Falco, Cloud Connector y seguridad cloud

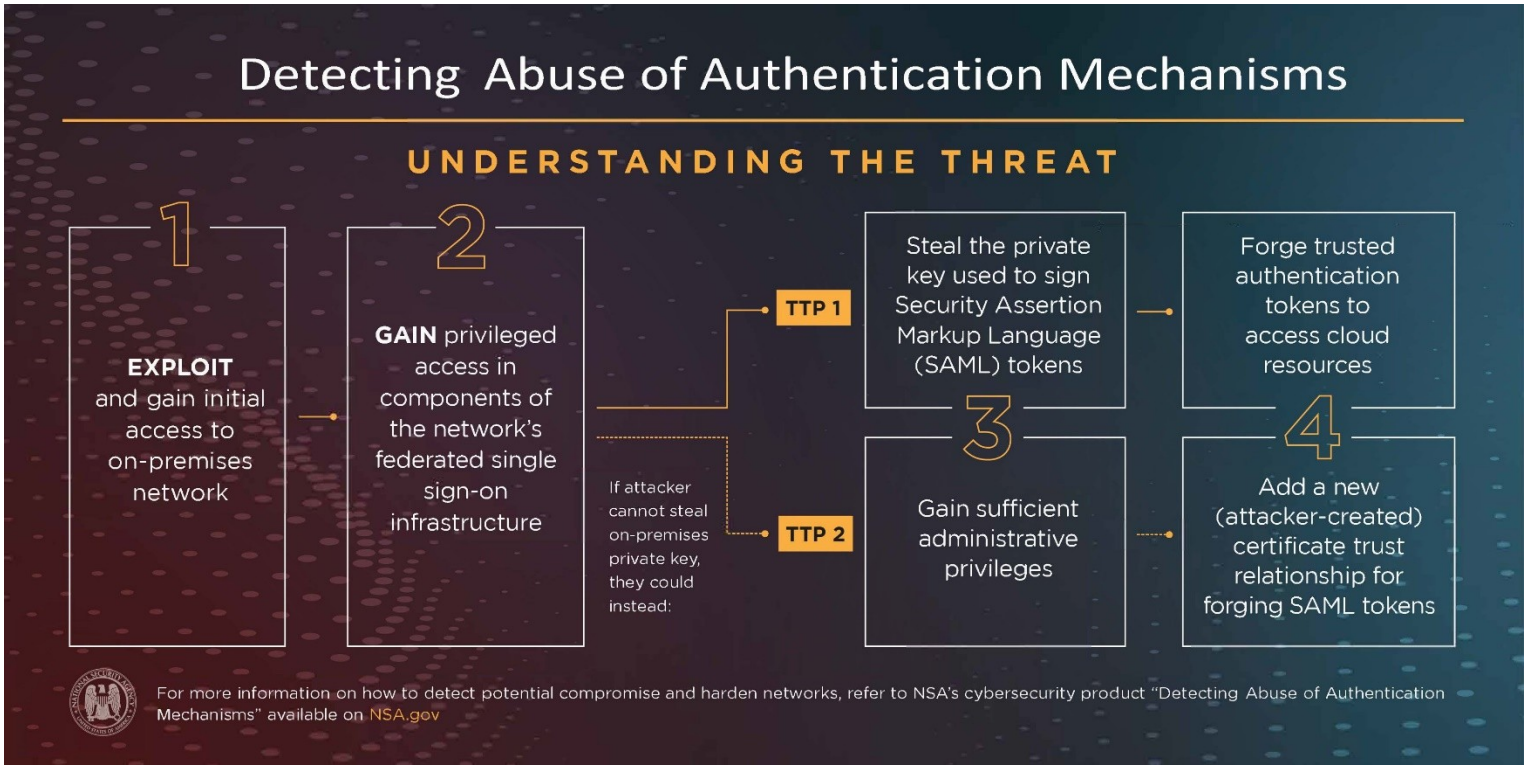
Cloud Connector con Falco: Seguridad runtime en cloud AWS

¿Qué es seguridad Cloud?

