リスクを残さないための
メール侵害分析と対応の勘所

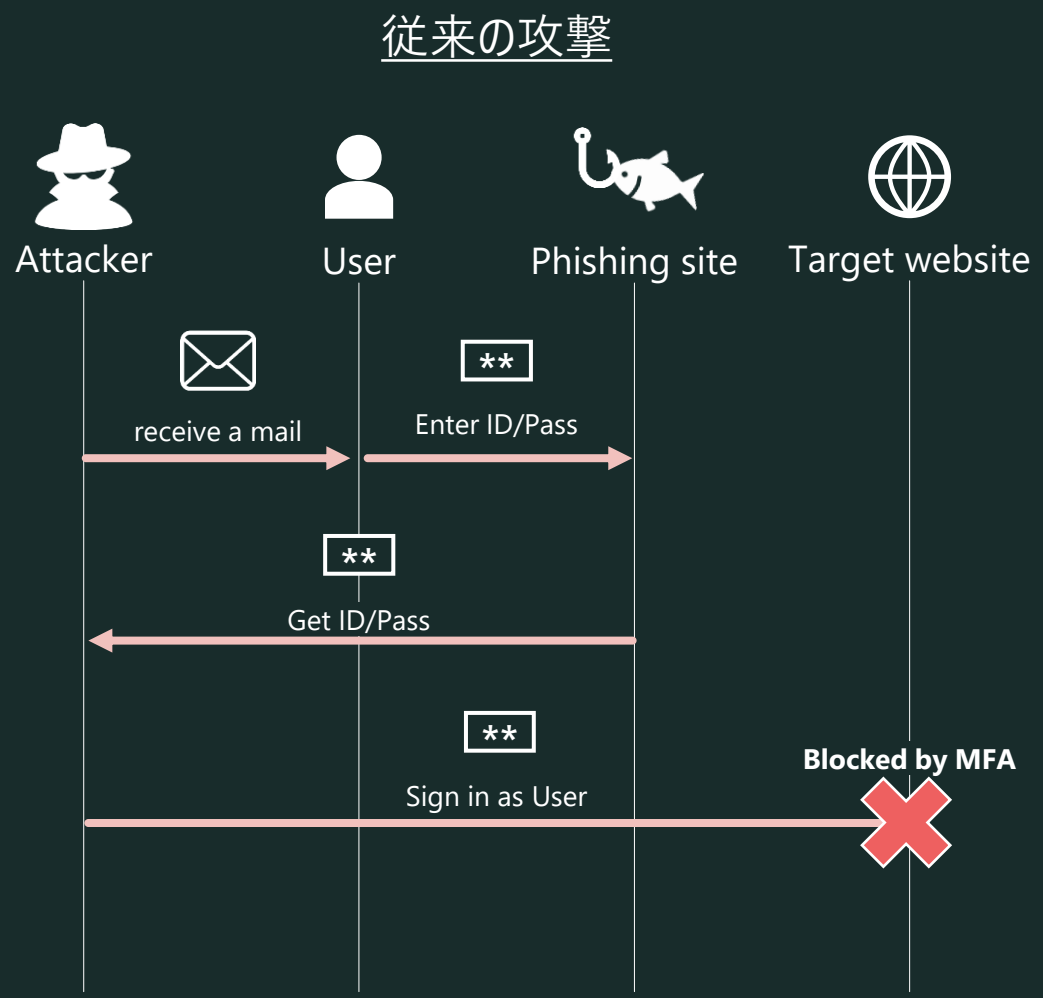
ITOCHU Cyber & Intelligence Inc.
Cybersecurity Analyst
Yumi Iida

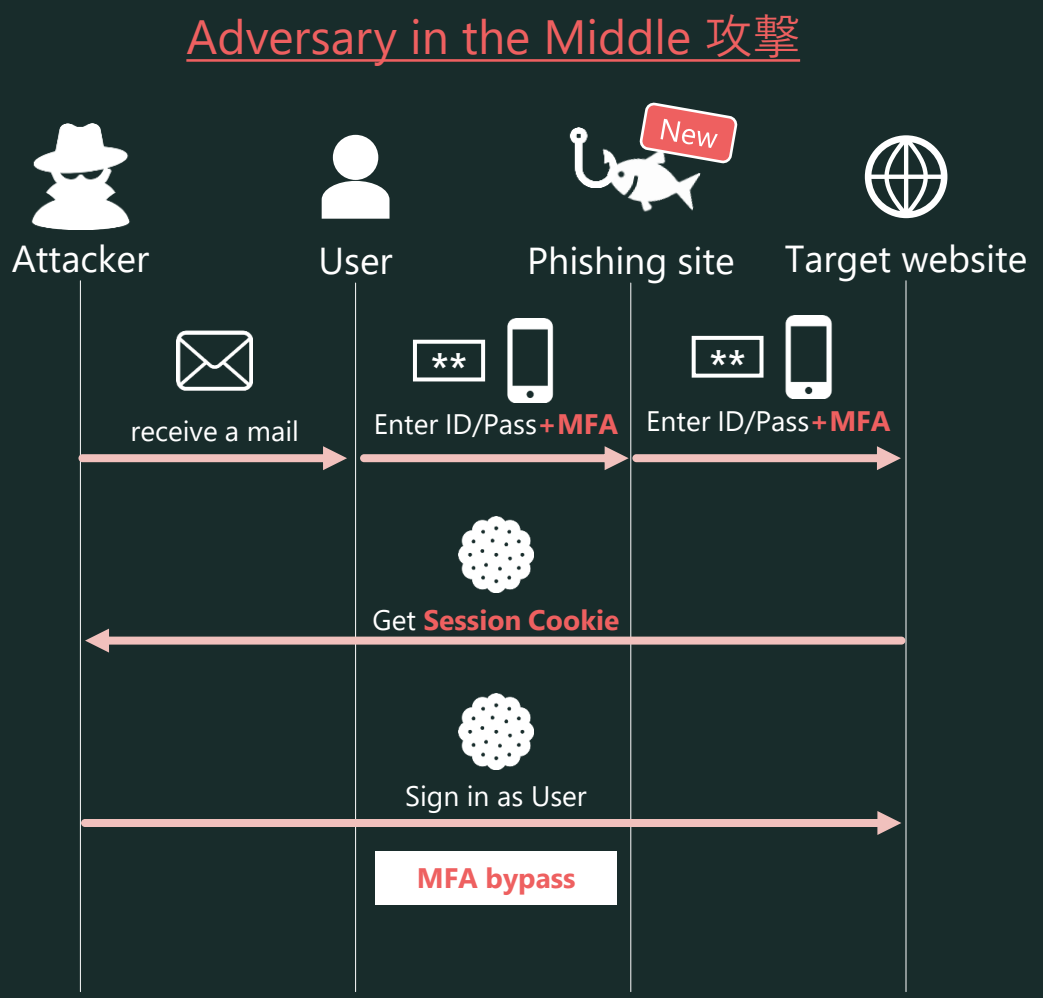
はじめに

- 2019 年から 2022 年にかけてフィッシング攻撃の報告件数は**約 4 倍**に*1
- 世界のメールサーバープロバイダーで **Microsoft 365** は **2 位**のシェア (13.5%) であり、多くの組織で使用される*2
- **Microsoft 365** を対象に 2021年よりBEC 対策として有効だった MFA を回避する攻撃 **AiTM (Adversary in the Middle)** が出現*3
- AiTM (別称 トークンリプレイ攻撃) の報告は 2022 年から 2023 年にかけて **30000 件/月から 70000 件/月に倍増**し、今後も有効な攻撃として報告されている *4

参考情報
*1 AWPG Report (https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf)
*2 Web Technology Surveys – Usage statistics of email server providers (https://w3techs.com/technologies/overview/email_server)
*3 Blog - From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud (https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/)
*4 Microsoft Digital Defense Report 2023 (https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023)

Adversary in the Middle (AiTM) 攻撃とは





インシデント発生時の課題

- 暫定対応がわからない
- 適切なログの選択、採取に時間を要する
- 攻撃の痕跡となるログがわからない
- 攻撃の痕跡への対応が体系的にまとまっていない . . .

適切でない初動対応によって**被害が拡大**することも

本講演の目的

実際に発生した M365 アカウント侵害インシデントをもとに以下を説明する

- インシデント発生時の初動対応
- インシデント調査の勘所
- 攻撃者の痕跡と該当ログの詳説
- インシデントを未然に防ぐ防御策

The goal:

✓インシデントレスポンスの勘所を理解し、侵害発生時にすぐ対応できるように

✓有効な防御策を把握する

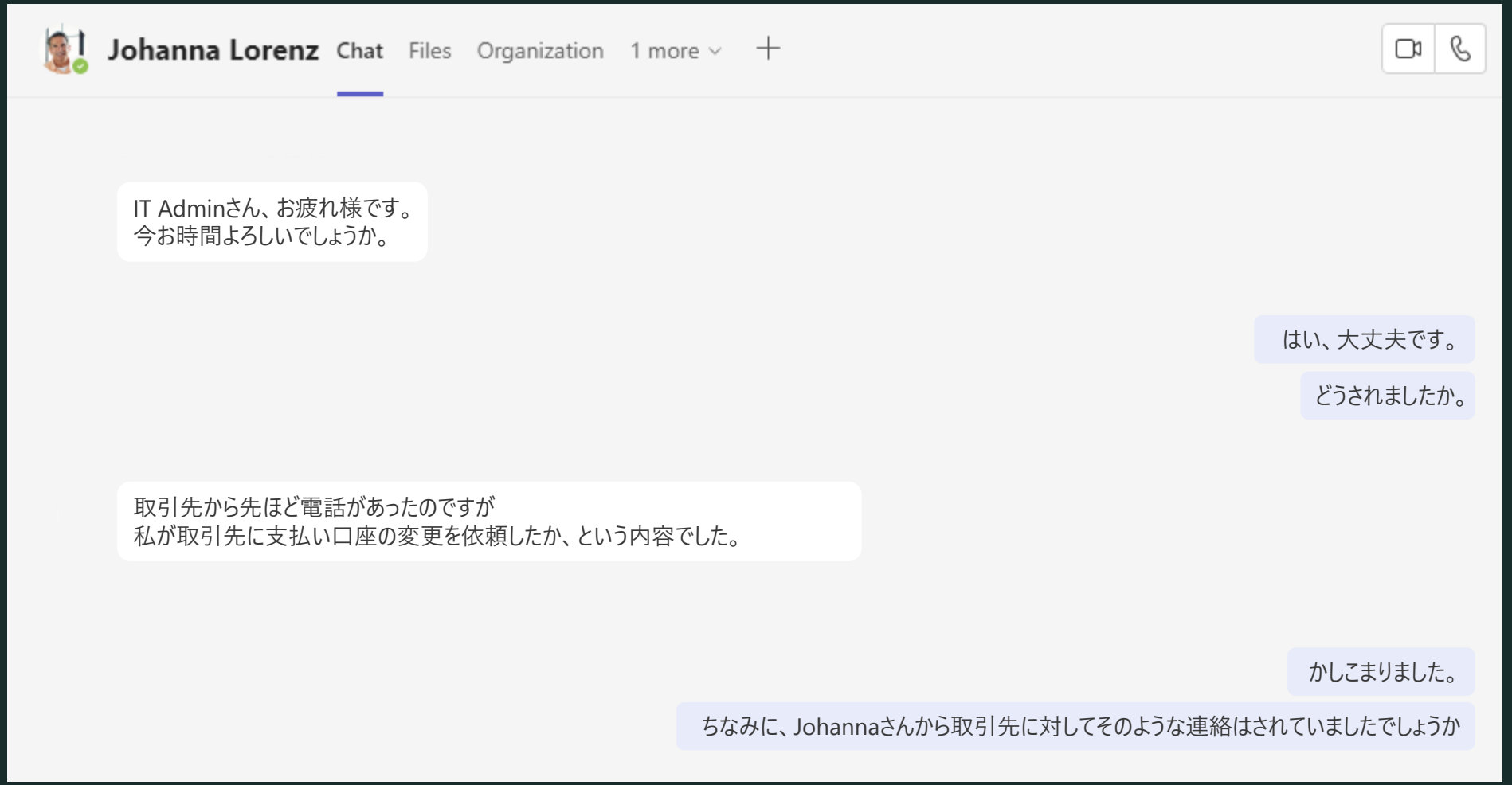
インシデント対応をしてみましょう

実際の侵害事例を元に、デモインシデントを作成した

あなたはとある商社の CSIRT に所属しています。
会社の IT 環境は以下の通りです。

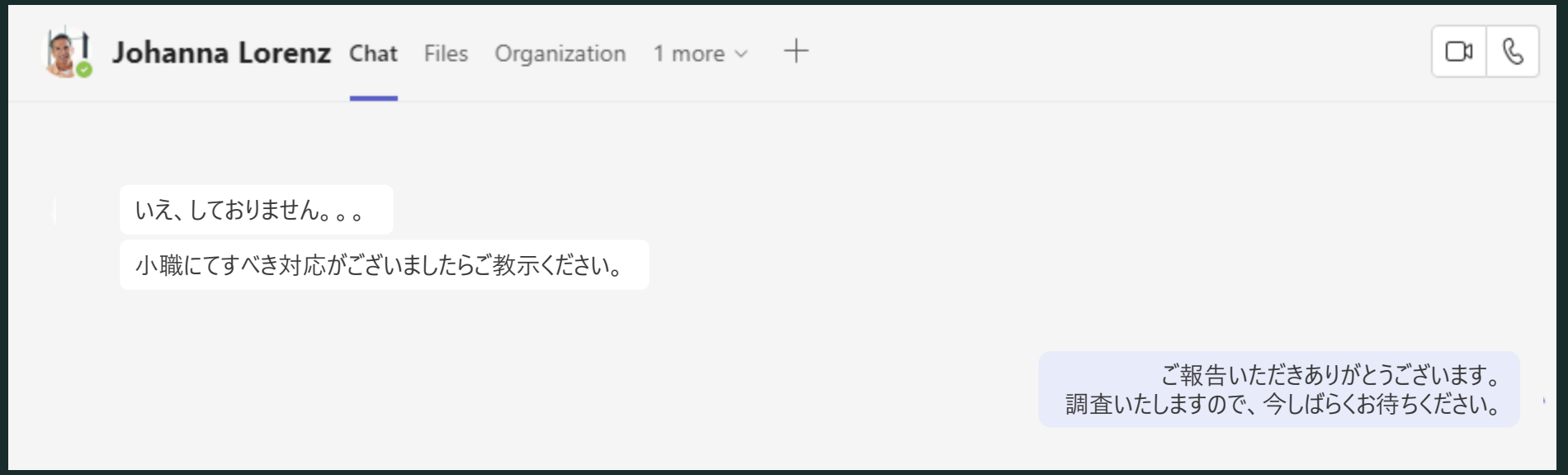
社員数	300人
ライセンス	Microsoft 365 Enterprise E3
メールサービス	Exchange Online only
多要素認証	Microsoft Authenticator (OTP アプリ) を使用

