Scale Your Auditing Events

Philipp Krenn

@xeraa
THIS IS FINE.
Learn about a breach from the press or users
Learn about a breach

Attackers asking for a ransom
Learn about a breach

Cloud provider's bill
Learn about a breach

YOURSSELF AFTER THE FACT
Learn about a breach

YOURSELF & YOU CAN PROVE NO HARM
TH-

This is not fine!!

Oh my god every things on fire

What the hell is my problem
No silver bullet
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
ALL THE THINGS!
Problem

How to centralize?
elastic

Developer 🥑
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
elastic cloud

https://cloud.elastic.co
AUDITBEAT
AUDITD MODULE

Correlate related events
Resolve UIDs 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 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-libaududit is a library for communicating with the Linux Audit Framework
**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
Demo
PS: MACHINE LEARNING
Detector: \texttt{distinct\_count (nginx.access.remote\_ip.keyword)}

Single time series analysis of cardinality nginx.access.remote_ip.keyword

Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 2h)
CONCLUSION
Auditd
Auditbeat
Logs, Dashboards,...
TRY

https://dashboard.xeraa.wtf

SSH: elastic-user@xeraa.wtf secret
Code

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

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

Philipp Krenn   @xeraa

PS: Sticker