery 14 techniques	Lateral Movement 5 techniques	Collection 5 techniques	Exfiltration 3 techniques	Impact 9 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain or Tenant Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (3)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)		Defacement (1)
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (3)	Network Sniffing	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal Application Access Token	Password Policy Discovery				Resource Hijacking
				Unused/Unsupported Cloud Regions	Steal or Forge Authentication Certificates	Permission Groups Discovery (1)				
				Use Alternate Authentication Material (2)	Steal Web Session Cookie	Software Discovery (1)				
				Valid Accounts (2)	Unsecured Credentials (3)	System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

# 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

```
FBot
Developed By: @J3mBotMaw0ttz
Contact: @buffer_0x0verfl0w

[WARNING] Use with caution. You are responsible for your actions
[WARNING] Developer assume no liability and are not responsible for any misuse or damage.
[INFO] Loading Bot List....
```

Choice Number	Bot Description
[1]	Random IP Address Generator [Custom Total]
[2]	Random IP Address Generator with IP Range [192.168.0.0-192.168.255.255]
[3]	HTTP IP Address Checker With Port Scanner [Port 80]
[4]	AWS API Key Generator [Custom Total]
[5]	Sendgrid API Key Generator [Custom Total]
[6]	Mass Laravel Validator [Get Laravel Site List]
[7]	Mass Laravel Database Scanner [Get PHPMyAdmin or Adminer Login]
[8]	Mass Laravel SMTP Scanner [Auto Test Send]
[9]	Mass Laravel Config Scanner [Get Laravel Config]
[10]	Mass Hidden Config Scanner [Get Misconfigure Config]
[11]	Mass CMS Scanner [Filter Site List by CMS]
[12]	Mass PHPUnit RCE Exploiter [Auto Upload Shell]
[13]	Mass Reverse IP Scanner [With Scrapystack API]
[14]	Mass Reverse IP Scanner [Unlimited Without Proxy]
[15]	Mass Reverse Domain to IP Address [Convert Domain to IP Address]
[16]	Mass Subdomain Enumeration Scanner [Unlimited Without Proxy]
[17]	Mass PayPal Email Validator [Live, Dead, Limited (Beta)]
[18]	Mass Email Validator [Check Email Validity]
[19]	Mass Twilio Checker [Format: PHONE_NUMBER ACCOUNT_SID TWILIO_CREDENTIALS]
[20]	Mass AWS Checker [Get Limit, Region, Account ID, Credentials, Identities]
[21]	Mass AWS EC2 Checker [Get EC2 Instance List]
[22]	Mass Sendgrid API Key Checker [Get Sendgrid API Key From Email]
[23]	Exit Program [Exit Bot]

```
[?] Enter Your Choice? [1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23]
```

