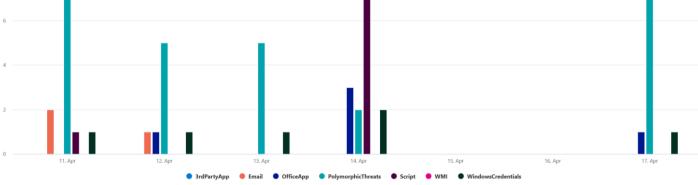
Microsoft Defender for Endpoint, Attack Surface Reduction rule

Attack Surface Reduction (ASR) rules are a set of security policies that are designed to reduce the potential attack surface of an operating system. In this sheet, I am going to share KQL use cases with graph for ASR rule.

| ActionType name | Details | Example |
|--|--|--|
| AsrOfficeChildProcessBlocked AsrLsassCredentialTheftBlocked AsrScriptExecutableDownloadBlocked | These ActionTypes capture ASR rule blocking activities. In particular, if you want to capture all ASR rule activities, then the "startswith" operator is a great choice. | <pre>DeviceEvents where Timestamp > ago(30d) where ActionType startswith "asr" extend Parsed = parse_json(AdditionalFields) where Parsed.IsAudit == "false"</pre> |
| AsrOfficeChildProcessAudited AsrLsassCredentialTheftAudited AsrScriptExecutableDownloadAudited | These ActionTypes capture ASR rule auditing activities. In particular, if you want to capture all ASR rule activities, then the "startswith" operator is a great choice. | DeviceEvents where Timestamp > ago(30d) where ActionType startswith "asr" extend Parsed = parse_json(AdditionalFields) where Parsed.IsAudit == "true" |

```
// ASR rule blocking activities
                                                                                                              AsrExecutableEmailContentBlocked 5.0 %
DeviceEvents
  where Timestamp > ago(30d)
                                                                                                                         AsrLsassCredentialTheftBlocked
  where ActionType startswith "asr"
                                                                      AsrUntrustedExecutableBlocked
  extend Parsed = parse_json(AdditionalFields)
  where Parsed.IsAudit == "false"
  summarize count() by ActionType
                                                                                                                               AsrObfuscatedScriptBlock
| render piechart
// ASR rule Auditing activities
DeviceEvents
 where Timestamp > ago(30d)
                                                                 AsrScriptExecutableDe
  where ActionType startswith "asr"
                                                                                                                         AsrOfficeChildProcessBlocked
  extend Parsed = parse json(AdditionalFields)
                                                                             AsrRansomwareBlocked
                                                                                                                         25.0 %
  where Parsed.IsAudit == "true"
  summarize count() by ActionType
                                                                                      croWin32ApiCallsBl
                                                                              5.0 %
  render piechart
```

```
// A graph showing ASR rule block activities per day
DeviceEvents
 where Timestamp > ago(30d)
 where ActionType startswith "asr"
 extend Parsed = parse_json(AdditionalFields)
 where Parsed.IsAudit == "false"
 summarize Email = countif(ActionType in ("AsrExecutableEmailContentBlocked", "AsrOfficeCommAppChildProcessBlocked")),
            Script = countif(ActionType in ("AsrObfuscatedScriptBlocked", "AsrScriptExecutableDownloadBlocked")),
                  = countif(ActionType in ("AsrPersistenceThroughWmiBlocked", "AsrPsexecWmiChildProcessBlocked")),
                       = countif(ActionType in ("AsrOfficeChildProcessBlocked", "AsrOfficeMacroWin32ApiCallsBlocked",
           OfficeApp
"AsrExecutableOfficeContentBlocked", "AsrOfficeProcessInjectionBlocked")),
            3rdPartyApp = countif(ActionType == "AsrAdobeReaderChildProcessBlocked"),
            WindowsCredentials = countif(ActionType == "AsrLsassCredentialTheftBlocked"),
            PolymorphicThreats = countif(ActionType in ("AsrUntrustedExecutableBlocked", "AsrUntrustedUsbProcessBlocked",
"AsrRansomwareBlocked", "AsrVulnerableSignedDriverBlocked")) by bin(Timestamp, 1d)
render columnchart
```



Reference: Attack surface reduction (ASR) rules reference

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide

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