Scale Your Auditing Events

Philipp Krenn

@xeraa
This is fine.
No silver bullet
AUDITD

https://github.com/linux-audit
"auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk. Viewing the logs is done with the ausearch or aureport utilities."
Monitor

File and network access
System calls
Commands run by a user
Security events
DEMO
UNDERSTANDING LOGS

More Rules

https://github.com/linux-audit/audit-userspace/tree/master/rules
Namespaces WIP

https://github.com/linux-audit/audit-kernel/issues/32#issuecomment-395052938
Problem

How to centralize?
Disclaimer

I build **HIGHLY** monitored Hello World apps
ELK Stack!
Get it?

E
Elasticsearch

L
Logstash

K
Kibana
Apparently, I’m an ELKB personality.
Filebeat Module: Auditd
Demo
AUDITBEAT
Auditd Module

- Correlate related events
- Resolve UUIDs to user names
- Native Elasticsearch integration
Auditd Module

eBPF powers on older kernels
Easier configuration
Written in Golang
This PR enhances `add_docker_metadata` with the ability to enrich events containing process IDs.

The processor uses cgroup membership data from `/proc/pid/cgroup` to determine if the process is running inside of a Docker container. It caches the PID -> CID mapping for 5 minutes (based on time of last access).

The default configuration sets `match_pids: [process.pid, process.ppid]`. It falls back to the PPID in case the process has exited before the processing occurs.
GO-LIBAUDIT

https://github.com/elastic/go-libaudit

go-libaudit is a library for communicating with the Linux Audit Framework
System Module

Easier configuration for host, process, socket, user

Added in 6.6 — not based on Auditd
Demo
File Integrity Module

inotify (Linux)
fsevents (macOS)
ReadDirectoryChangesW (Windows)
hash_types

blake2b_256, blake2b_384, blake2b_512, md5, sha1, sha224, sha256, sha384, sha512, sha512_224, sha512_256, sha3_224, sha3_256, sha3_384, sha3_512, xxh64
Elastic SIEM
- **key**: ecs
  
  **title**: ECS
  
  **description**: ECS Fields.
  
  **fields**:
  - **name**: '@timestamp'
    
    **level**: core
    
    **required**: true
    
    **type**: date
    
    **description**: 'Date/time when the event originated.'

    This is the date/time extracted from the event, typically representing when the event was generated by the source.

    If the event source has no original timestamp, this value is typically populated by the first time the event was received by the pipeline.

    *Required field for all events."
  
  **example**: '2016-05-23T08:05:34.853Z'
  
  - **name**: labels
    
    **level**: core
<table>
<thead>
<tr>
<th>User</th>
<th>Failures</th>
<th>Last Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>4040</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>admin</td>
<td>1406</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>test</td>
<td>1356</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>user</td>
<td>524</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>guest</td>
<td>400</td>
<td>7 hours ago</td>
</tr>
<tr>
<td>123456</td>
<td>334</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>oracle</td>
<td>312</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>support</td>
<td>270</td>
<td>5 hours ago</td>
</tr>
<tr>
<td>tomcat</td>
<td>226</td>
<td>5 hours ago</td>
</tr>
</tbody>
</table>
Demo
Conclusion
Auditd
Auditbeat
Logs, Dashboards, SIEM
I can share that we do use auditbeat to monitor our Elastic Cloud infra, some thousands VMs and bare metal servers, since it was first released. We should be publishing a blog post about it on elastic.co in the near future.
Code

https://github.com/xeraaa/auditbeat-in-action
Similar Solutions

https://github.com/slackhq/go-audit
https://github.com/Scribery/aushape
QUESTIONS?

Philipp Krenn  @xeraa

PS: Sticker