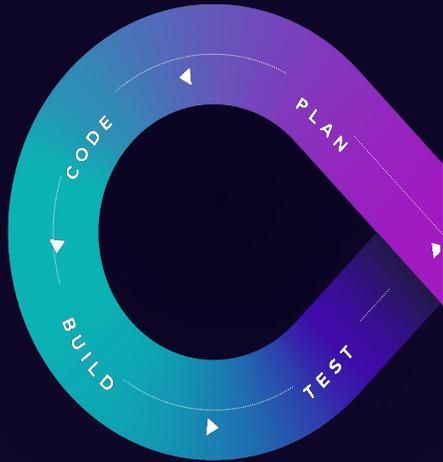


# Need to identify cloud security gaps



# 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**

# 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**

# 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**

# Cloud Native Security

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

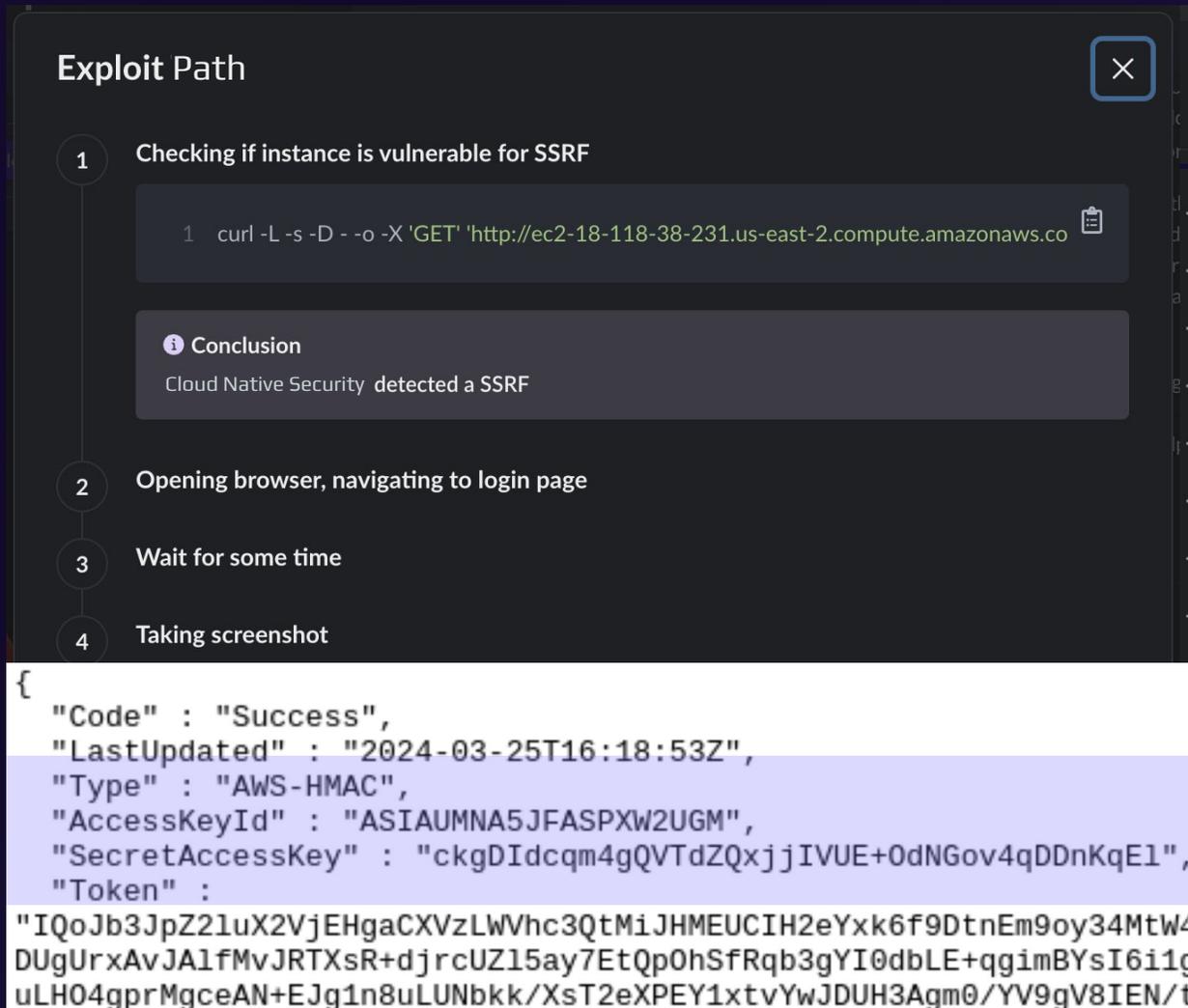
The image shows a screenshot of the SentinelOne Cloud Native Security dashboard. At the top left is the SentinelOne logo and the text "SentinelOne® CLOUD NATIVE SECURITY".

Key components of the dashboard include:

- Open vs Resolved Issues:** A line graph showing the number of open and resolved issues over time.
- Issue Cards:** Several cards displaying security alerts, such as:
  - aws RDS Credentials Leaked:** A verified issue where RDS credentials for instance `prod-users-us` were leaked by an `anonymous user` at a public repository `anon-hacker/rds-cred`. It includes a detection time of 67 seconds and a source link.
  - The SQL servers are publicly accessible:** A triaged issue with 2 total issues and a severity of 4 (indicated by 4 red dots).
  - aws IAM users don't have MFA active:** An issue with 4 total issues and a severity of 4.
  - Azure blob containers allow public access:** An issue with 12 total issues and a severity of 4.
- Code Snippet:** A snippet of JavaScript code for connecting to a MySQL database, with a red circle highlighting the password field: 

```
const mysql = require('mysql');
const con = mysql.createConnection({
  host: 'prod-users-us.cjabyd
  cxprf.ap-south-1.rds.amazonaws.com',
  user: 'admin',
  password: '$234/PSDDEMKSA**'
});
con.connect(function(err) {
  if (err) throw err;
  console.log('Connected!');
con.end();
});
```
- Compliance Score:** A badge indicating a 96% Compliance Score for AICPA SOC 2.
- Issues - By Severity:** A summary bar showing 786 Open Issues and 12301 Resources.

