Key points for analyzing and responding to email intrusions

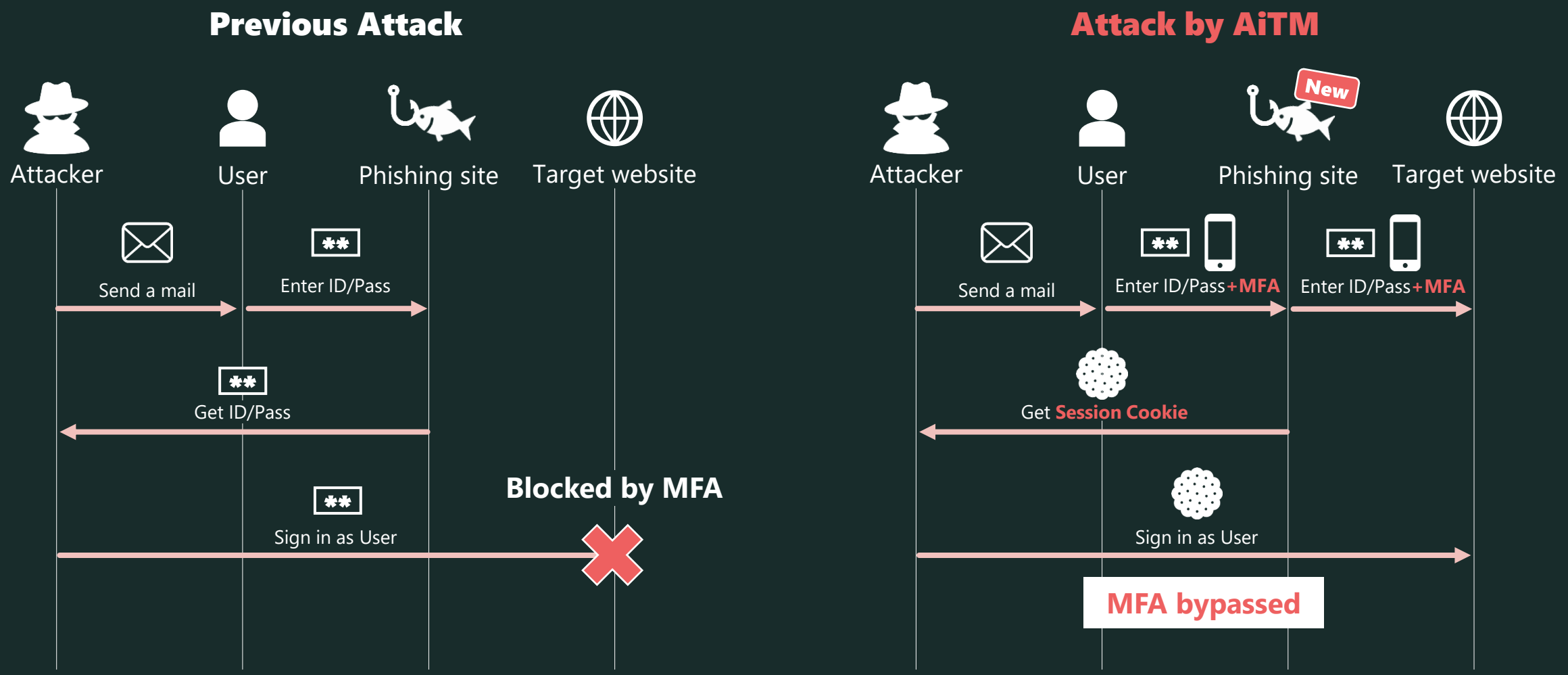
ITOCHU Cyber & Intelligence Inc.
Cybersecurity Analyst
Yumi Iida

Background

- From 2019 to 2022, the number of reported phishing attacks increased by about **4 times**.*1
- **Microsoft 365** is the **2nd** most popular email server provider in the world, with a market share of **13.5%**. It is used by many organizations.*2
- In 2021, a new attack called **AiTM** (**Adversary in the Middle**) emerged that can bypass MFA, which had been effective in defending against BEC attacks. *3
- AiTM (aka Token Replay attacks) **doubled from 30,000 to 70,000 per month** between 2022 and 2023. Reports suggests it will remain effective in the future. *4

Reference:
*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)

What is AiTM?


Previous Attack
Attacker
User
Phishing site
Target website
Send a mail
Enter ID/Pass
Get ID/Pass
Sign in as User
Blocked by MFA
Attack by AiTM
New
Attacker
User
Phishing site
Target website
Send a mail
Enter ID/Pass+MFA
Enter ID/Pass+MFA
Get Session Cookie
Sign in as User
MFA bypassed

Challenges in Incident Response

- Unclear initial response
- Time-consuming to select and collect appropriate logs
- Unclear what logs suggest attack traces
- Lack of systematic response in case attack traces are found

Inappropriate response can lead to the expansion of damage

Purpose of this presentation

It will cover the following topics based on a real-world M365 account intrusion incident:

- Initial response to an incident
- Key points of incident investigation
- Details of attacker traces and associated logs
- Incident prevention

The goal:

- ✓ Understand the key points of incident response for quickly and effectively
- ✓ Understand effective defense measures

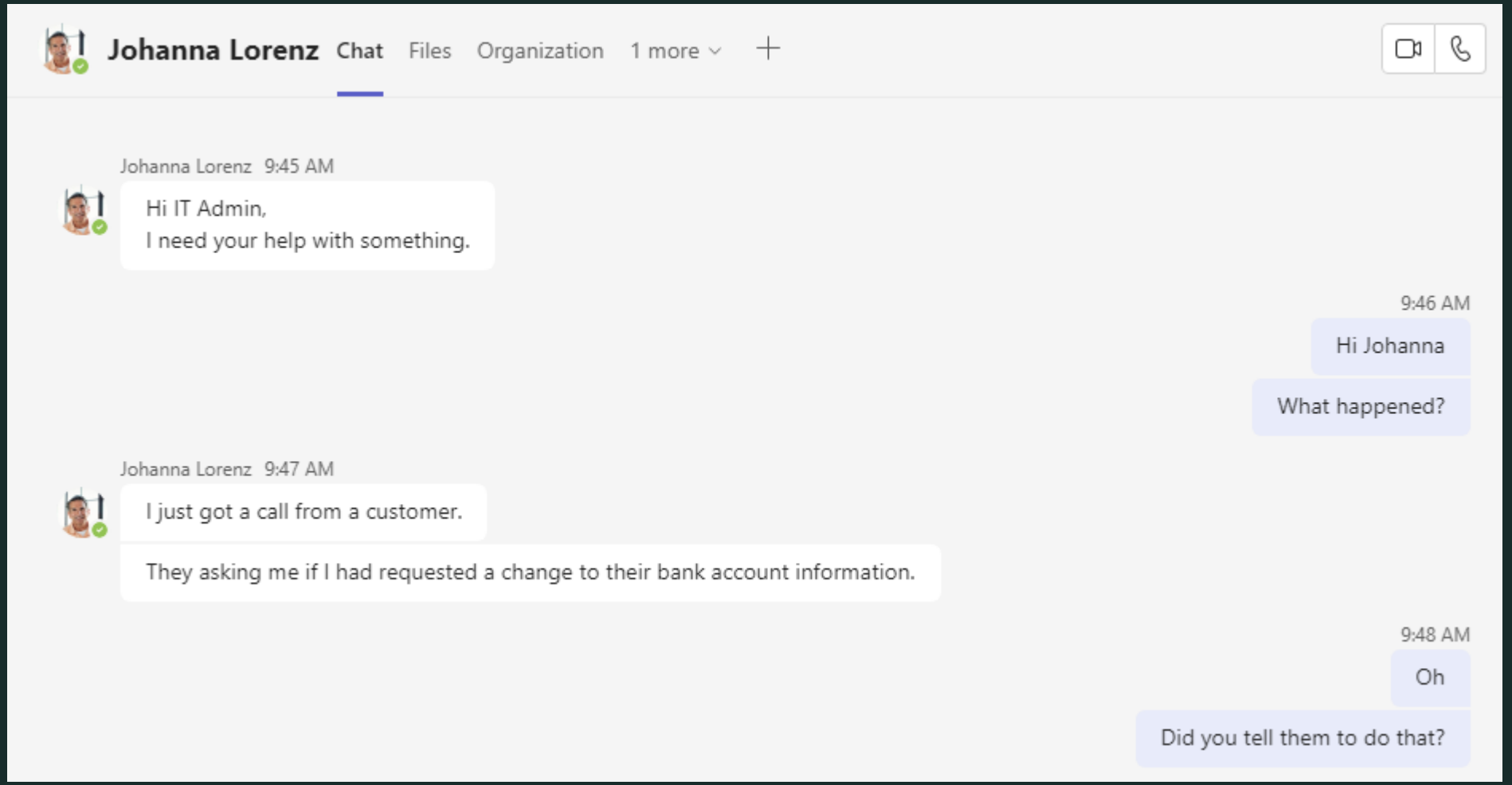
Let's practice incident response!

Created a demo incident based on a real-world Microsoft 365 incident.

You are a CSIRT member of a certain trading company.
The company's IT environment is as follows.

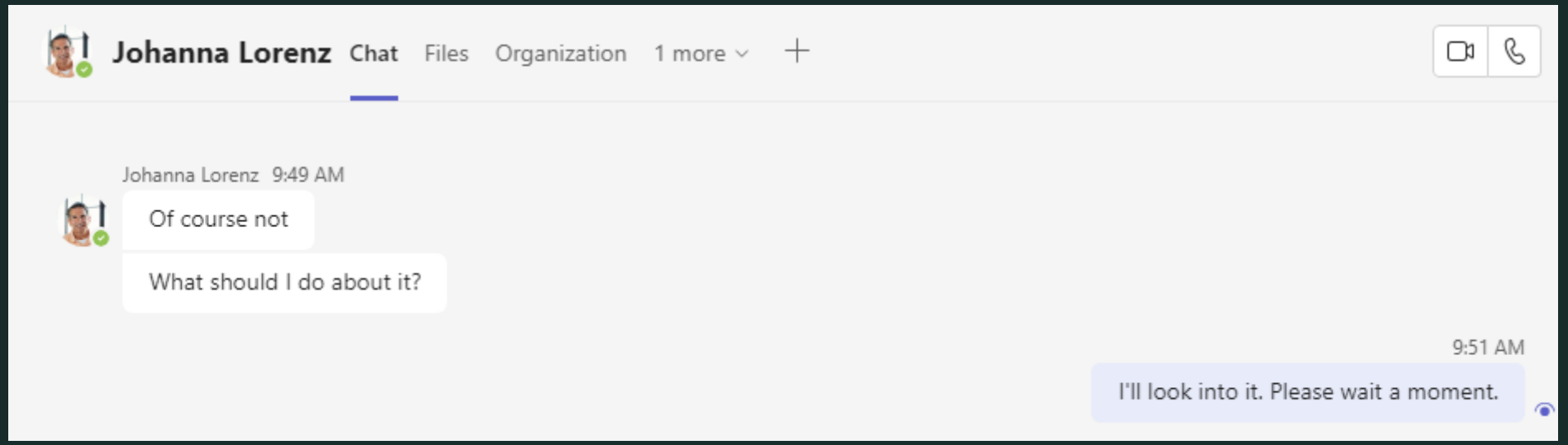
Employees:	300
Licenses:	Microsoft 365 Enterprise E3
Mail service:	Exchange Online only
Multi-factor authentication:	Microsoft Authenticator (OTP app)

Incident Occurred!



* Johanna is the default user.

Incident Occurred!



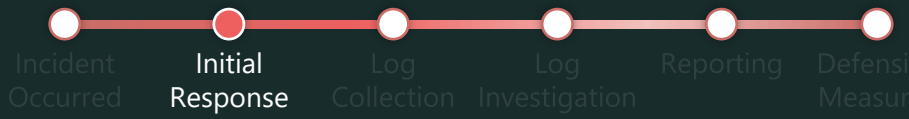
* Johanna is the default user.

What are the steps for the incident response?