- Detectar el uso de recursos Cloud de uso no intencionado
- Salvaguarda en caso de fallos de seguridad en mecanismos de autenticación de cuentas Cloud, errores de configuración, permisos y roles demasiado permisivos, etc.
- Un actor malicioso podría:
  - Crear recursos de computación con coste
  - Emplear recursos de computación existentes, disminuyendo rendimiento
  - Acceder y exfiltrar datos privados
  - Cifrar y destruir datos, interrumpir procesos de trabajo

Caso: Solarwinds

- Hack a Solarwinds Orion en 2020
  - Orion: Gestión de redes, utilizada por Microsoft, US Army, NSA, US Treasury, 425 empresas de la lista Fortune 500
  - SVR (antigua KGB), objetivo espionaje
  - “Supply chain attack”, instalan backdoor en Orion
  - Comprometen sistema on-premise de autenticación Single Sign On en cloud, falsifican tokens de autenticación
  - Persistencia, movimiento lateral, búsqueda de información
- https://www.bankinfosecurity.com/nsa-warns-over-hacking-tactics-that-target-cloud-resources-a-15635



https://www.bankinfosecurity.com/nsa-warns-over-hacking-tactics-that-target-cloud-resources-a-15635

¿Qué es Cloud Connector?

- Detección de eventos de seguridad runtime en Cloud
  - Los eventos se detectan en cuanto ocurren:
    - Creación de nuevos recursos no habituales, convertir recursos privados en públicos, eliminar encriptación de datos, crear recursos para exponer a Internet recursos internos.
  - Complementa a herramientas de análisis estático
- Proyecto de uso gratuito creado por Sysdig
  - De momento no es *open source*
- Compatible con:
  - AWS, soporte completo, despliegue con CloudFormation
  - *Google Cloud Platform, versión preliminar, despliegue Helm chart*
  - En desarrollo para *Azure*

QUANTIKA 14

Delete bucket encryption

Finding ID: 8121ae00-2cd2-415f-b66c-fd020396b3c5

CRITICAL

A encryption configuration for a bucket has been deleted (requesting user=arn:aws:iam::999999999999:user/user.name, requesting IP=85.85.13.13, AWS region=us-east-1, bucket=cloudconnector-demo)

Workflow status: New

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID
99999999999

Severity (normalized)
90

Created at
2020-09-09T15:37:37Z

Updated at
2020-09-09T15:37:37Z

Product name
Default

Severity label
CRITICAL

Company name
Personal

Types and Related Findings

Types: Unusual Behaviors

Resources

Resources detail: AWS::::Account:999999999999

Resource type	Resource ID
AwsAccount	AWS::::Account:999999999999

Groups | N. Virginia | Support

Hub > Findings

ings

Actions | Workflow status | Create insight

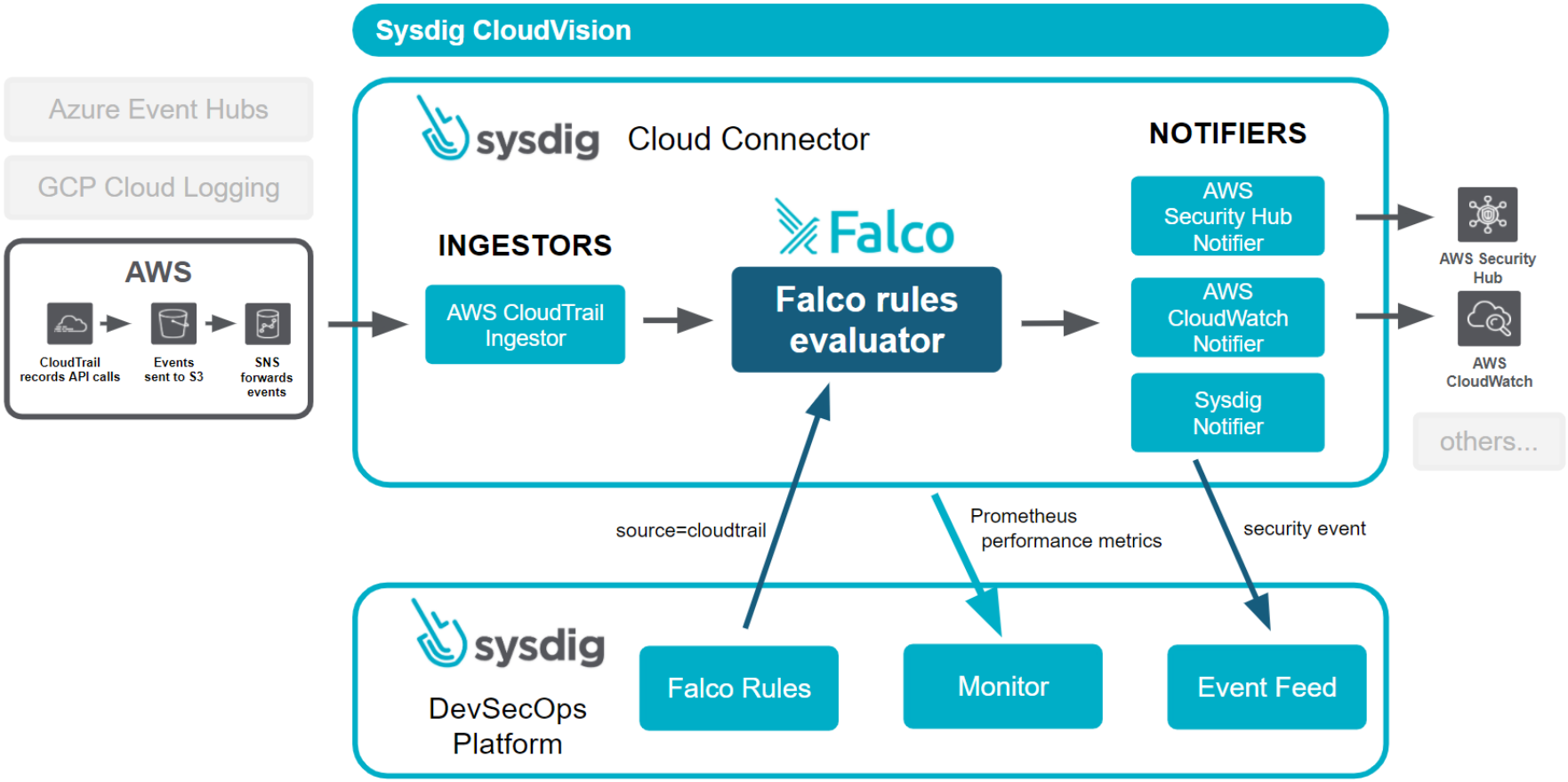
ing is a security issue or a failed security check.

