SentinelOne

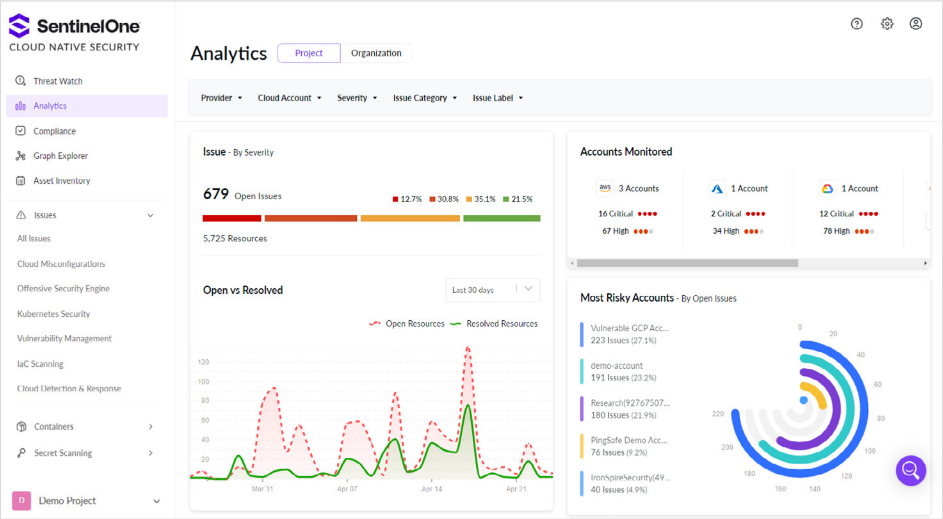
Cloud Native Security

Agentless CNAPP. Get started in moments, realize value in minutes.

More Signal, Less Noise. Better Outcomes.

Prior generations of cloud security solutions are noisy and inefficient, with data silos and poorly integrated solutions leading to wasted cycles chasing down alerts, context, and false positives. Threat actors find novel ways of infiltrating cloud infrastructure and deal serious damage to an organization's cloud footprint and business reputation. Far better to clearly highlight the most critical problems to address first, so that security teams can focus their attention and create better cloud security outcomes.

Cloud Native Security (CNS) is our agentless CNAPP that delivers multi-cloud insights spanning asset discovery, misconfigurations, vulnerability management, and more. It goes beyond simple attack path analysis, to automate red-teaming of identified issues and present evidence of exploitability. It cuts through noise and enhances collaboration, so that you can prioritize and solve faster.



Issue - By Severity

679 Open Issues

🟥 12.7% 🟥 30.8% 🟧 35.1% 🟩 21.5%

5,725 Resources

Accounts Monitored

aws 3 Accounts	1 Account	1 Account
16 Critical ●●●●	2 Critical ●●●●	12 Critical ●●●●
67 High ●●●	34 High ●●●	78 High ●●●

Most Risky Accounts - By Open Issues

Vulnerable GCP Acc...
223 Issues (27.1%)

demo-account
191 Issues (23.2%)

Research(92767507...
180 Issues (21.9%)

PingSafe Demo Acc...
76 Issues (9.2%)

IronSpireSecurity(49...
40 Issues (4.9%)

Cloud Native Security delivers multi-cloud support for:

aws

Azure

Google Cloud

ORACLE Cloud Infrastructure

Alibaba Cloud

DigitalOcean

Key Benefits

- Instant Visibility
- Connect in Minutes
- Stop Leaked Credentials
- Multi-Cloud Support
- Verified Exploit Paths™ for Better Prioritization
- Convenient Compliance Dashboards

PeerSpot

> “
>
> I've used [other CNAPPs]. CNS significantly reduced false positives and detection time. I'm always happy to recommend CNS.
>
> CISO
> SOFTWARE COMPANY