インシデント発生！



* Johanna さんは既定ユーザーです

インシデント発生！



* Johanna さんは既定ユーザーです

どのように調査・対応を進めればいいでしょうか

インシデント発生 → 初動対応 → ログ収集 → ログ調査 → 報告 → 防御策実装

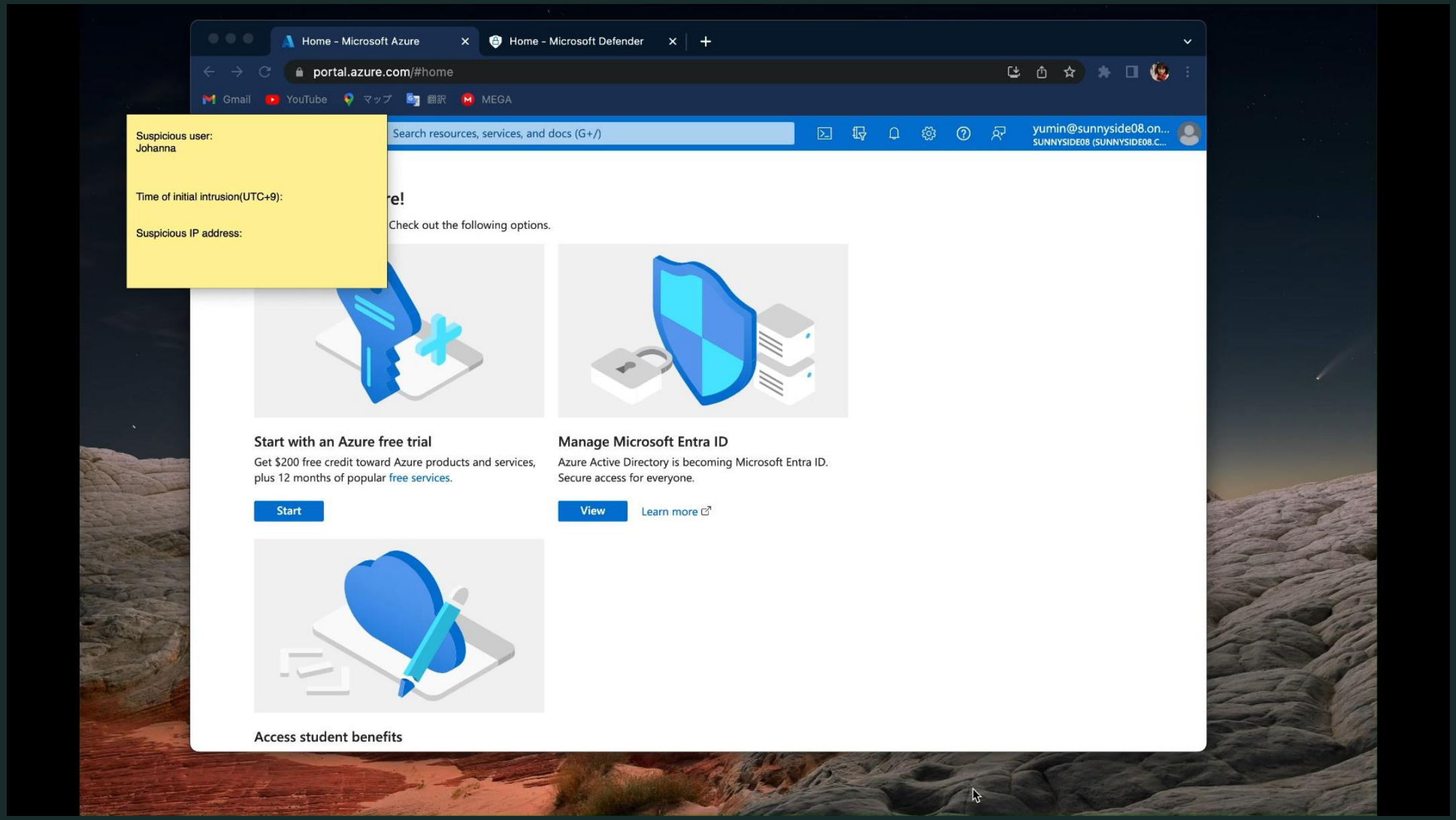
初動対応

初動対応

以下のいずれを実施しますか？

- 会社のネットワークを切断する
- Johanna さんのパソコンを回収・ディスククリーンアップする
- Johanna さんのアカウントを削除する
- Johanna さんのアカウントのセッション無効化 + パスワードリセット

DEMO 初動対応


Home - Microsoft Azure
Home - Microsoft Defender
portal.azure.com/#home
Gmail
YouTube
マップ
翻訳
MEGA
Suspicious user:
Johanna
Time of initial intrusion(UTC+9):
Suspicious IP address:
Search resources, services, and docs (G+/)
yumin@sunnyside08.on...
SUNNYSIDE08 (SUNNYSIDE08.C...
Check out the following options.
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Manage Microsoft Entra ID
Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.
View
Learn more
Access student benefits

DEMO 初動対応

✓被害を食い止める

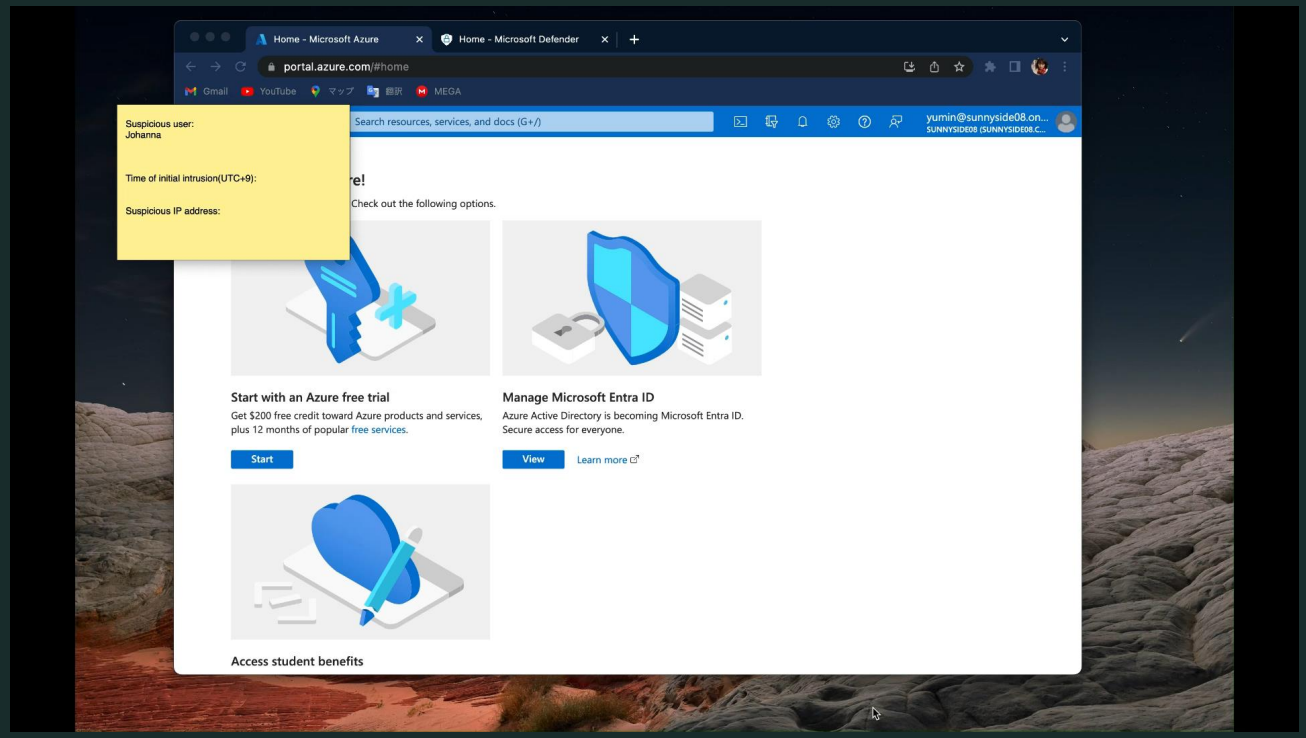
- セッションの切断
- 不審な多要素認証情報等の登録を削除

✓痕跡を消さない

- 「削除」は基本的に行わない
- 「無効化」オプションを模索する

✓被害の範囲を特定する

- 同様の被害が組織でないか



不正サインインを防ぐ

- ✓ 条件付きアクセスポリシーで Intune 管理された準拠済みまたは Microsoft Entra ハイブリッド参加済みデバイスからのサインインのみ許可する

  License: Entra ID Premium P1, Intune

- ✓ 条件付きアクセスポリシーで認証強度の高い方法 (Windows Hello for Business / FIDO2 Security Key …etc)によるサインインのみ許可する

  License: Entra ID Premium P1, 認証強度の高い端末

参考情報
条件付きアクセスの認証強度　https://learn.microsoft.com/ja-jp/entra/identity/authentication/concept-authentication-strengths

ログ収集・調査

ログの収集・調査

- 必要なログがわからない
- ログが保管されていない
- ログの調査方法がわからない
- 不審な痕跡が見つかったが対応がわからない

必要なログ / 保持期間 / 調査方針 を整理していく

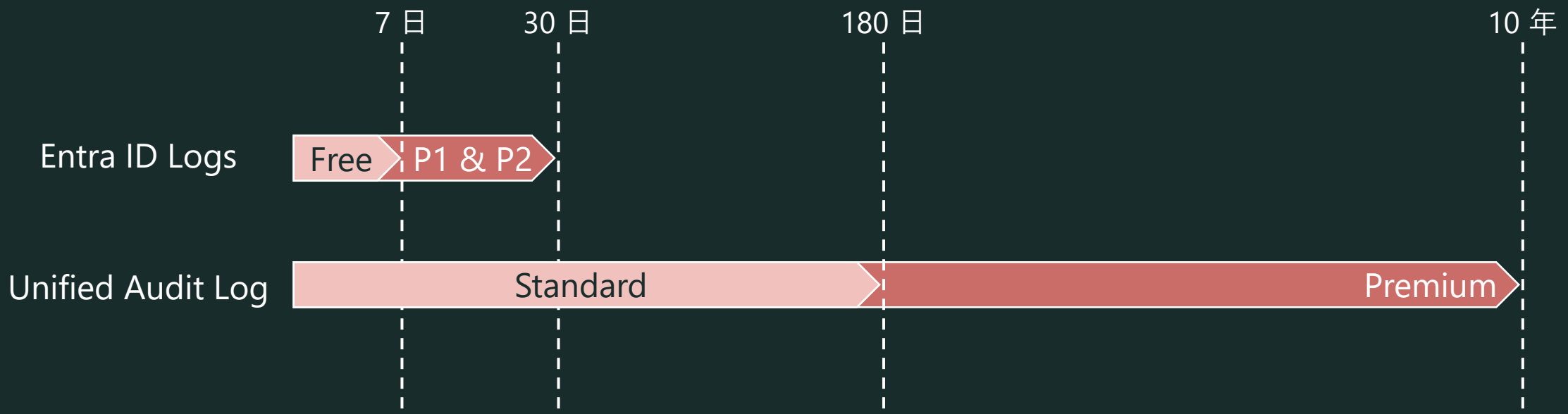
ログの収集

調査に使用するログ

ログの種類	目的
Entra ID Sign-in logs	不審サインインおよび接続元 IP の確認
Entra ID Audit logs	不審アクティビティの確認 例) セキュリティ情報の登録、アプリの登録...等
Unified Audit Log	特定ユーザーにおけるメール、ファイル関連の不審アクティビティの特定

ログの収集

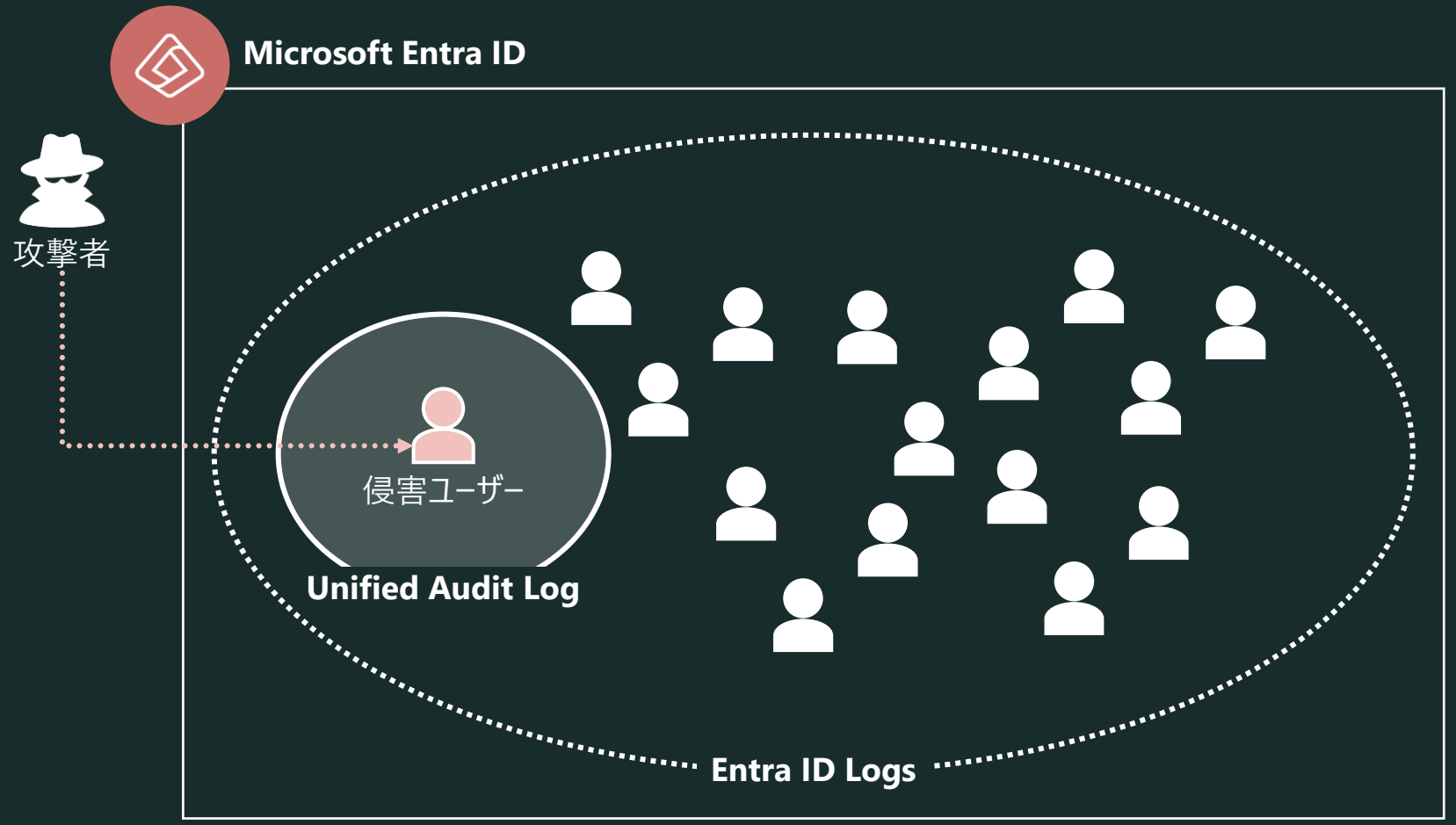
ログ種類別の保持期間



参考情報
Microsoft Entra のデータ保持　https://learn.microsoft.com/ja-jp/entra/identity/monitoring-health/reference-reports-data-retention#activity-reports
既定の監査ログの保持ポリシー　https://learn.microsoft.com/ja-jp/purview/audit-log-retention-policies#default-audit-log-retention-policy