Product name is Default | Workflow status is NEW | Workflow status is NOTIFIED | Record state is ACTIVE | Add filters

1 ...

Severity	Workflow status	Company	Product	Title	Resource ID	Resource type	Status	Updated at
MEDIUM	NEW	Personal	Default	Allocate a New Elastic IP Address to AWS Account	AWS::::Account:	AwsAccount		6 days ago
CRITICAL	NEW	Personal	Default	Delete bucket encryption	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an HTTP Target Group without SSL	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an Internet-facing AWS Public Facing Load Balancer	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an Internet-facing AWS Public Facing Load Balancer	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an HTTP Target Group without SSL	AWS::::Account:	AwsAccount		7 days ago
CRITICAL	NEW	Personal	Default	Delete bucket encryption	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Put inline policy in group to allow access to all resources	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an HTTP Target Group without SSL	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Create an HTTP Target Group without SSL	AWS::::Account:	AwsAccount		7 days ago
INFORMATIONAL	NEW	Personal	Default	Create an AWS user	AWS::::Account:	AwsAccount		7 days ago
MEDIUM	NEW	Personal	Default	Associate an Elastic IP Address to an AWS Network Interface	AWS::::Account:	AwsAccount		7 days ago

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use


Sysdig CloudVision
Azure Event Hubs
GCP Cloud Logging
AWS
CloudTrail records API calls
Events sent to S3
SNS forwards events
sysdig
Cloud Connector
INGESTORS
AWS CloudTrail Ingestor
Falco
Falco rules evaluator
NOTIFIERS
AWS Security Hub Notifier
AWS CloudWatch Notifier
Sysdig Notifier
AWS Security Hub
AWS CloudWatch
others...
source=cloudtrail
Prometheus performance metrics
security event
sysdig
DevSecOps Platform
Falco Rules
Monitor
Event Feed

Documentación Cloud Connector

- Documentación oficial: https://docs.sysdig.com/en/aws-cloud-auditing-with-sysdig-cloud-connector.html

- Documentación proyecto: https://sysdiglabs.github.io/cloud-connector/
  - Instalación: https://sysdiglabs.github.io/cloud-connector/deployment-cloudformation.html
  - Listado de reglas incluidas: https://sysdiglabs.github.io/cloud-connector/rules/cloudtrail.html
- Artículo de Blog https://sysdig.com/blog/aws-threat-detection-cloudtrail/

Instalación de Cloud Connector en AWS

- Activar AWS Security Hub
- Desplegar plantilla CloudFormation
- AWS tarda 10 minutos aproximadamente en activar CloudTrail y comenzar a enviar eventos
- Una vez funcionando, los eventos se detectan rápidamente