Verified Exploit Paths™

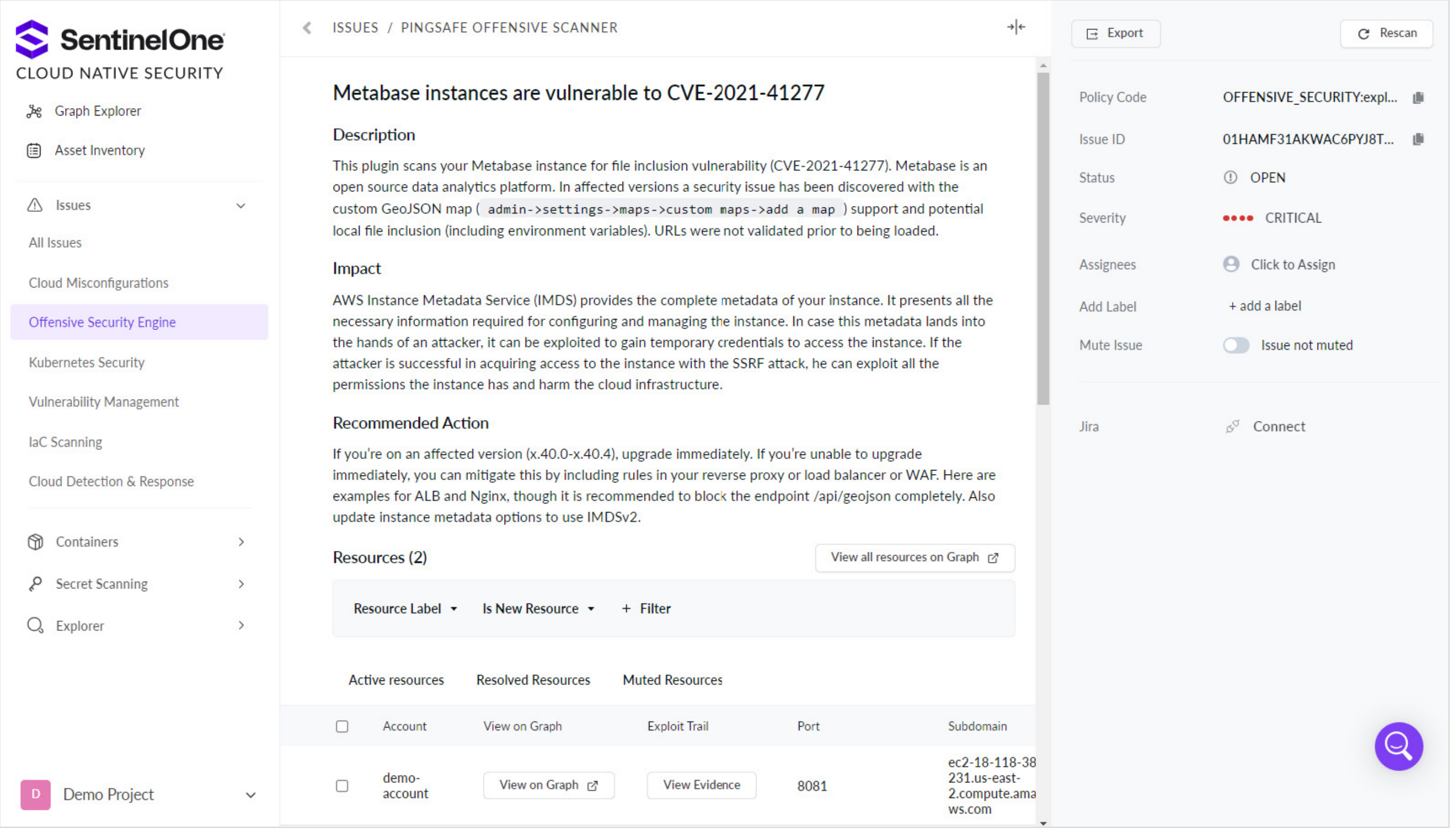
A primary challenge facing securing teams is sifting through the thousands of critical alerts created across multiple cloud security tools to find which ones are the ones which are most vital to improving risk posture. CNS goes beyond theoretical attack path analysis, to safely and automatically probe issues identified by our agentless CNAPP, and present evidence of exploitability.

> Evidence of exploitability is created, evidence which helps to differentiate the truly critical alerts from the theoretical possible attack scenarios.

By using these Verified Exploit Paths, security teams can better prioritize their security backlog and more effectively collaborate cross-functionally, to solve the most important issues first and optimize the business' cloud risk posture.

PeerSpot

> “
>
> The offensive security feature is something no one else offers.
>
> Cloud Security Engineer
>
> FINANCIAL SERVICES, 10K+ EMPLOYEES



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
□	demo-account	View on Graph	View Evidence	8081	ec2-18-118-38231.us-east-2.compute.ama ws.com

Policy Code	OFFENSIVE_SECURITY:expl...
Issue ID	01HAMF31AKWAC6PYJ8T...
Status	OPEN
Severity	●●●● CRITICAL
Assignees	Click to Assign
Add Label	+ add a label
Mute Issue	Issue not muted
Jira	Connect