ログの調査

ログ種類別に推奨される調査範囲



ログの収集・調査

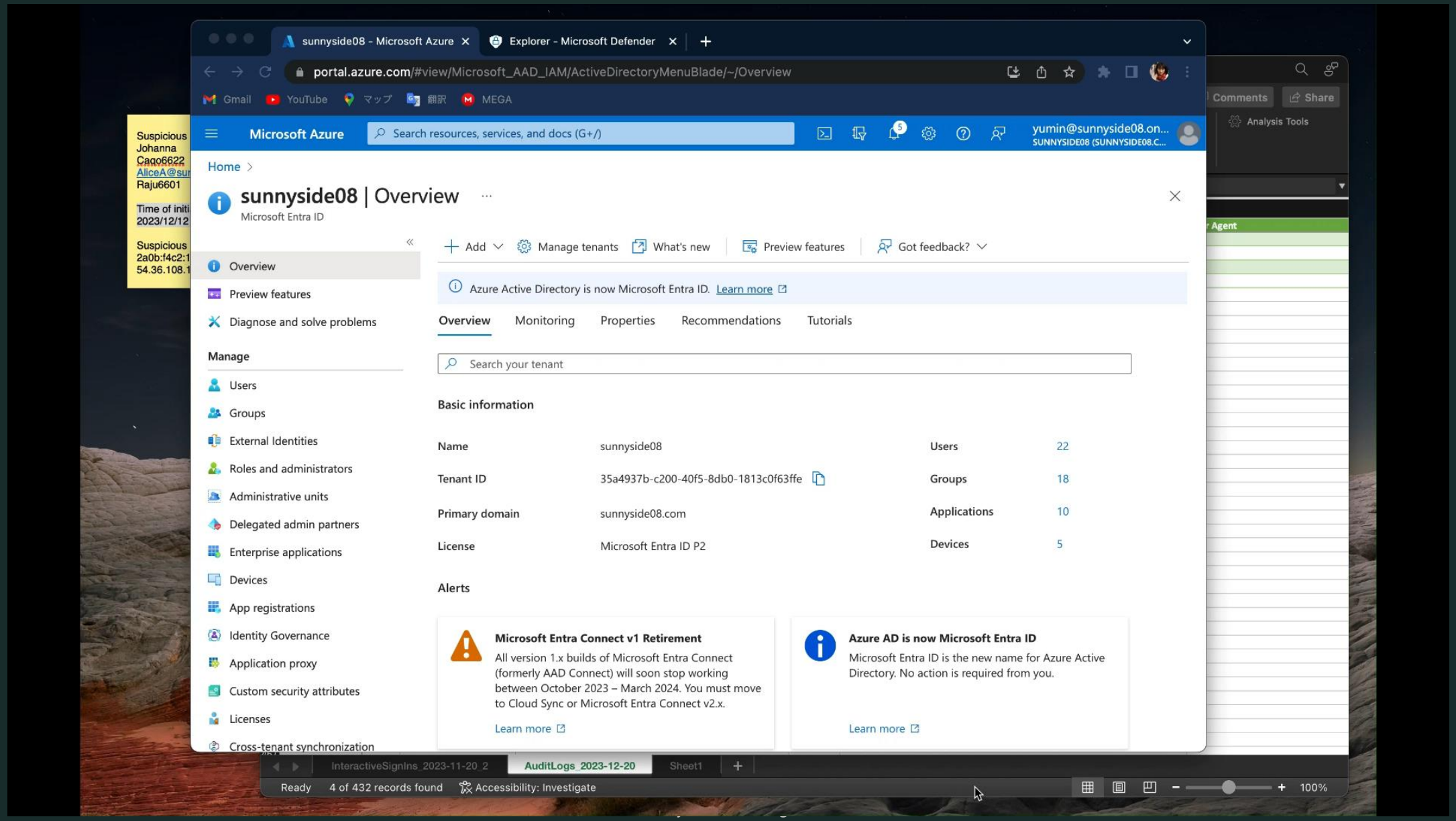
Points

- ✓ **ライセンス**と**ログ保持期間**の事前把握を!!!
- ✓ **既知の侵害**を起点に探索するとよい

▼参考

ログの種類	目的	調査範囲	ライセンス	保持期間
Entra ID Sign-in logs	不審サインインおよび接続元 IP の確認	テナント全体	Free	7 days
			P1	30 days
			P2	30 days
Entra ID Audit logs	不審アクティビティの確認 例) セキュリティ情報の登録、アプリの登録...等	テナント全体	同上	同上
Unified Audit Log	特定ユーザーにおけるメール、ファイル関連の不審アクティビティの特定	特定ユーザー	Audit (Standard)	180 days
			Audit (Premium)	10 years

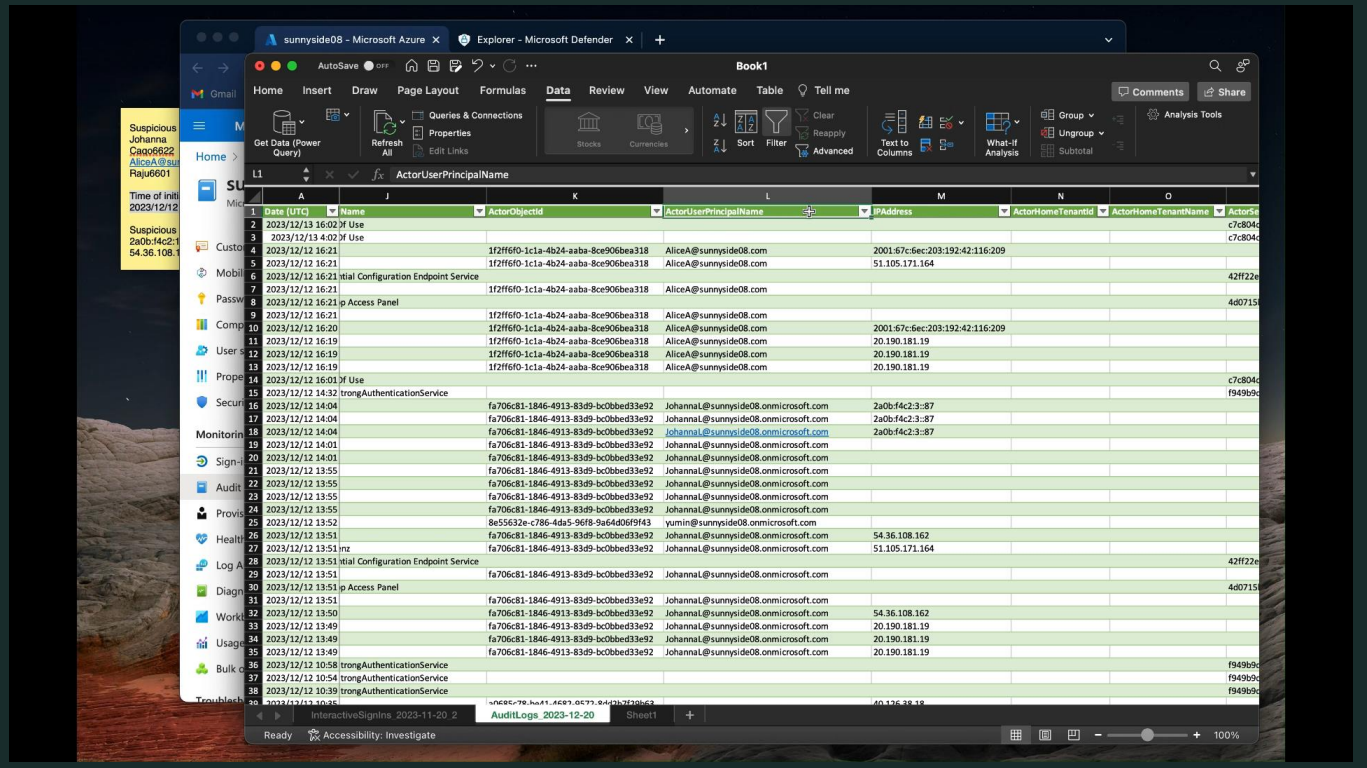
DEMO Entra ID Audit Logs の収集・調査



DEMO Entra ID Audit Logs の収集・調査

✓被害の特定と応答

- 不審なセキュリティ情報の登録を発見---> 削除
- 不審アプリの登録を発見---> 無効化、内容確認



攻撃の痕跡①,②　ユーザーのセキュリティ情報,端末の登録

実インシデントでは以下のような攻撃が見られた

今回のデモインシデントでは取り上げなかったが、端末の登録も過去に発生している

	A	C	D	E	F	H	I
1	Date (UTC)	Service	Category	Activity	Result	User Agent	ActorTyp
2	2023-06-23T16:15:11.6719696+00:0	Authentication Methods	UserManagement	User started security info registrati	Success		User
3	2023-06-23T16:15:21.7346546+00:0	Core Directory	UserManagement	Update user	Success		Application
4	2023-06-23T16:15:22.8336397+00:0	Core Directory	UserManagement	Update user	Success		User
5	2023-06-23T16:15:22.936093+00:00	Authentication Methods	UserManagement	User registered security info	Success		
6	2023-06-23T16:19:41.7904811+00:0	Core Directory	UserManagement	Update user	Success		
7	2023-06-23T16:19:52.496551+00:00	Core Directory	Device	Add registered owner to device	Success		Application
8	2023-06-23T16:19:52.5005549+00:0	Core Directory	Device	Add registered users to device	Success		Application
9	2023-06-23T16:19:52.7843714+00:0	Device Registration Service	Device	Register device	Success		
10	2023-06-27T16:47:25.6283145+00:0	Core Directory	UserManagement	Update user	Success		Application

セキュリティ情報の登録

端末の登録

Attacker's goal

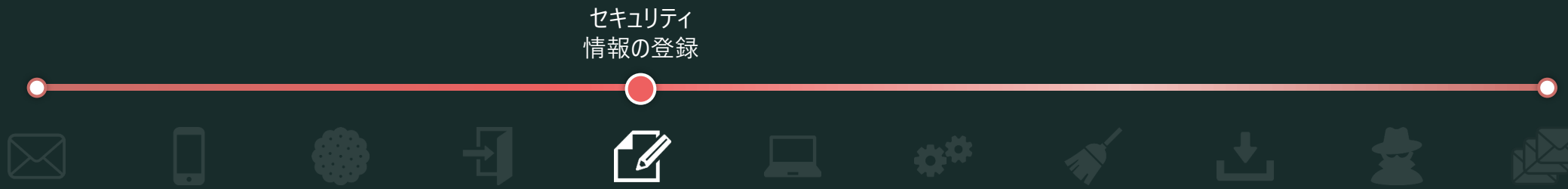
✓ セキュリティ情報の登録

窃取した Session Cookie が無効になった後も、MFA デバイスを使用して継続して不正サインインができる

✓ 端末の登録

アクセス元が Entra ID 登録済みデバイスに絞られている高価値な資産へアクセス可能に

セキュリティ情報の登録を防ぐ



✓ 条件付きアクセスポリシーで“信頼できる場所”以外からのセキュリティ情報の登録をブロックまたは MFA 等を要求する

※セキュリティ情報 (多要素認証) 未登録のユーザーはロックアウトされるため要注意

License: Entra ID Premium P1

参考情報 Microsoft Entra ID の統合されたセキュリティ情報登録
https://learn.microsoft.com/ja-jp/entra/identity/authentication/howto-registration-mfa-sspr-combined#create-a-policy-to-require-registration-from-a-trusted-location

攻撃の痕跡③　アプリ導入

実インシデントでは以下のような攻撃が見られた

*収集できたデータの都合上 Unified Audit Log を表示している

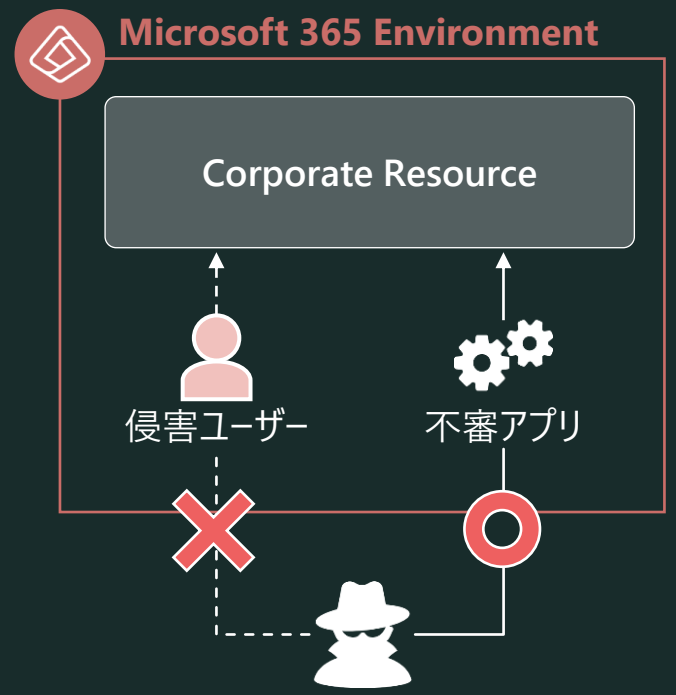
	B	C	D	F	G	H	I	J	K	L
1	CreationDate	Recor	Operation	AuditDat	Associate	Associate	dminUnitsNames			
34	8/29/2023 8:40:56 PM	15	UserLoggedIn	{"CreationTime":"2023-08-29						
35	8/29/2023 8:41:46 PM	8	Add application.	{"CreationTime":"2023-08-29						
36	8/29/2023 8:41:46 PM	8	Add owner to application.	{"CreationTime":"2023-08-29						
37	8/29/2023 8:41:47 PM	8	Add service principal.	{"CreationTime":"2023-08-29						
38	8/29/2023 8:41:47 PM	8	Add owner to service principa	{"CreationTime":"2023-08-29						
39	8/29/2023 8:42:15 PM	8	Update service principal.	{"CreationTime":"2023-08-29						
40	8/29/2023 8:42:16 PM	8	Update application.	{"CreationTime":"2023-08-29						
41	8/29/2023 8:42:16 PM	8	Update application Certificates	{"CreationTime":"2023-08-29						
42	8/29/2023 8:42:54 PM	15	UserLoginFailed	{"Cre		8-29				
43	8/29/2023 8:43:00 PM	8	Add app role assignment grar	{"Cre		8-29				
44	8/29/2023 8:43:00 PM	15	UserLoggedIn	{"CreationTime":"2023-08-29						
45	8/29/2023 8:43:00 PM	8	Consent to application.	{"CreationTime":"2023-08-29						
46	8/29/2023 8:43:00 PM	8	Add delegated permission gra	{"CreationTime":"2023-08-29						
47	8/29/2023 8:43:02 PM	15	UserLoggedIn	{"CreationTime":"2023-08-29						

