Microsoft Defender as SIEM

Microsoft Sentinel がなくてもここまで出来る！
追加コストをかけずに Defender XDR のデータを活用しよう！

本日の内容

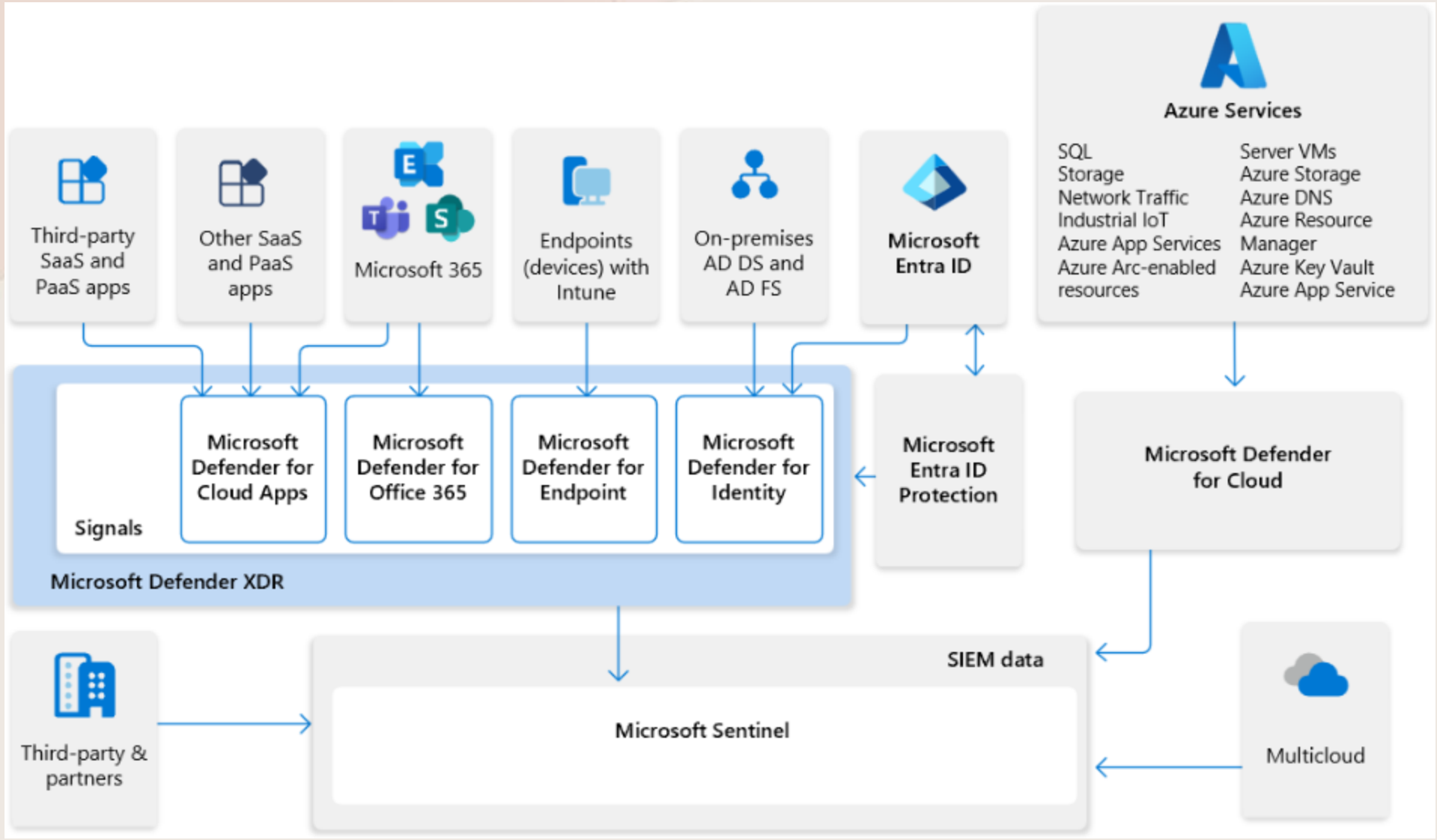
SIEM としての Defender XDR

使えそうなテーブル（データ）