Incident Occurred → Initial Response → Log Collection → Log Investigation → Reporting → Defensive Measures

Initial Response

Initial Response

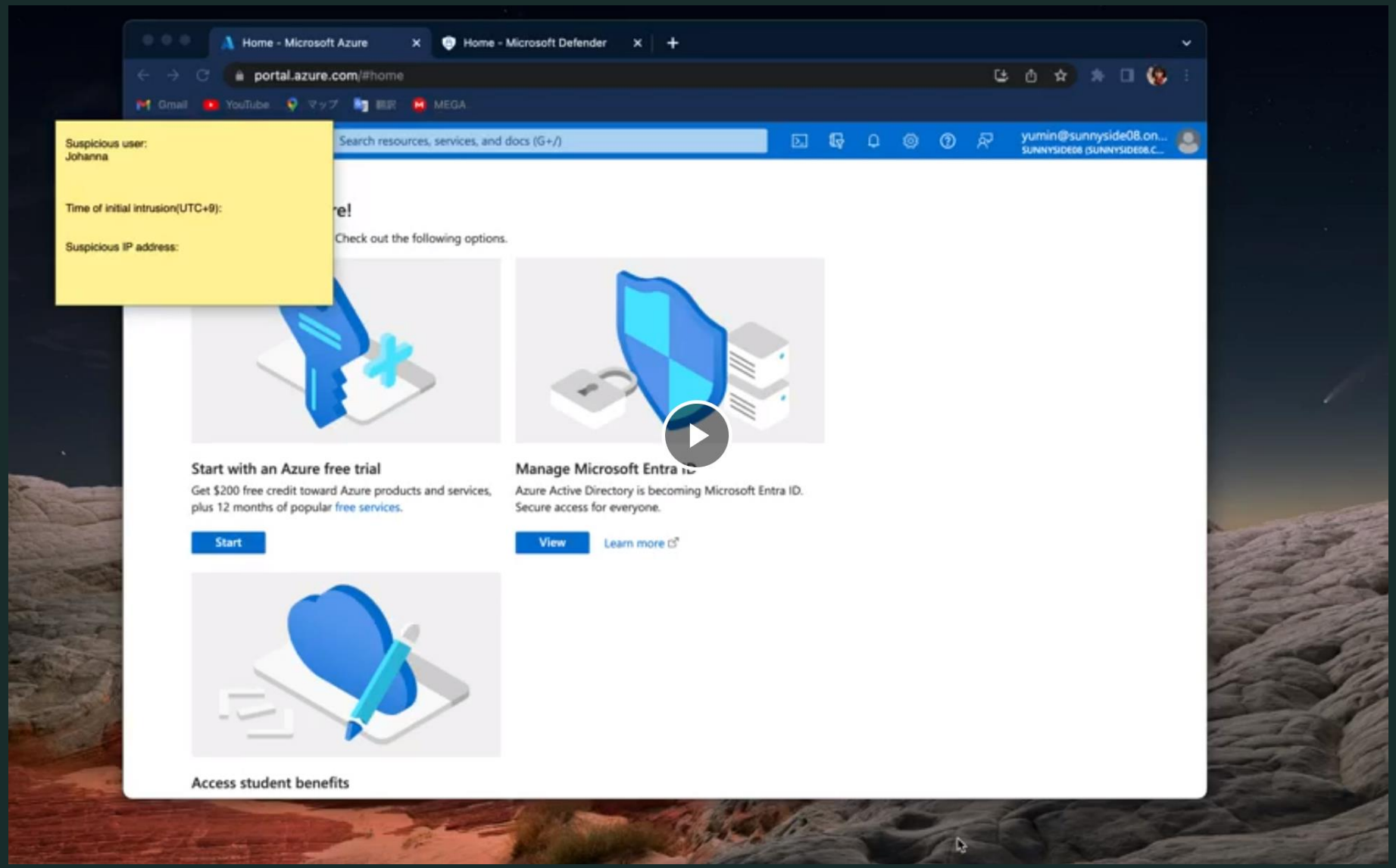


Which do you do?

- Disconnect the company network
- Collect and clean up Johnna's computer
- Delete Johanna's account
- Disable Johanna's account session and reset his password

DEMO Initial Response

Incident Occurred | Initial Response | Log Collection | Log Investigation | Reporting | Defensive Measures



DEMO Initial Response

✓ **Contain the intrusion**

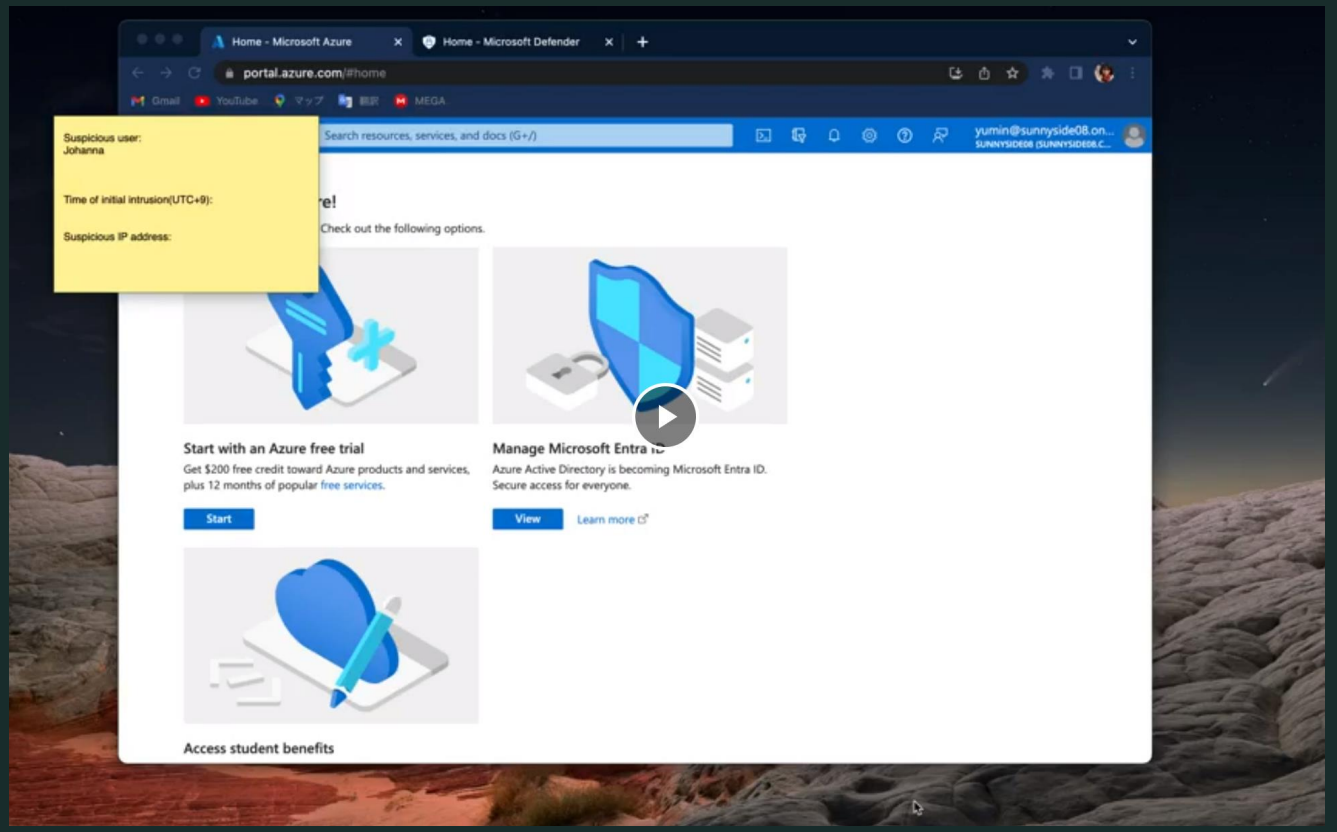
- Disconnect the session
- Remove the registered suspicious security info

✓ **Do not erase the traces**

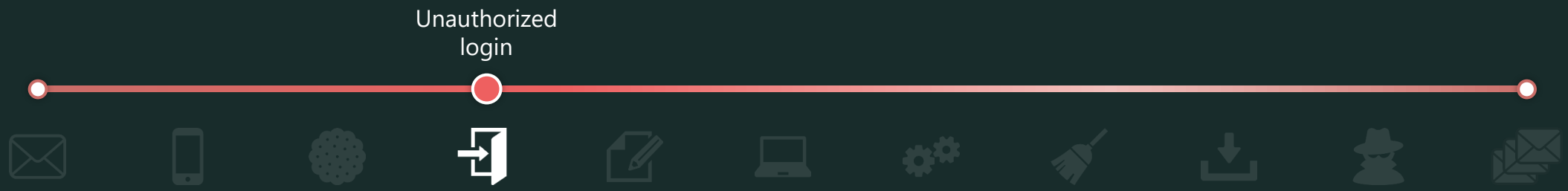
- Do not generally “delete”
- Explore the “disable” option

✓ **Identify the scope of the intrusion**

- Check for similar intrusion within the organization



Prevent unauthorized login



- ✓ Use conditional access policy to allow sign-ins only from devices that are hybrid-joined to Entra ID or managed by Intune and have passed compliance checks.

  License: Entra ID Premium P1, Intune

- ✓ Use conditional access policy to require strong authentication methods (Windows Hello for Business, FIDO2 security key, etc.) for sign-ins.

  License: Entra ID Premium P1, Device with string auth methods

Reference: Conditional Access authentication strength
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths

Log Collection & Investigation

Log Collection & Investigation

Here are common problems in incident response:

- Unclear what logs are needed
- Logs are not being stored
- Don’t know how to investigate it
- Found attacker’s trace, but don’t know how to respond

Let’s organize the necessary logs, retention periods,
and investigation and response policies.

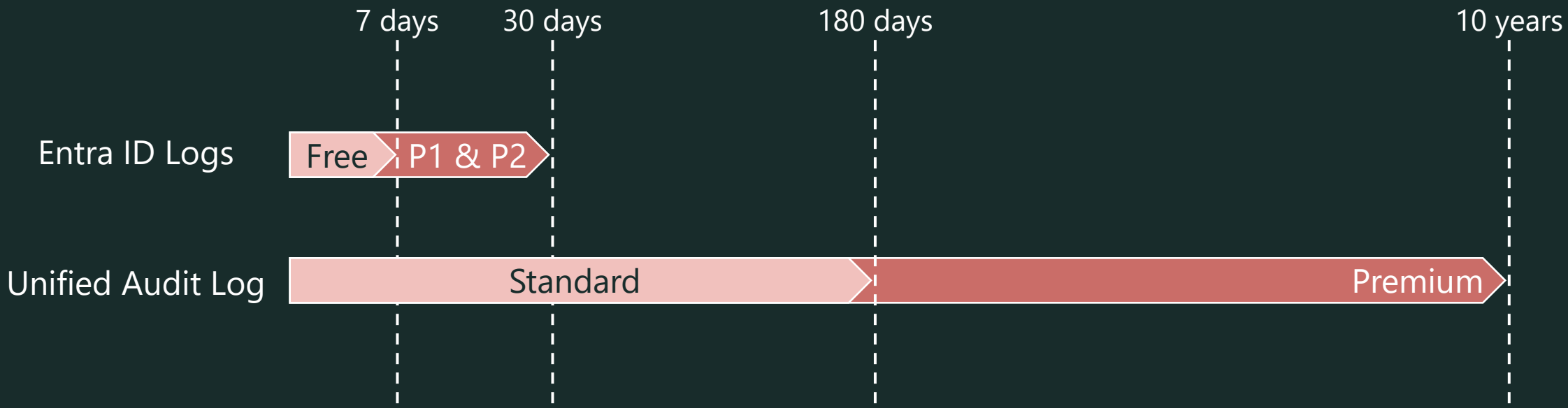
Log Collection

Logs for investigation

Log type	Purpose
Entra ID Sign-in logs	Check for suspicious sign-ins and source IP addresses.
Entra ID Audit logs	Check for suspicious activities. e.g. Register security information or apps
Unified Audit Log	Identify suspicious email and file-related activities for specific users.

Log Collection

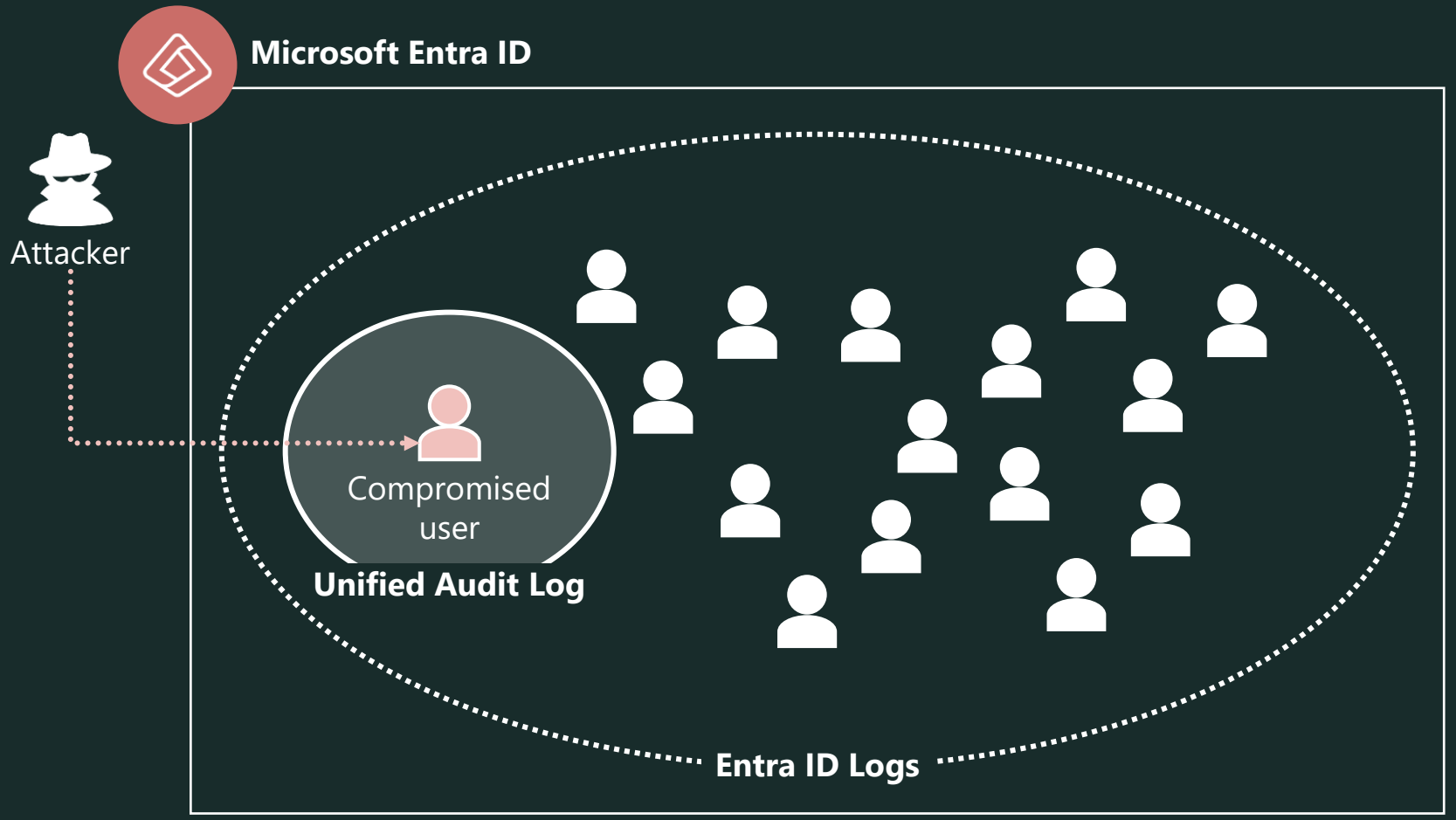
Log type and license-specific data retention periods



