THIS IS FINE.
TH-

THIS IS NOT FINE!

OH MY GOD EVERY THINGS ON FIRE

WHAT THE HELL IS MY PROBLEM
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

*Yourself after the fact*
Learn about a breach

YOURSSELF BUT UNSURE ABOUT HARM
Learn about a breach

Yourselves & you can prove no harm
No silver bullet
Questions: https://sli.do/xeraa
Answers: https://twitter.com/xeraa
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."
Watching file access
Monitoring system calls
Recording commands run by a user
Recording security events
Monitoring network access
Demo
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?
Disclaimer

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

Elasticsearch
Logstash
Kibana
Apparently, I’m an ELKB personality.
Filebeat Module: Auditd
DEMO
AUDITBEAT
Auditd Module

Correlate related events
Resolve UIDs to user names
Native Elasticsearch integration
AUDITD MODULE

eBPF powers on older kernels
Run side by side with Auditd
Easier configuration
Enhance add_docker_metadata to enrich based on PID

#6100

exekias merged 2 commits into elastic:master from andrewkroh:feature/libbeat/docker-pid-metadata on 18 Jan

andrewkroh commented on 17 Jan

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.
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
DEMO
See MOAR

Kibana visualizations & dashboards
PS: Machine Learning
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,...
https://cloud.elastic.co
Next Steps

https://dashboard.xeraa.wtf

SSH: elastic-user@xeraa.wtf secret
QUESTIONS?

Philipp Krenn

@xeraa

PS: Sticker