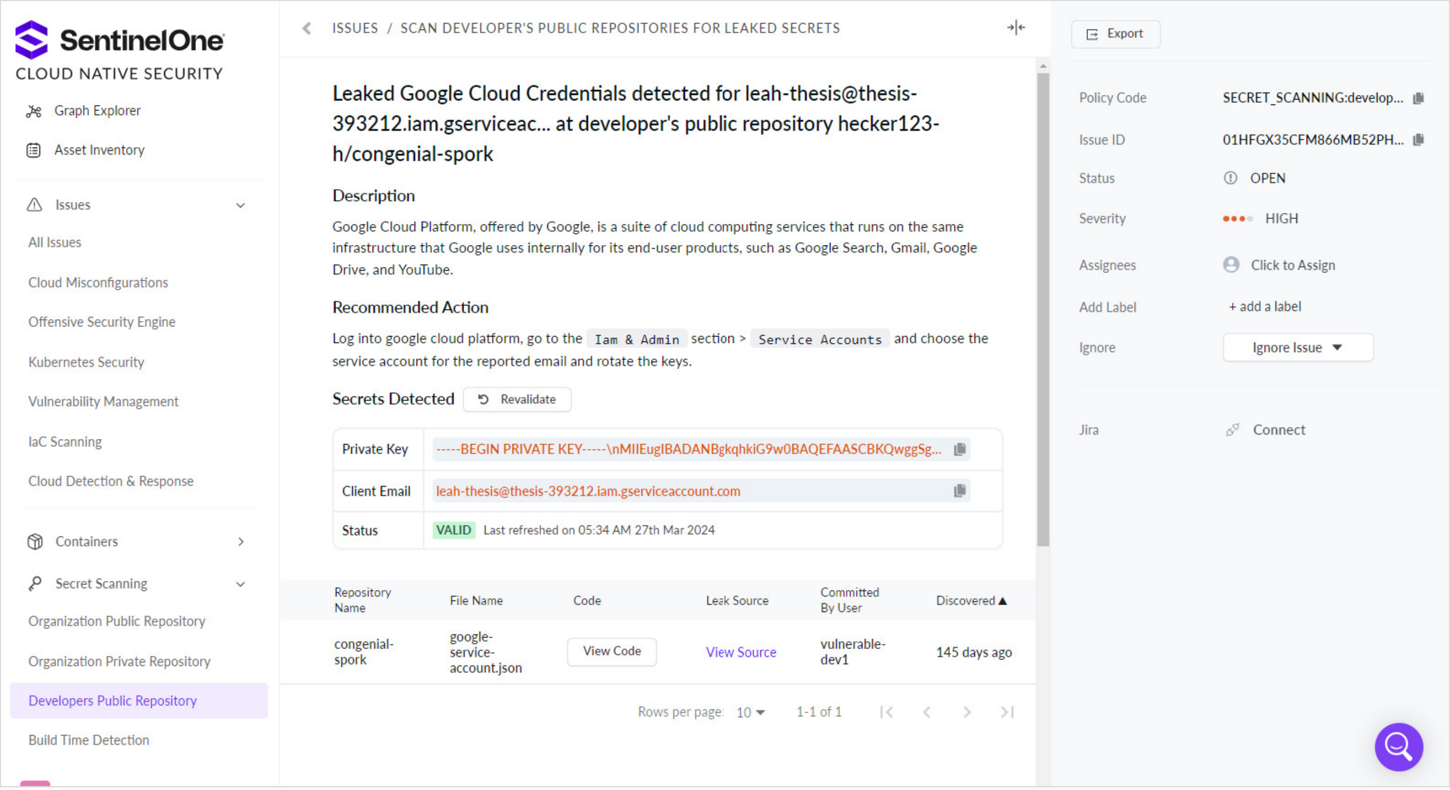
Secrets Scanning

Another exciting capability within CNS is its Secrets Scanning, which can identify well over 750 distinct types of secrets and credentials hardcoded across code repositories. Compromised credentials such as these remain one of the primary causes of cloud security failures, providing a point of entry for threat actors who have automated means of notification when such credentials are posted in clear text to code repositories. Said another way, attackers use the credentials and secrets to simply login, not hack in, to your cloud accounts. CNS periodically scans public and private repositories for the organization, as well as public repositories of associated developers, to prevent leakage of secrets and credentials.

71%

YoY increase in attacks using credentials

IBM X-Force Threat Intelligence Index 2024



Leaked Google Cloud Credentials detected for leah-thesis@thesis-393212.iam.gserviceac... at developer's public repository hecker123-h/congenial-spork

Description

Google Cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, Google Drive, and YouTube.

Recommended Action

Log into google cloud platform, go to the `Iam & Admin` section > `Service Accounts` and choose the service account for the reported email and rotate the keys.

Secrets Detected

Private Key	-----BEGIN PRIVATE KEY-----\nMIIEugIBADANBgkqhkiG9w0BAQEFAASCBKQwggSg...
Client Email	leah-thesis@thesis-393212.iam.gserviceaccount.com
Status	VALID Last refreshed on 05:34 AM 27th Mar 2024

Repository Name	File Name	Code	Leak Source	Committed By User	Discovered ▲
congenial-spork	google-service-account.json	View Code	View Source	vulnerable-dev1	145 days ago

Rows per page: 10 1-1 of 1

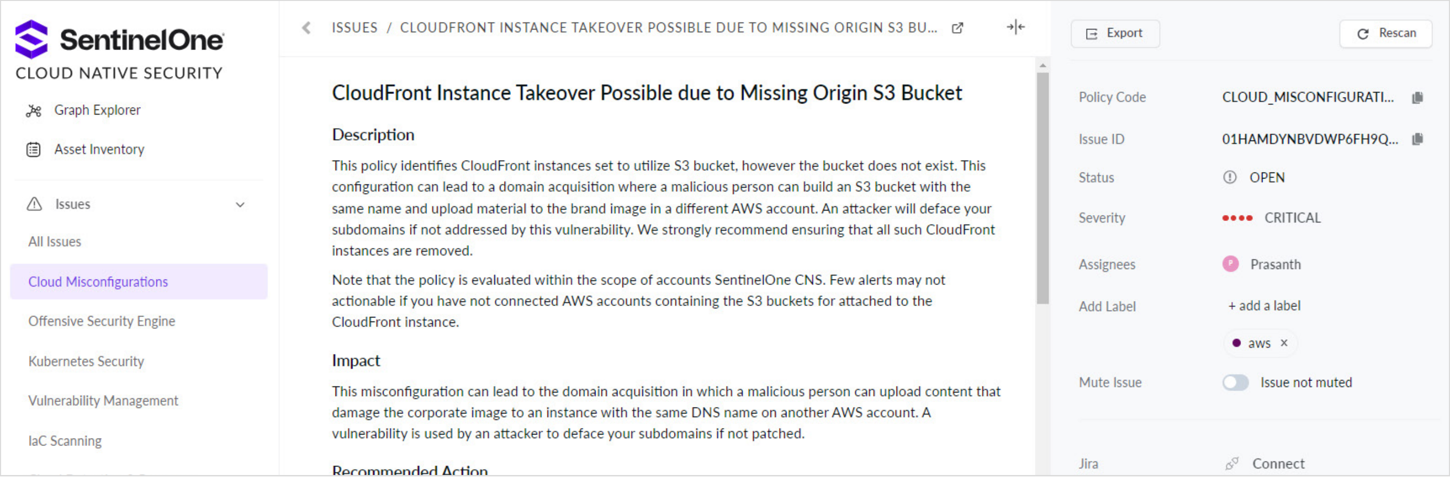
Policy Code	SECRET_SCANNING:develop...
Issue ID	01HFGX35CFM866MB52PH...
Status	OPEN
Severity	HIGH
Assignees	Click to Assign
Add Label	+ add a label
Ignore	Ignore Issue
Jira	Connect