References
Microsoft Entra data retention: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention#activity-reports
Default audit log retention policy: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies#default-audit-log-retention-policy

Log Investigation

Recommended investigation scope for log types



Log Investigation

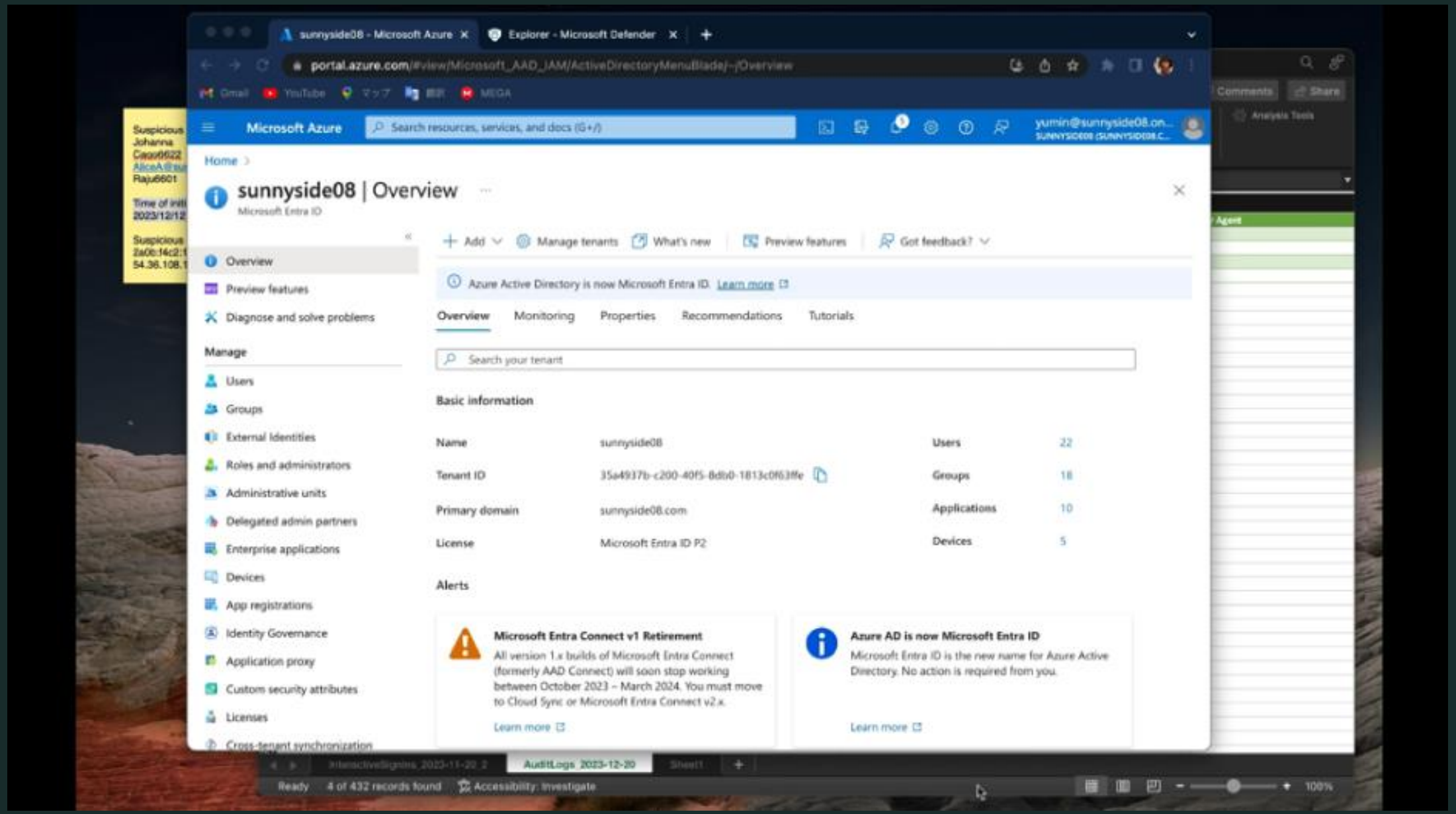
Points

- ✓ Be aware of the **licenses** and log **retention periods** in advance!
- ✓ It is also a good idea to start the exploration from **known intrusions**.

▼ Reference

Log type	Purpose	Scope	License	Data Retention
Entra ID Sign-in logs	Check for suspicious sign-ins and source IP addresses.	Entire tenant	Free	7 days
			P1	30 days
			P2	30 days
Entra ID Audit logs	Check for suspicious activities. e.g. Register security information or apps	Entire tenant	As above	As above
Unified Audit Log	Identify suspicious email and file-related activities for specific users.	Specific user	Audit (Standard)	180 days
			Audit (Premium)	10 years

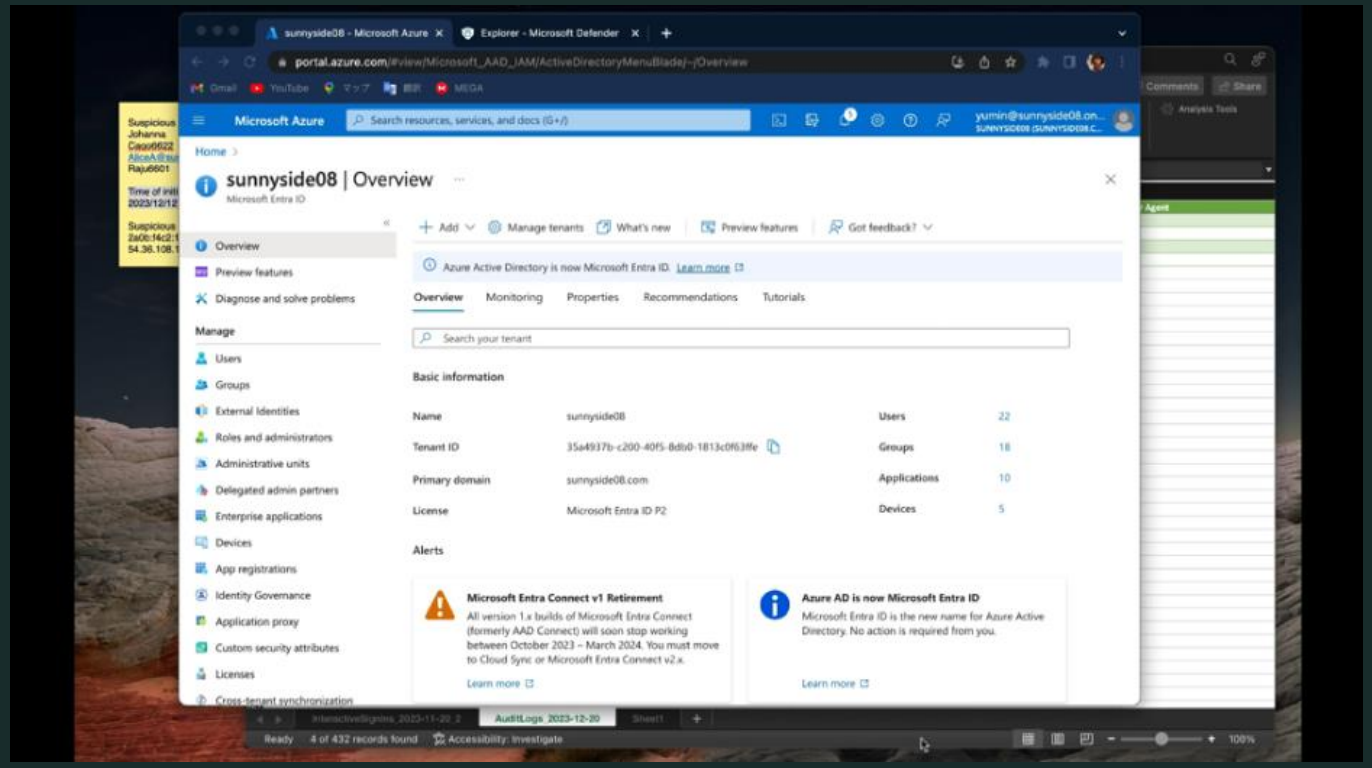
DEMO Entra ID Audit Logs Collection & Investigation



DEMO Entra ID Audit Logs Collection & Investigation

✓**Identify and respond to intrusion**

- Detect suspicious security info → delete it
- Detect suspicious application → disable it, check this contents



Attack traces 1,2: User registered security info, device

We found following attacks in real incidents:

*Device registration was not covered in this demo, but it has been seen in the past.

	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		User
6	2023-06-23T16:19:41.7904811+00:0	Core Directory	UserManagement	Update user	Success		Application
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

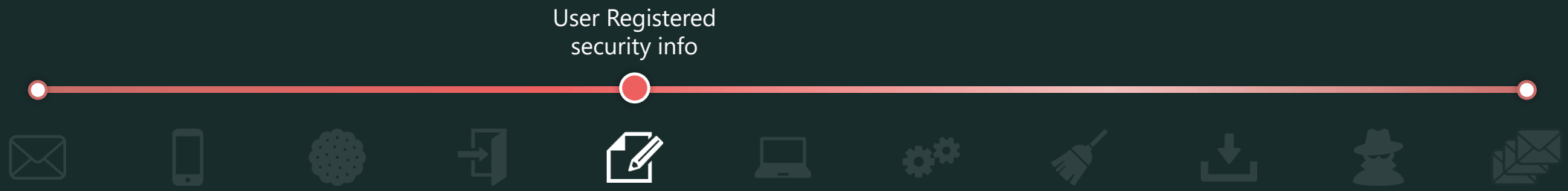
User registered security info

Register device

Attacker's goal

- ✓ User registered security info
  Even after the Session Cookie is invalidated, unauthorized sign-ins can still use MFA device.
- ✓ Register device
  Attackers can access high-value assets that are limited to Entra ID-registered devices.

Prevent user from registering security info



- ✓ Use conditional access policy to block or require MFA for security info registration from anywhere other than a "trusted location".

  *Users who are not registered with security info (multi-factor authentication) will be locked out.

  License: Entra ID Premium P1

Reference: Enable combined security information registration in Microsoft Entra ID
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-registration-mfa-sspr-combined#create-a-policy-to-require-registration-from-a-trusted-location

Attack traces 3: Add application

Real incidents have shown the following attacks:

*We only collected Unified Audit Log in this real incident due to data retention period.

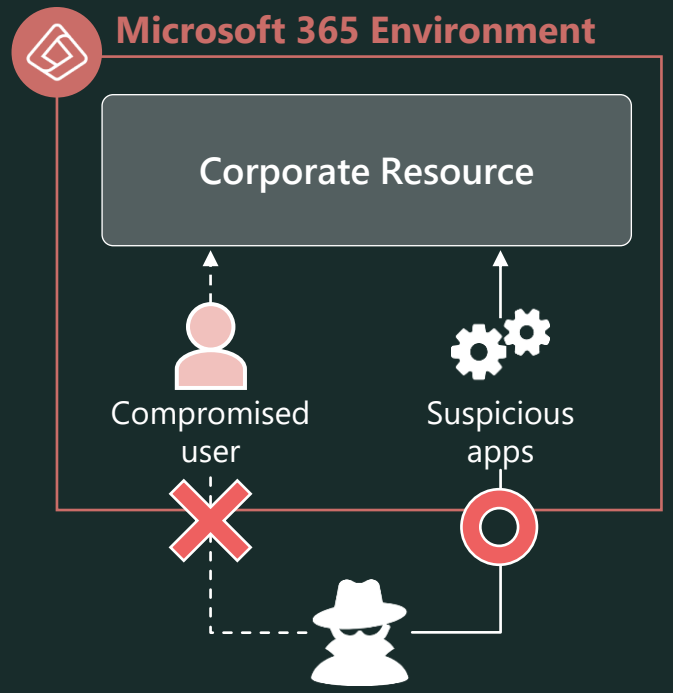
	B	C	D	F	G	H	I	J	K	L
1	CreationDate	Recor	Operation	AuditDat	Associate	Associate	dminUnitsNames			
34	8/29/2023 8:40:56 PM	15	UserLoggedIn	{"CreationTime":"2023-08-29						
35	8/29/2023 8:41:46 PM	8	Add application.	{"CreationTime":"2023-08-29						
36	8/29/2023 8:41:46 PM	8	Add owner to application.	{"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						
43	8/29/2023 8:43:00 PM	8	Add app role assignment grar	{"Cre						
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						

Add application

Attacker's goal

✓ Information can be stolen depending on the API permissions of the app.