アプリ導入

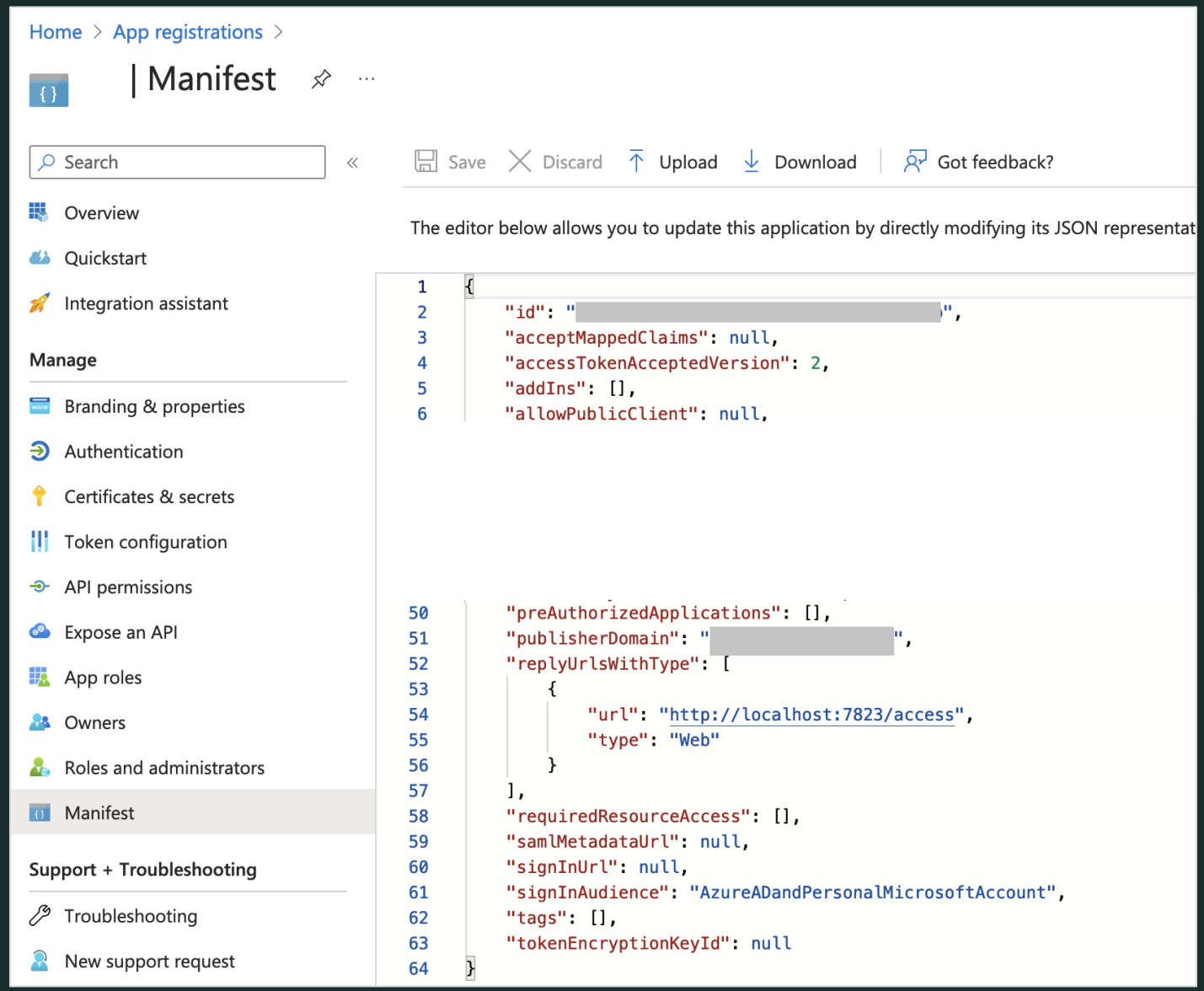
Attacker's goal

✓ アプリのもつAPI権限に応じて情報窃取が可能

攻撃の痕跡③　アプリ導入



✓ 実インシデントでは右記 [Manifest] を持つアプリ登録を確認



アプリ導入を防ぐ

✓ 一般ユーザーによるアプリの登録を防ぐ
- Azure ポータルより[ユーザーはアプリケーションを登録できる] を [いいえ] とする

License: Entra ID Free

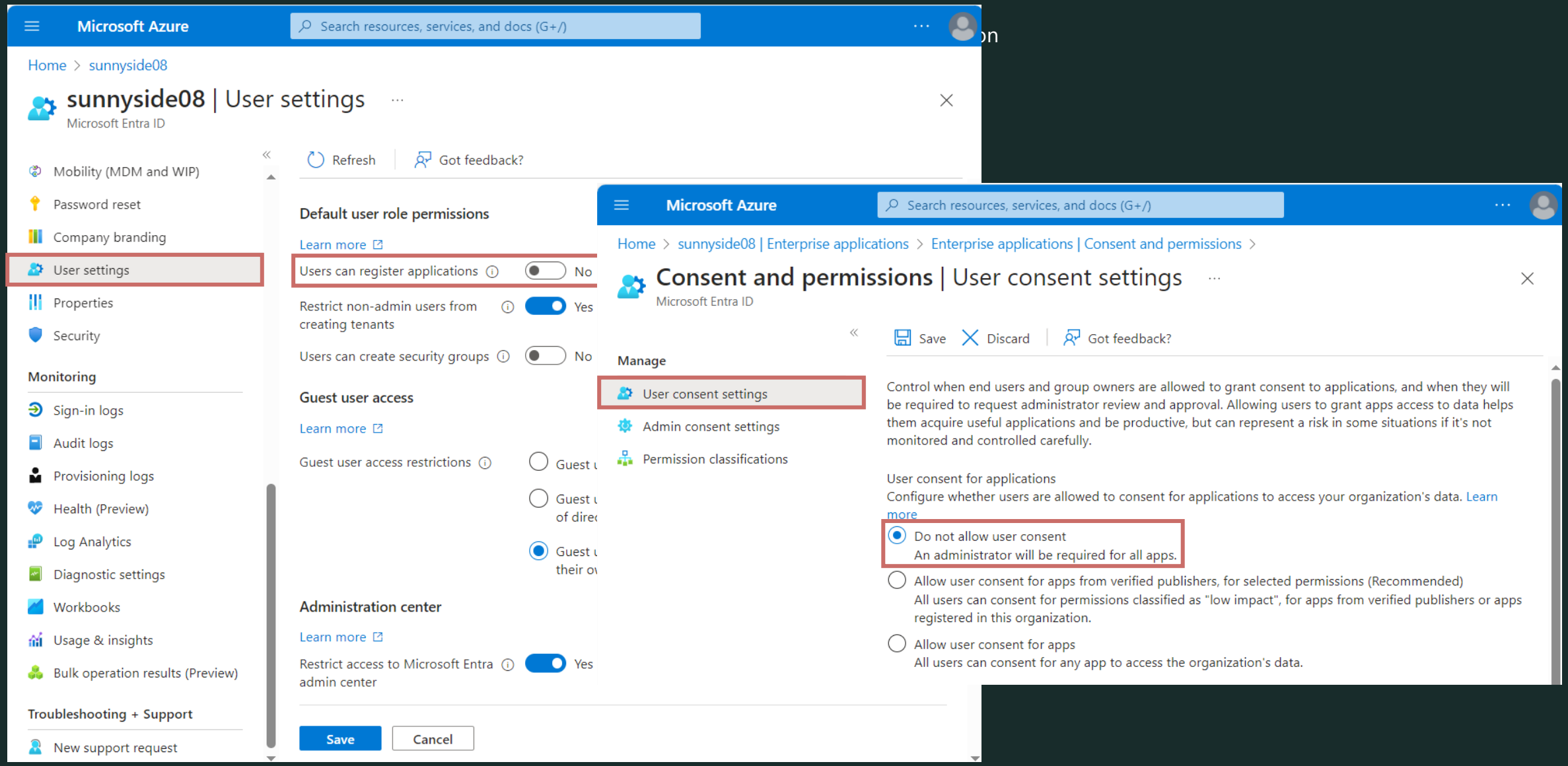
✓ 一般ユーザーによるアプリケーションへの同意を許可しない
- 一般ユーザーが同意を行うことで [エンタープライズ アプリケーション] にサービス プリンシパルを登録させない
- Azure ポータルより [エンタープライズ アプリケーション] > [同意とアクセス許可] にて [ユーザーの同意を許可しない] 設定とする

License: Entra ID Free

参考情報
アプリケーション登録またはアプリケーションへの同意を作成する既定の機能を無効にするには
https://learn.microsoft.com/ja-jp/entra/identity/role-based-access-control/delegate-app-roles#to-disable-the-default-ability-to-create-application-registrations-or-consent-to-applications

参考 : エンタープライズ アプリケーションに、管理者の知らないアプリケーションが追加されている!
https://jpazureid.github.io/blog/azure-active-directory/enterpriseapps-multitenantapps/

アプリ導入を防ぐ


Microsoft Azure
Search resources, services, and docs (G+/)
Home > sunnyside08
sunnyside08 | User settings
Microsoft Entra ID
Refresh
Got feedback?
Mobility (MDM and WIP)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Health (Preview)
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Default user role permissions
Learn more
Users can register applications
No
Restrict non-admin users from creating tenants
Yes
Users can create security groups
No
Guest user access
Learn more
Guest user access restrictions
Administration center
Learn more
Restrict access to Microsoft Entra admin center
Yes
Save
Cancel
Microsoft Azure
Search resources, services, and docs (G+/)
Home > sunnyside08 | Enterprise applications > Enterprise applications | Consent and permissions >
Consent and permissions | User consent settings
Microsoft Entra ID
Manage
User consent settings
Admin consent settings
Permission classifications
Save
Discard
Got feedback?
Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.
User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more
Do not allow user consent
An administrator will be required for all apps.
Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
Allow user consent for apps
All users can consent for any app to access the organization's data.

ログの収集・調査

Unified Audit Log 編

ログの収集 – Unified Audit Log

- Unified Audit Log のログ種類 *抜粋

#	RecordType	説明
1	ExchangeAdmin	Exchange 管理者監査ログからのイベント。
2	ExchangeItem	単一のアイテムに対して実行されるアクション (単一の電子メール メッセージの作成や受信など) の、Exchange メールボックス監査ログからのイベント。
3	ExchangeItemGroup	複数のアイテムに対して実行できるアクション (1 つ以上の電子メール メッセージの移動や削除など) の、Exchange メールボックス監査ログからのイベント。
4	SharePoint	SharePoint イベント。
6	SharePointFileOperation	SharePoint ファイル操作イベント。
7	OneDrive	Skype for Business イベント。
8	AzureActiveDirectory	Microsoft Entra イベント。
15	AzureActiveDirectoryStsLogon	Microsoft Entra ID でのセキュリティで保護されたトークン サービス (STS) ログオン イベント。

参考情報
AuditLogRecordType: https://learn.microsoft.com/ja-jp/office/office-365-management-api/office-365-management-activity-api-schema#auditlogrecordtype

ログの調査 – Unified Audit Log

- データスキーマ

	A	B	C	D	E
1	CreationDate	UserIds	RecordType	Operations	AuditData
2	2023/12/11 6:53	GradyA@sunnyside08.onmicrosoft.com	ExchangeAdmin	Remove-InboxRule	{"AppAccessContext":{"IssuedAtTime":"2023-12-11T00:12:44","UniqueTokenId
3	2023/12/11 6:33	GradyA@sunnyside08.onmicrosoft.com	ExchangeAdmin	New-InboxRule	023-12-11T06:53:00","Id":"5d65261a-df5f-4fc4-af09-08dbfa15d069","Operatio
4	2023/12/11 1:08	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	InboxRule","OrganizationId":"35a4937b-
			angeItem	Create	c200-40f5-8db0-1813c0f63ffe","RecordType":1,"ResultStatus":"True","UserKey"
			angeItem	Send	Workload":"Exchange","ClientIP":"157.113.166.14:13260","ObjectId":"GradyA
			angeItem	Create	¥¥17097852595923320833","UserId":"GradyA@sunnyside08.onmicrosoft.com",""
			angeItem	Send	ce00-000000000000","ClientAppId":"","ExternalAccess":false,"OrganizationNam
			angeItem	Create	r":"OS3P286MB1255
			angeItem	Send	(15.20.7068.030)","Parameters":[{"Name":"AlwaysDeleteOutlookRulesBlob","V
					Name":"Identity","Value":"f0af9d5e-1cc7-4fbd-9c19-818339d1ecc5¥¥17097852
					b5eb-61c3-1d01-2c6c4b0589d9","SessionId":"1a38c29e-b0bc-4623-a84e-5f6a4
					b33f-46ad-bee4-4a03e961a2e2"]}
11	2023/12/11 1:05	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	
12	2023/12/11 1:05	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"CreationTime":"2023-12-11T01:05:04","Id":"76fdd351-f7bf-4622-fef1-08dbf9
13	2023/12/11 1:01	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"CreationTime":"2023-12-11T01:01:10","Id":"b373f43d-faff-454d-9f02-08dbf9
14	2023/12/11 0:54	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"CreationTime":
15	2023/12/11 0:54	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"CreationTime":
16	2023/12/11 0:53	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"CreationTime":
17	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"CreationTime":"2023-12-11T00:44:42","Id":"97cbe468-fbf6-490e-b946-08db
18	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"CreationTime":"2023-12-11T00:44:42","Id":"97cbe468-fbf6-490e-b946-08db
19	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"CreationTime":"2023-12-11T00:44:04","Id":"14d0000f-712a-4ea7-c4d4-08db