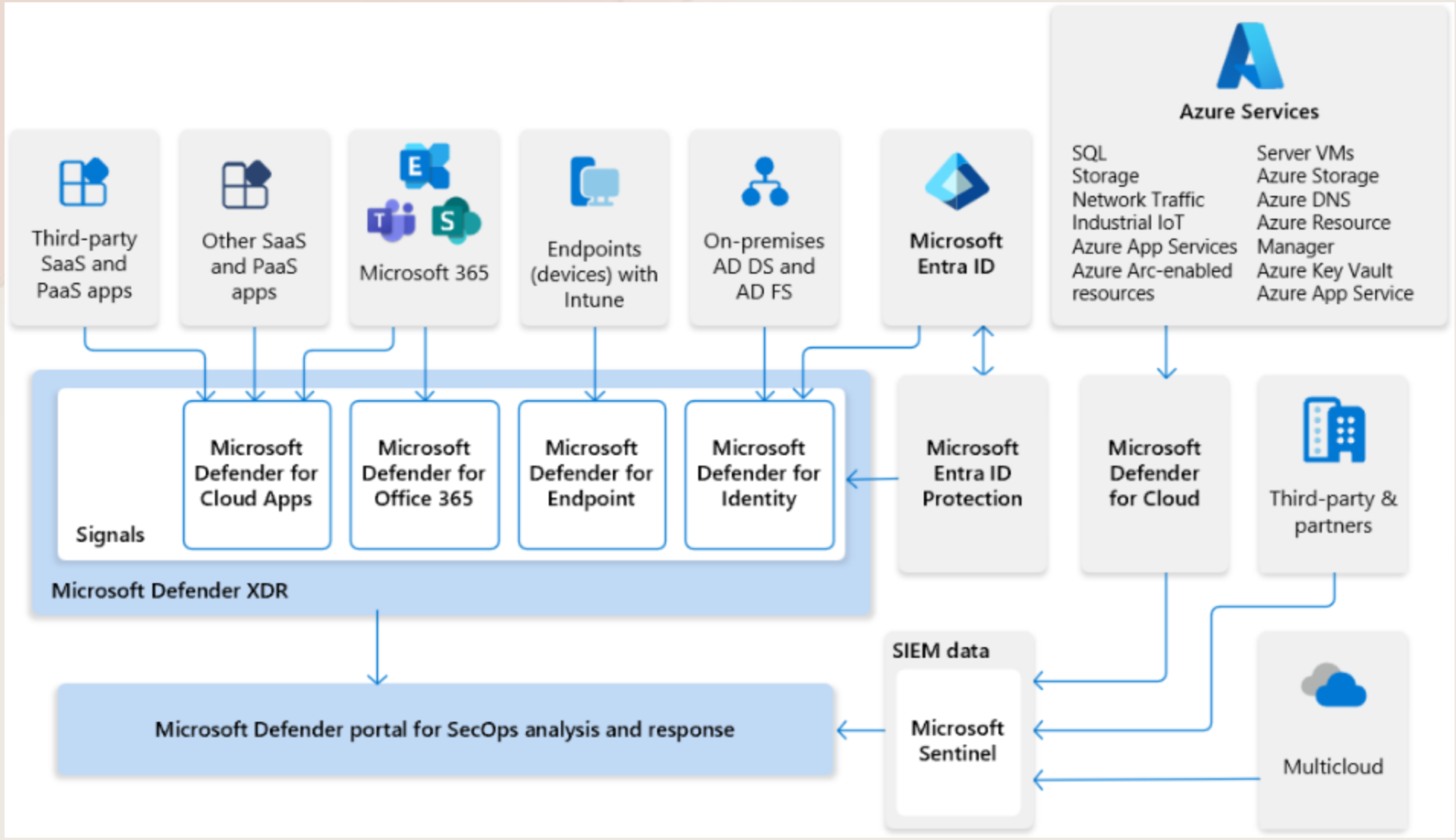
基本的なアイディア（アーキテクチャ）

活用例

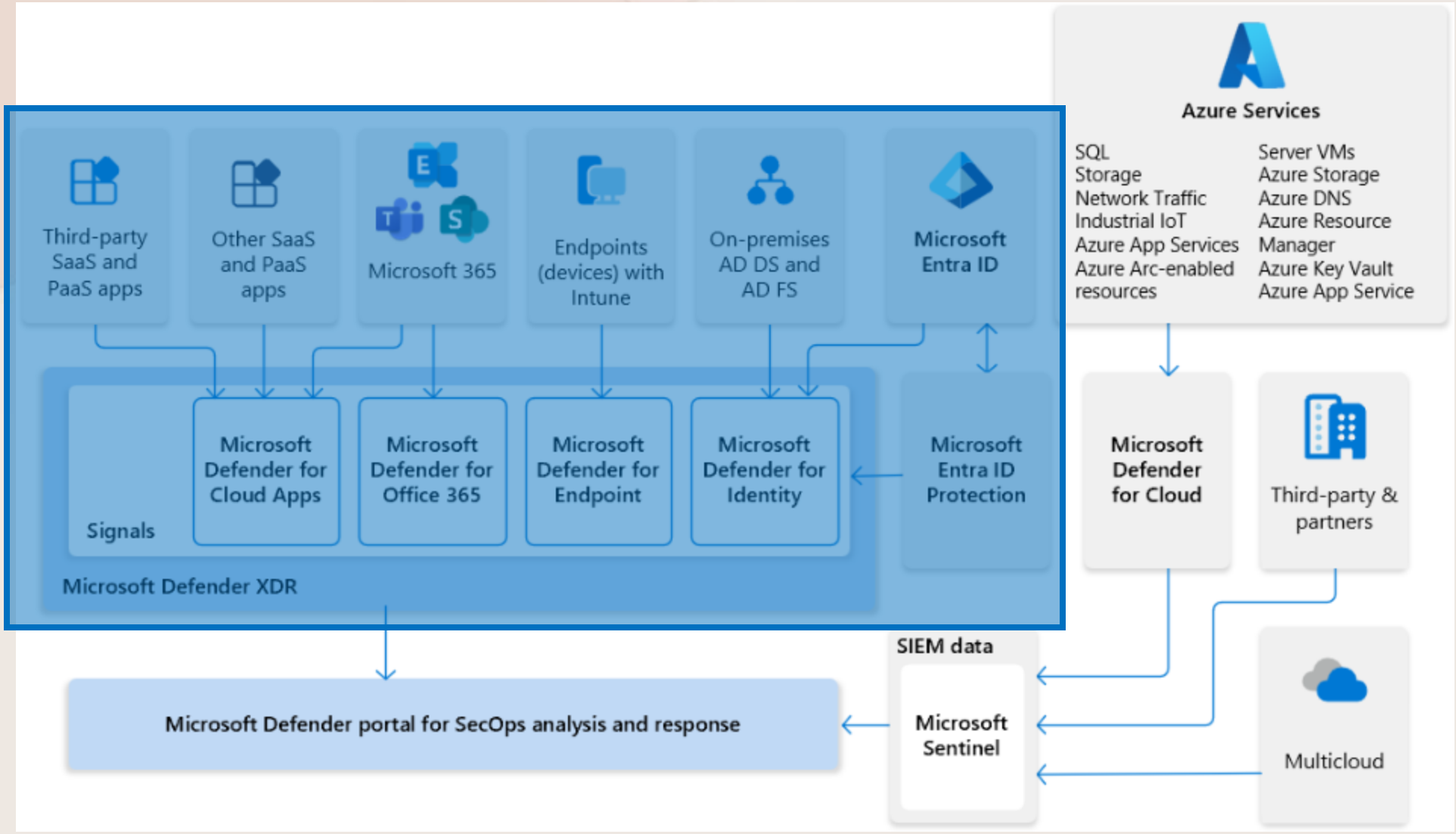
Microsoft Sentinel から見た Microsoft Defender XDR との統合



Microsoft Defender XDR から見た Microsoft Sentinel との統合



この範囲のデータだけでもすごくない？ ！



Microsoft Defender XDR と Microsoft Sentinel の SIEM としての比較

	Microsoft Defender XDR	Microsoft Sentinel
データ ソース	M365 の世界	あらゆるデータ ソース
課金	ユーザー ライセンス	従量課金
データ保持	30 日間（固定）	数年間（任意）
クエリ	KQL	KQL

