

What is Sigma?


Sigma is...

an open source, SIEM agnostic framework used to write rules for analyzing logs.

https://github.com/SigmaHQ/sigma

But Why?

Open Source FTW

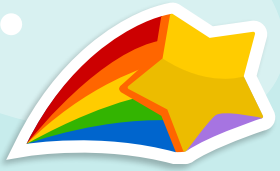
Everyone can contribute!

Sharing is Caring

Easy way to share threat detections regardless of platform/SIEM

YAML

You can never get enough YAML amirite LOL (especially Eric) (it's his favorite)



Sigma Rule

```yaml
title: AWS Root Credentials
id: 8ad1600d-e9dc-4251-b0ee-a65268f29add
status: test
description: Detects AWS root account usage
references:
    - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
author: vitaliy0x1
date: 2020/01/21
modified: 2022/10/09
tags:
    - attack.privilege_escalation
    - attack.t1078.004
logsource:
    product: aws
    service: cloudtrail
detection:
    selection_usertype:
        userIdentity.type: Root
    selection_eventtype:
        eventType: AwsServiceEvent
    condition: selection_usertype and not selection_eventtype
falsepositives:
    - AWS Tasks That Require AWS Account Root User Credentials https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html
level: medium
```

Converted to an ElastAlert Rule

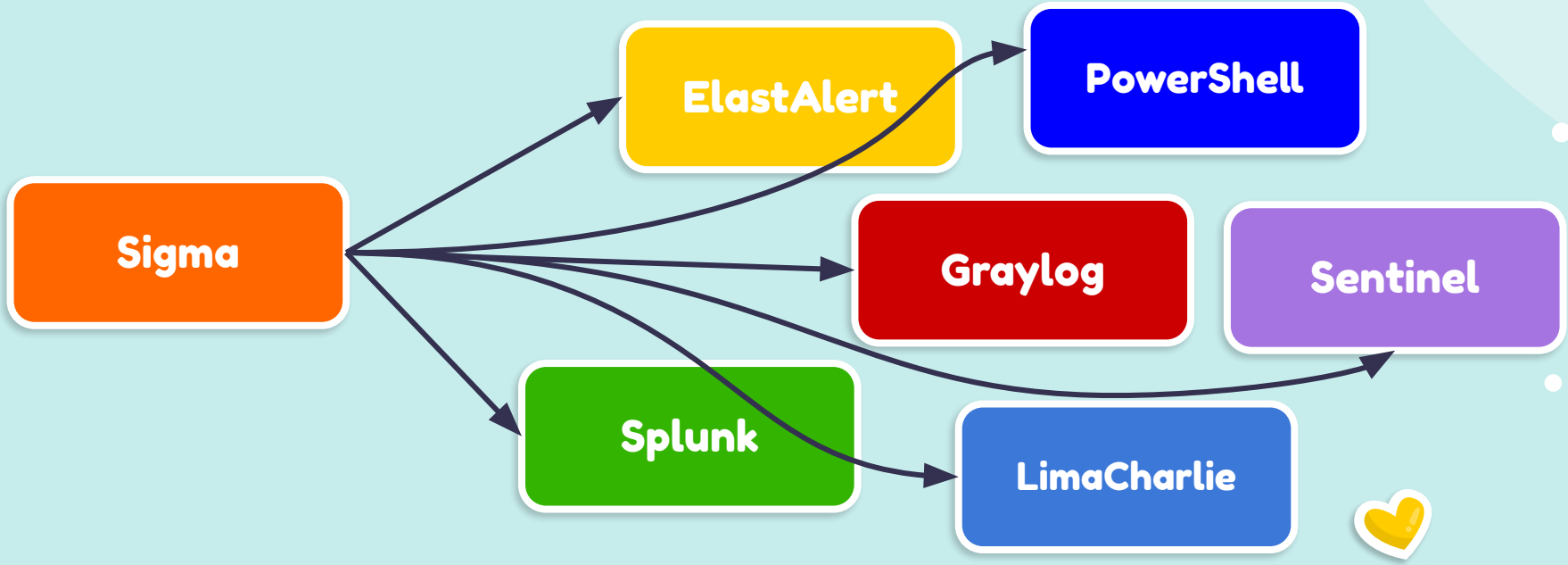
```
alert:
- post
description: Detects AWS root account usage
filter:
- query:
    query_string:
      query: (userIdentity.type:"Root" AND (NOT (eventType:"AwsServiceEvent")))
http_post_ignore_ssl_errors: true
http_post_static_payload:
  rule:
    description: Detects AWS root account usage
    id: 8ad1600d-e9dc-4251-b0ee-a65268f29add
    level: medium
    references:
    - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
    status: experimental
    title: AWS Root Credentials
  threat:
    tactic:
      name:
      - privilege_escalation
    technique:
      id:
      - t1078.004
http_post_url:
index:
is_enabled: true
name: AWS-Root-Credentials_0
priority: 3
realert:
  minutes: 0
timestamp_field: index_time
timestamp_type: iso
type: any
use_strftime_index: true
```

Converted to a LimaCharlie Rule

```yaml
version: 3
rules:
  AWS Root Credentials:
    detect:
      op: and
      rules:
      - case sensitive: false
        op: is
        path: event/userIdentity.type
        value: Root
      - case sensitive: false
        not: true
        op: is
        path: event/eventType
        value: AwsServiceEvent
      event: unknown
    respond:
    - action: report
      name: AWS Root Credentials
      metadata:
        tags:
        - attack.privilege_escalation
        - attack.t1078.004
        description: Detects AWS root account usage
        status: test
        id: 8ad1600d-e9dc-4251-b0ee-a65268f29add
        references:
        - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
        level: medium
        author: vitaliy0x1
        falsepositives:
        - AWS Tasks That Require AWS Account Root User Credentials https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html
        logsource: LimaCharlie
    is_enabled: true
```

Conversion Process

Supported Formats



...AND MOAR!!!

Hooray!

infosec.exchange/@shortstack
infosec.exchange/@recon_infosec