Session 6 | KQL Ingestion

Session 6 | KQL Ingestion

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/

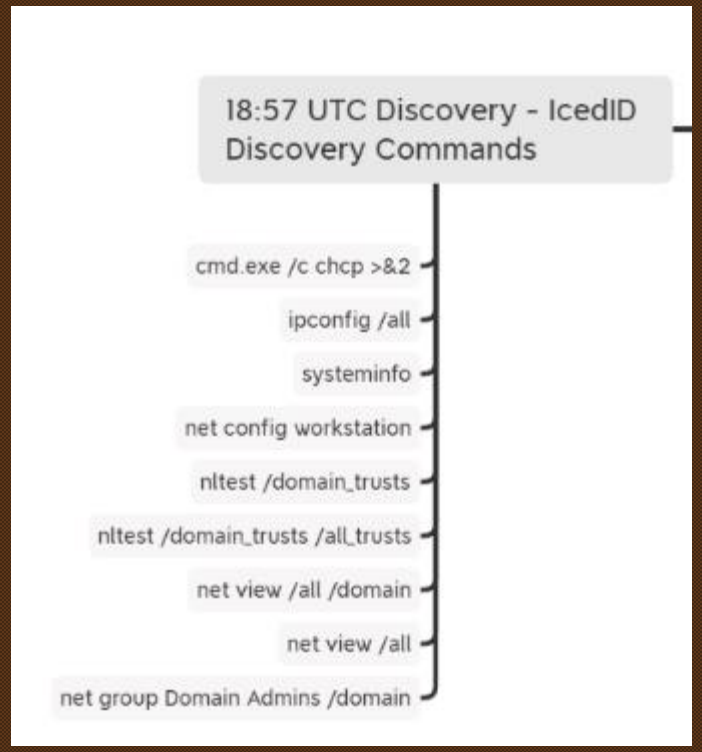
Show | Agenda

Welcome
What's new in KQL
Working with IOCs
Learning KQL
KQL Tools
What did you do with KQL this month?

What’s new

Working with IOCs

https://thedfirreport.com/2022/04/25/quantum-ransomware/



KQL Tools

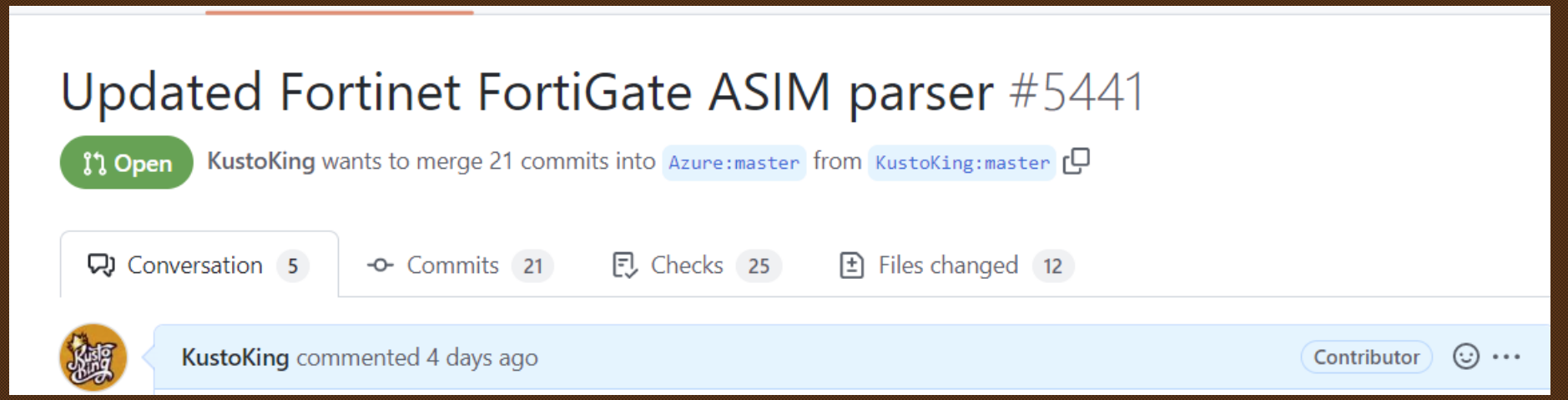
Parse versus Extract

parse : subsequent

extract : can be based on regex

Browser Extensions

What did you do with KQL



https://github.com/Azure/Azure-Sentinel/pull/5441

Questions?

Thanks for attending