Microsoft Defender XDR のデータだけ扱うのであれば、
（ライセンスは支払っているので）追加コストをかけずに SIEM として活用できる！

特に使えそうなテーブルはこの辺

Defender 脆弱性の管理

- DeviceBaselineComplianceAssess...
- DeviceBaselineComplianceAssess...
- DeviceBaselineComplianceProfiles
- DeviceTvmBrowserExtensions
- DeviceTvmBrowserExtensionsKB
- DeviceTvmCertificateInfo
- DeviceTvmHardwareFirmware
- DeviceTvmInfoGathering
- DeviceTvmInfoGatheringKB
- DeviceTvmSecureConfigurationAs...
- DeviceTvmSecureConfigurationAs...
- DeviceTvmSoftwareEvidenceBeta
- **DeviceTvmSoftwareInventory**
- **DeviceTvmSoftwareVulnerabilities**
- DeviceTvmSoftwareVulnerabilities...

デバイス

- **DeviceEvents**
- DeviceFileCertificateInfo
- **DeviceFileEvents**
- DeviceImageLoadEvents
- DeviceInfo
- DeviceLogonEvents
- DeviceNetworkEvents
- **DeviceNetworkInfo**
- DeviceProcessEvents
- DeviceRegistryEvents

メールとコラボレーション

- **EmailAttachmentInfo**
- **EmailEvents**
- EmailPostDeliveryEvents
- EmailUrlInfo
- **UrlClickEvents**

アプリと ID

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- **CloudAppEvents**
- IdentityDirectoryEvents
- **IdentityInfo**
- IdentityLogonEvents
- IdentityQueryEvents

アラートと動作

- AlertEvidence
- **AlertInfo**
- BehaviorEntities
- BehaviorInfo

露出管理

- ExposureGraphEdges
- ExposureGraphNodes

特に使えそうなテーブルはこの辺

Defender 脆弱性の管理

- DeviceBaselineComplianceAssess...
- DeviceBaselineComplianceAssess...
- DeviceBaselineComplianceProfiles
- DeviceTvmBrowserExtensions
- DeviceTvmBrowserExtensionsKB
- DeviceTvmCertificateInfo
- DeviceTvmHardwareFirmware
- DeviceTvmInfoGathering
- DeviceTvmInfoGatheringKB
- DeviceTvmSecureConfigurationAs...
- DeviceTvmSecureConfigurationAs...
- DeviceTvmSoftwareEvidenceBeta
- DeviceTvmSoftwareInventory
- DeviceTvmSoftwareVulnerabilities
- DeviceTvmSoftwareVulnerabilities...

デバイス

- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents
- DeviceImageLoadEvents
- DeviceInfo
- DeviceLogonEvents
- DeviceNetworkEvents
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceRegistryEvents

メールとコラボレーション

- EmailAttachmentInfo
- EmailEvents
- EmailPostDeliveryEvents
- EmailUrlInfo
- UrlClickEvents

アプリと ID

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- CloudAppEvents
- IdentityDirectoryEvents
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents

アラートと動作

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo

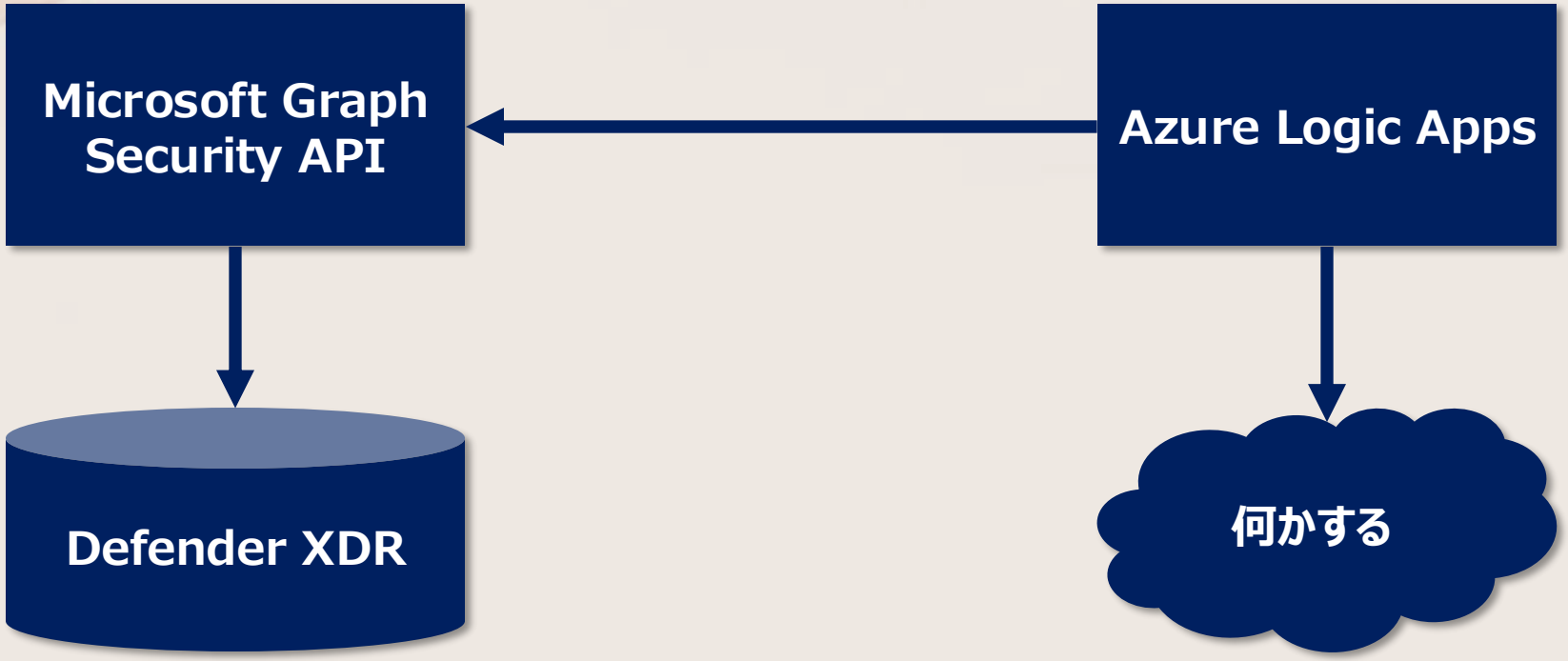
露出管理

- ExposureGraphEdges
- ExposureGraphNodes

基本アーキテクチャ

Defender XDR の情報を Microsoft Graph Security API で取得して何かする

https://graph.microsoft.com/v1.0/security/runHuntingQuery



基本アーキテクチャ

「何かする」の具体的なイメージ

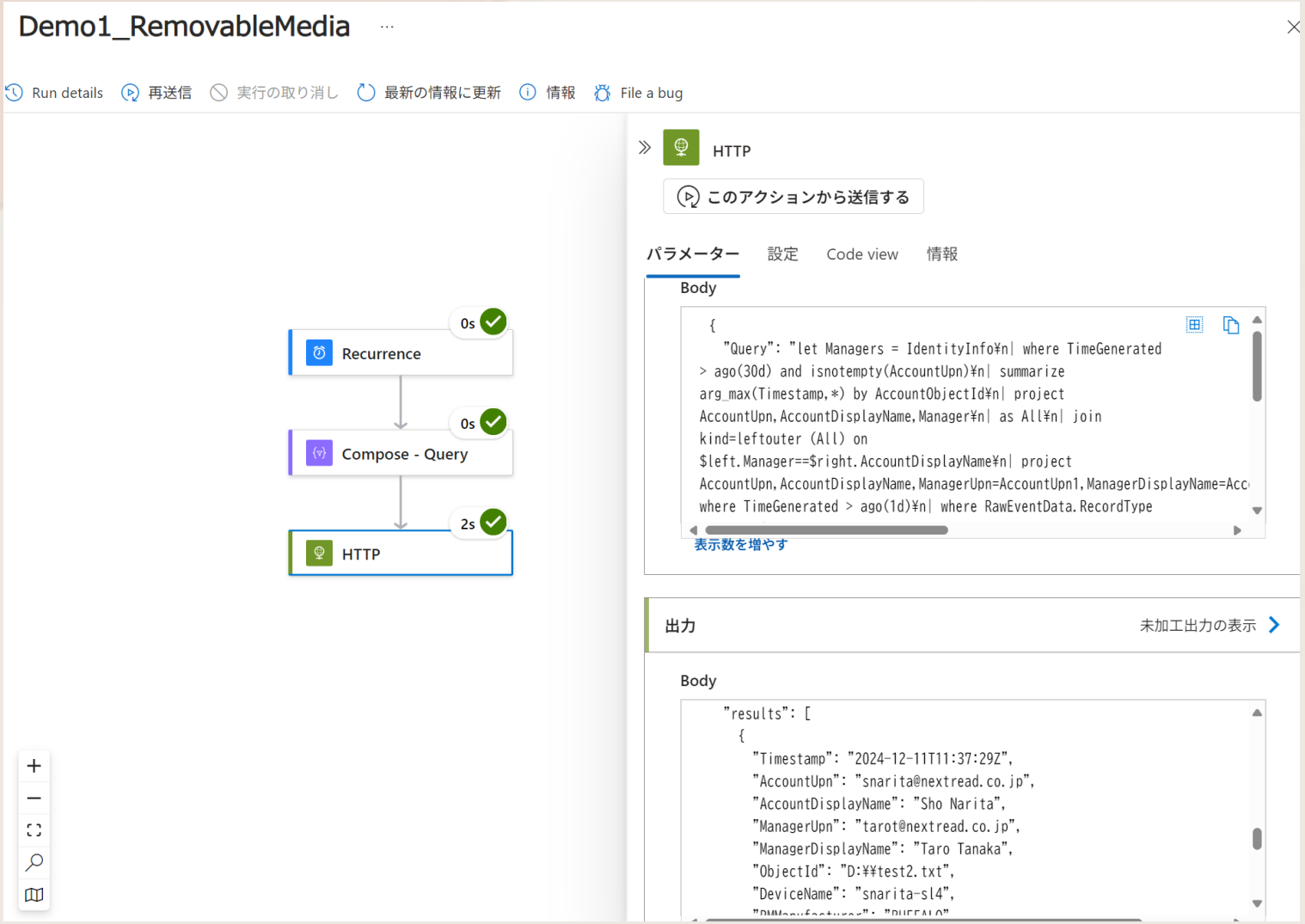
基本アーキテクチャ

Azure Logic Apps で Advanced hunting を実行するための権限を付与する

https://qiita.com/narisho/items/cf60dd0c66e6d153ed44

基本アーキテクチャ

Azure Logic Apps で Advanced hunting を実行する



活用例 ① USB 書出しを上司に確認する

テーブル	説明
CloudAppEvents	O365 や MDA に接続した SaaS のアクティビティ ログ。MDE で管理されたデバイスの USB 書出しログも含まれる。
IdentityInfo	AD や Entra ID のユーザーに関する情報。上司（manager 属性）の情報も含まれる。

Query

```
let Managers = IdentityInfo
| where TimeGenerated > ago(30d) and isnotempty(AccountUpn)
| summarize arg_max(Timestamp,*) by AccountObjectId
| project AccountUpn,AccountDisplayName,Manager
| as All
| join kind=leftouter (All) on $left.Manager==$right.AccountDisplayName
| project AccountUpn,AccountDisplayName,ManagerUpn=AccountUpn1,ManagerDisplayName=AccountDisplayName1;
CloudAppEvents
| where TimeGenerated > ago(1d)
| where RawEventData.RecordType == 63 and ActionType in ("FileCreatedOnRemovableMedia","FileCopiedToRemovableMedia")
| extend UserId=tostring(RawEventData.UserId),ObjectId=RawEventData.ObjectId,DeviceName=RawEventData.DeviceName,RemovableMedia=RawEventData.RemovableMediaDeviceAttributes
| extend RMManufacturer=RemovableMedia.Manufacturer,RMModel=RemovableMedia.Model,RMSerialNumber=RemovableMedia.SerialNumber
| join kind=leftouter (Managers) on $left.UserId==$right.AccountUpn
| project Timestamp,AccountUpn,AccountDisplayName,ManagerUpn,ManagerDisplayName,ObjectId,DeviceName,RMManufacturer,RMModel
```

Getting started | **Results** | Query history

Export | Show empty columns | 2 items | Search | 00:01.809 | Low | Chart type | Full screen