CSPM

CSPM (Cloud Security Posture Management) pinpoints misconfigured cloud resources and ensures compliance to industry standards. Agentless onboarding creates an asset inventory within minutes of connecting to a cloud account. With over 2,000 checks built-in, CNS ensures that any newly instantiated and misconfigured cloud resource – be it a cloud compute instance, container, etc – is identified in near-real time.

Users can create custom policies via simple rego scripts, to cover compliance requirements unique to your organization.

And of course, easy-to-understand dashboards provide a real-time compliance score to multiple standards such as NIST, CIS, MITRE and more.



CloudFront Instance Takeover Possible due to Missing Origin S3 Bucket

Description

This policy identifies CloudFront instances set to utilize S3 bucket, however the bucket does not exist. This configuration can lead to a domain acquisition where a malicious person can build an S3 bucket with the same name and upload material to the brand image in a different AWS account. An attacker will deface your subdomains if not addressed by this vulnerability. We strongly recommend ensuring that all such CloudFront instances are removed.

Note that the policy is evaluated within the scope of accounts SentinelOne CNS. Few alerts may not actionable if you have not connected AWS accounts containing the S3 buckets for attached to the CloudFront instance.

Impact

This misconfiguration can lead to the domain acquisition in which a malicious person can upload content that damage the corporate image to an instance with the same DNS name on another AWS account. A vulnerability is used by an attacker to deface your subdomains if not patched.

Recommended Action

Policy Code	CLOUD_MISCONFIGURATI...
Issue ID	01HAMDYNBVDWP6FH9Q...
Status	OPEN
Severity	CRITICAL
Assignees	Prasanth
Add Label	+ add a label aws ×
Mute Issue	Issue not muted
Jira	Connect

KSPM

Kubernetes is a widely-adopted container orchestration platform, notorious for overly promiscuous configurations that create unique security challenges for containerized workloads. Enter Kubernetes Security Posture Management. KSPM goes well beyond CSPM which is ill-suited to the intricacies of Kubernetes network configurations and interpod communications.

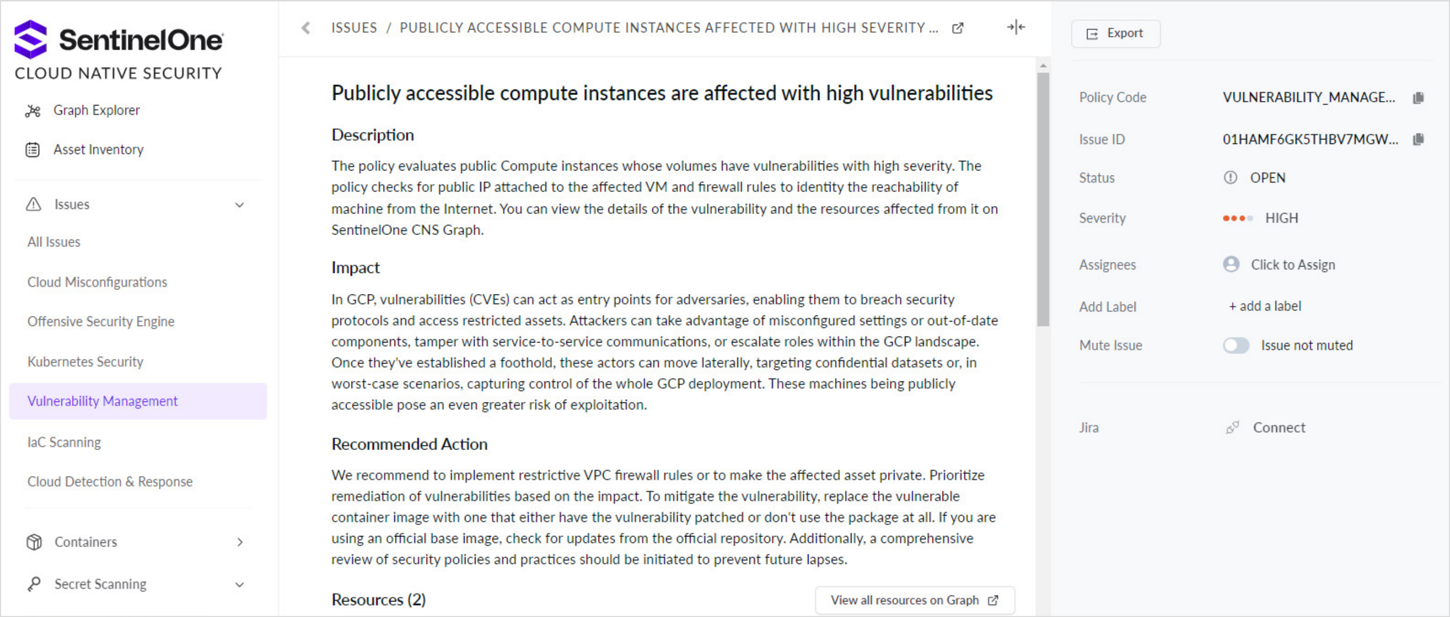
The KSPM capabilities within Cloud Native Security deliver comprehensive visibility into workloads, nodes, pods, containers, and the Kubernetes API, enabling continuous monitoring and evaluation of your Kubernetes security stance. CNS offers insights into your compliance posture, encompassing CIS Benchmarks for EKS, GKE, and AKS, the managed K8s services from the 3 leading cloud service providers, as well as the CIS Kubernetes Framework. With SentinelOne, customers may craft cluster-security policies, pinpointing overly permissive roles, and detecting namespaces lacking proper labeling to enforce Kubernetes-specific pod security standards.

