



Query Optimization with AI

Uncoder AI

Released on April 16

Detection Rules

Microsoft Sentinel Query (Kusto)

Select Platform

TRANSLATE

AI Tools Save As Contribute

```
1 // Some URL are wrapped with a safelink
2 // Let's get the the unwrapped url and clicks
3 AlertInfo
4 | where ServiceSource =~ "Microsoft Defender for Office 365"
5 | join (
6     AlertEvidence
7     | where EntityType == "Url"
8     | project AlertId, RemoteUrl
9 )
10 on AlertId
11 | join (
12     AlertEvidence
13     | where EntityType == "MailMessage"
14     | project AlertId, NetworkMessageId
15 )
16 on AlertId
17 // Get the unique NetworkMessageId for the email containing the Url
18 | distinct RemoteUrl, NetworkMessageId
19 | join EmailEvents on NetworkMessageId
20 // Get the email RecipientEmailAddress and ObjectId from the email
21 | distinct RemoteUrl, NetworkMessageId, RecipientEmailAddress, RecipientObjectId
22 | join kind = inner IdentityInfo on $left.RecipientObjectId == $right.AccountObjectId
23 // get the UserSid of the Recipient
24 | extend OnPremSid = AccountSID
25 | distinct RemoteUrl, NetworkMessageId, RecipientEmailAddress, RecipientObjectId, OnPremSid
26 // Get the Url click event on the recipient device.
27 | join kind = inner
28     (DeviceEvents
29     | where ActionType == "BrowserLaunchedToOpenUrl" | where isnotempty(RemoteUrl)
30     | project UrlDeviceClickTime = Timestamp, UrlClickedByUserSid = RemoteUrl,
31       InitiatingProcessAccountSid, DeviceName, DeviceId, InitiatingProcessFileName
```

AI-generated Query Optimization

The provided Microsoft Sentinel Query is quite complex and involves multiple joins. To optimize it for better performance (i.e., faster search speed), I'll provide suggestions to improve its efficiency.

Optimized Query:

```
AlertInfo
| where ServiceSource =~ "Microsoft Defender for Office 365"
| join (
    AlertEvidence
    | where EntityType == "Url"
    | project AlertId, RemoteUrl
) on AlertId
| join (
    AlertEvidence
    | where EntityType == "MailMessage"
    | project AlertId, NetworkMessageId
) on AlertId
| distinct RemoteUrl, NetworkMessageId
| join kind=inner EmailEvents on NetworkMessageId
| project RemoteUrl, NetworkMessageId, RecipientEmailAddress, RecipientObjectId
| join kind=inner IdentityInfo on $left.RecipientObjectId == $right.AccountObjectId
| extend OnPremSid = AccountSID
| distinct RemoteUrl, NetworkMessageId, RecipientEmailAddress, RecipientObjectId, OnPremSid
| join kind=inner (
    DeviceEvents
    | where ActionType == "BrowserLaunchedToOpenUrl" and isnotempty(RemoteUrl)
    | project UrlDeviceClickTime = Timestamp, UrlClickedByUserSid = RemoteUrl,
      InitiatingProcessAccountSid, DeviceName, DeviceId, InitiatingProcessFileName
) on $left.OnPremSid == $right.InitiatingProcessAccountSid and $left.RemoteUrl == $right.UrlClickedByUserSid
| distinct UrlDeviceClickTime, RemoteUrl, NetworkMessageId, RecipientEmailAddress, RecipientObjectId,
  OnPremSid, UrlClickedByUserSid, DeviceName, DeviceId, InitiatingProcessFileName
| sort by UrlDeviceClickTime desc
```

Query performance can become a bottleneck. Uncoder AI analyzes a query and either confirms it's optimal or suggests performance improvements. For this purpose, Uncoder AI uses Llama 3.3 customized for detection engineering and threat intelligence processing, hosted at SOC Prime SOC 2 Type II private cloud for maximum security, privacy, and IP protection.

- Practical and specific suggestions
- Multiple languages supported
- Data doesn't leave SOC Prime's infrastructure

48 languages supported in production