Filters: Add filter

Timestamp	AccountUpn	AccountDisplayName	ManagerUpn	ManagerDisplayName	ObjectId	DeviceName	RMManufacturer	RMModel
Dec 11, 2024 8:37:29 PM	snarita@nextread.co.jp	Sho Narita	tarot@nextread.co.jp	Taro Tanaka	D:\test2.txt	snarita-sl4	BUFFALO	USB Flash Disk
Dec 11, 2024 8:37:26 PM	snarita@nextread.co.jp	Sho Narita	tarot@nextread.co.jp	Taro Tanaka	D:\test1.txt	snarita-sl4	BUFFALO	USB Flash Disk

活用例 ② 組織で初めてメールされた宛先ドメインのメールを確認する

テーブル	説明
EmailEvents	Exchange Online のメール送受信ログ。日時、件名、送信者、受信者、送信者 IP、リスク有無などを含む。
EmailAttachmentInfo	メールの添付ファイルの情報。ファイル名、ファイルタイプ、サイズ、ハッシュなどの情報を含む。

Query

```
let lookback = 1d;
EmailEvents
| where TimeGenerated > ago(30d) and EmailDirection=='Outbound' and DeliveryAction=='Delivered'
| extend RecipientDomain = tostring(split(RecipientEmailAddress,'@')[1])
| as All
| where TimeGenerated > ago(lookback)
| distinct RecipientDomain
| join kind=leftanti (
    All
    | where TimeGenerated < ago(lookback)
    | distinct RecipientDomain
    ) on RecipientDomain
| join kind=inner (All) on RecipientDomain
| project Timestamp,NetworkMessageId,SenderFromAddress,RecipientEmailAddress,Subject
```

Getting started | **Results** | Query history

Export | Show empty columns | 1 item | Search

Filters: Add filter

Timestamp	NetworkMessageId	SenderFromAddress	RecipientEmailAddress	Subject
Dec 2, 2024 3:46:5...	c88fc18e-1459-48f8-eba2-08dd129d1a0a	snarita@nextread.co.jp	dummy@dummy.com	RE: Question about the continuation of...

活用例 ③ リスクが大きい脆弱性をユーザーに自動通知する

テーブル	説明
DeviceTvmSoftwareVulnerabilities	OS、OS バージョン、ソフトウェア、ソフトウェア バージョン、CVE、脆弱性の緊急度などを含む。
DeviceTvmSoftwareVulnerabilitiesKB	CVE のスコア、緊急度、脆弱性の説明、Exploit 公開有無などの情報を含む。

Query

```
1  DeviceTvmSoftwareVulnerabilities
2  | project DeviceName,OSPlatform,SoftwareVendor,SoftwareName,SoftwareVersion,CveId
3  | join kind=leftouter (
4      DeviceTvmSoftwareVulnerabilitiesKB
5      | project CveId,CvssScore,IsExploitAvailable,VulnerabilityDescription
6      ) on CveId
7  | where IsExploitAvailable == true
8  | project-away CveId1
```

Getting started | **Results** | Query history

Export | Show empty columns | 3 items | Search | 00:00.240 | Low | Chart type | Full screen

Filters: Add filter

DeviceName	OSPlatform	SoftwareVendor	SoftwareName	SoftwareVersion	CveId	CvssScore	IsExploitAvailable	VulnerabilityDescription
snarita-sl4	Windows11	microsoft	teams	1.5.0.8070	CVE-2023-5217	8.8	1	Summary: A heap buffer over...
snarita-sl4	Windows11	microsoft	teams	1.5.0.8070	CVE-2023-4863	8.8	1	Summary: The vulnerability is ...
snarita-sl4	Windows11	7-zip	7-zip	19.0.0.0	CVE-2022-29072	7.8	1	Summary: 7-Zip through 21.0...

まとめ

- Microsoft 365 のセキュリティ機能を使っていれば、Defender XDR にログが溜まっている -> 既に SIEM を持っているようなもの
- Graph Security API と Azure Logic Apps を組み合わせて、ほぼノーコストでセキュリティ対応の自動化を実現できる
- Defender XDR の Advanced hunting のテーブルを見ながら、ぜひアイディアを考えてみてください

ありがとうございます

Sho Narita
https://qiita.com/narisho
https://x.com/narisho