Vulnerability Scanning

Vulnerabilities in container images can lead to unauthorized access, data leakage, and more. To more easily manage risk, CNS now includes vulnerability scanning of container images within your ECS & EKS clusters. The solution creates a software bill of materials (SBOM), which is a detailed inventory of components, libraries, and dependencies within a container. Moreover, CNS delivers graph-based visualization of K8s clusters, business services, and images.

Together these capabilities:

- Streamline compliance and auditing
- Pinpoint services and images requiring immediate attention
- Clarify relationships among components
- Improve prioritization



Publicly accessible compute instances are affected with high vulnerabilities

Description

The policy evaluates public Compute instances whose volumes have vulnerabilities with high severity. The policy checks for public IP attached to the affected VM and firewall rules to identity the reachability of machine from the Internet. You can view the details of the vulnerability and the resources affected from it on SentinelOne CNS Graph.

Impact

In GCP, vulnerabilities (CVEs) can act as entry points for adversaries, enabling them to breach security protocols and access restricted assets. Attackers can take advantage of misconfigured settings or out-of-date components, tamper with service-to-service communications, or escalate roles within the GCP landscape. Once they've established a foothold, these actors can move laterally, targeting confidential datasets or, in worst-case scenarios, capturing control of the whole GCP deployment. These machines being publicly accessible pose an even greater risk of exploitation.

Recommended Action

We recommend to implement restrictive VPC firewall rules or to make the affected asset private. Prioritize remediation of vulnerabilities based on the impact. To mitigate the vulnerability, replace the vulnerable container image with one that either have the vulnerability patched or don't use the package at all. If you are using an official base image, check for updates from the official repository. Additionally, a comprehensive review of security policies and practices should be initiated to prevent future lapses.

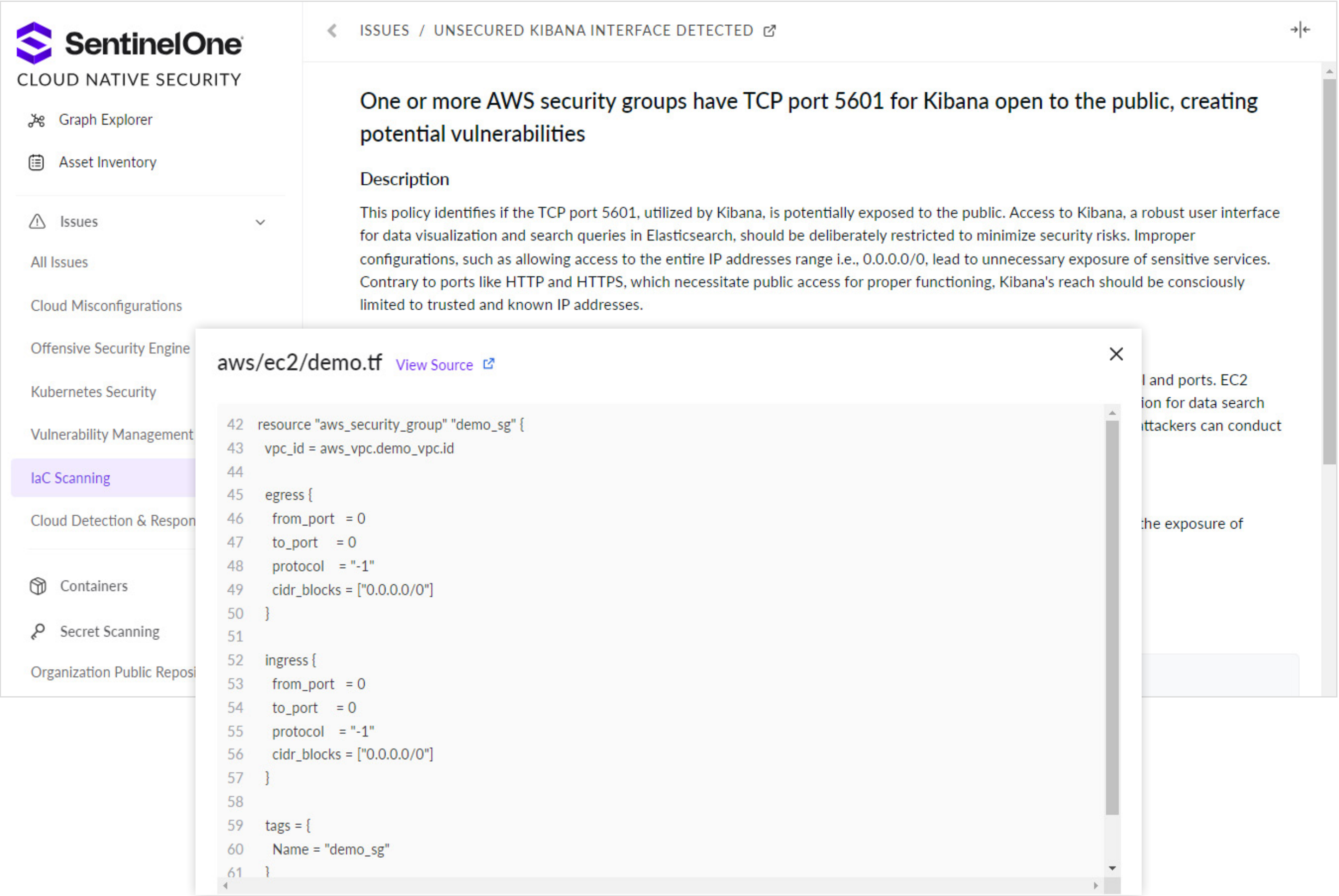
Resources (2)