Attack traces 3: Add application



✓ We found the following **[Manifest]** in the app registration in the real incident.

Home > App registrations >

| Manifest

Search

Save | Discard | Upload | Download | Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

The editor below allows you to update this application by directly modifying its JSON representat

```
{
    "id": "[redacted]",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": 2,
    "addIns": [],
    "allowPublicClient": null,
    "preAuthorizedApplications": [],
    "publisherDomain": "[redacted]",
    "replyUrlsWithType": [
        {
            "url": "http://localhost:7823/access",
            "type": "Web"
        }
    ],
    "requiredResourceAccess": [],
    "samlMetadataUrl": null,
    "signInUrl": null,
    "signInAudience": "AzureADandPersonalMicrosoftAccount",
    "tags": [],
    "tokenEncryptionKeyId": null
}
```

Prevent add application

✓ Prevent general users from “Add application”
- In the Azure portal, set "Users can register applications" to "No".

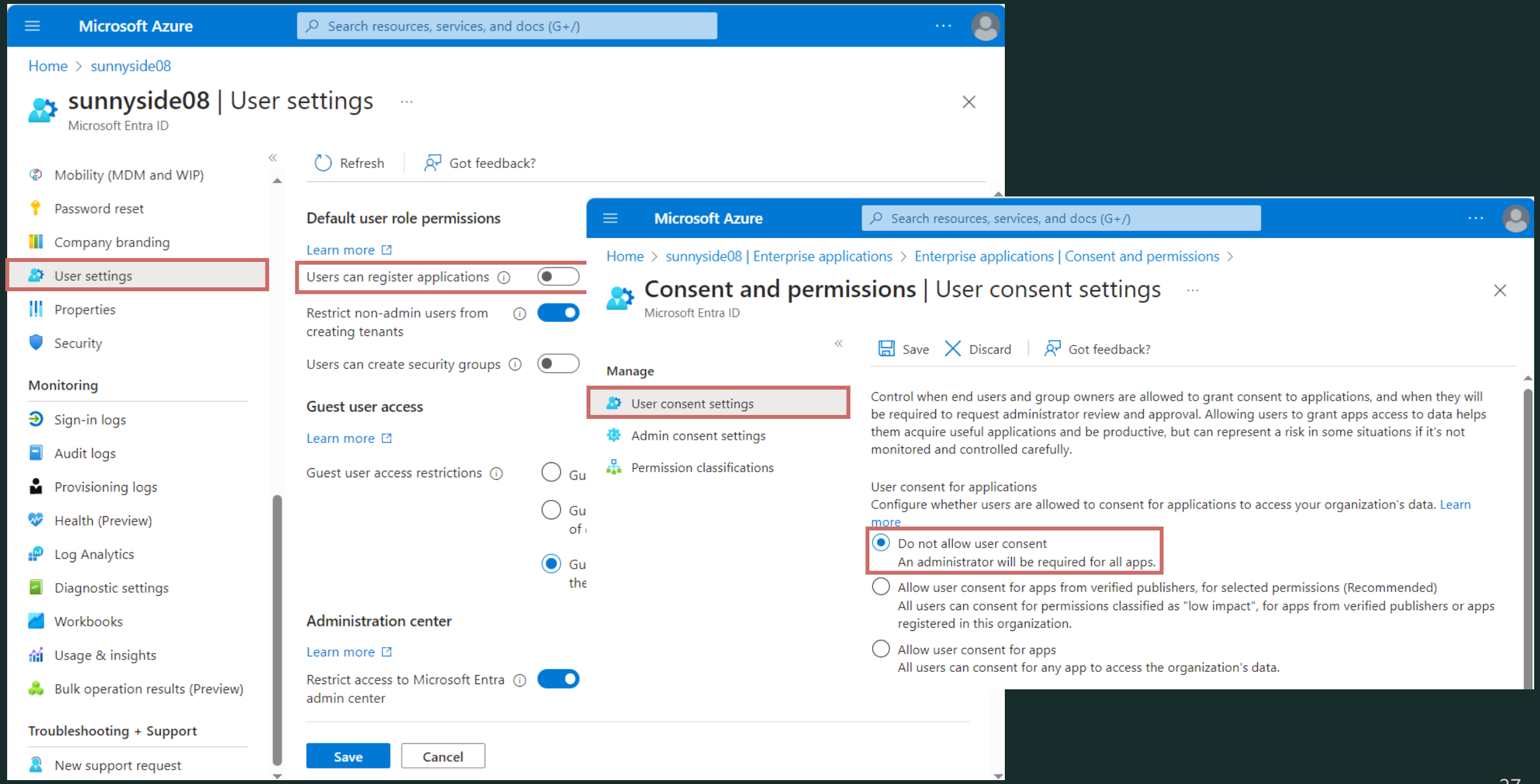
License: Entra ID Free

✓ Do not allow general users from “Consent to application”
- Do not allow general users to register service principals to [Enterprise Applications] by granting consent.
- In the Azure portal, at [Enterprise Applications] > [User consent settings], set “Do not allow user consent”.

License: Entra ID Free

Reference:
To disable the default ability to create application registrations or consent to applications
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#to-disable-the-default-ability-to-create-application-registrations-or-consent-to-applications
Applications that are not known to administrators are added to enterprise applications!
https://jpazureid.github.io/blog/azure-active-directory/enterpriseapps-multitenantapps/

Prevent add application



Unified Audit Log Chapter

Log Collection & Investigation

Log collection – Unified Audit Log

- Log types for Unified Audit Log *Excerpt

#	RecordType	Description
1	ExchangeAdmin	Events from the Exchange admin audit log.
2	ExchangeItem	Events from an Exchange mailbox audit log for single-item actions, such as creating or receiving an email message.
3	ExchangeItemGroup	Events from an Exchange mailbox audit log for multi-item actions, such as moving or deleting one or more email messages.
4	SharePoint	SharePoint events.
6	SharePointFileOperation	SharePoint file operation events.
7	OneDrive	OneDrive for Business events.
8	AzureActiveDirectory	Microsoft Entra events.
15	AzureActiveDirectoryStsLogon	Microsoft Entra events.

Reference:
AuditLogRecordType https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema#auditlogrecordtype

Log investigation – Unified Audit Log

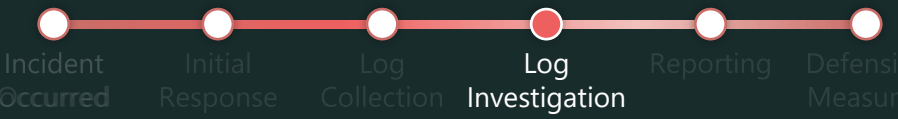
- Data Scheme

	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
11	2023/12/11 1:05	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	Name":"Identity","Value":"f0af9d5e-1cc7-4fbd-9c19-818339d1ecc5¥¥17097852
12	2023/12/11 1:05	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	b5eb-61c3-1d01-2c6c4b0589d9","SessionId":"1a38c29e-b0bc-4623-a84e-5f6a4
13	2023/12/11 1:01	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	b33f-46ad-bee4-4a03e961a2e2"]}
14	2023/12/11 0:54	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	
15	2023/12/11 0:54	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"CreationTime":"2023-12-11T01:05:04","Id":"76fdd351-f7bf-4622-fef1-08dbf9
16	2023/12/11 0:53	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"CreationTime":"2023-12-11T01:01:10","Id":"b373f43d-faff-454d-9f02-08dbf9
17	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"Creat
18	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Send	{"Creat
19	2023/12/11 0:44	GradyA@sunnyside08.onmicrosoft.com	ExchangeItem	Create	{"Creat
					{"CreationTime":"2023-12-11T00:44:42","Id":"97cbe468-fbf6-490e-b946-08db
					{"CreationTime":"2023-12-11T00:44:42","Id":"97cbe468-fbf6-490e-b946-08db
					{"CreationTime":"2023-12-11T00:44:04","Id":"14d0000f-712a-4ea7-c4d4-08db

Many UALs have the following common fields:
`RecordType, CreationDate, UserIds, Operations, AuditData, ResultIndex, ResultCount, Identity, IsValid, ObjectState`

AuditData is JSON,
so PowerQuery is required to parse it if necessary.

Log collection – Unified Audit Log



Points

✓ Prioritize and investigate RecordType based on **characteristic attack methods**.

<How to get>

✓ GUI:

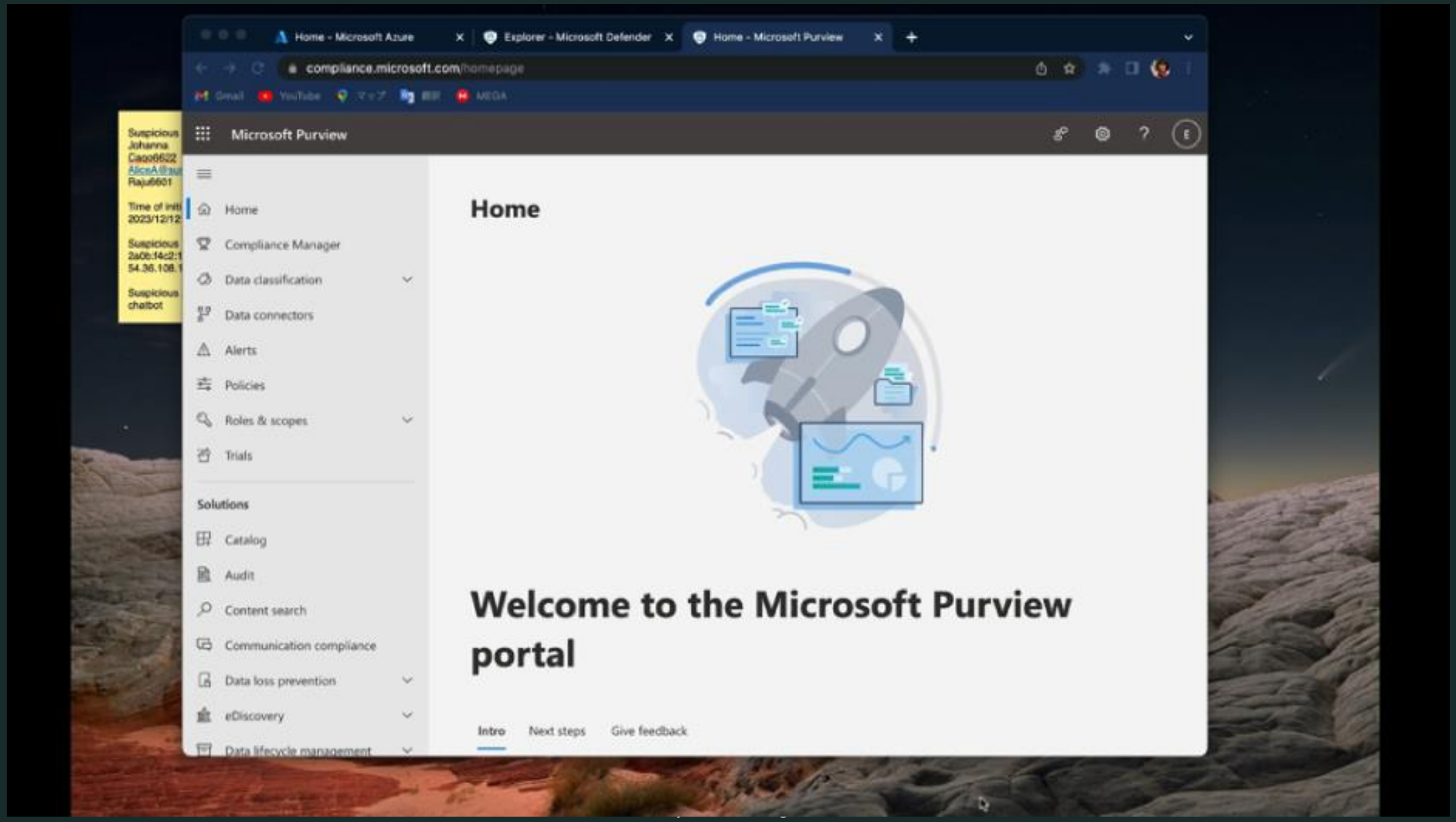
1. Go to Microsoft Purview (https://compliance.microsoft.com/) and navigate to [Solutions | Audit].
2. Specify the information you want to get in [Activities] and [Users], and click [Search].
3. Click [Completed] to export the results.

✓ Exchange PowerShell:

1. Connect to Exchange PowerShell
2. Use the `Search-UnifiedAuditLog` cmdlet to download a CSV file of UAL to your local computer.

