sysdig

How to keep you (multi) cloud environments safe

Mateo Burillo

Product Manager - Sysdig Secure

CSPM, CWPP, CIEM, CNAPP, QWERTY, ASDP@1

Let’s start with some definitions

- Intimidating at first, but they are the same security concepts you are already familiar with
  - Slightly modified and adapted to the new stack
- Quote for Gartner: “Through 2025, 99% of cloud security failures will be the customer’s fault.”
- How do we extend the concepts of configuration hardening, security perimeter or anomaly detection to the cloud?

CSPM

Tool that unifies the use cases that protect the *cloud control plane*, track *cloud resources*, and verify the *static configuration of the cloud*.

> According to Gartner, Through 2025, 99% of cloud security failures will be the customer's fault.

Gartner®

CIEM

Focuses on ***managing and reducing the risk*** *of excessive permissions* and entitlements in the cloud

> **According to Gartner, 75% of security failures will result from inadequate management of identities, access, and privileges by 2023, up from 50% in 2020**

Gartner®

CWPP

Platform that unifies the use cases that would ***enable*** security-focused teams to ***reduce cloud risk*** by addressing numerous potential threats in their cloud workloads.

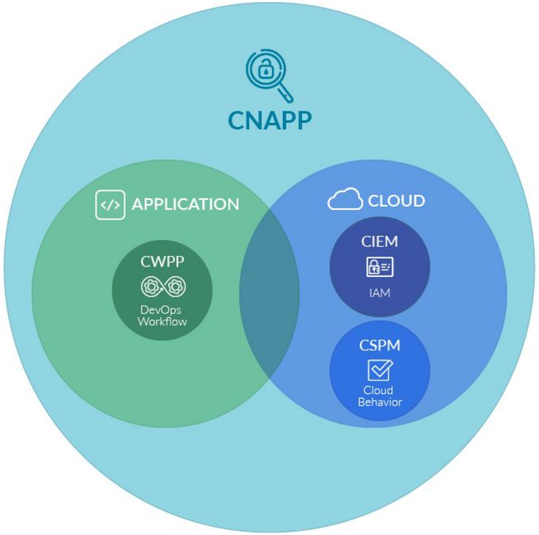
> **According to Gartner, By 2022, at least 25% of DevOps processes will utilize developer-driven by declarative intent-based policies, enabling developers to define and configure validated security controls for enhancing application and workload security (up from just under 5% in 2020)**

Gartner®

sysdig

CNAPP

Unify *cloud security on an end-to-end basis by tying together siloed views of risk so organizations can assess and address security gaps*



Cloud Security Requires a New Approach

Software Vulnerabilities

Managing Configs and Permissions

Detecting Threats

Meeting Compliance

>99% of cloud breaches will have a root cause of misconfigurations or mistakes through 2025”[1]

88% of cloud identities are non-human[2]

73% of accounts have public S3 buckets[2]

Traditional tools cannot keep up with cloud native

Source: 1) Gartner Report 2) Sysdig 2022 Container Usage Report

sysdig

Cloud provider’s security services

Disparate offering…where to start?

May not be enough

- ✓ Do you still have physical data centers?
- ✓ Do you work in multi-cloud environments?
- ✓ Is your cloud journey still uncertain?
- ✓ Filling the gaps that CSPs leave empty