Policy Code	VULNERABILITY_MANAGE...
Issue ID	01HAMF6GK5THBV7MGW...
Status	OPEN
Severity	●●●○ HIGH
Assignees	Click to Assign
Add Label	+ add a label
Mute Issue	Issue not muted
Jira	Connect

For example, consider a publicly accessible cloud compute instance, such as an Amazon EC2, Azure VM, or Google Cloud Compute Engine. Now, there are potentially perfectly valid reasons for having a public internet-facing compute instance. However, if such instances are running with high severity vulnerabilities, with widely available exploit packages, then SecOps will want to prioritize response action, such as updating the host OS image, to resolve the vulnerability before it is exploited. Moreover, Graph Explorer (discussed in a section below) can streamline the investigation, visualizing the relationship between a misconfiguration and vulnerability.

Infrastructure as Code (IaC) Scanning

Golden IaC templates are a great means of preventing resource misconfigurations from entering the DevOps pipeline, by providing consistent, repeatable, and appropriate configurations codified according to best practices. The IaC scanning capabilities within CNS shifts security left, to scan templates and pinpoint misconfigurations before they reach production. CNS identifies pre-production issues in IaC templates and container configuration files like Terraform, CloudFormation, and Kubernetes (both Helm and manifests).



One or more AWS security groups have TCP port 5601 for Kibana open to the public, creating potential vulnerabilities

Description

This policy identifies if the TCP port 5601, utilized by Kibana, is potentially exposed to the public. Access to Kibana, a robust user interface for data visualization and search queries in Elasticsearch, should be deliberately restricted to minimize security risks. Improper configurations, such as allowing access to the entire IP addresses range i.e., 0.0.0.0/0, lead to unnecessary exposure of sensitive services. Contrary to ports like HTTP and HTTPS, which necessitate public access for proper functioning, Kibana's reach should be consciously limited to trusted and known IP addresses.