Reference:
Audit New Search: https://learn.microsoft.com/en-us/purview/audit-new-search#get-started-with-audit-new-search
Use a PowerShell script to search the audit log: https://learn.microsoft.com/en-us/purview/audit-log-search-script

DEMO Unified Audit Log Collection and investigation



DEMO Unified Audit Log Collection and investigation

✓Identify intrusion

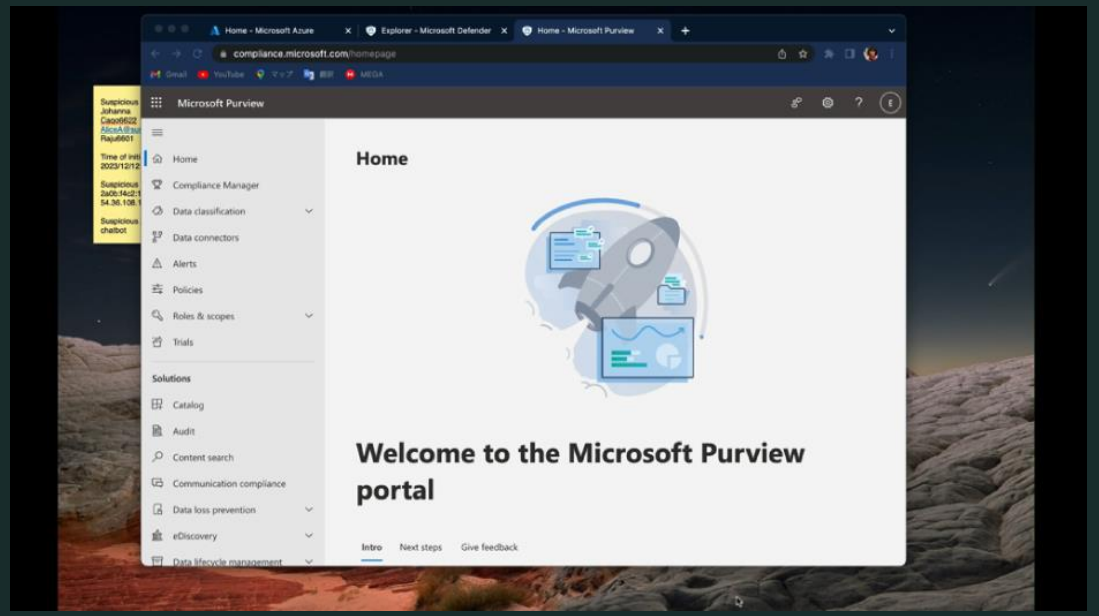
Priority	RecordType	Verification
1	**ExchangeAdmin**	Inbox-Rule created or deleted?
2	ExchangeItem	Unusual email reading/deletion activities?
2	SharePointFileOperation	Unusual File (SharePoint, OneDrive) reading/deletion activities?

✓Investigate other intrusion

- Identifying attacker activity that crosses RecordType based on "`SessionId`"

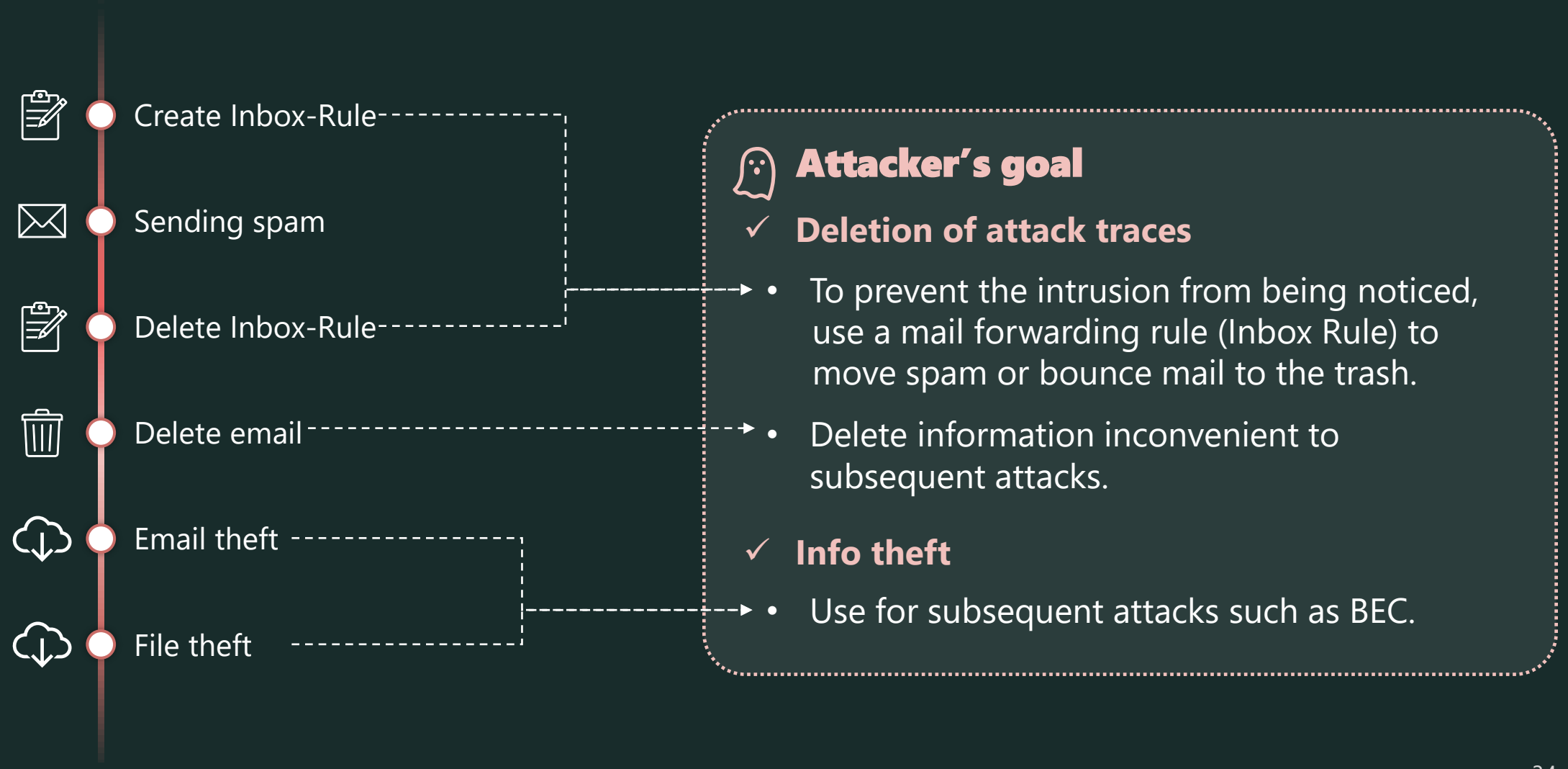
✓Response

- If you find suspicious Inbox-Rule
  → User Interview, delete it.



Attack traces 4,5: Deletion of attack traces ~ Info theft

We found the following attack traces in the Unified Audit Log by real incidents:



Attack traces 4: Deletion of attack traces

- Create Inbox-Rule
- Sending spam
- Delete Inbox-Rule
- Delete email
- Email theft
- File theft

	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					

Attack traces 4: Deletion of attack traces

- Create Inbox-Rule
- Sending spam
- Delete Inbo
- Delete ema
- Email theft
- File theft

	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					
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					

InboxRule:
automatically forward replies to spam emails sent by attackers to the deleted folder
→Prevent users from noticing the intrusion

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

Attack traces 4: Deletion of attack traces

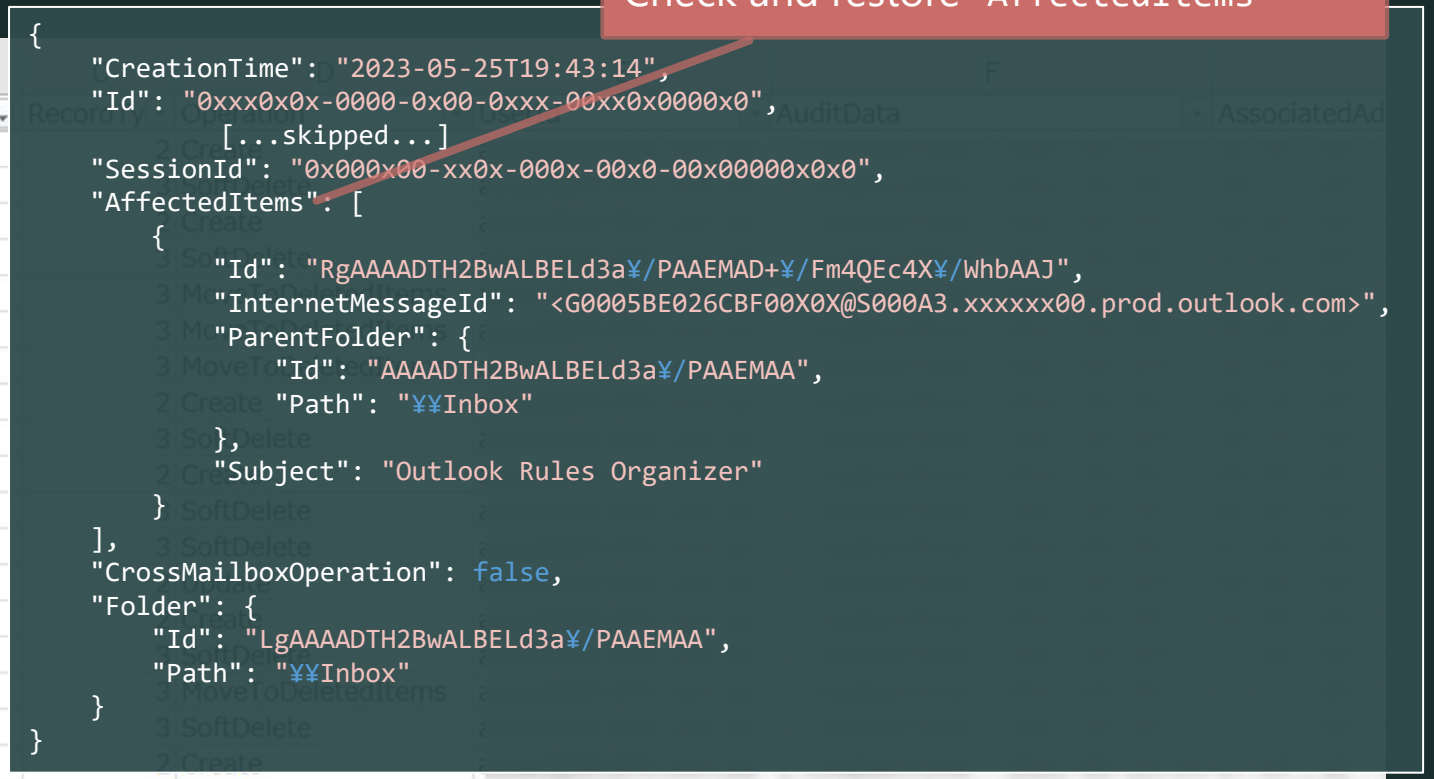
- Create Inbox-Rule
- Sending spam
- Delete Inbox-Rule
- **Delete email**
- Email theft
- File theft

	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]

Attack traces 4: Deletion of attack traces

- Create Inbox-Rule
- Sending spam
- Delete Inbox-Rule
- **Delete email**
- Email theft
- File theft

Check and restore "AffectedItems"



```
{
    "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

Attack traces 4: Deletion of attack traces

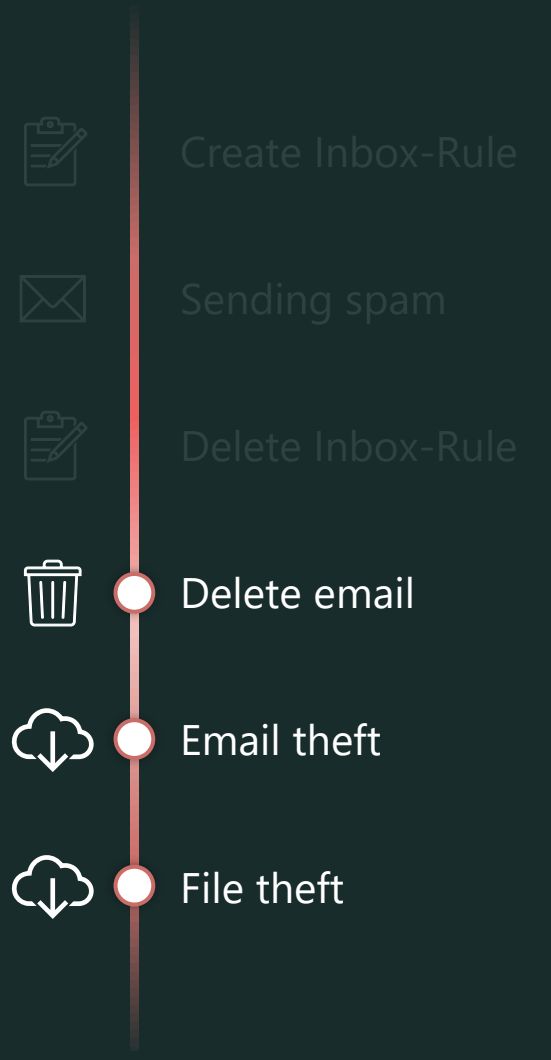
- Create Inbox-Rule
- Sending spam
- Delete Inbox-Rule
- **Delete email**
- Email theft
- File theft

	B	C	D	E	F	
1	CreationDate	RecordTy	Operation	UserId	AuditData	AssociatedAd
38	5/25/2023 11:36:35	2	Create			
39	5/25/2023 11:38:12	3	SoftDelete			
40	5/25/2023 11:49:50	2	Create			
41	5/25/2023 11:51:01	3	SoftDelete			
42	5/25/2023 11:55:10	3	MoveToDeletedItems			
43	5/25/2023 11:55:25	3	MoveToDeletedItems			
44	5/25/2023 11:55:25	3	MoveToDeletedItems			
45	5/25/2023 11:58:14	2	Create			
46	5/25/2023 11:59:19	3	SoftDelete			
47	5/25/2023 12:04:50	2	Create			
48	5/25/2023 12:06:43	3	SoftDelete			
49	5/25/2023 12:07:35	3	SoftDelete			
50	5/25/2023 12:09:50	2	Update			
51	5/25/2023 12:10:40	2	Create			
52	5/25/2023 12:11:49	3	SoftDelete			
53	5/25/2023 12:11:57	3	MoveToDeletedItem			
54	5/25/2023 12:12:12	3	SoftDelete			
55	5/25/2023 14:17:54	2	Create			
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			

To identify attacker activities, use properties such as "`SessionId`" and "`ClientIP`", "`ClientInfoString`".
* Similar to attack traces of "Info theft"

Attack traces 4,5: Deletion of attack traces ~ Info theft

Other than the "SessionId", you can distinguish between the activities of attackers and general users:



✓ exs. general user activities

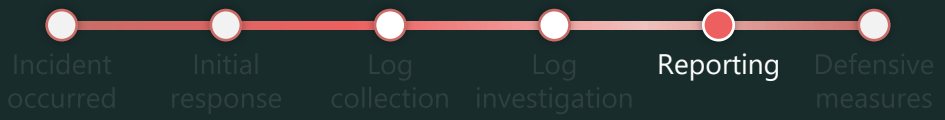
```
{
    "CreationTime": "2023-05-27T06:12:43",

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

✓ exs. attacker activities

```
{
    "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...]
}
```

Reporting

Report writing



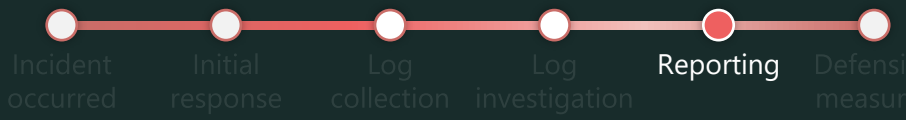
In addition to analyzing incidents, it is important to accurately communicate the results and remaining actions to users.