Unify and simplify: same tool, same concepts

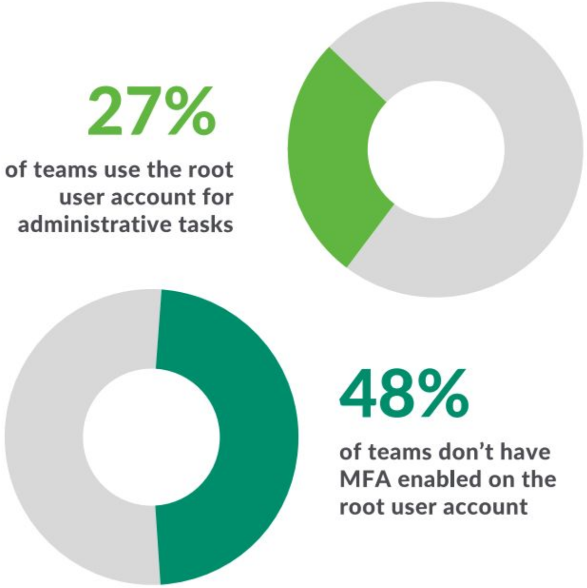
Container/K8s	Cloud
Image scanning	Cloud security (CSPM)
Runtime security	Threat detection
Incident response	Incident response
Monitoring & troubleshooting	Monitoring & troubleshooting

← Continuous compliance (PCI, NIST, etc.) →

CSPM Best Practices

Cloud Misconfigurations

- Lock down cloud control plane
- Conduct risk assessments at planned intervals
- Perform security awareness training



27%

of teams use the root user account for administrative tasks

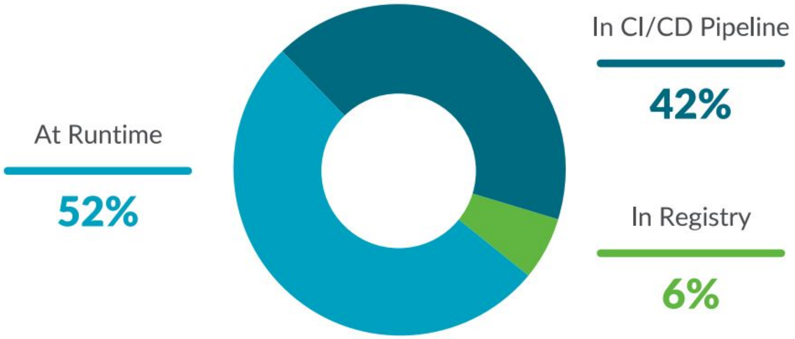
48%

of teams don't have MFA enabled on the root user account

Protect the New Perimeter of the Cloud

- Restrict Network Access
- Enable VPC Logs for VPC Subnets
- You need to detect unusual activity

Where Images are Scanned

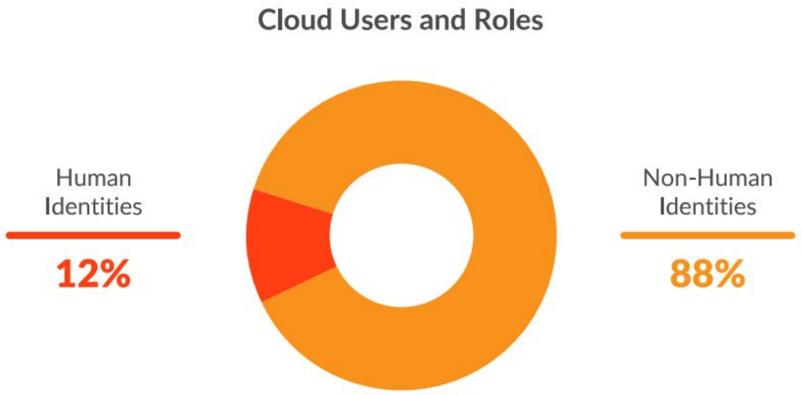


CSPM Example and demo

sysdig

Apply IAM Best Practices

- Apply the Principle of Least Privilege access
- Evaluate privileges and flag any that may be excessive
- Centralize identity and access wherever possible



