#FIRSTCON24

EMAIL BREACH ANALYSIS AND RESPONSE TIPS TO AVOID RISK

Yumi Iida (ITOCHU Cyber & Intelligence Inc., JP)

Presenter introduction

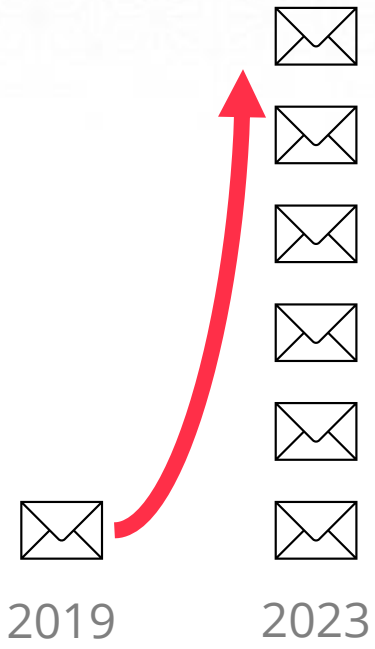
Yumi Iida

Cybersecurity Architect
ITOCHU Cyber & Intelligence

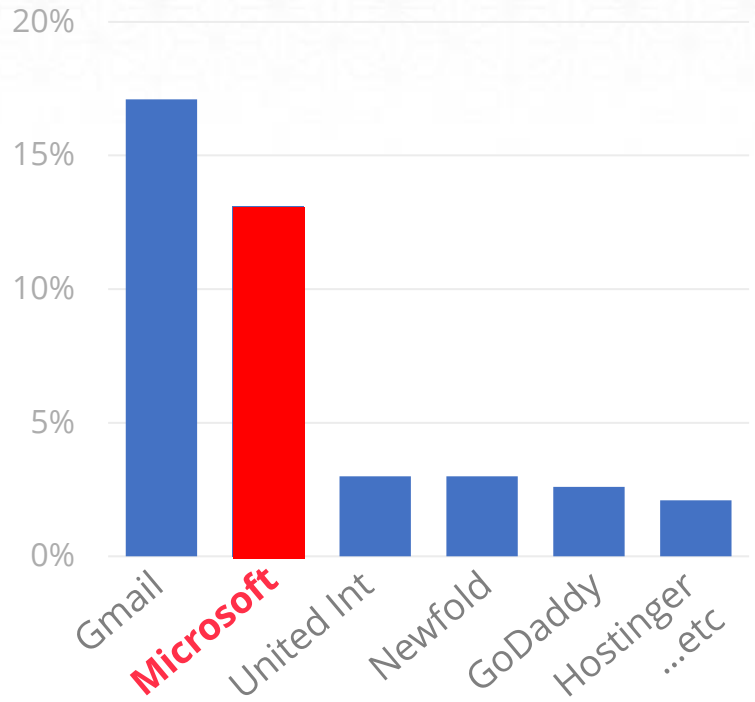
Contact: iida-yumi@itochu.co.jp

Background

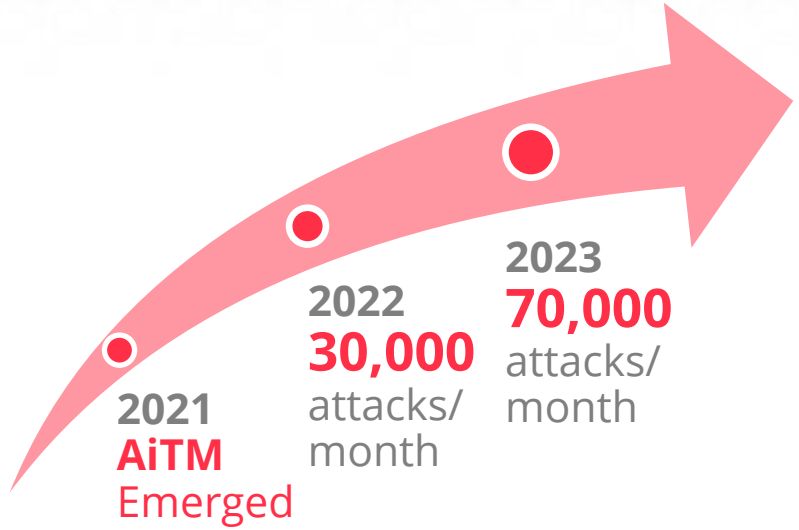
The number of phishing attacks *1



Market shares of email server providers *2

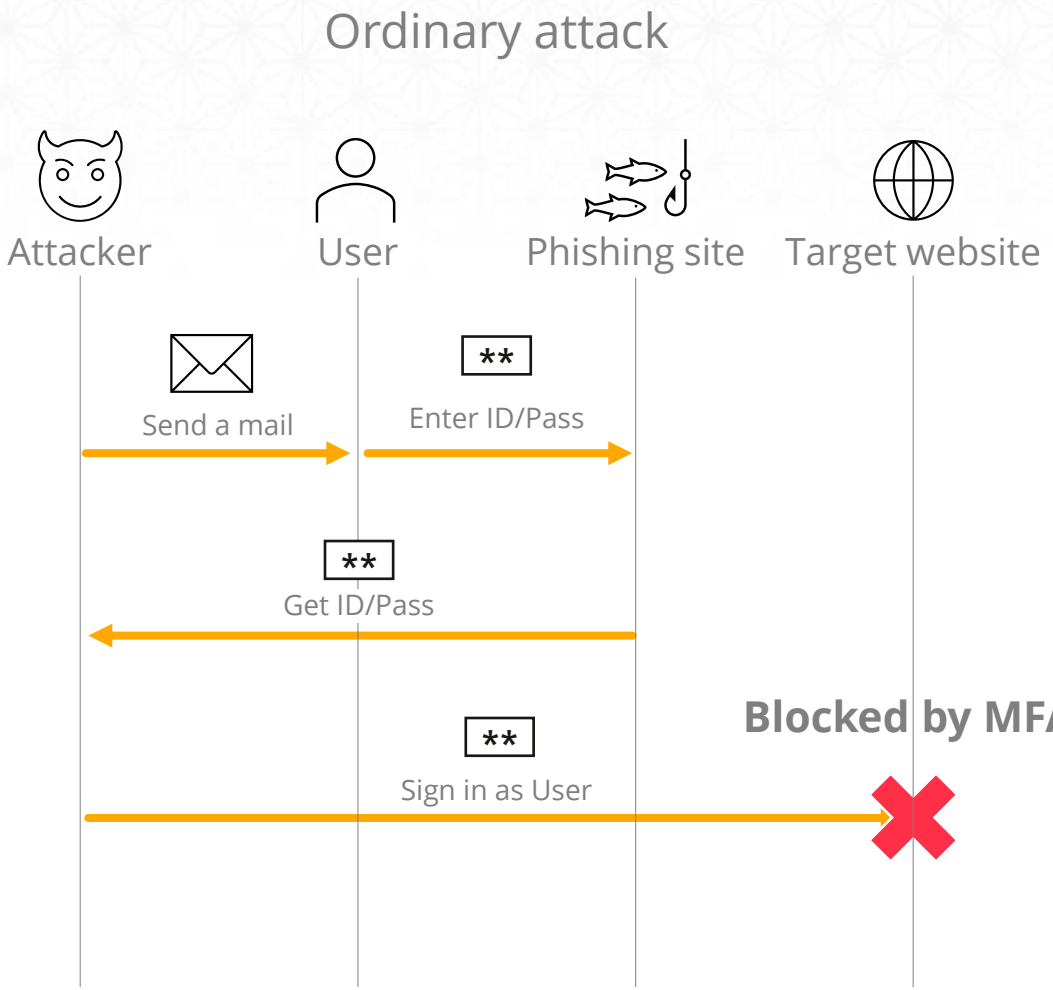


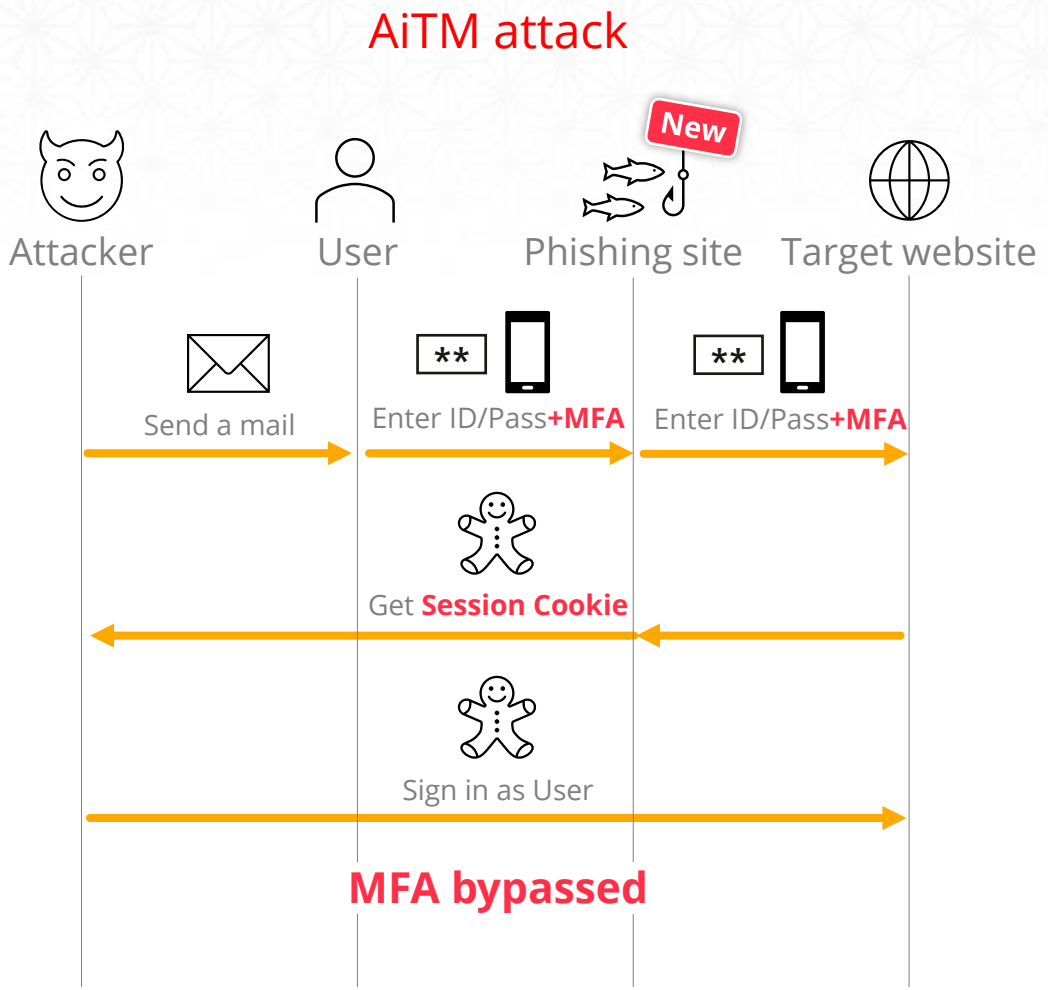
History of AiTM *3,4



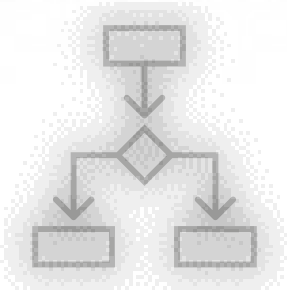
References:
*1 APWG PHISHING ACTIVITY TRENDS REPORTS (https://apwg.org/trendsreports/)
*2 Web Technology Surveys – Usage statistics of email server providers (https://w3techs.com/technologies/overview/email_server)
*3 Blog - From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to 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?

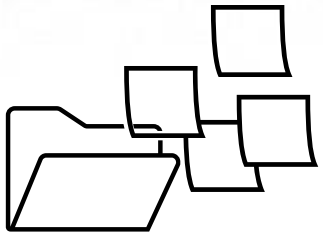

Ordinary attack
Attacker
User
Phishing site
Target website
Send a mail
**
Enter ID/Pass
**
Get ID/Pass
**
Sign in as User
Blocked by MFA


AiTM attack
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

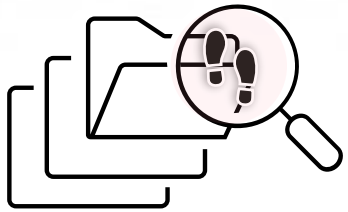
Challenges in incident response



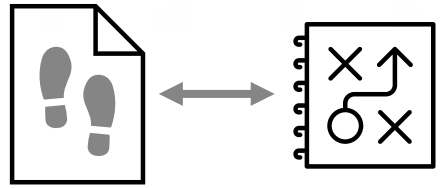
Unclear initial response procedures



Selecting and collecting relevant logs



Identifying log entries indicating attack traces



Linking attack traces to effective response measures

An Inadequate response can lead to **the expansion of damage**

Purpose of this presentation

We'll cover the following topics **based on a real-world M365 account intrusion incident:**

- Initial response procedures
- Key points of incident investigation
- Details of attacker traces and associated logs
- Defensive measures

Let's practice incident response!