多くの UAL にて以下 Field が共通である

`CreationDate, UserIds, RecordType, Operations, AuditData, ResultIndex, ResultCount, Identity, IsValid, ObjectState`

AuditData が JSON からなるため
場合に応じて PowerQuery を用いたパースが必要

ログの調査 – Unified Audit Log

Points

✓ 特徴的な攻撃手法を理解して、順序付けて RecordType を調査

<取得方法>

✓GUI

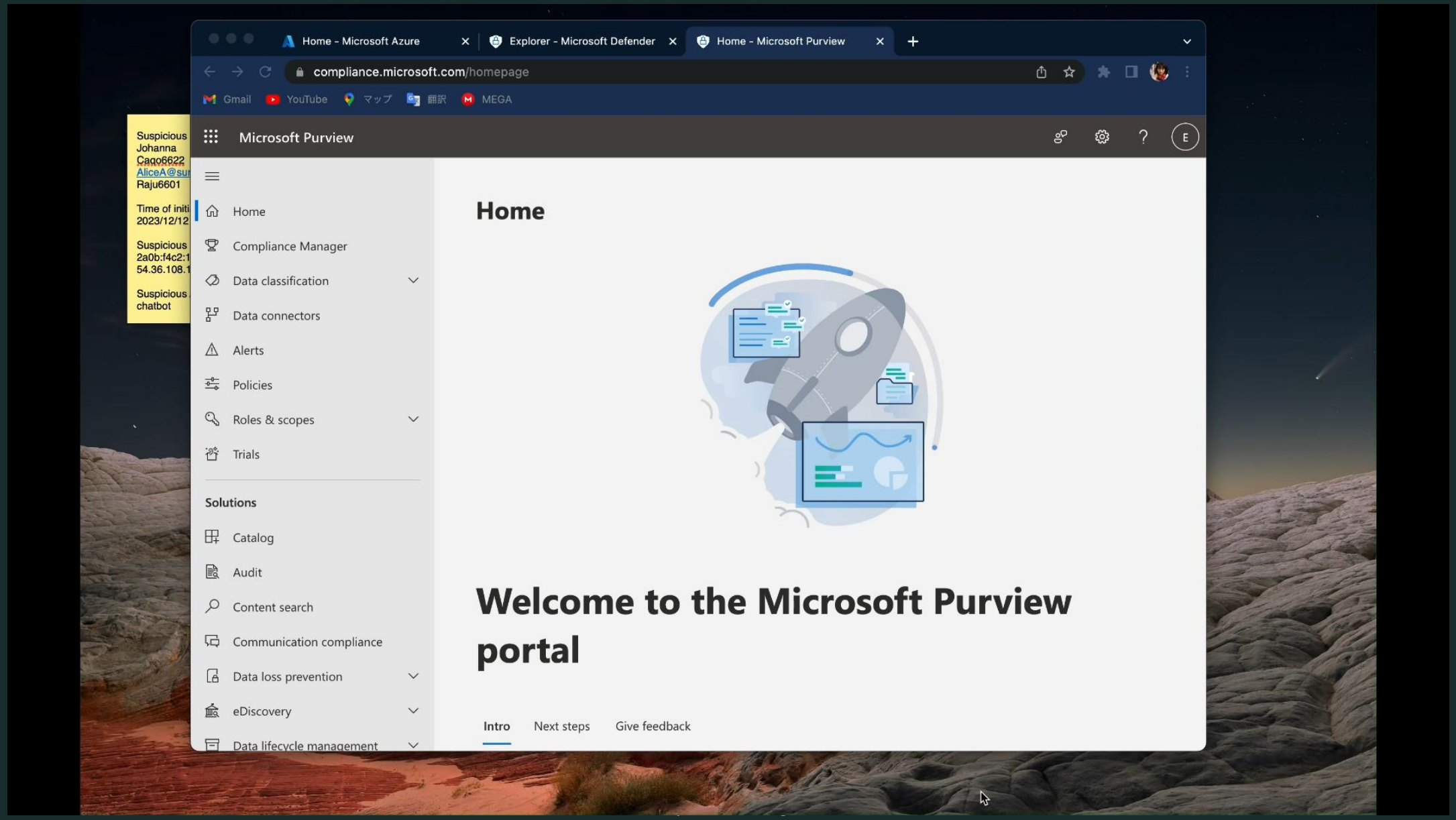
1. Microsoft Purview (https://compliance.microsoft.com/) にアクセスし、[Solutions | Audit] に遷移する
2. [Activities], [Users] で取得したい情報を指定し、[Search] をクリックする
3. [Completed] をクリックすると画面遷移した先で [Export] できる

✓Exchange PowerShell

1. Exchange Powershell に接続する
2. `Search-UnifiedAuditLog` によってローカルに UAL の csv をダウンロードする

参考情報
新しい検索の監査　https://learn.microsoft.com/ja-jp/purview/audit-new-search#get-started-with-audit-new-search
PowerShell スクリプトを使用して監査ログを検索する　https://learn.microsoft.com/ja-jp/purview/audit-log-search-script

DEMO Unified Audit Log の収集・調査



DEMO Unified Audit Log の収集・調査

✓被害の特定

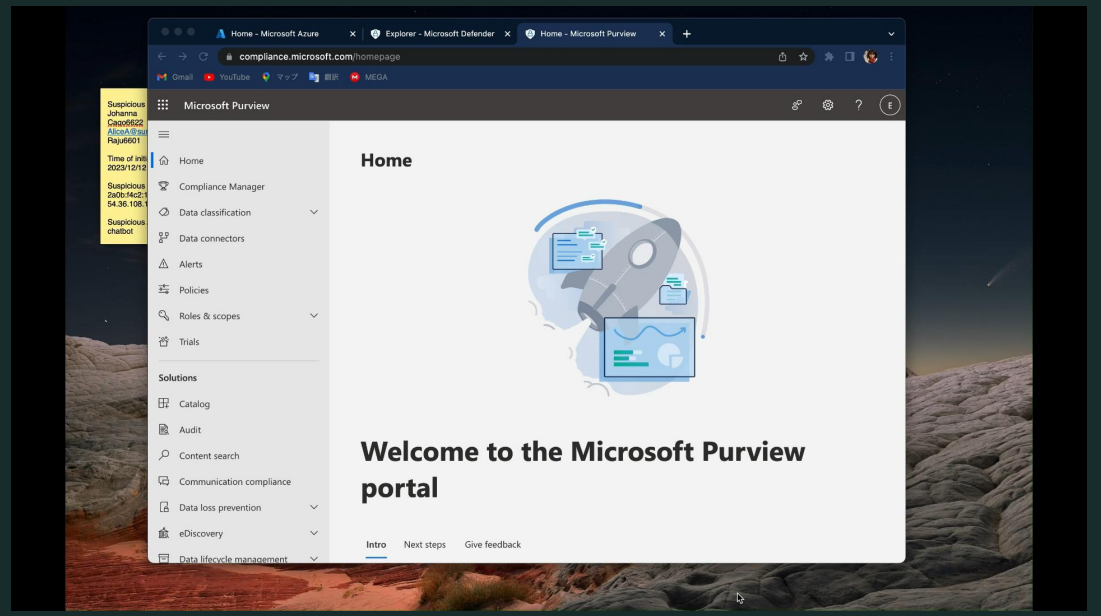
優先順位	RecordType	確認ポイント
1	**ExchangeAdmin**	InboxRule が作成・削除されていないか？
2	ExchangeItem	そのほかのメール閲覧・削除アクティビティはないか？
2	SharePointFileOperation	ファイル (SharePoint, OneDrive) の閲覧・削除アクティビティはないか？

✓他被害の調査

- “SessionId”を起点にRecordTypeを横断した攻撃者アクティビティを特定

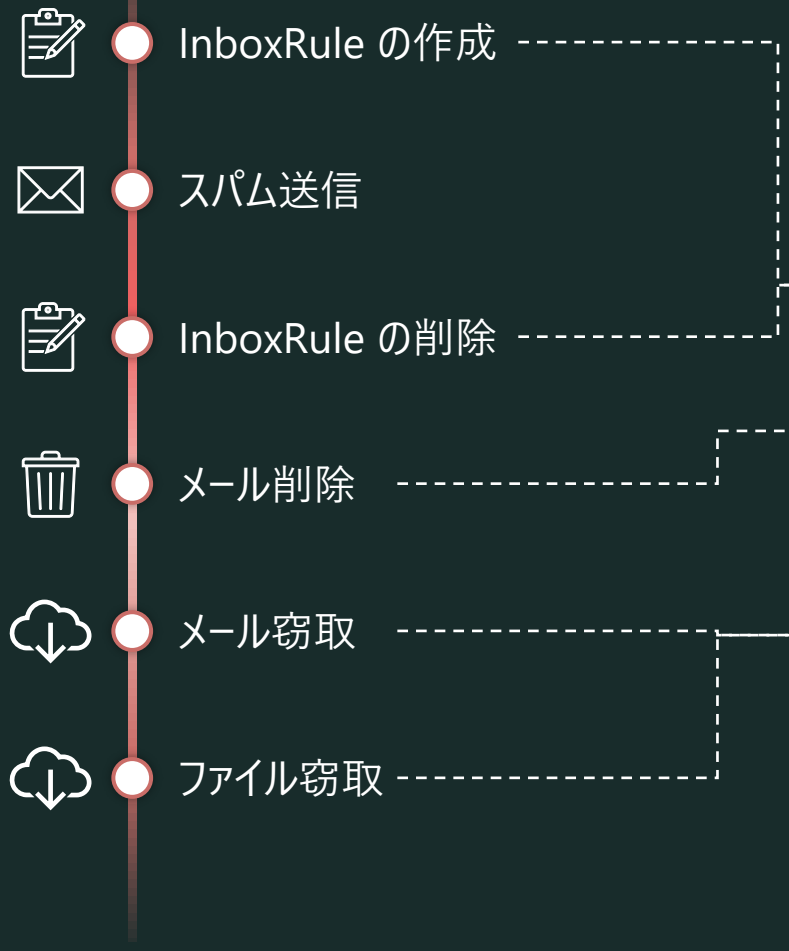
✓応答

- 不審な InboxRule を発見---> ユーザーヒアリング、削除



攻撃の痕跡④,⑤　侵害痕跡の削除～情報窃取

実インシデントより、Unified Audit Log を使用して以下の痕跡 (順不同) を確認できる



Attacker's goal

✓ **侵害痕跡の削除**

- スパムの大量送信やバウンスメール
  をゴミ箱に移動させ、侵害に気づかせない
- 後続の攻撃に都合の悪い情報の削除

✓ **情報窃取**

- BEC 等の後続の攻撃に使用

攻撃の痕跡④　侵害痕跡の削除

- InboxRule の作成
- スパム送信
- InboxRule の削除
- メール削除
- メール窃取
- ファイル窃取

*RecordType = 1 (ExchangeAdmin)

	A	B	C	D	E	F	G	H
1	CreationDate	RecordTyp	Operation	UserId	AuditD	Associa	Associa	dAdminUnitsN
9	6/16/2023 7:51:04 PM	2	MailboxLogin					
10	6/16/2023 7:54:02 PM	1	New-InboxRule					
11	6/17/2023 6:05:22 PM	2	MailboxLogin					
12	6/17/2023 6:05:22 PM	2	MailboxLogin					
13	6/19/2023 11:15:08 A	2	MailboxLogin					
14	6/19/2023 2:19:52 PM	2	Create					
15	6/19/2023 2:29:32 PM	2	Create					
16	6/19/2023 2:32:22 PM	1	New-InboxRule					
17	6/19/2023 2:34:28 PM	2	Update					
18	6/19/2023 2:43:59 PM	2	Update					
19	6/19/2023 2:44:09 PM	2	Update					
20	6/19/2023 2:44:21 PM	2	Create					
21	6/19/2023 2:45:46 PM	2	Create					
22	6/19/2023 2:46:45 PM	2	Update					
23	6/19/2023 2:46:49 PM	2	Update					
24	6/19/2023 2:46:55 PM	2	Update					
25	6/19/2023 2:50:28 PM	2	Create					
26	6/19/2023 2:53:34 PM	1	New-InboxRule					
27	6/19/2023 4:50:34 PM	2	Update					
28	6/19/2023 4:50:49 PM	2	Create					
29	6/19/2023 4:52:45 PM	2	Create					
30	6/19/2023 4:54:36 PM	2	Create					

攻撃の痕跡④　侵害痕跡の削除

- InboxRule の作成
- スパム送信
- InboxRule
- メール削除
- メール窃取
- ファイル窃取

	A	B	C	D	E	F	G	H
1	CreationDate	RecordTyp	Operation	UserId	AuditD	Associa	Associa	dAdminUnitsN
9	6/16/2023 7:51:04 PM	2	MailboxLogin					
10	6/16/2023 7:54:02 PM	1	New-InboxRule					
11	6/17/2023 6:05:22 PM	2	MailboxLogin					
12	6/17/2023 6:05:22 PM	2	MailboxLo					
13	6/19/2023 11:15:08 A	2	MailboxLo					
14	6/19/2023 2:19:52 PM	2	Create					
21	6/19/2023 2:45:46 PM	2	Create					
22	6/19/2023 2:46:45 PM	2	Update					
23	6/19/2023 2:46:49 PM	2	Update					
24	6/19/2023 2:46:55 PM	2	Update					
25	6/19/2023 2:50:28 PM	2	Create					
26	6/19/2023 2:53:34 PM	1	New-Inbo					
27	6/19/2023 4:50:34 PM	2	Update					
28	6/19/2023 4:50:49 PM	2	Create					
29	6/19/2023 4:52:45 PM	2	Create					
30	6/19/2023 4:54:36 PM	2	Create					

攻撃者が送信したスパムメールへの返信を
削除済みフォルダに自動転送する InboxRule
→ユーザーが侵害に気づかないように

```
"Parameters": [
        {
            "Name": "MoveToFolder",
            "Value": "Deleted Items"
        },
        {
            "Name": "Name",
            "Value": ".."
        },
        {
            "Name": "SubjectOrBodyContainsWords",
            "Value": "Re: <spam mail title>"
        },
        {
            "Name": "MarkAsRead",
            "Value": "True"
        },
        {
            "Name": "StopProcessingRules",
            "Value": "False"
        }
    ]
```

