Microsoft Defender for Endpoint, Web Protection Hunting

Microsoft Defender for Endpoint's web protection comprises of several features, including web threat protection, web content filtering, and custom indicators. Therefore, in this cheat sheet, I am going to share hunting queries related to web protection.

ActionType name	Details	Example

SmartScreenUrlWarning	This ActionType captures activity related to 'MDE Indicators: [block]', 'MDE Web Content Filtering', 'MDA - Unsanctioned app', and 'Microsoft Defender SmartScreen' performed by Edge browser.	`DeviceEvents`
		`| where Timestamp > ago(7d)`
		`| where ActionType == "SmartScreenUrlWarning"`

ExploitGuardNetworkProtectionBlocked	This ActionType captures activity related to 'MDE Indicators: [block]', 'MDE Web Content Filtering' and 'MDA - Unsanctioned app' performed by 3rd party browsers such Chrome, Firefox and so on.	`DeviceEvents`
		`| where Timestamp > ago(7d)`
		`| where ActionType == "ExploitGuardNetworkProtectionBlocked"`

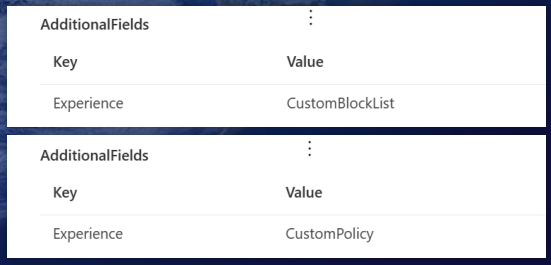
SmartScreenUserOverride	This ActionType captures 'MDE Indicators: [Warn]' and 'MDA Monitored app' activities by Edge browser.	`DeviceEvents`
		`| where Timestamp > ago(7d)`
		`| where ActionType == "SmartScreenUserOverride"`

NetworkProtectionUserBypassEvent	This ActionType captures 'MDE Indicators: [Warn]' and 'MDA Monitored app' activities by.3rd party browsers such Chrome, Firefox and so on.	`DeviceEvents`
		`| where Timestamp > ago(7d)`
		`| where ActionType == "NetworkProtectionUserBypassEvent"`

In [AdditionalFields] parameter, depending on what you want to find, you can select the appropriate value for the field.

- ✓ **MDE - Url Indicators - "CustomBlockList"**
- ✓ **MDE - Web Content Filtering - "CustomPolicy"**
- ✓ **MDA - Unsanctioned app - "CasbPolicy"**
- ✓ **Microsoft Defender SmartScreen - "Malicious"**
- ✓ **Microsoft Defender SmartScreen - "Phishing"**

Ex) [AdditionalFields] parameter



// **Edge browser** - Microsoft SmartScreen

```
DeviceEvents
| where Timestamp > ago(7d)
| where ActionType == "SmartScreenUrlWarning"
| extend ParsedFields=parse_json(AdditionalFields)
| summarize MDE_IoC = make_list_if(RemoteUrl, Experience=tostring(ParsedFields.Experience) == "CustomBlockList"),
            MDE_WCF = make_list_if(RemoteUrl, Experience=tostring(ParsedFields.Experience) == "CustomPolicy"),
            MDA_CASB = make_list_if(RemoteUrl, Experience=tostring(ParsedFields.Experience) == "CasbPolicy"),
            Edge_SS = make_list_if(RemoteUrl, Experience=tostring(ParsedFields.Experience) in ("Malicious", "Phishing"))
by DeviceId, DeviceName
```

// **Bypass** - MDE Indicators Warn & MDA Monitored app

```
DeviceEvents
| where Timestamp > ago(7d)
| where ActionType in ("SmartScreenUserOverride", "NetworkProtectionUserBypassEvent")
| extend Browser = case(
        InitiatingProcessFileName has "msedge", "Edge",
        InitiatingProcessFileName has "chrome", "Chrome",
        InitiatingProcessFileName has "firefox", "Firefox",
        InitiatingProcessFileName has "opera", "Opera",
"3rd party browser")
| project Timestamp, DeviceId, DeviceName, ActionType, Browser, RemoteUrl
```

GitHub : 03-kql-mde-webprotection.md
https://github.com/LearningKijo/KQL/blob/main/KQL-Effective-Use/03-kql-MDE-WebProtection.md

Reference : Web Protection
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-protection-overview?view=o365-worldwide