CIEM example and demo

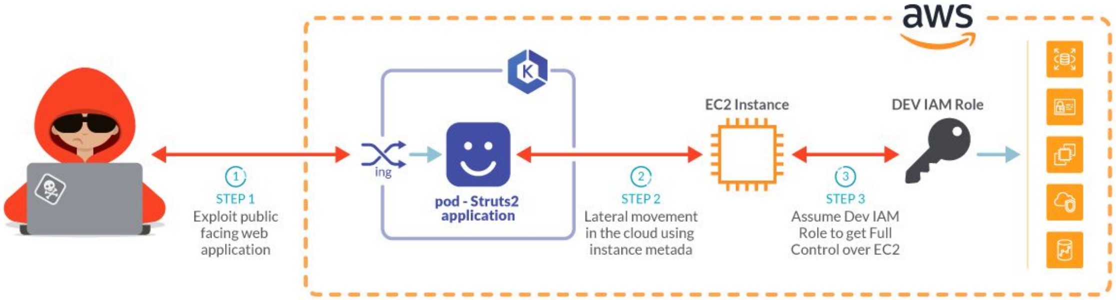
sysdig

Cloud Security Monitoring with Falco

sysdig

Get Real Time Visibility with Falco

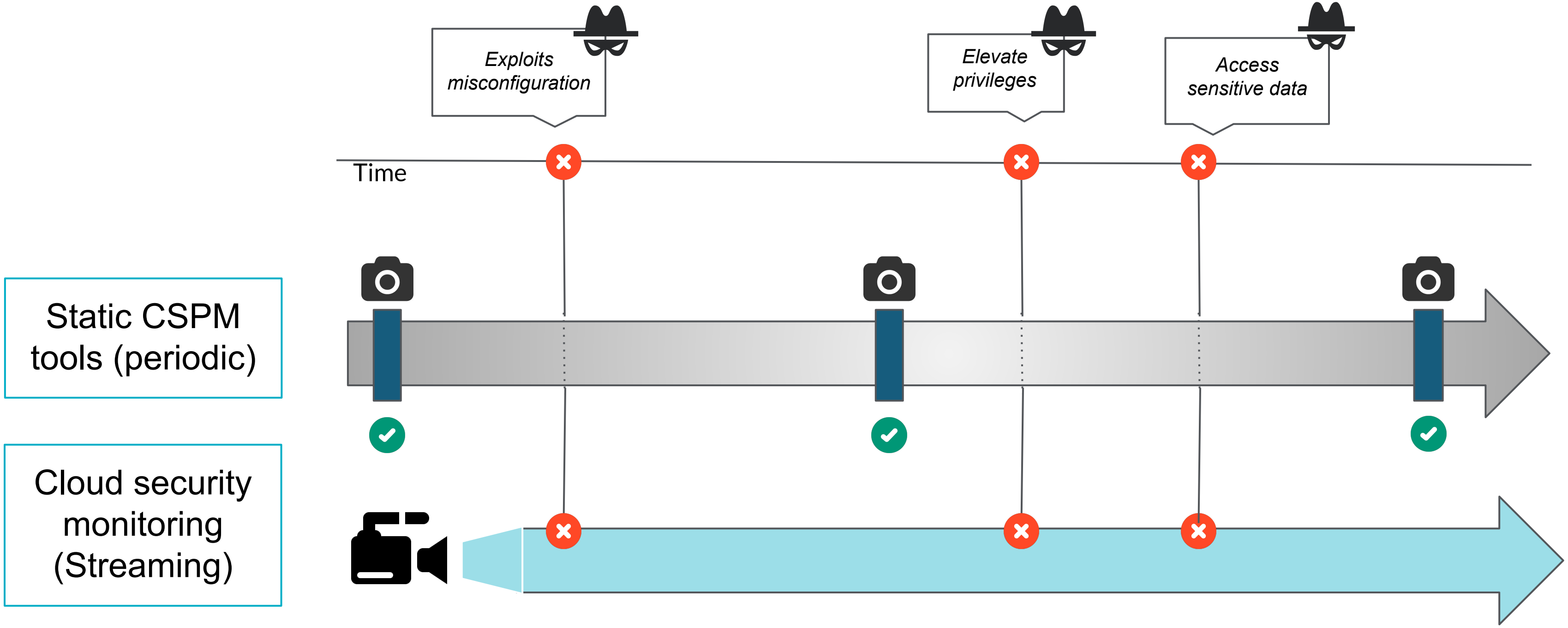
- Monitor configuration changes
- Detect unusual behavior
- Uncover data exfiltration