We detected following suspicious activity in your logs, Please confirm whether these were expected and check the following action items:

1. Suspicious sign-in
   Between 13:50:17 and 14:11:43 UTC on December 12, 2023, we observed suspicious sign-ins to Johanna's account from the following user agent and IP address:
   Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
   2a0b:f4c2:1::1 , , US
   54.36.108.162 Saarbruecken, Saarland, DE … etc
2. Account activity
   Between 13:55:36 and 14:04:58 UTC on December 12, 2023, the following activities were performed on Johanna's account with her permissions:
   - Added the following application:
     TargetDisplayName: chatbot
     TargetObjectId: 80cf2cdc-2178-400b-ab98-a0677b6bd694
   - Delegated the following permissions to the application:
     ConsentType: AllPrincipals
     Scope: Mail.ReadWrite MailboxSettings.ReadWrite User.Read
3. Security info
   The following security information was registered on Johanna’s account . . .
4. Mail forwarding rules
   The following mail forwarding rules were created on Johanna's account . . .

1. Summary of the intrusion

Report writing



In addition to analyzing incidents, it is important to accurately communicate the results and remaining actions to users.

5. Suspicious Activity by Johanna's account
   Sent an email titled "REVISED INVOICE" at 5:03 UTC on December 12, 2023.
   Downloaded the following information between 5:12:10 and 5:15:38 UTC on December 12, 2023:
      PO_EcoGreenLand_inc.docx
      Comprehensive ERP System Requirements.docx

We have confirmed that the following actions have been taken for each activity:
- Disabled the suspicious application
- Deleted the suspicious security information
- Deleted the suspicious mail forwarding rules

2. Summary of incident response activities

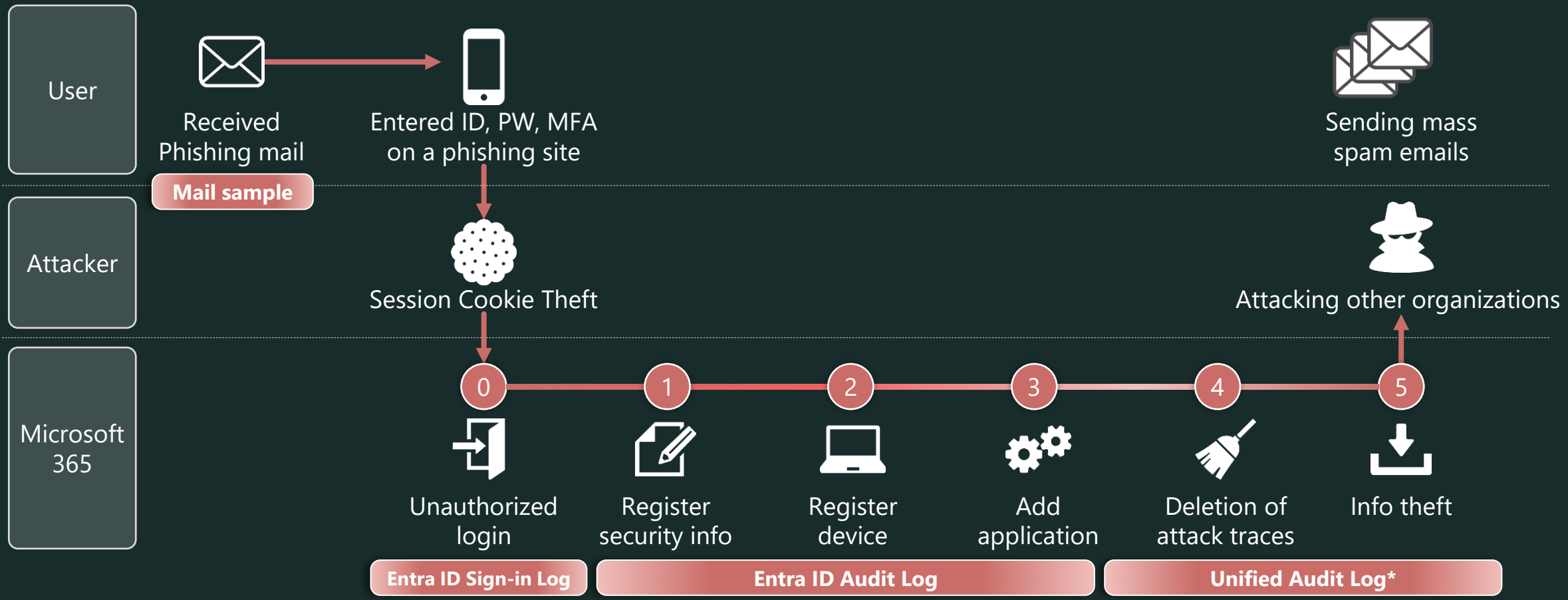
We would like you to take the following actions:
- Delete the suspicious application
- Issue a company-wide notification about the downloaded information and sent email

Thank you for your time and attention.

3. Request for additional action

Defensive Measures

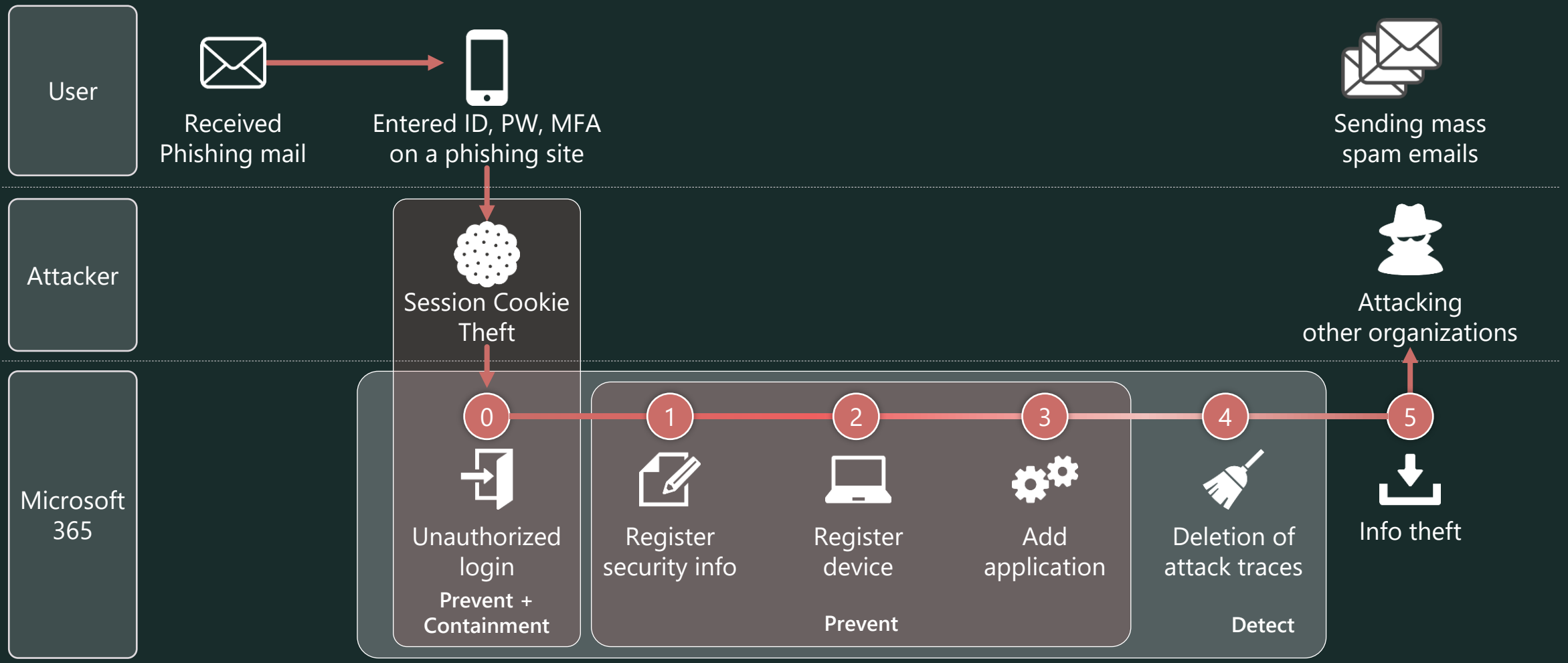
Incident Flow



* If you have E5 or Entra ID Premium P2, it is recommended to check Identity Protection alerts before Entra ID Logs.
* Unified Audit Log provides all the necessary attacker's traces, but we sometimes use Entra ID Logs for general incident checking.

Defensive Measures

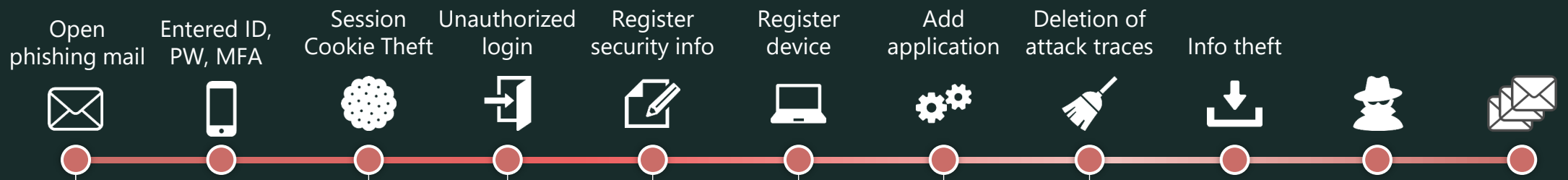
The following prevent, containment, and detect measures were introduced:



Summary

* It does not cover all possible attack scenarios. There have been reports of APTs using methods not listed below, such as abusing Power Platform, First Party Apps, and inviting guest users.

Initial Response is most important!



1. Disable sessions if they are still active.
2. Reset the password of the compromised user.
3. Delete suspicious security info from the compromised user.
4. Disable suspicious registered devices.
5. Delete suspicious mail forwarding rules.

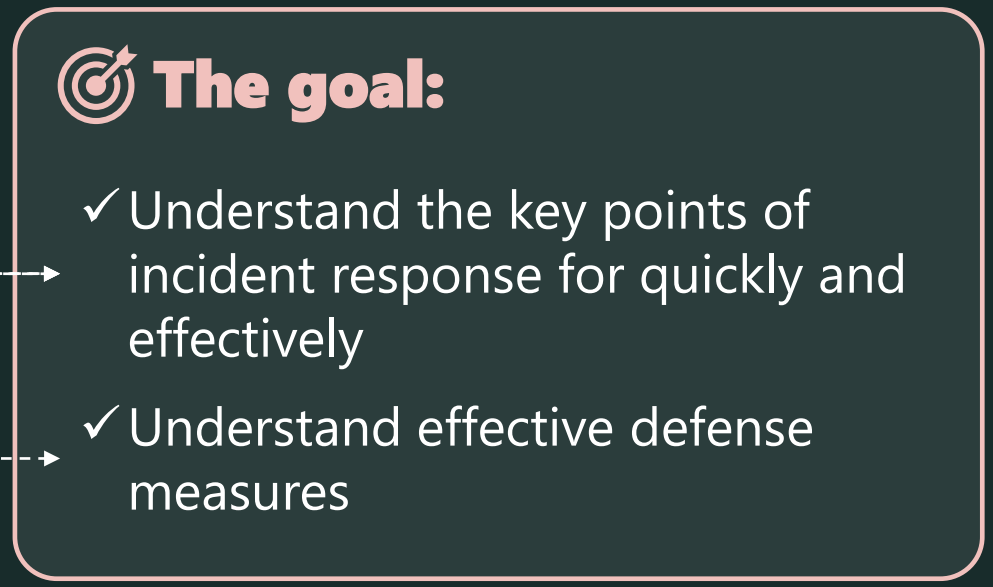
Repeat

6. Disable Entra ID apps that were registered before or after the intrusion.
7. Request, collect, and investigate logs.
8. Investigate other recipients of the intrusion-starting email.
9. Investigate suspicious sign-ins before and after receiving the email to identify other compromised users.