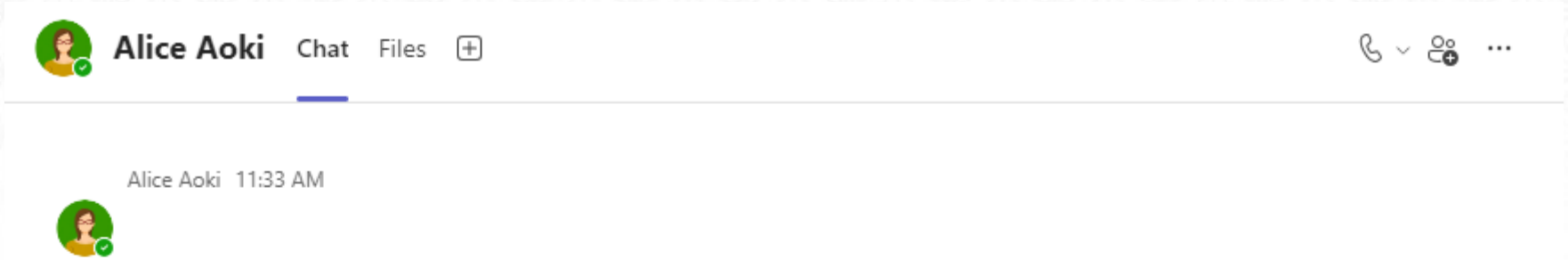
- Created a demo incident according to several actual cases.

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

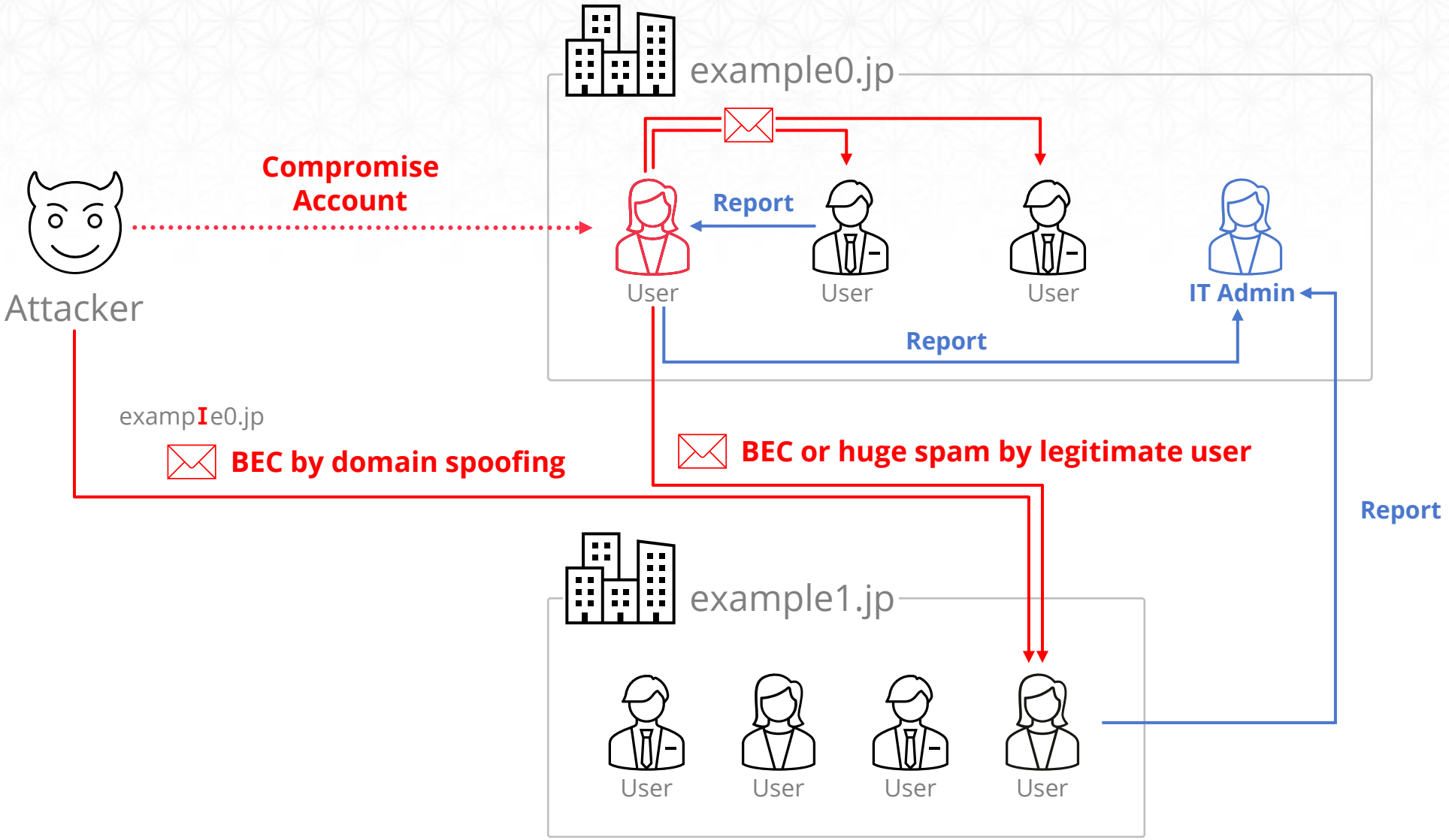
Employees:	300
License:	Microsoft 365 Enterprise E3
Mail service:	Exchange Online only
MFA:	Microsoft Authenticator (OTP app)