# Offensive Security Engine



The screenshot displays a window titled "Exploit Path" with a close button. It shows a sequence of four steps:

- 1 Checking if instance is vulnerable for SSRF**
  - Terminal command: `curl -L -s -D - -o -X 'GET' 'http://ec2-18-118-38-231.us-east-2.compute.amazonaws.co'`
  - Conclusion**: Cloud Native Security detected a SSRF
- 2 Opening browser, navigating to login page**
- 3 Wait for some time**
- 4 Taking screenshot**

Below the steps, a JSON response is shown:

```
{  
  "Code" : "Success",  
  "LastUpdated" : "2024-03-25T16:18:53Z",  
  "Type" : "AWS-HMAC",  
  "AccessKeyId" : "ASIAUMNA5JFASPXW2UGM",  
  "SecretAccessKey" : "ckgDI dcqm4gQVTdZQxjjIVUE+0dNGov4qDDnKqE1",  
  "Token" :  
  "IQoJb3JpZ21uX2VjEHgaCXVzLWVhc3QtMiJHMEUCIH2eYxk6f9DtnEm9oy34MtW4V  
  DUgUrxAvJA1fMvJRTXsR+djrcUZ15ay7EtQp0hSfRqb3gYI0dbLE+qgimBYsI6i1g  
  uLH04gprMgceAN+EJg1n8uLUNbkk/XsT2eXPEY1xtvYwJDUH3Agm0/YV9gV8IEN/t
```

- 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**

# ISM and 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 adds 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.

ISSUES / CLOUD MISCONFIGURATIONS

## Cloud Misconfigurations

1 Issue(s)    Search: mfa    Status is Open    Severity is High    Provider is Amazon Web S...

All Issues (1)

**aws** MFA not Configured on AWS Root Account User

### MFA not Configured on AWS Root Account User

**Description**  
This policy aims to ensure that the AWS root account, the highest level of access within an AWS environment, has Multi-Factor Authentication (MFA) enabled. MFA represents a critical security control, supplementing the traditional username and password with the AWS Management Console will necessitate both a password and an authentication code from an AWS MFA device.

**Impact**  
Without MFA, the root account is an easy target for unauthorized access and potential misuse. Given the elevated permissions of the root account, an attack could lead to catastrophic outcomes, including but not limited to data breaches, unauthorized access to sensitive information, and account takeover.

**Recommended Action**  
To fortify the security of your AWS root account, enabling MFA is highly recommended. Please note that this action cannot be performed via the AWS CLI and requires using the AWS Management Console.

**Note:** We will refresh the resources associated with this issue every four hours upon the generation of a new credential report by AWS. If you have already taken action to resolve the reported resource, we will refresh the report as short as every four hours. When a report is requested, IAM first verifies whether a report for the AWS account has been generated within the preceding four hours. If a recent report is found, we will refresh the report.

**Read more about the issue** →

**Compliance**  
CIS AWS v1.4.0    CIS AWS v1.5.0    ISO 27001    PCI DSS v3.2.1    SOC2    RBI MD-ITF    ISO/IEC 27001:2022    MITRE ATT&CK v10.0    PCI DSS v4.0    CIS AWS v1.5.0

**Affected Account**  
aws:DB

**Resources (1)**

Active resources	Resolved Resources	Muted Resources
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Account	View on Graph	Resource Name
DB	View on Graph	<root_account>
	Link	Resource Link
		Resource Title
		AWS IAM User
		Region
		us-east-1

AWS IAM User has MFA not Configured on AWS Root Account User

MFA not Configured on AWS Root Account User

testing123 AWS IAM User

<root\_account> AWS IAM User

# Available via demonstration and Proof of Value

Fast and agentless onboarding



Discovering cloud inventory



Context establishment



Verified Exploit Paths



**Thank You**