Summary

It covered the following topics based on a real-world M365 account intrusion incident:

- Initial response to an incident
- Key points of incident investigation
- Details of attacker traces and associated logs
- Incident prevention

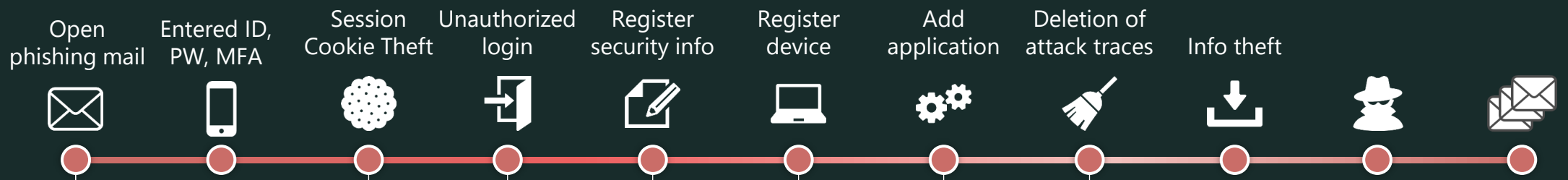


Thank you

Appendix: Reference of Initial Response

* It does not cover all possible attack scenarios. There have been reports of APTs using methods not listed below, such as abusing Power Platform, First Party Apps, and inviting guest users.

Summary of Initial Response



1. Disable sessions if they are still active.
2. Reset the password of the compromised user.
3. Delete suspicious security info from the compromised user.
4. Disable suspicious registered devices.
5. Delete suspicious mail forwarding rules.

Repeat

6. Disable Entra ID apps that were registered before or after the intrusion.
7. Request, collect, and investigate logs.
8. Investigate other recipients of the intrusion-starting email.
9. Investigate suspicious sign-ins before and after receiving the email to identify other compromised users.

Details of Initial Response

1. Disable sessions if they are still active.
   - Access the Azure Portal (https://portal.azure.com/) with an account with user administrator or higher permissions.
   - Search for the compromised user in [Microsoft Entra ID] - [Users] and navigate to the user screen.
   - Perform [Revoke sessions]. *Confirm that Continuous Access Evaluation is enabled in advance.

2. Reset the password of the compromised user.
   - Similarly, perform [Reset password] on the user screen.

3. Delete suspicious security info from the compromised user.
   - Switch to the [Authentication methods] section on the user screen.
   - Check for suspicious security information in “Usable authentication methods".
   - If found, click [...] - [Delete] in order.

4. Disable suspicious registered devices.
   - Switch to the [Devices] section on the user screen.
   - Select a suspicious device and click [Disable].

Details of Initial Response

5. Delete suspicious mail forwarding rules.
   - Import the ExchangeOnlineManagement module on the connecting PC in advance.
     ```
     Import-Module ExchangeOnlineManagement
     ```
   - Connect to Exchange Online using PowerShell.
     ```
     Connect-ExchangeOnline -UserPrincipalName admin@example.com
     ```
   - Check for existing InboxRules about compromised user.
     ```
     Get-InboxRule -Mailbox Joker@example.com
     ```
   - Remove suspicious InboxRules about compromised user.
     ```
     Remove-InboxRule -Mailbox Joker@example.com -Identity "ProjectA-MoveToFolderA“
     ```

6. Disable Entra ID apps that were registered before or after the intrusion.
   - Access the Azure Portal (https://portal.azure.com/) with an account with application viewer or higher permissions.

     【Enterprise applications】
     - Navigate to [Microsoft Entra ID] - [Enterprise applications] - [All applications].
     - Sort by [Add filters] - [Created on == Last 7 days (*reference)] and check if there are any new app registrations before and after the incident, if any, select it.
     - Switch to the [Properties] section and set “Enable for users to sign-in?" to "No".
     - Delete apps after the incident response is complete. (Cont.)

Details of Initial Response

6. (Cont.) Disable Entra ID apps that were registered before or after the intrusion.
   - Access the Azure Portal (https://portal.azure.com/) with an account with application viewer or higher permissions.

     【App registrations】
     - Navigate to [Microsoft Entra ID] - [App registrations] - [All applications].
     - Sort by [Created on] for apps created before and after the incident, if there are any suspicious apps, select them.
     - Switch to the [Certificates & secrets] section and delete the secret if any.
     - Switch to the [API permissions] section and delete suspicious permissions.
     - Delete apps after the incident response is complete.

7. Request, collect, and investigate logs.

   【 Entra ID Logs 】
   - Access the Azure Portal (https://portal.azure.com/).
   - Navigate to [Microsoft Entra ID] - [Monitoring] - [Sign-in logs] or [Audit logs] and click [Download].

   【 Unified Audit Log 】
   - Connect to Exchange Online using PowerShell.
   - Use `Search-UnifiedAuditLog` to get logs. (Cont.)

Details of Initial Response

7. (Cont.) Request, collect, and investigate logs.
   【 Unified Audit Log 】
   - The following is a reference example that outputs multiple RecordTypes in bulk.

```
$recordTypes = @("ExchangeAdmin", "ExchangeItem", "ExchangeItemGroup", "AzureActiveDirectory",
"AzureActiveDirectoryStsLogon", "SharePoint", "SharePointFileOperation", "OneDrive")
$startDate = "12/1/2023“
$endDate = "12/14/2023" $userId = Joker@example.com
$resultSize = 5000 $outputPath = "/Users/admin/file/UAL/JohannaL_UAL.csv“
foreach ($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 }
```

8. Investigate other recipients of the intrusion-starting email.
   - Access Microsoft Defender (https://security.microsoft.com/).
   - Navigate to [Email & collaboration] - [Explorer].
   - Investigate whether there are any users who have received similar emails to the compromised user.

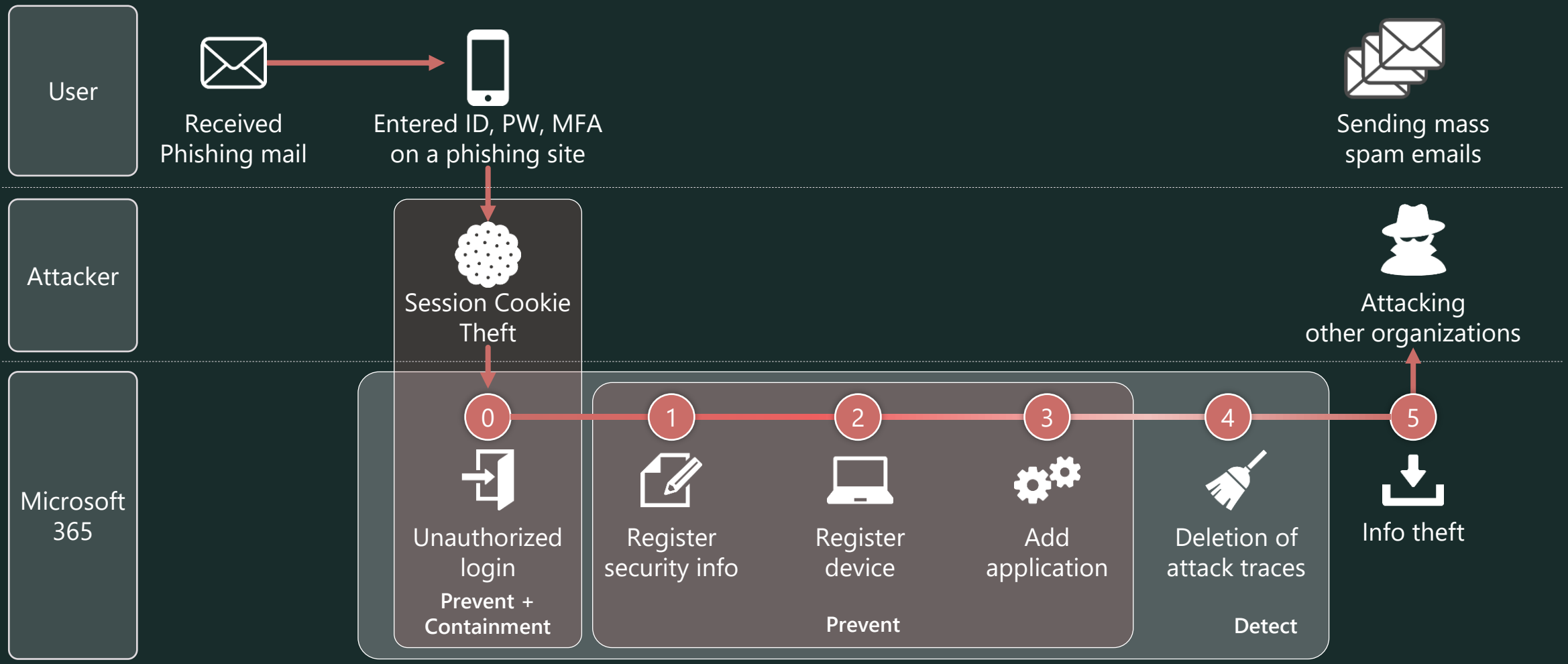
9. Investigate suspicious sign-ins before and after receiving the email to identify other compromised users.

Appendix: List of defensive measures

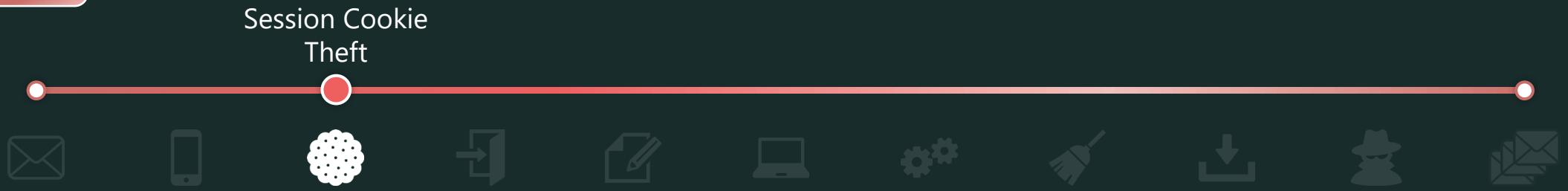
* Includes a restatement of defenses mentioned within the slides of this volume.

* It does not cover all possible attack scenarios. There have been reports of APTs using methods not listed below, such as abusing Power Platform, First Party Apps, and inviting guest users.

Defensive Measures



Prevent



✓ Use conditional access policy to allow use tokens only from devices on which they were issued.

* This feature is still in preview and is only available in Office 365 Exchange Online and Office 365 SharePoint Online.

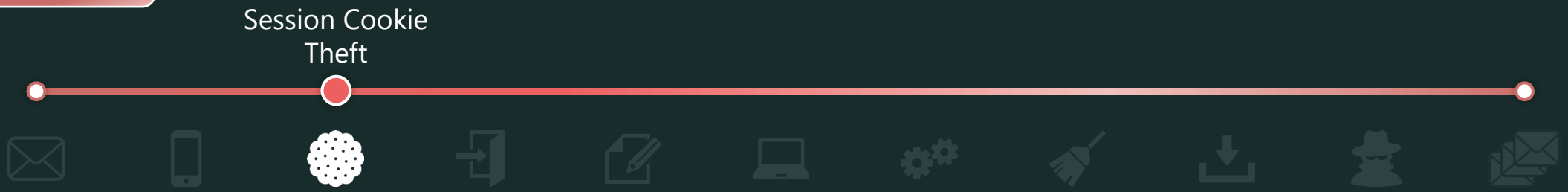
License: Entra ID Premium P2

Policy settings:

- [Assignments]
  - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
  - [Target resources] - [Cloud apps]: Office 365 Exchange Online, Office 365 SharePoint Online
- [Access controls] - [Session]: Require token protection for sign-in sessions (Preview)

Reference:
Conditional Access: Token protection (preview) https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection

Containment



✓ Limit the session duration of Outlook on the Web (OWA) to 1 hour.

- The non-persistent session token issued by Microsoft Entra ID for accessing OWA is 24 hours by default, so create a conditional access policy to require reauthentication after 1 hour.

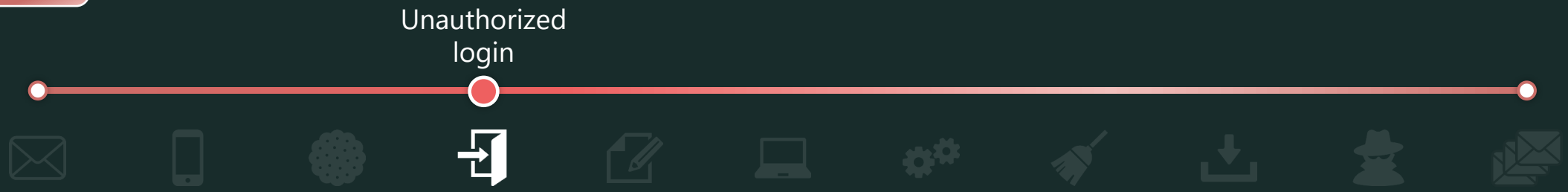
License: Entra ID Premium P1

Policy settings:

- [Assignments]
  - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
  - [Target resources] - [Cloud apps]: Office 365 Exchange Online
  - [Conditions] - [Client apps]: Browser
- [Access controls] - [Session]: [Sign-in frequency] - [Periodic reauthentication = 1 Hours]

Reference: Configure authentication session management with Conditional Access
https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime#policy-1-sign-in-frequency-control

Prevent



- ✓ Use conditional access policy to allow sign-ins only from devices that are hybrid-joined to Entra ID or managed by Intune and have passed compliance checks.