攻撃の痕跡④　侵害痕跡の削除

- InboxRule の作成
- スパム送信
- InboxRule の削除
- メール削除
- メール窃取
- ファイル窃取

	B	C	D	E	F	
1	CreationDate	RecordTy	Operation	UserId	AuditData	AssociatedAd
38	5/25/2023 11:36:35	2	Create	[redacted]	[redacted]	[redacted]
39	5/25/2023 11:38:12	3	SoftDelete	[redacted]	[redacted]	[redacted]
40	5/25/2023 11:49:50	2	Create	[redacted]	[redacted]	[redacted]
41	5/25/2023 11:51:01	3	SoftDelete	[redacted]	[redacted]	[redacted]
42	5/25/2023 11:55:10	3	MoveToDeletedItems	[redacted]	[redacted]	[redacted]
43	5/25/2023 11:55:25	3	MoveToDeletedItems	[redacted]	[redacted]	[redacted]
44	5/25/2023 11:55:25	3	MoveToDeletedItems	[redacted]	[redacted]	[redacted]
45	5/25/2023 11:58:14	2	Create	[redacted]	[redacted]	[redacted]
46	5/25/2023 11:59:19	3	SoftDelete	[redacted]	[redacted]	[redacted]
47	5/25/2023 12:04:50	2	Create	[redacted]	[redacted]	[redacted]
48	5/25/2023 12:06:43	3	SoftDelete	[redacted]	[redacted]	[redacted]
49	5/25/2023 12:07:35	3	SoftDelete	[redacted]	[redacted]	[redacted]
50	5/25/2023 12:09:50	2	Update	[redacted]	[redacted]	[redacted]
51	5/25/2023 12:10:40	2	Create	[redacted]	[redacted]	[redacted]
52	5/25/2023 12:11:49	3	SoftDelete	[redacted]	[redacted]	[redacted]
53	5/25/2023 12:11:57	3	MoveToDeletedItems	[redacted]	[redacted]	[redacted]
54	5/25/2023 12:12:12	3	SoftDelete	[redacted]	[redacted]	[redacted]
55	5/25/2023 14:17:54	2	Create	[redacted]	[redacted]	[redacted]
56	5/25/2023 14:46:23	2	Create	[redacted]	[redacted]	[redacted]
57	5/25/2023 19:43:14	1	New-InboxRule	[redacted]	[redacted]	[redacted]
58	5/25/2023 19:43:14	3	HardDelete	[redacted]	[redacted]	[redacted]
59	5/25/2023 19:43:54	1	New-InboxRule	[redacted]	[redacted]	[redacted]
60	5/26/2023 1:40:33	2	Create	[redacted]	[redacted]	[redacted]
61	5/27/2023 6:12:38	2	Create	[redacted]	[redacted]	[redacted]
62	5/27/2023 6:12:43	3	SoftDelete	[redacted]	[redacted]	[redacted]

攻撃の痕跡④　侵害痕跡の削除

- InboxRule の作成
- スパム送信
- InboxRule の削除
- メール削除
- メール窃取
- ファイル窃取

"AffectedItems" について、確認・復元する

```
{
    "CreationTime": "2023-05-25T19:43:14",
    "Id": "0xxx0x0x-0000-0x00-0xxx-00xx0x0000x0",
          [...skipped...]
    "SessionId": "0x000x00-xx0x-000x-00x0-00x00000x0x0",
    "AffectedItems": [
        {
            "Id": "RgAAAADTH2BwALBELd3a¥/PAAEMAD+¥/Fm4QEc4X¥/WhbAAJ",
            "InternetMessageId": "<G0005BE026CBF00X0X@S000A3.xxxxxx00.prod.outlook.com>",
            "ParentFolder": {
                "Id": "AAAADTH2BwALBELd3a¥/PAAEMAA",
                "Path": "¥¥Inbox"
            },
            "Subject": "Outlook Rules Organizer"
        }
    ],
    "CrossMailboxOperation": false,
    "Folder": {
        "Id": "LgAAAADTH2BwALBELd3a¥/PAAEMAA",
        "Path": "¥¥Inbox"
    }
}
```

	B		
1	CreationDate		
38	5/25/2023 11:36:35		
39	5/25/2023 11:38:12		
40	5/25/2023 11:49:50		
41	5/25/2023 11:51:01		
42	5/25/2023 11:55:10		
43	5/25/2023 11:55:25		
44	5/25/2023 11:55:25		
45	5/25/2023 11:58:14		
46	5/25/2023 11:59:19		
47	5/25/2023 12:04:50		
48	5/25/2023 12:06:43		
49	5/25/2023 12:07:35		
50	5/25/2023 12:09:50		
51	5/25/2023 12:10:40		
52	5/25/2023 12:11:49		
53	5/25/2023 12:11:57		
54	5/25/2023 12:12:12		
55	5/25/2023 14:17:54		
56	5/25/2023 14:46:23	2	Create
57	5/25/2023 19:43:14	1	New-InboxRule
58	5/25/2023 19:43:14	3	HardDelete
59	5/25/2023 19:43:54	1	New-InboxRule
60	5/26/2023 1:40:33	2	Create
61	5/27/2023 6:12:38	2	Create
62	5/27/2023 6:12:43	3	SoftDelete

攻撃の痕跡④　侵害痕跡の削除

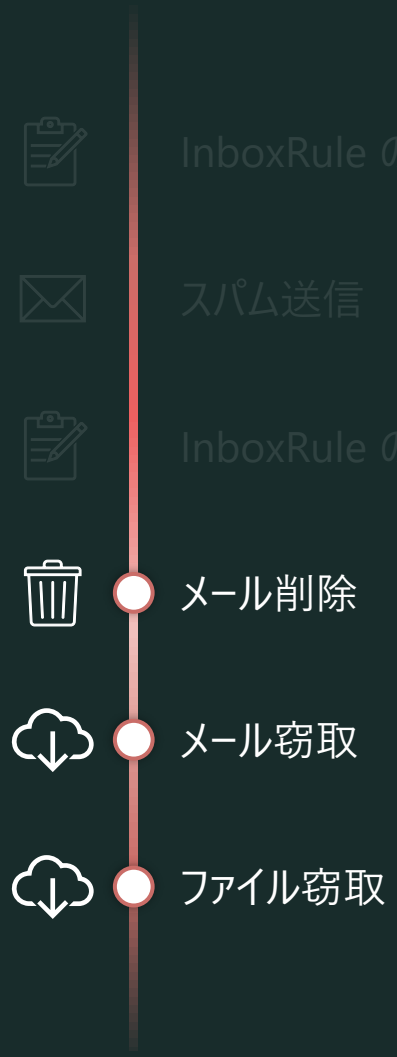
- InboxRule の作成
- スパム送信
- InboxRule の削除
- **メール削除**
- メール窃取
- ファイル窃取

	B	C	D	E	F	
1	CreationDate	RecordTy	Operation	UserId	AuditData	AssociatedAd
38	5/25/2023 11:36:35	2	Create	a		
39	5/25/2023 11:38:12	3	SoftDelete	a		
40	5/25/2023 11:49:50	2	Create	a		
41	5/25/2023 11:51:01	3	SoftDelete	a		
42	5/25/2023 11:55:10	3	MoveToDeletedItems	a		
43	5/25/2023 11:55:25	3	MoveToDeletedItems	a		
44	5/25/2023 11:55:25	3	MoveToDeletedItems	a		
45	5/25/2023 11:58:14	2	Create	a		
46	5/25/2023 11:59:19	3	SoftDelete	a		
47	5/25/2023 12:04:50	2	Create	a		
48	5/25/2023 12:06:43	3	SoftDelete	a		
49	5/25/2023 12:07:35	3	SoftDelete	a		
50	5/25/2023 12:09:50	2	Update	a		
51	5/25/2023 12:10:40	2	Create	a		
52	5/25/2023 12:11:49	3	SoftDelete	a		
53	5/25/2023 12:11:57	3	MoveToDeletedItems	a		
54	5/25/2023 12:12:12	3	SoftDelete	a		
55	5/25/2023 14:17:54	2	Create	a		
56	5/25/2023 14:46:23	2	Create	a		
57	5/25/2023 19:43:14	1	New-InboxRule	a		
58	5/25/2023 19:43:14	3	HardDelete	a		
59	5/25/2023 19:43:54	1	New-InboxRule	a		
60	5/26/2023 1:40:33	2	Create	a		
61	5/27/2023 6:12:38	2	Create	a		
62	5/27/2023 6:12:43	3	SoftDelete	a		

情報窃取でも共通しているが、
一般ユーザーも実施する操作であるため
"SessionId"や"ClientIP"、"ClientInfoString"
等のプロパティを確認

攻撃の痕跡④,⑤　侵害痕跡の削除～情報窃取

“SessionId”以外の手法では、以下のように侵害痕跡と思われるアクティビティとそうでないものを見分けられる



✓ 一般ユーザアクティビティ例

```
{
    "CreationTime": "2023-05-27T06:12:43",

            [...skipped...]

    "Workload": "Exchange",
    "ClientIP": "20.100.101.102",
    "UserId": "user@example.com",
    "ClientIPAddress": "203.0.113.0",
    "ClientInfoString":
"Client=MSExchangeRPC",
    "ClientProcessName": "OUTLOOK.EXE",
    "ClientRequestId": "{00X0XXXX-000X-0X00-
0X00-X00X0XXXX000}",
    "ClientVersion": "16.0.16327.20200",
    "ExternalAccess": false,

            [...skipped...]
}
```

✓ 攻撃者アクティビティ例

```
{
    "CreationTime": "2023-05-27T06:12:43",

            [...skipped...]

    "Workload": "Exchange",
    "ClientIP": “20.100.101.102",
    "UserId": "user@example.com",
    "AppId": "00000002-0000-0ff1-ce00-
000000000000",
    "ClientIPAddress": "20.100.101.102",
    "ClientInfoString":
"Client=OWA;Action=ViaProxy",
    "ExternalAccess": false,

            [...skipped...]
}
```

報告

調査レポートの作成

インシデントは分析のみでなく、結果や残対応まで正確にユーザーに伝えましょう

いただいたログより以下の不審なアクティビティがありました、想定外の操作ではないかご確認ください。
1. 不審なサインイン
2023/12/12 13:50:17 - 14:11:43 (UTC) の間、Johanna 氏のアカウントへの以下 UserAgent および IP からの不審サインインが見られた
Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
2a0b:f4c2:1::1 , , US ...(略)

2. 2023/12/12 13:55:36 - 14:04:58 (UTC) の間に Johanna 氏の権限で
・下記アプリケーションを追加
TargetDisplayName: chatbot
TargetObjectId: 80cf2cdc-2178-400b-ab98-a0677b6bd694
・アプリケーションに以下の権限を委任
ConsentType: AllPrincipals
Scope: Mail.ReadWrite MailboxSettings.ReadWrite User.Read

3. 以下セキュリティ情報の登録　...(略)

4. 以下転送ルールの作成　...(略)

① 侵害内容のサマリ

調査レポートの作成

インシデントは分析のみでなく、結果や残対応まで正確にユーザーに伝えましょう

5. Johanna 氏のアカウントで発生した不審アクティビティ
2023/12/12 5:03 (UTC) に "REVISED INVOICE" メールを送信した
2023/12/12 5:12:10 - 5:15:38(UTC) に以下情報のダウンロードが確認されました
- PO_EcoGreenLand_inc.docx
- Comprehensive ERP System Requirements.docx

各アクティビティについて、以下対応が完了していることを確認しています。
2. 不審アプリの無効化
3. 不審セキュリティ情報の削除
4. 不審転送ルールの削除

貴社にて、以下対応をお願いいたします。
2. 不審アプリの削除
5. ダウンロードされた情報や送信済みメールに対する各社注意喚起

お忙しいところ恐れ入りますが、どうぞよろしくお願いいたします。

② 侵害への対応サマリ

③ 追加の依頼事項

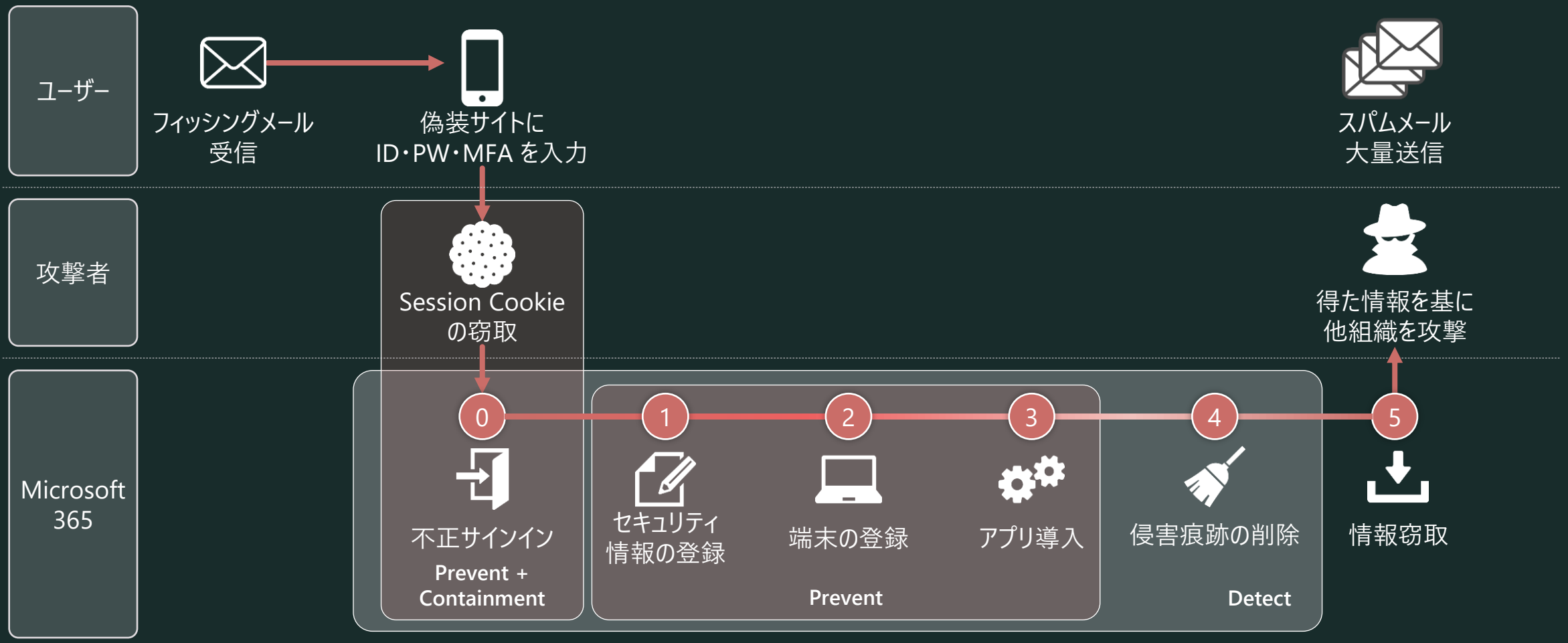
防御策の実装

インシデントの流れ

* E5, Entra ID Premium P2 を持っている場合は、Entra ID Logs の前に Identity Protectionのアラート確認がおすすめです。
* Unified Audit Log は Entra ID Log と類似した証跡を提供しますが、一部の痕跡は Entra ID Log で調査することを推奨します。