l and ports. EC2
ion for data search
ttackers can conduct

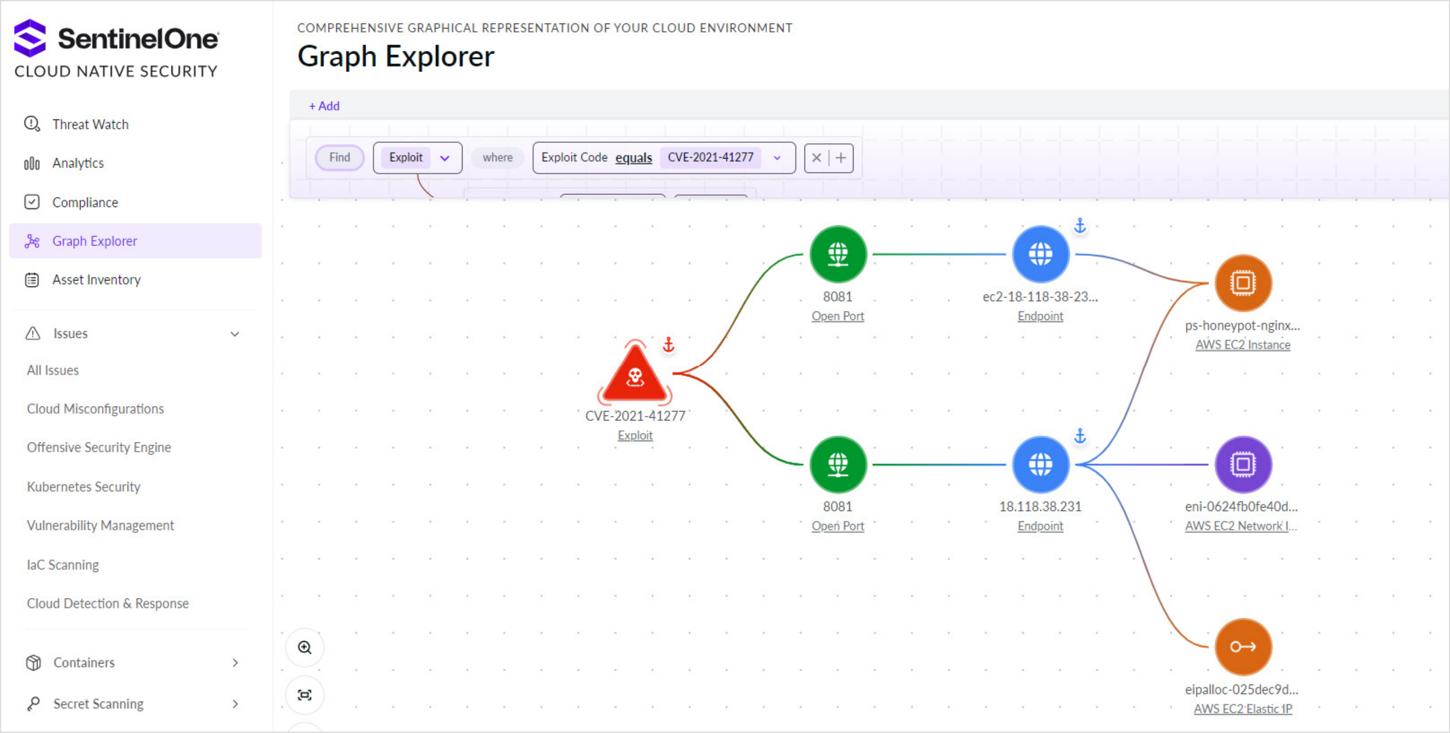
the exposure of

aws/ec2/demo.tf

```
resource "aws_security_group" "demo_sg" {
  vpc_id = aws_vpc.demo_vpc.id

  egress {
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }

  ingress {
    from_port   = 0
    to_port     = 0
    protocol    = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }

  tags = {
    Name = "demo_sg"
  }
```

Graph Explorer

Graph Explorer facilitates investigation of Verified Exploit Paths through visual analysis of the potential blast radius of cloud resources affected by an identified vulnerability. It also includes a convenient means of intuitively writing queries via the visual interface, to quickly create and apply custom policies to a specific resource group with a few simple clicks.



