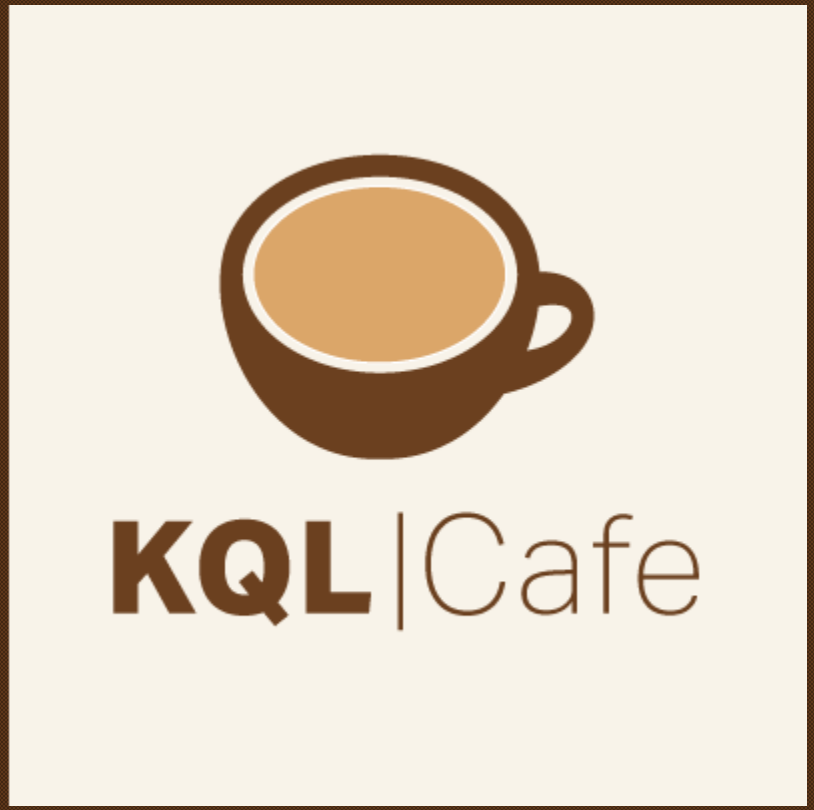
Session 5-2023 |


KQL|Cafe

Your | hosts

Alex Verboon

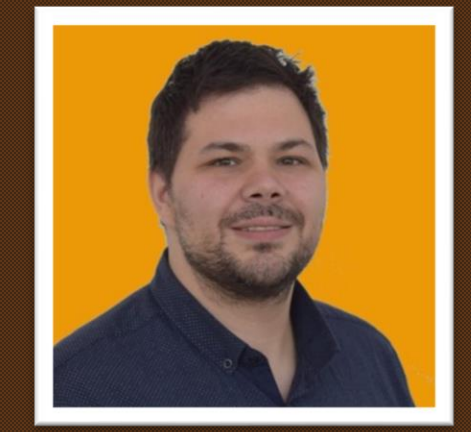
https://twitter.com/alexverboon

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

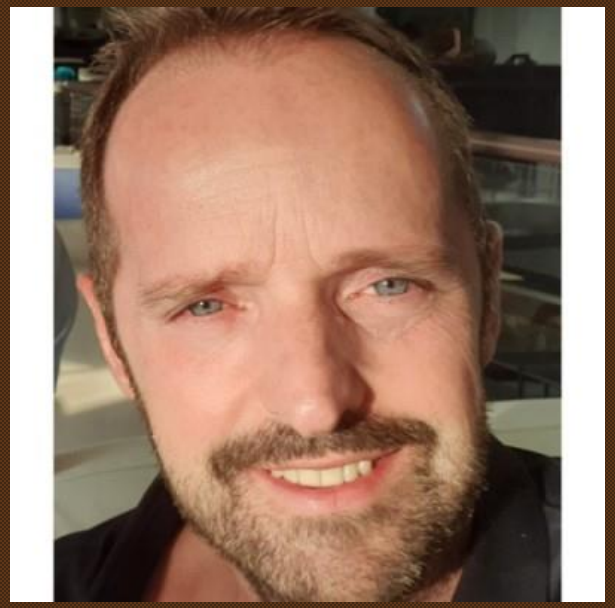
https://www.kustoking.com/

Show | Agenda

Welcome
What is new/updates for KQL
Our KQL Guest
What did you do with KQL this month?

summarize hint.strategy=shuffle

Today's | Guest



Clive Watson
Solutions Director @ Quorum Cyber, Microsoft Security MVP

Clive Watson (@clive_watson) / Twitter

What did you do with KQL this month?

search for domains based on the 10 Most Abused Top Level Domains

```
// search for domains based on the 10 Most Abused Top Level Domains
// https://www.spamhaus.org/statistics/tlds/
let abusedTLD = dynamic(["rest", "okinawa", "live", "beauty", "bar", "fit", "gq", "cfd", "zone", "top"]);
DeviceNetworkEvents
| where isnotempty(RemoteUrl)
| extend tld = tostring(split(RemoteUrl, ".")[-1])
| where tld in~ (abusedTLD)
| summarize
   StartTime = min(Timestamp),
   EndTime = max(Timestamp),
   NameCount = count()
   by RemoteUrl, RemoteIP, tld
| order by NameCount desc
```

What did you do with KQL this month?

TI Sign-In Logs

```
let ioc_lookBack = 90d;
let IncTitle = "TI map IP entity to SigninLogs";
SecurityIncident
| where TimeGenerated > ago(90d)
| where Title == IncTitle
| summarize arg_max(TimeGenerated,*) by IncidentNumber
| mv-expand AlertIds
| extend AlertId = tostring(AlertIds)
| join  (SecurityAlert)
on $left. AlertId == $right. SystemAlertId
| mv-expand parse_json(Entities)
| extend EType = tostring((Entities.Type))
| where EType == 'ip'
| extend IPAddress = tostring(Entities.Address)
// Count the # of alerts per IP address
| summarize Alertcount = dcount(SystemAlertId) by IPAddress
| join kind=innerunique  (ThreatIntelligenceIndicator
    | where TimeGenerated >= ago(ioc_lookBack) and ExpirationDateTime > now()
    | summarize LatestIndicatorTime = arg_max(TimeGenerated, *) by IndicatorId
    | where Active == true
    // Picking up only IOC's that contain the entities we want
    | where isnotempty(NetworkIP)
       or isnotempty(EmailSourceIpAddress)
       or isnotempty(NetworkDestinationIP)
       or isnotempty(NetworkSourceIP)
    // As there is potentially more than 1 indicator type for matching IP, taking NetworkIP first, then others if that is empty.
    // Taking the first non-empty value based on potential IOC match availability
    | extend TI_ipEntity = iff(isnotempty(NetworkIP), NetworkIP, NetworkDestinationIP)
    | extend TI_ipEntity = iff(isempty(TI_ipEntity) and isnotempty(NetworkSourceIP), NetworkSourceIP, TI_ipEntity)
    | extend TI_ipEntity = iff(isempty(TI_ipEntity) and isnotempty(EmailSourceIpAddress), EmailSourceIpAddress, TI_ipEntity)
) on $left. IPAddress ==  $right.TI_ipEntity
| project IPAddress, Alertcount, LatestIndicatorTime, SourceSystem, ConfidenceScore, Description, ThreatType, Tags
// find the successfull sign-ins
| join SigninLogs
on $left. IPAddress == $right. IPAddress
| where ResultType != 0
| summarize SignInAttemps = dcount(CorrelationId) by IPAddress, Alertcount, Description, ThreatType, Tags, AutonomousSystemNumber, Location
```

Thanks for attending