防御策の実装

インシデント発生　初動対応　ログ収集　ログ調査　報告　防御策実装



まとめ

*全ての侵害シナリオは網羅できていないため、ご了承ください。下記以外に Power Platform や First Party App の悪用、ゲストユーザーの招待といった手法を用いるAPTの事例が報告されています。

初動対応が一番大切！

1. 侵害時刻より現在がセッション有効期間内の場合、セッションを無効化
2. 侵害ユーザーのパスワードリセット
3. 侵害ユーザーの不審なセキュリティ情報の削除
4. 侵害ユーザーの不審な登録端末の無効化
5. 侵害ユーザーの不審なメール転送ルールの削除
6. 侵害前後で登録された Entra ID アプリの無効化

繰り返し

7. ログ取得依頼・採取・調査
8. 侵害起点メールの他受信者の調査
9. メール受信前後の不審なサインインの調査、他侵害ユーザの特定

まとめ

実際に発生した M365 アカウント侵害インシデントをもとに以下を説明しました

- インシデント発生時の初動対応
- インシデント調査の勘所
- 攻撃者の痕跡と該当ログの詳説
- インシデントを未然に防ぐ防御策

The goal:

✓インシデントレスポンスの勘所を理解し、
侵害発生時にすぐ対応できるように

✓有効な防御策を把握する

Thank you

Appendix: 初動対応参考

*全ての侵害シナリオは網羅できていないため、ご了承ください。下記以外に Power Platform や First Party App の悪用、ゲストユーザーの招待といった手法を用いるAPTの事例が報告されています。

初動対応 まとめ

1. 侵害時刻より現在がセッション有効期間内の場合、セッションを無効化
2. 侵害ユーザーのパスワードリセット
3. 侵害ユーザーの不審なセキュリティ情報の削除
4. 侵害ユーザーの不審な登録端末の無効化
5. 侵害ユーザーの不審なメール転送ルールの削除
6. 侵害前後で登録された Entra ID アプリの無効化

繰り返し

7. ログ取得依頼・採取・調査
8. 侵害起点メールの他受信者の調査
9. メール受信前後の不審なサインインの調査、他侵害ユーザの特定

初動対応 詳細

1. 侵害時刻より現在がセッション有効期間内の場合、セッションを無効化
   - ユーザー管理者以上の権限を持つアカウントで Azure Portal (https://portal.azure.com/) にアクセスする
   - [Microsoft Entra ID] - [ユーザー] にて侵害されたユーザーを検索し、ユーザー画面に遷移する
   - [セッションの取り消し] を行う

   ※事前に継続的アクセス評価 (Continuous Access Evaluation) が有効であることを確認する

2. 侵害ユーザーのパスワードリセット
   - 同様にユーザー画面にて[パスワードのリセット]を行う

3. 侵害ユーザーの不審なセキュリティ情報の削除
   - ユーザー画面にて [認証方法] セクションに切り替える
   - 「使用可能な認証方法」にて不審なセキュリティ情報がないか確認する
   - あった場合は右端の [...] - [削除] の順にクリックする

4. 侵害ユーザーの不審な登録端末の削除
   - ユーザー画面にて [デバイス] セクションに切り替える
   - 不審なデバイスを選択し、[無効にする] をクリックする

初動対応 詳細

5. 侵害ユーザーの不審なメール転送ルールの削除
   - 接続元PCにて事前に ExchangeOnlineManagement モジュールをインストールする
     ```
     Import-Module ExchangeOnlineManagement
     ```
   - Exchnage Online に Powershell で接続する
     ```
     Connect-ExchangeOnline -UserPrincipalName admin@example.com
     ```
   - 事前に存在する InboxRule を確認する
     ```
     Get-InboxRule -Mailbox Joker@example.com
     ```
   - 不審な InboxRule を削除する
     ```
     Remove-InboxRule -Mailbox Joker@example.com -Identity "ProjectA-MoveToFolderA"
     ```

6. 侵害前後で登録された Entra ID アプリの無効化
   - アプリケーション閲覧者以上の権限を持つアカウントで Azure Portal (https://portal.azure.com/) にアクセスする

     【 エンタープライズ アプリケーション 】
     - [Microsoft Entra ID] - [エンタープライズ アプリケーション] - [すべてのアプリケーション] の順に遷移する
     - [フィルターの追加] - [作成日 == 過去7日間(*参考)] でソートし、インシデント発生前後で新規アプリの登録がないか確認する、ある場合は選択する
     - [プロパティ] セクションに切り替え、「ユーザーのサインインが有効になっていますか?」を”いいえ”にする
     - インシデントレスポンスが完了したら削除する

     【 アプリの登録 】
     - [Microsoft Entra ID] - [アプリの登録] - [すべてのアプリケーション]の順に遷移する
     - [作成日] でインシデント発生前後にできたアプリをソートする、不審なアプリがある場合は選択する
     - [証明書とシークレット] セクションに切り替え、シークレットがある場合は削除する
     - [API のアクセス許可] セクションに切り替え、不審なアクセス許可は削除する
     - インシデントレスポンスが完了したら削除する

初動対応 詳細

7. ログ取得依頼・採取・調査

【 Entra ID Logs 】

- Azure Portal (https://portal.azure.com/) にアクセスする
- [Microsoft Entra ID] - [監視と正常性] - [サインイン ログ] または [監査ログ] に遷移し、[ダウンロード] をクリックする

【 Unified Audit Log 】

- Exchnage Online に Powershell で接続する

```
Connect-ExchangeOnline -UserPrincipalName admin@example.com
```

- Search-UnifiedAuditLog を使用してログを取得する。以下は複数のRecordTypeを一括出力した参考例である。

```
$recordTypes = @("ExchangeAdmin", "ExchangeItem", "ExchangeItemGroup", "AzureActiveDirectory",
"AzureActiveDirectoryStsLogon", "SharePoint", "SharePointFileOperation", "OneDrive")
$startDate = "12/1/2023″
$endDate = "12/14/2023" $userId = Joker@example.com
$resultSize = 5000 $outputPath = "/Users/admin/file/UAL/Joker_UAL.csv″
Foreach ($recordType in $recordTypes)
{ $auditlog = Search-UnifiedAuditLog –UserIds $userId –ResultSize $resultSize –StartDate
$startDate –EndDate $endDate –RecordType $recordType $auditlog
| Select-Object –Property CreationDate,UserIds,RecordType,Operations,AuditData
| Export-Csv -Append -Path $outputPath -NoTypeInformation -Force }
```

初動対応 詳細

8. 侵害起点メールの他受信者の調査
   - Microsoft Defender (https://security.microsoft.com/)にアクセスする
   - [Email & collaboration] - [Explorer] の順に遷移する
   - 侵害されたユーザーと同様のメールを受信しているユーザーがいないか調査する

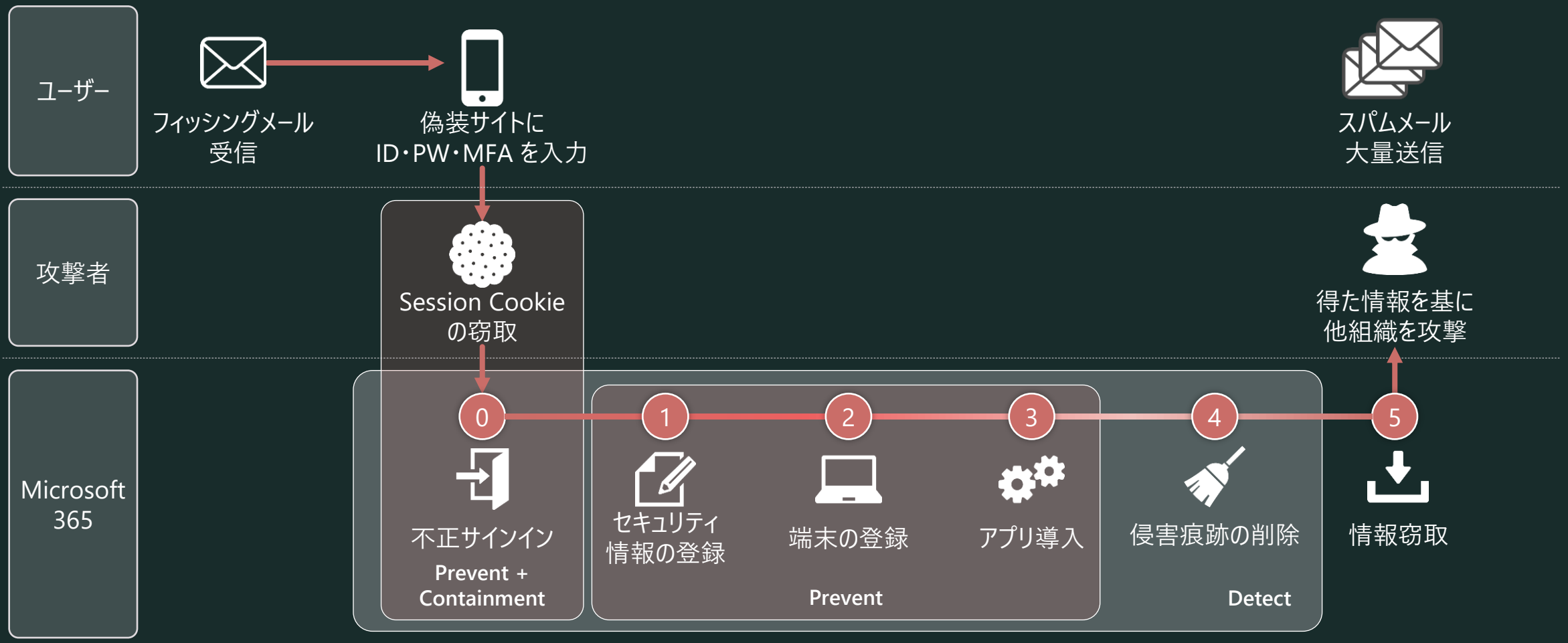
9. メール受信前後の不審なサインインの調査、他侵害ユーザの特定

Appendix: 防御策一覧

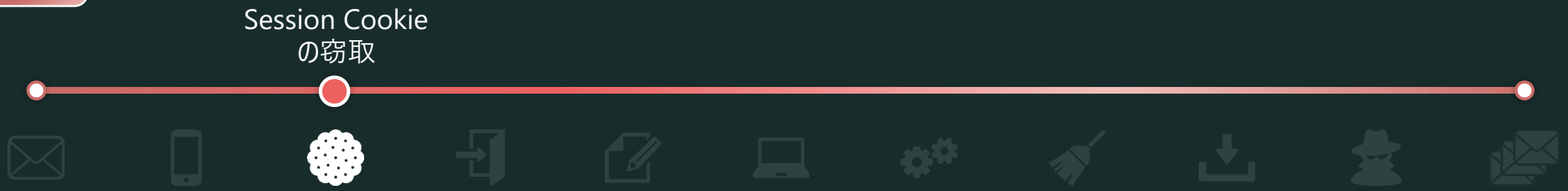
* 本編スライド内で触れた防御策の再掲を含みます。

*全ての侵害シナリオは網羅できていないため、ご了承ください。下記以外に Power Platform や First Party App の悪用、ゲストユーザーの招待といった手法を用いるAPTの事例が報告されています。

防御策 まとめ



Prevent



✓ 条件付きアクセスポリシーでトークンが発行されたデバイスからのみトークンを使用できるようにする

*本機能はプレビュー中のため、Office 365 Exchange Online, Office 365 SharePoint Onlineでのみ有効

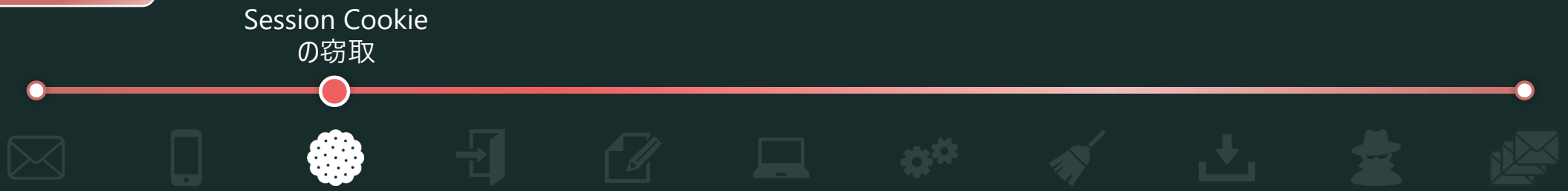
License: Entra ID Premium P2

Policy settings:

- [割り当て]
  - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
  - [ターゲット リソース] - [クラウド アプリ]: Office 365 Exchange Online, Office 365 SharePoint Online
- [アクセス制御] - [セッション]: サインイン セッションにトークン保護を必要にする (プレビュー)

参考情報
条件付きアクセス: トークン保護 (プレビュー) https://learn.microsoft.com/ja-jp/entra/identity/conditional-access/concept-token-protection

Containment



✓ Outlook on the Web (OWA) のセッションを最大 1 時間に制限する

- Microsoft Entra ID が発行する OWA にアクセス可能な非永続的なセッショントークンは既定で 24 時間のため、1 時間経過したら再認証を求めるよう、条件付きアクセスポリシーを作成する

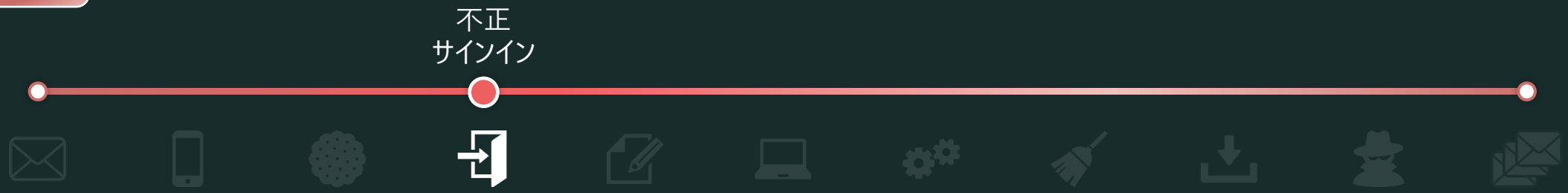
License: Entra ID Premium P1

Policy settings:

- [割り当て]
  - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
  - [ターゲット リソース] - [クラウド アプリ]: Office 365 Exchange Online
  - [条件] - [クライアント アプリ]: ブラウザー
- [アクセス制御] - [セッション]: [サインインの頻度] - [定期的な再認証 = 1 時間]

参考情報 条件付きアクセスを使用して認証セッション管理を構成する
https://learn.microsoft.com/ja-jp/entra/identity/conditional-access/howto-conditional-access-session-lifetime#policy-1-sign-in-frequency-control

