Microsoft Sentinel

- Ingestion Lag
- Rule Sample
- Union Alert
- Splunk to Sentinel Logic
- Microsoft Security

Ingestion Lag

```
| where ingestionTime > 5m
```

Setting:

- Run query every 5m
- Lookup data from the last 24 hours
- Stop running query after alert disabled

Rule Sample

Log Analytics:

> Logs

Rules

> Analytics

```
OfficeActivity
| where ingestion_time() > ago(5m)
| where tolower(OfficeWorkload) matches regex "onedrive|sharepoint" and tolower(Operation)
matches regex "filesyncdownload|filedownload" and UserId != "app@sharepoint"
| summarize initial_time = min(TimeGenerated), end_time =
max(datetime_add("Second",1,TimeGenerated)), operation=make_set(Operation,5),
workload=make_set(OfficeWorkload,5), file_name=make_set(SourceFileName,5),
file_count=dcount(OfficeId) by bin(TimeGenerated,5m),UserId, ClientIP
| project-rename src_ip=ClientIP, src_user=UserId
| where file_count>500
```

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,
```

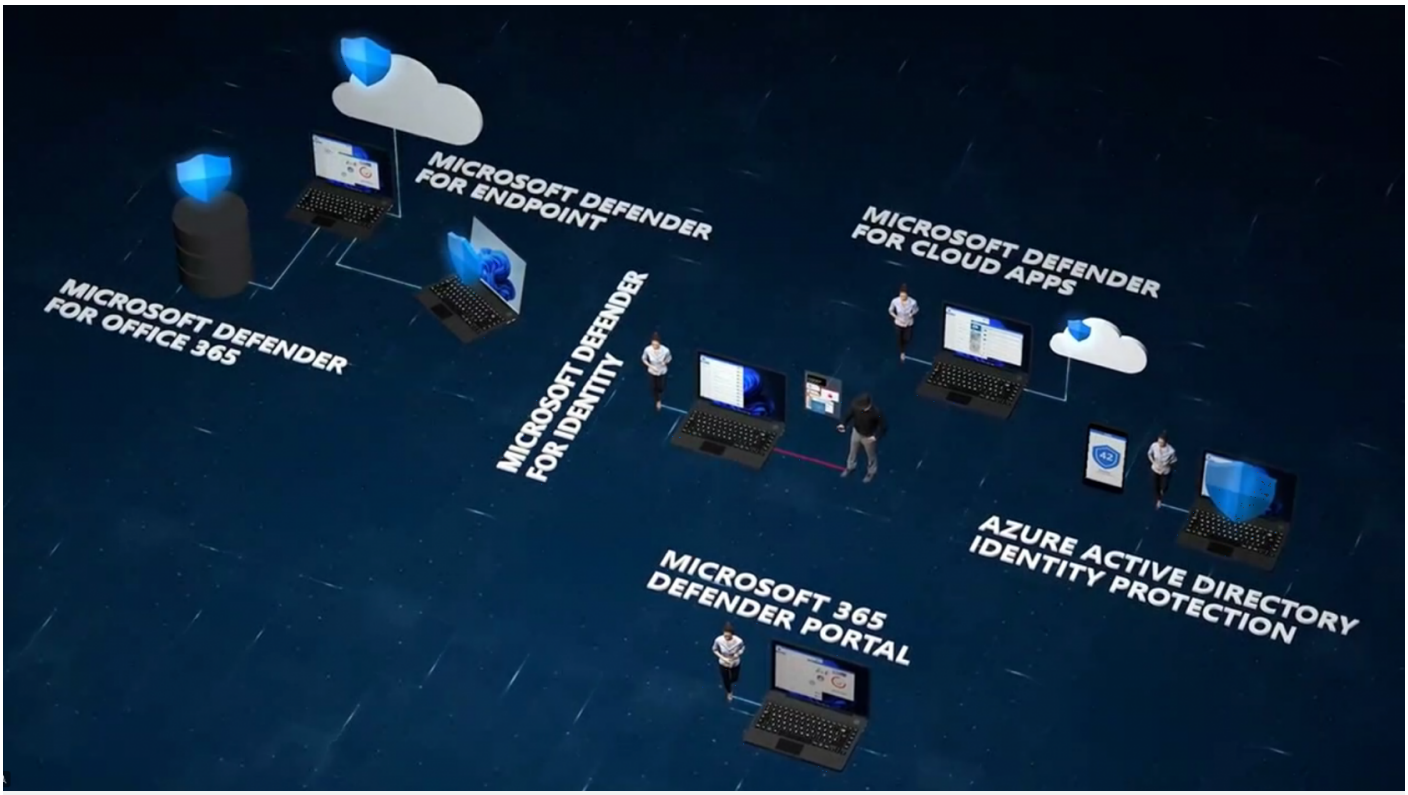
```
PreviousIPAddress
| extend AccountCustomEntity = UserPrincipalName
| extend IPCustomEntity = CurrentIPAddress
```

Splunk to Sentinel Logic

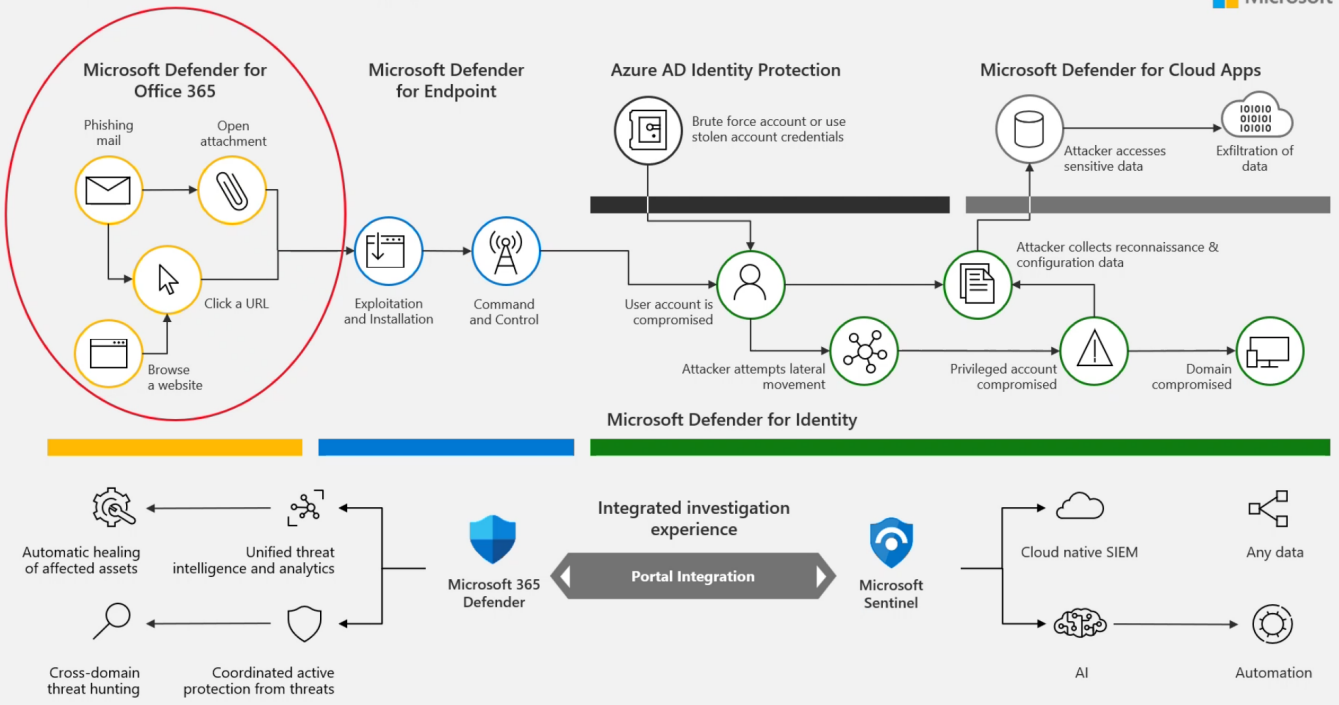
bin time doc

> | summarize initial_time = min(TimeGenerated), end_time = max(datetime_add("Second",1,TimeGenerated)) by bin(TimeGenerated,15m), src_user

Microsoft Security



Defend Across Attack Chains



The cloud kill chain model