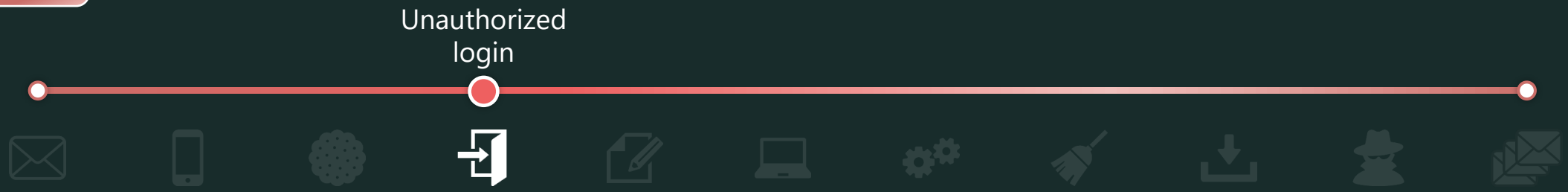
  License: Entra ID Premium P1, Intune

  Policy settings:

  - [Assignments]
    - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
    - [Target resources] - [Cloud apps]: All cloud apps
  - [Access controls] - [Grant] - [Grant access]:

    “Require device to be marked as compliant” or “Require Microsoft Entra hybrid joined device”

Prevent



✓ Use conditional access policy to require strong authentication methods (Windows Hello for Business, FIDO2 security key, etc.) for sign-ins.

License: Entra ID Premium P1, Device with string auth methods

Policy settings:

- [Assignments]
  - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
  - [Target resources] - [Cloud apps]: All cloud apps
- [Access controls] - [Grant] - [Grant access]: “Require authentication strength”

Reference:
Conditional Access authentication strength: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths

Detect

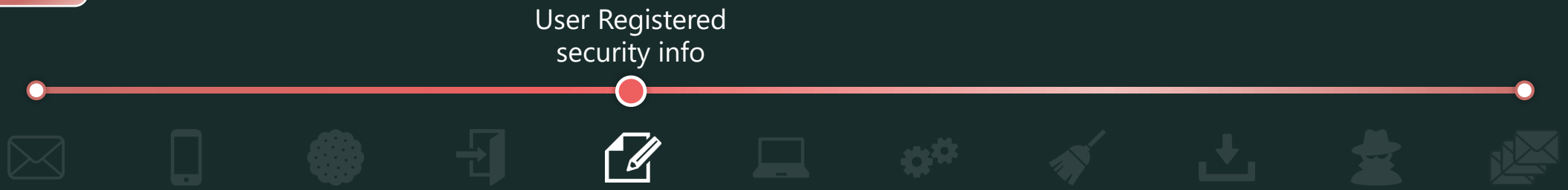
- ✓ Detect accesses from two or more countries within 10 minutes (as a guide) in Entra ID Interactive Sign-in logs.

  License: Entra ID Free + SIEM

- ✓ Send an alert to administrators if the sign-in risk is medium or higher in Entra ID Identity Protection.

  License: Entra ID Premium P2

Prevent



✓ Use conditional access policy to block or require MFA* for security info registration from anywhere other than a "trusted location".

*Users who are not registered with security info (multi-factor authentication) will be locked out.

*You can require not only MFA but devices to be marked as compliant or to have joined Microsoft Entra.

License: Entra ID Premium P1

Policy settings:

- [Assignments]
  - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
  - [Target resources] - [User actions]: Register security information
  - [Conditions] – [Locations]: Exclude trusted locations.
- [Access controls] - [Grant] - [Grant access]: Require your favorite options (e.g., MFA, device to be marked as compliant).

Reference: Enable combined security information registration in Microsoft Entra ID
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-registration-mfa-sspr-combined#create-a-policy-to-require-registration-from-a-trusted-location

Detect

User Registered security info

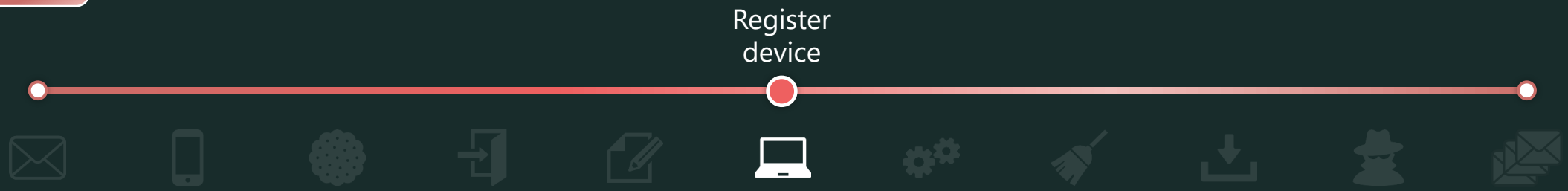
✓ Export Entra ID audit logs to SIEM and monitor the following attributes.

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



✓ Use conditional access policy to block or require MFA* for device registration from anywhere other than a "trusted location".

*You can require not only MFA but devices to be marked as compliant or to have joined Microsoft Entra.

License: Entra ID Premium P1

Policy settings:

- [Assignments]
  - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
  - [Target resources] - [User actions]: Register or join devices
  - [Conditions] – [Locations]: Exclude trusted locations.
- [Access controls] - [Grant] - [Grant access]: Require your favorite options (e.g., MFA, device to be marked as compliant).

Reference:
Conditional Access: Target resources - User actions: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-cloud-apps#user-actions

Detect

✓ Send device registration notifications to users.

In the Intune admin center, set up enrollment notifications for newly registered devices to users.

This will allow users to be aware of any unexpected device registrations and contact IT administrators.

License: Entra ID Premium P1 + Intune

Reference:
Set up enrollment notifications https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-notifications

Detect

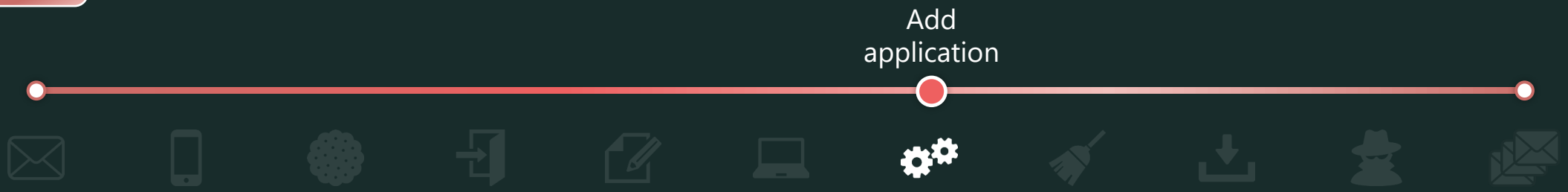
✓ Export Entra ID audit logs to SIEM and monitor the following attributes.

License: Entra ID Premium P1+ SIEM

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

Reference:
Set up enrollment notifications https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-notifications

Prevent



✓ Prevent general users from “Add application”

- In the Azure portal, set "Users can register applications" to "No".

License: Entra ID Free

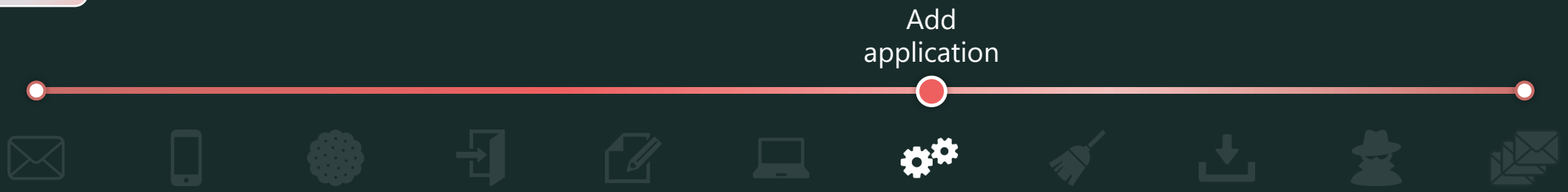
✓ Do not allow general users from “Consent to application”

- Do not allow general users to register service principals to [Enterprise Applications] by granting consent.
- In the Azure portal, at [Enterprise Applications] > [User consent settings], set “Do not allow user consent”.

License: Entra ID Free

Reference:
To disable the default ability to create application registrations or consent to applications
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#to-disable-the-default-ability-to-create-application-registrations-or-consent-to-applications
Applications that are not known to administrators are added to enterprise applications!
https://jpazureid.github.io/blog/azure-active-directory/enterpriseapps-multitenantapps/

Detect



✓ Export Entra ID audit logs to SIEM and monitor the following attributes.

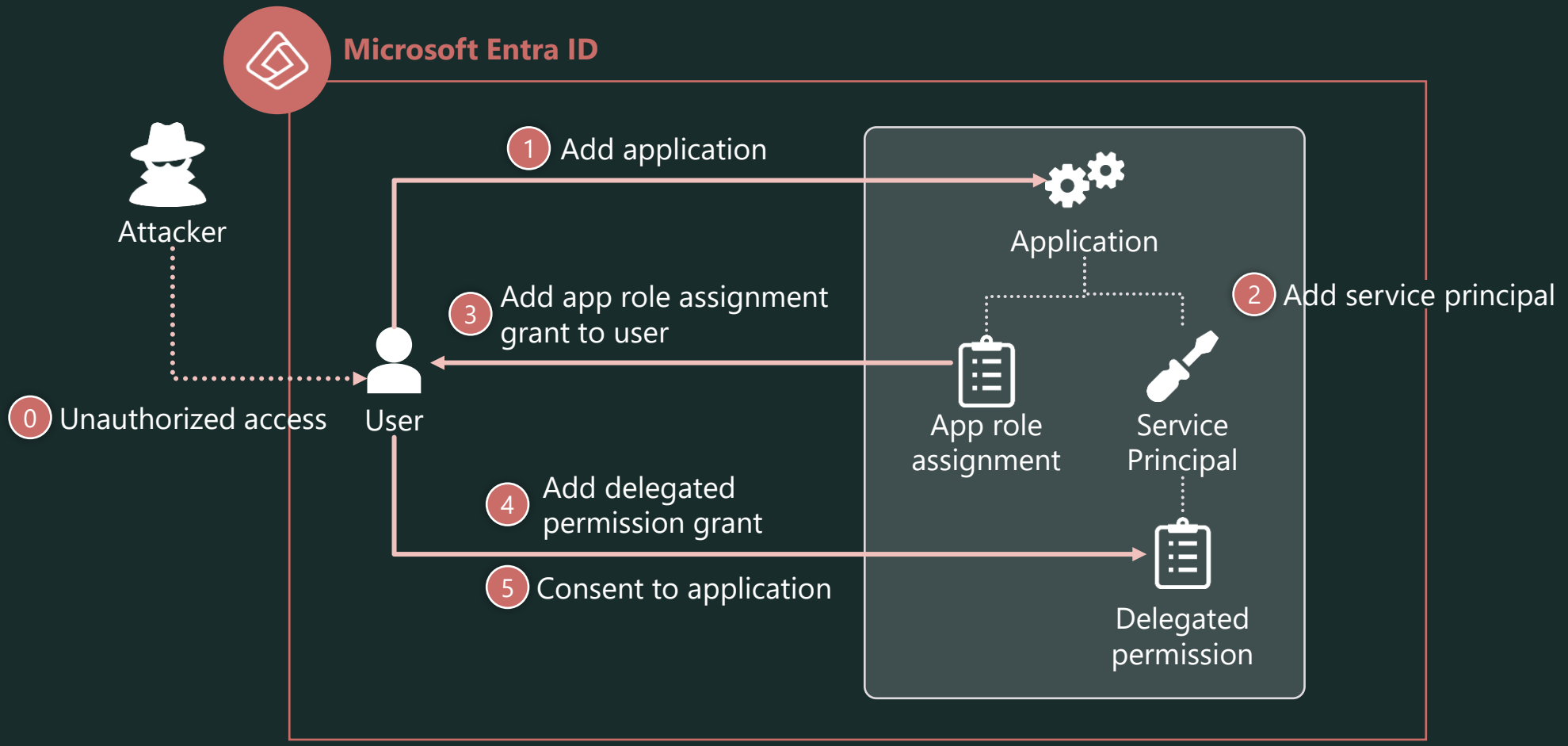
License: Entra ID Free + SIEM

#	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

About Entra ID Audit logs output during app addition

The following is an image of the log output when an app is added in Entra ID.

* Please contact Microsoft for accurate information as this is just an image.



Detect

✓ Detect mail forwarding rule creation

Export the Unified Audit Log to SIEM and monitor the following attributes.

*Other traces can be seen from the Unified Audit Log are omitted because it is difficult to distinguish from normal activities.

License: Audit (Standard) + Exchange Online + SIEM

RecordType	Operation	Activity
ExchangeAdmin	New-InboxRule	Create mail forwarding rules (InboxRule)

ITOCHU Cyber & Intelligence Inc.