Union Alert

```
// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.
set query_now = datetime(2022-03-23T02:57:37.9729472Z);
let Alert1 =
SecurityAlert
| where AlertName == "Unfamiliar sign-in properties"
| extend UserPrincipalName = tostring(parse_json(ExtendedProperties).["User Account"])
| extend Alert1Time = TimeGenerated
| extend Alert1 = AlertName
| extend Alert1Severity = AlertSeverity
;
let Alert2 =
SecurityAlert
| where AlertName == "Atypical travel"
| extend UserPrincipalName = tostring(parse_json(ExtendedProperties).["User Account"])
| extend Alert2Time = TimeGenerated
| extend Alert2 = AlertName
| extend Alert2Severity = AlertSeverity
| extend CurrentLocation =
strcat(tostring(parse_json(tostring(parse_json(Entities)[1].Location)).CountryCode), "|",
tostring(parse_json(tostring(parse_json(Entities)[1].Location)).State), "|",
tostring(parse_json(tostring(parse_json(Entities)[1].Location)).City))
| extend PreviousLocation =
strcat(tostring(parse_json(tostring(parse_json(Entities)[2].Location)).CountryCode), "|",
tostring(parse_json(tostring(parse_json(Entities)[2].Location)).State), "|",
tostring(parse_json(tostring(parse_json(Entities)[2].Location)).City))
| extend CurrentIPAddress = tostring(parse_json(Entities)[1].Address)
| extend PreviousIPAddress = tostring(parse_json(Entities)[2].Address)
;
Alert1
| join kind=inner Alert2 on UserPrincipalName
| where abs(datetime_diff('minute', Alert1Time, Alert2Time)) <=10
| extend TimeDelta = Alert1Time - Alert2Time
| project UserPrincipalName, Alert1, Alert1Time, Alert1Severity, Alert2, Alert2Time,
Alert2Severity, TimeDelta, CurrentLocation, PreviousLocation, CurrentIPAddress,
PreviousIPAddress
```

```
| extend AccountCustomEntity = UserPrincipalName
| extend IPCustomEntity = CurrentIPAddress
```

Revision #1
Created 2022-03-24 13:18:18 UTC by Clinton
Updated 2022-03-24 13:18:41 UTC by Clinton