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.	<pre>DeviceEvents where Timestamp > ago(7d) where ActionType == "SmartScreenUrlWarning"</pre>
ExploitGuardNetworkProtectionBlocked	This ActionType captures activity related to 'MDE Indicators: [block]', 'MDE Web Content Filtering' and 'MDA - Unsanctioned app' performed by 3 rd party browsers such Chrome, Firefox and so on.	<pre>DeviceEvents where Timestamp > ago(7d) where ActionType == "ExploitGuardNetworkProtectionBlocked"</pre>
SmartScreenUserOverride	This ActionType captures 'MDE Indicators: [Warn]' and 'MDA Monitored app' activities by Edge browser.	<pre>DeviceEvents where Timestamp > ago(7d) where ActionType == "SmartScreenUserOverride"</pre>
NetworkProtectionUserBypassEvent	This ActionType captures 'MDE Indicators: [Warn]' and 'MDA Monitored app' activities by.3 rd party browsers such Chrome, Firefox and so on.	<pre>DeviceEvents where Timestamp > ago(7d) where ActionType == "NetworkProtectionUserBypassEvent"</pre>

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

AdditionalFields ::

Key Value

Experience CustomBlockList

AdditionalFields ::

Key Value

Experience CustomPolicy
```

```
// Edge browser - Microsoft SmartScreen
```

// Bypass - MDE Indicators Warn & MDA Monitored app

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

Disclaimer: The views and opinions expressed herein are those of the author and do not necessarily reflect the views of company.