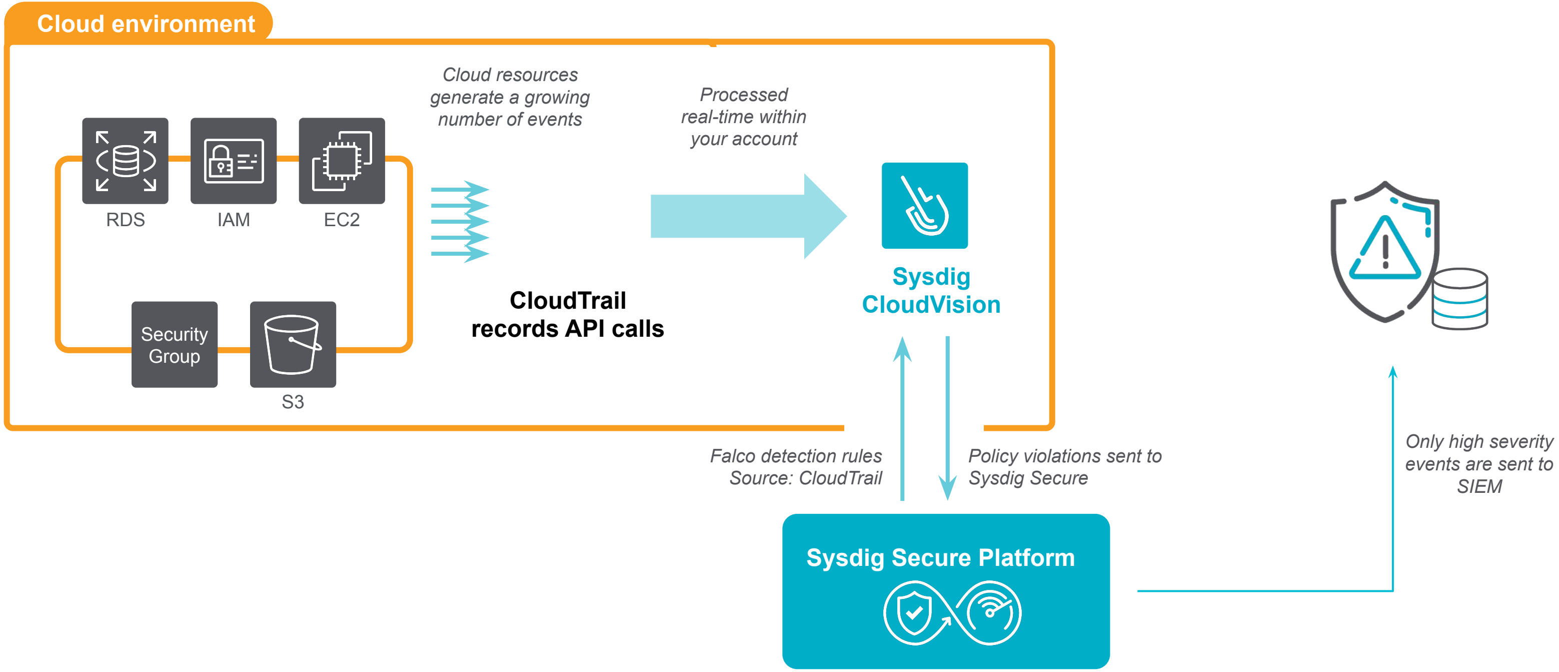
aws
1
STEP 1
Exploit public facing web application
ing
pod - Struts2 application
2
STEP 2
Lateral movement in the cloud using instance metada
EC2 Instance
3
STEP 3
Assume Dev IAM Role to get Full Control over EC2
DEV IAM Role

CWPP Example and demo

Periodic Snapshots vs Streaming Detection


Exploits misconfiguration
Elevate privileges
Access sensitive data
Time
Static CSPM tools (periodic)
Cloud security monitoring (Streaming)

