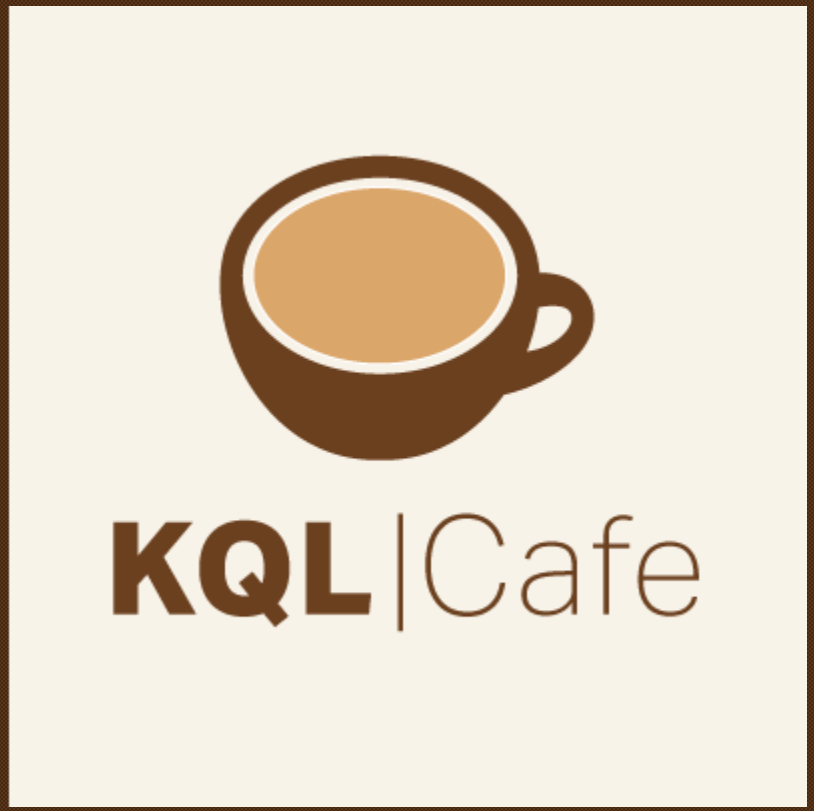
Session 10 | KQL Hunting



Session 10 | KQL Hunting

Your | hosts

Alex Verboon

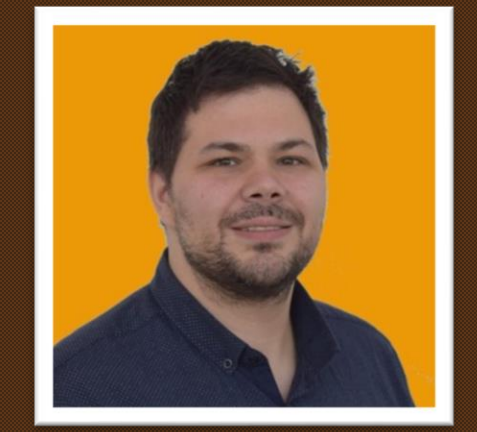
https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Gianni Castaldi



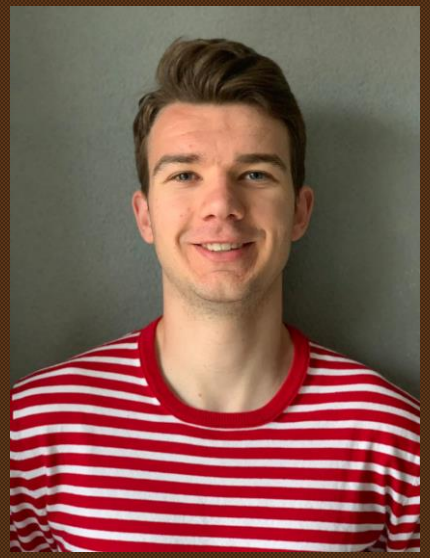
https://twitter.com/castello_johnny

https://www.linkedin.com/in/giannicastaldi/

https://github.com/KustoKing

https://www.kustoking.com/

Today's | Guest
Bert-Jan Pals



Twitter: https://twitter.com/bertjancyber
Github: https://github.com/Bert-JanP/Hunt

Show | Agenda

Welcome
What's new in KQL
Learning KQL
Our KQL Guest
What did you do with KQL this month?

DeviceTvmHardwareFirmware

- Item 1
- Item 2
- Item 3
- Item 4

base64_encode_tostring

- Item 1
- Item 2
- Item 3
- Item 4

Bert-Jan Pals

- Item 1
- Item 2
- Item 3
- Item 4

Date Size

Item 1
Item 2
Item 3
Item 4

User added to Privileged LocalGroup

Item 1
Item 2
Item 3
Item 4

Check local admins

Item 1
Item 2
Item 3
Item 4

Questions?

Thanks for attending