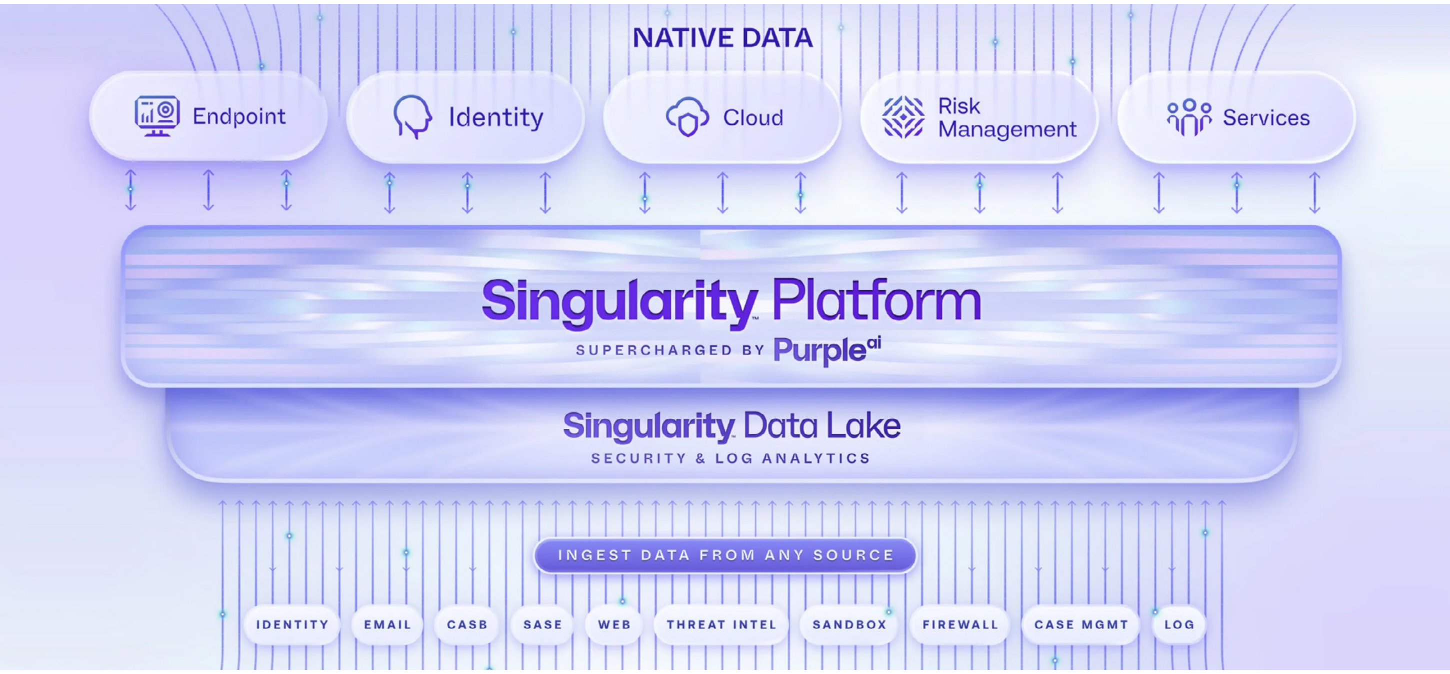
COMPREHENSIVE GRAPHICAL REPRESENTATION OF YOUR CLOUD ENVIRONMENT

Graph Explorer

Find Exploit where Exploit Code equals CVE-2021-41277

Cloud Security in The Singularity™ Platform

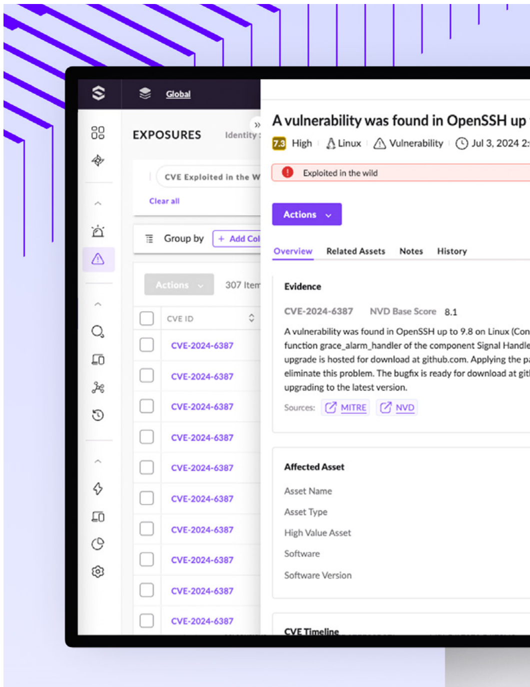
The Singularity™ Platform offers comprehensive threat prevention, detection, and response that is easy to use and which spans across complex enterprise environments.



Singularity™ integrates SentinelOne's high-performance security solutions spanning endpoint (EDR, Endpoint Detection & Response), cloud (CNAPP, Cloud Native Application Protection Platform), and identity (ITDR, Identity Threat Detection & Response). An enterprise can combine and customize these native solutions to their specifications, all managed from a single console and security data lake.

Security practitioners need visibility into ALL relevant, actionable events from the entire enterprise security estate to enrich investigations with necessary context and provide a means to hunt across alerts from cross-telemetry data sources. To address this need, the Singularity™ Platform leverages a centralized security data lake, ingesting telemetry from both SentinelOne-native endpoint, cloud and identity solutions as well as an ever-growing list of 3rd-party security tools and sources used by our customers. The Singularity™ Data Lake provides SecOps practitioners the ability to contextually visualize and automatically respond to any high-value security alerts by leveraging a single, cloud-scale repository that offers the greatest retention period and cost efficiency of any vendor in the market.

Used by some of the industry's largest and most respected IR and MDR partners, the Singularity™ Platform delivers immediate time-to-value, ensuring a future-proof solution that will continuously evolve to meet the growing cybersecurity needs of our customers.



A vulnerability was found in OpenSSH up

Exploited in the wild

Evidence

CVE-2024-6387 NVD Base Score 8.1

A vulnerability was found in OpenSSH up to 9.8 on Linux (Con
function grace_alarm_handler of the component Signal Handle
upgrade is hosted for download at github.com. Applying the pa
eliminate this problem. The bugfix is ready for download at git
upgrading to the latest version.

Affected Asset

Asset Name
Asset Type
High Value Asset
Software
Software Version

CVE Timeline

Cloud Native Security Packaging

Feature	Foundations	Pro
Cloud Misconfigurations & Compliance (CSPM)	✓	✓
Vulnerability Scanning (agentless)	✓	✓
Security Graph	✓	✓
Container and K8s Security (KSPM)	✓	✓
Verified Exploit Paths™	✓	✓
Cloud Detection & Response (CDR)	✓	✓
Secret Scanning (Public + Private)		✓
IaC Scanning		✓
Auto Remediation + Integration with Web Hooks		✓

Singularity™ Platform

Proactively resolve threats in real-time at the site of the cybersecurity battle: the computing and cloud edge.

Ready for a Demo?
Visit SentinelOne.com for more details.

Innovative. Trusted. Recognized.

MITRE ENGENUITY.

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

PeerSpot

98% willing to recommend

CNAPP ranks highly in customer satisfaction, innovation, and performance

Gartner. Peer Insights.

97% of Gartner Peer Insights™

CNAPP Reviewers Recommend Singularity Cloud Security By SentinelOne

FedRAMP

TEVORA
PCI DSS Attestation
HIPAA Attestation

AICPA SOC

STAR LEVEL ONE

VB 100 VIRUS

SE Labs BEST Innovator WINNER 2021

SE Labs AAA

Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733