Reduce SIEM costs



Cloud resources generate a growing number of events

CloudTrail records API calls

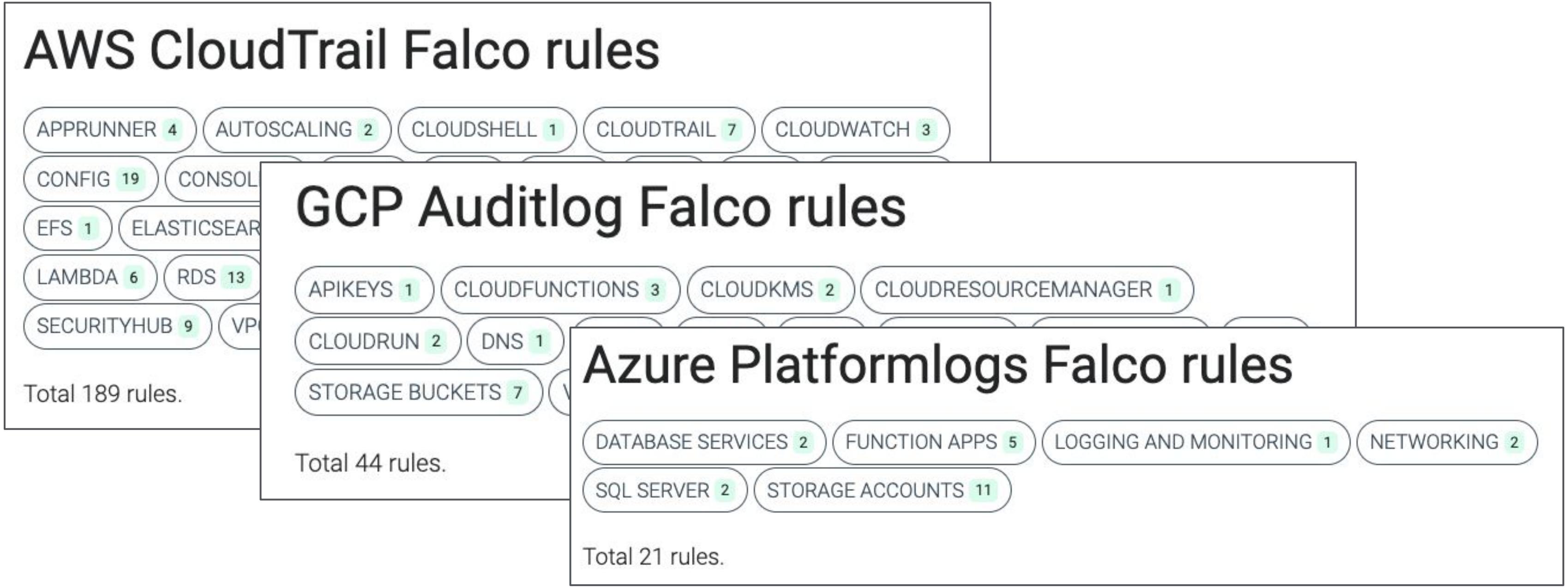
Processed real-time within your account

Falco detection rules Source: CloudTrail

Policy violations sent to Sysdig Secure

Only high severity events are sent to SIEM

Get Real Time Visibility with Falco



AWS CloudTrail Falco rules

APPRUNNER 4 | AUTOSCALING 2 | CLOUDSHELL 1 | CLOUDTRAIL 7 | CLOUDWATCH 3

CONFIG 19 | CONSOL

EFS 1 | ELASTICSEAR

LAMBDA 6 | RDS 13

SECURITYHUB 9 | VP

Total 189 rules.

GCP Auditlog Falco rules

APIKEYS 1 | CLOUDFUNCTIONS 3 | CLOUDKMS 2 | CLOUDRESOURCEMANAGER 1

CLOUDRUN 2 | DNS 1

STORAGE BUCKETS 7 | V

Total 44 rules.