Prevent



✓ 条件付きアクセスポリシーで Intune 管理された準拠済みまたは Microsoft Entra ハイブリッド参加済みデバイスからのサインインのみ許可する

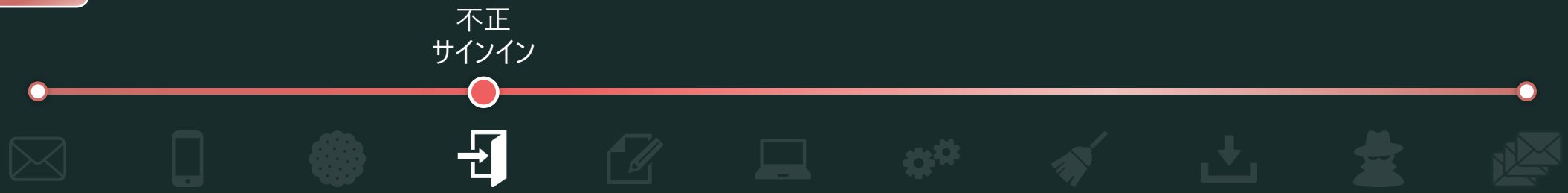
License: Entra ID Premium P1, Intune

Policy settings:

- [割り当て]
  - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
  - [ターゲット リソース] - [クラウド アプリ]: すべてのクラウド アプリ
- [アクセス制御] - [許可] - [アクセス権の付与]:

  “デバイスは準拠しているとしてマーク済みである必要があります” または “Microsoft Entra ハイブリッド参加済みデバイスが必要”

Prevent



- ✓ 条件付きアクセスポリシーで認証強度の高い方法 (Windows Hello for Business / FIDO2 Security Key …etc) によるサインインのみ許可する

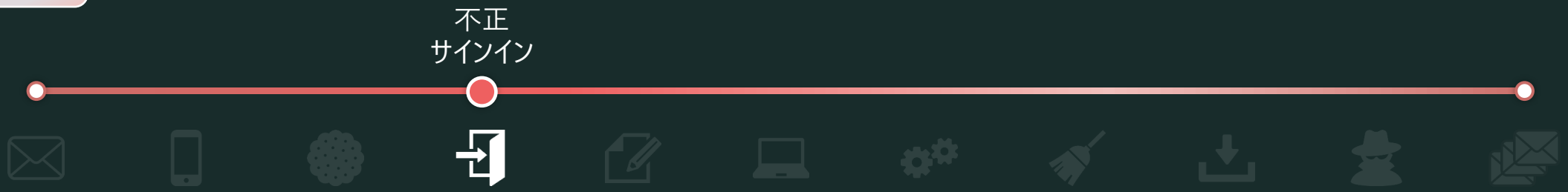
  License: Entra ID Premium P1, 認証強度の高い端末

  Policy settings:

  - [割り当て]
    - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
    - [ターゲット リソース] - [クラウド アプリ]: すべてのクラウド アプリ
  - [アクセス制御] - [許可] - [アクセス権の付与]: “認証強度が必要”

参考情報
条件付きアクセスの認証強度　https://learn.microsoft.com/ja-jp/entra/identity/authentication/concept-authentication-strengths

Detect

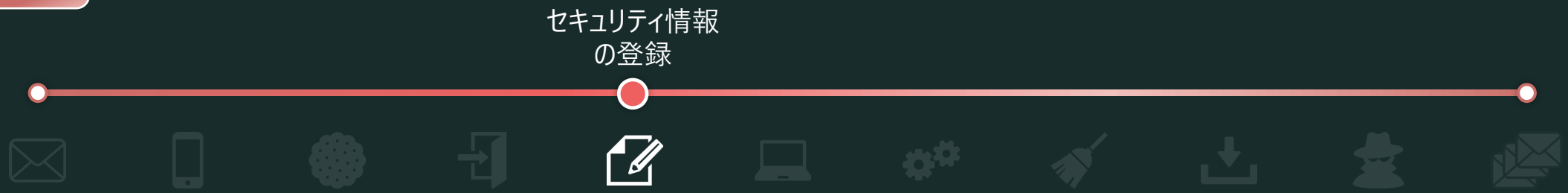


- ✓ Entra ID Interactive Sign-in logs にて 10 分以内に 2 か所以上 (*目安) の国からアクセスがあった場合検知する
  License: Entra ID Free + SIEM

- ✓ Entra ID Identity Protection にてサインインリスクが中以上の場合、多要素認証またはパスワードリセットを要求する
  License: Entra ID Premium P2

参考情報
リスク ポリシーを構成して有効にする　https://learn.microsoft.com/ja-jp/entra/id-protection/howto-identity-protection-configure-risk-policies

Prevent



✓ 条件付きアクセスポリシーで“信頼できる場所”以外からセキュリティ情報の登録があったときに MFA 等の要求またはブロックする

※セキュリティ情報（多要素認証）未登録のユーザーはロックアウトされるため要注意

License: Entra ID Premium P1

Policy settings:

- [割り当て]
  - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
  - [ターゲット リソース] - [ユーザー操作]: セキュリティ情報の登録
  - [条件] - [場所]: “すべての信頼できる場所”を対象外にする
- [アクセス制御] - [許可] - [アクセス権の付与]: 任意のオプションを選択 (例 多要素認証を要求する、デバイスは準拠しているとしてマーク済みである必要があります...等)

参考情報 Microsoft Entra ID の統合されたセキュリティ情報登録
https://learn.microsoft.com/ja-jp/entra/identity/authentication/howto-registration-mfa-sspr-combined#create-a-policy-to-require-registration-from-a-trusted-location

Detect

✓ Entra ID 監査ログを SIEM に出力し、以下の属性を監視する

License: Entra ID Free + SIEM

Service	Authentication Methods
Category	UserManagement
Activity	User changed default security info User started security info registration User registered security info User updated security info User deleted security info
Results	Success / Failure

Service	Azure MFA
Category	UserManagement
Activity	User registered security info
Results	Success / Failure

Prevent

✓ 条件付きアクセスポリシーで“信頼できる場所”以外から端末の登録があったときに MFA 等の要求またはブロックする

License: Entra ID Premium P1

Policy settings:

- [割り当て]
  - [ユーザー]: [対象] にて "すべてのユーザー" または "ユーザーとグループの選択" を選ぶ *Break glass account は対象外とする
  - [ターゲット リソース] - [ユーザー操作]: デバイスの登録または参加
  - [条件] - [場所]: “すべての信頼できる場所”を対象外にする
- [アクセス制御] - [許可] - [アクセス権の付与]: 任意のオプションを選択 (例 多要素認証を要求する、デバイスは準拠しているとしてマーク済みである必要があります...等)

参考情報
条件付きアクセス: ターゲット リソース - ユーザー操作　https://learn.microsoft.com/ja-jp/entra/identity/conditional-access/concept-conditional-access-cloud-apps#user-actions

Detect

✓ ユーザーにデバイス登録通知をする

Intune 管理センターにて、ユーザーに新しく登録されたデバイスの通知設定を行う
これによりユーザーは自身の予期しないデバイス登録に気づきIT管理者に連絡できる

License: Entra ID Premium P1 + Intune

参考情報
Intune で登録通知を設定する　https://learn.microsoft.com/ja-jp/mem/intune/enrollment/enrollment-notifications

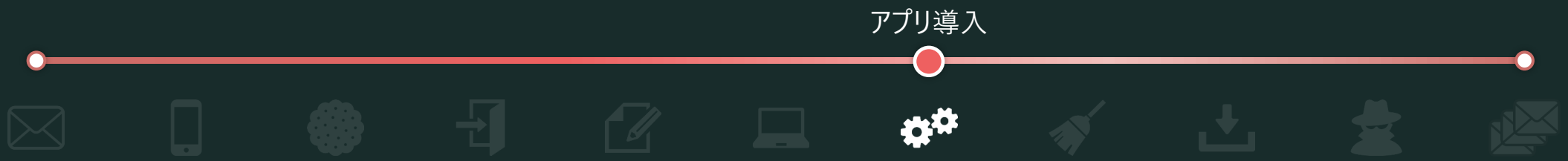
Detect

✓ Entra ID 監査ログを SIEM に出力し、以下の属性を監視する

License: Entra ID Premium P1

Service	Device Registration Service
Category	Device
Activity	Register device
Results	Success / Failure

Prevent



✓ 一般ユーザーによるアプリの登録を防ぐ

- Azure ポータルより[ユーザーはアプリケーションを登録できる] を [いいえ] とする

License: Entra ID Free

✓ 一般ユーザーによるアプリケーションへの同意を許可しない

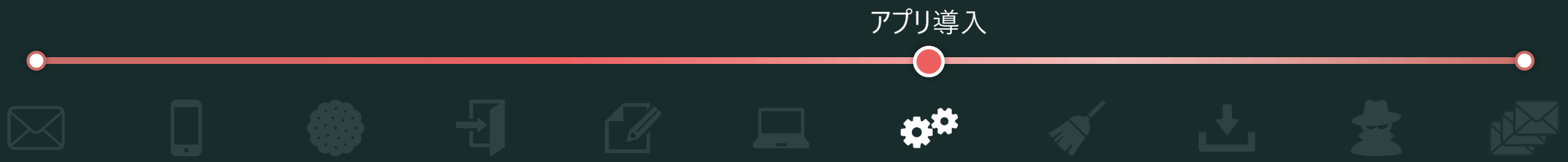
- 一般ユーザーが同意を行うことで [エンタープライズ アプリケーション] にサービス プリンシパルを登録させない
- Azure ポータルより [エンタープライズ アプリケーション] > [同意とアクセス許可] にて [ユーザーの同意を許可しない] 設定とする

License: Entra ID Free

参考情報
アプリケーション登録またはアプリケーションへの同意を作成する既定の機能を無効にするには
https://learn.microsoft.com/ja-jp/entra/identity/role-based-access-control/delegate-app-roles#to-disable-the-default-ability-to-create-application-registrations-or-consent-to-applications

参考 : エンタープライズ アプリケーションに、管理者の知らないアプリケーションが追加されている!
https://jpazureid.github.io/blog/azure-active-directory/enterpriseapps-multitenantapps/

Detect



✓ Entra ID 監査ログを SIEM に出力し、以下の属性を監視する

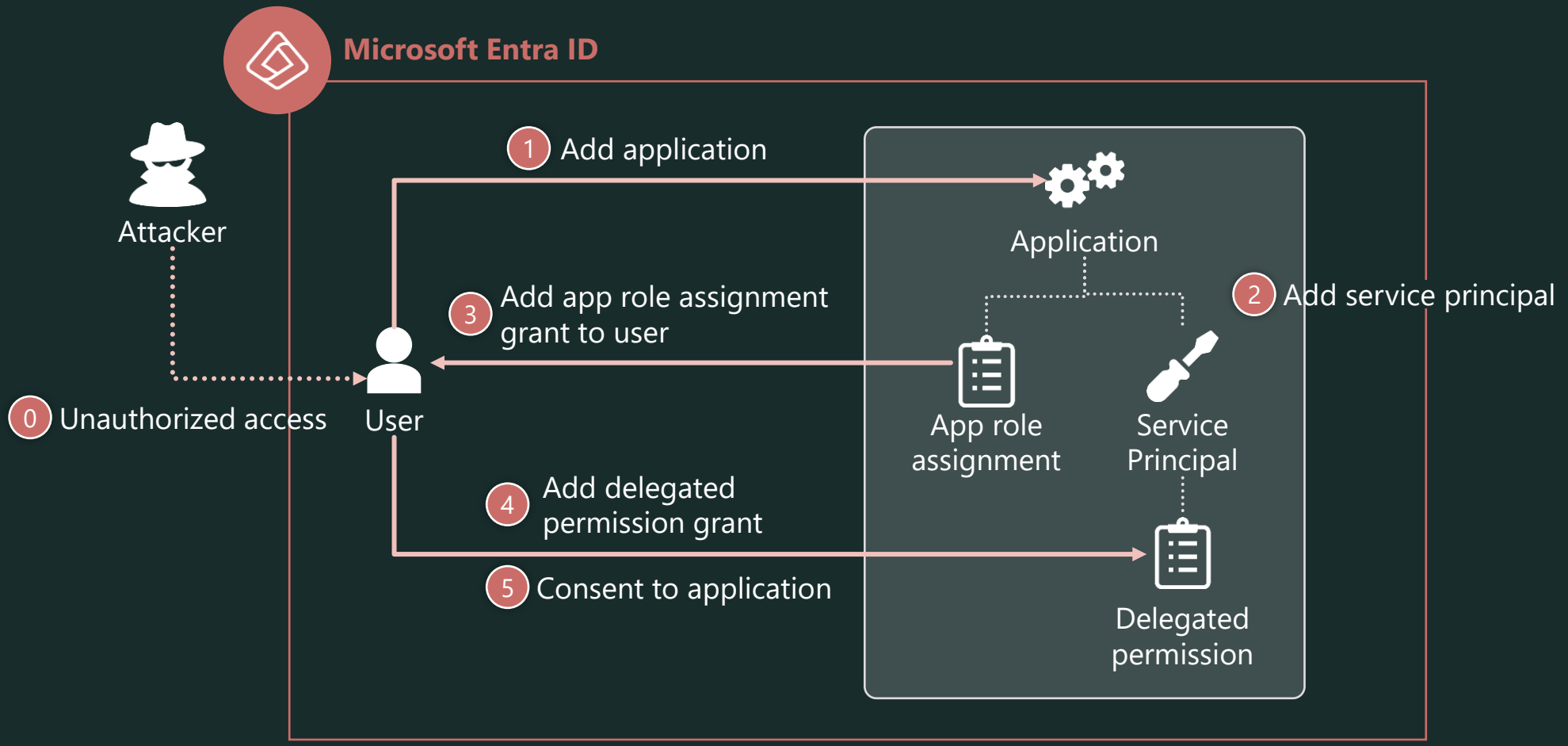
License: Entra ID Free + SIEM

#	Service	Category	Activity
1	Core Directory	ApplicationManagement	Add application
2			Add service principal
3		UserManagement	Add app role assignment grant to user
4		ApplicationManagement	Add delegated permission grant
5			Consent to application

アプリ導入時のログ出力について

Entra ID においてアプリ導入された際のログ出力イメージを以下に示す。

*イメージのため、正確な情報は Microsoft にご確認ください。



Detect

✓ メール転送ルールの作成を検知する

Unified Audit Log を SIEM 等に出力し、下記の属性を監視する

*Unified Audit Log からわかるメール転送ルール以外の痕跡は正常アクティビティとの判別が困難なため割愛

License: Audit (Standard) + Exchange Online + SIEM

RecordType	Operation	ふるまい
ExchangeAdmin	New-InboxRule	メール転送ルール (InboxRule) の作成

ITOCHU Cyber & Intelligence Inc.