Azure Platformlogs Falco rules

DATABASE SERVICES 2 | FUNCTION APPS 5 | LOGGING AND MONITORING 1 | NETWORKING 2

SQL SERVER 2 | STORAGE ACCOUNTS 11

Total 21 rules.

https://cloudsec.sysdig.com/

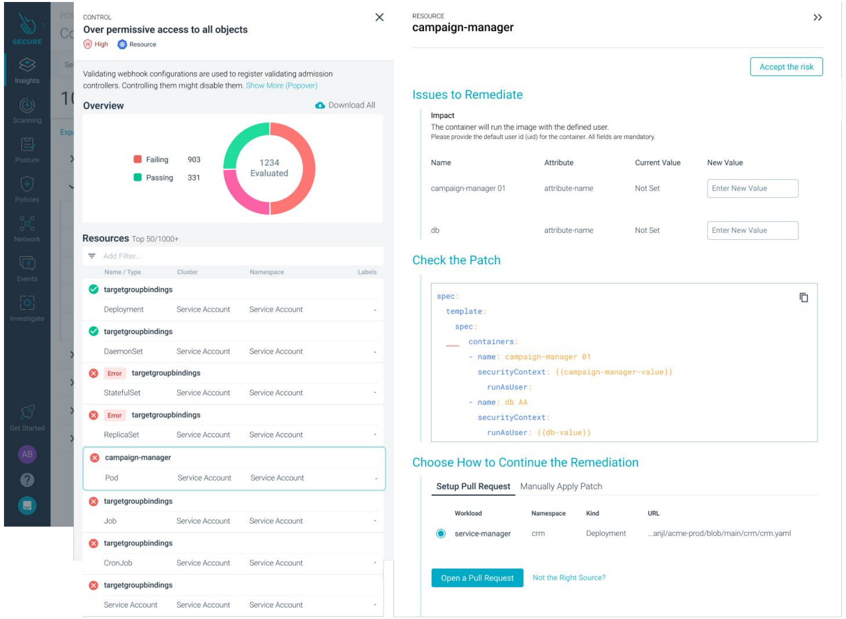
sysdig

Where do we go from here?

sysdig

Guided Remediation

- Sysdig will directly connect to the source definitions
- Fix the runtime but also declarative files!
- Automatically open PRs with pre-computed patches



CONTROL

Over permissive access to all objects

High Resource

Validating webhook configurations are used to register validating admission controllers. Controlling them might disable them. Show More (Popover)

Overview

🟥 Failing	903
🟩 Passing	331

Resources Top 50/1000+

Name / Type	Cluster	Namespace	Labels
✓ targetgroupbindings			
Deployment	Service Account	Service Account	-
✓ targetgroupbindings			
DaemonSet	Service Account	Service Account	-
✗ Error targetgroupbindings			
StatefulSet	Service Account	Service Account	-
✗ Error targetgroupbindings			
ReplicaSet	Service Account	Service Account	-
✗ campaign-manager			
Pod	Service Account	Service Account	-
✗ targetgroupbindings			
Job	Service Account	Service Account	-
✗ targetgroupbindings			
CronJob	Service Account	Service Account	-
✗ targetgroupbindings			
Service Account	Service Account	Service Account	-

RESOURCE

campaign-manager

Issues to Remediate

Impact

The container will run the image with the defined user.

Please provide the default user id (uid) for the container. All fields are mandatory.

Name	Attribute	Current Value	New Value
campaign-manager 01	attribute-name	Not Set	Enter New Value
db	attribute-name	Not Set	Enter New Value

Check the Patch

```
spec:
  template:
    spec:
      containers:
      - name: campaign-manager 01
        securityContext: {{campaign-manager-value}}
          runAsUser:
      - name: db AA
        securityContext:
          runAsUser: {{db-value}}
```

Choose How to Continue the Remediation

	Workload	Namespace	Kind	URL
●	service-manager	crm	Deployment	...anjl/acme-prod/blob/main/crm/crm.yaml

sysdig

Seeing is Securing