An incident

* Alice is the **default** user.

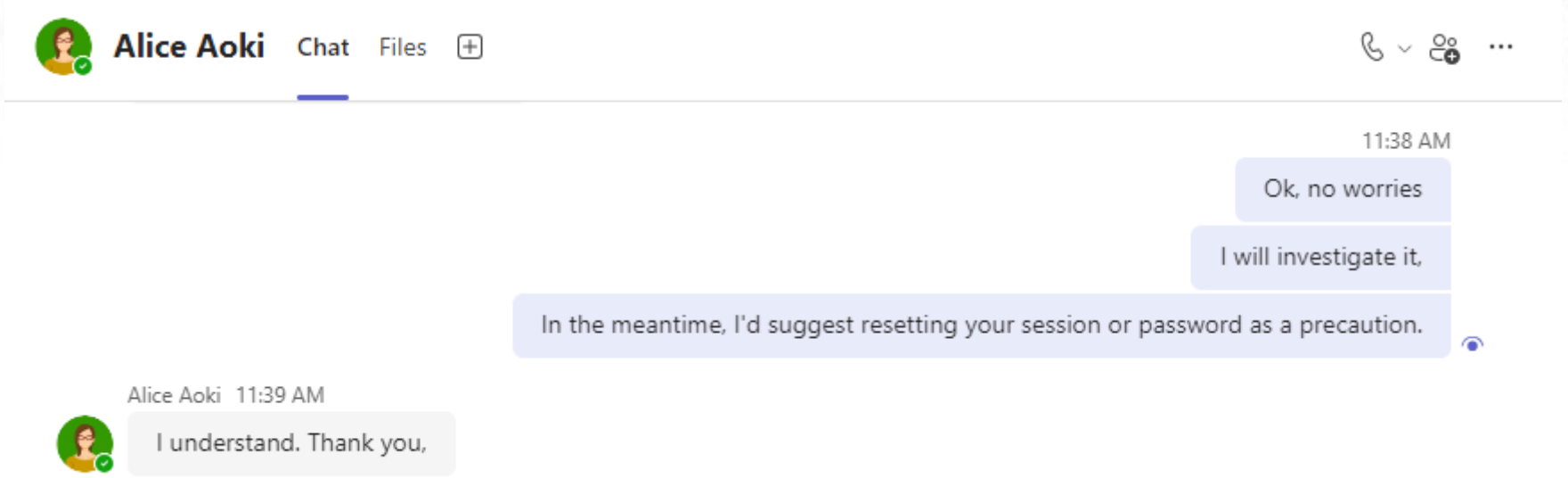


An incident

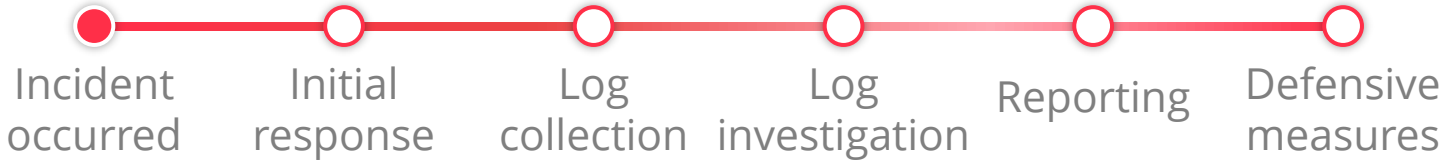

example0.jp
Compromise Account
Attacker
User
Report
User
User
IT Admin
Report
exampIe0.jp
BEC by domain spoofing
BEC or huge spam by legitimate user
Report
example1.jp
User
User
User
User

An incident

* Alice is the **default** user.



What are the steps for the incident response?



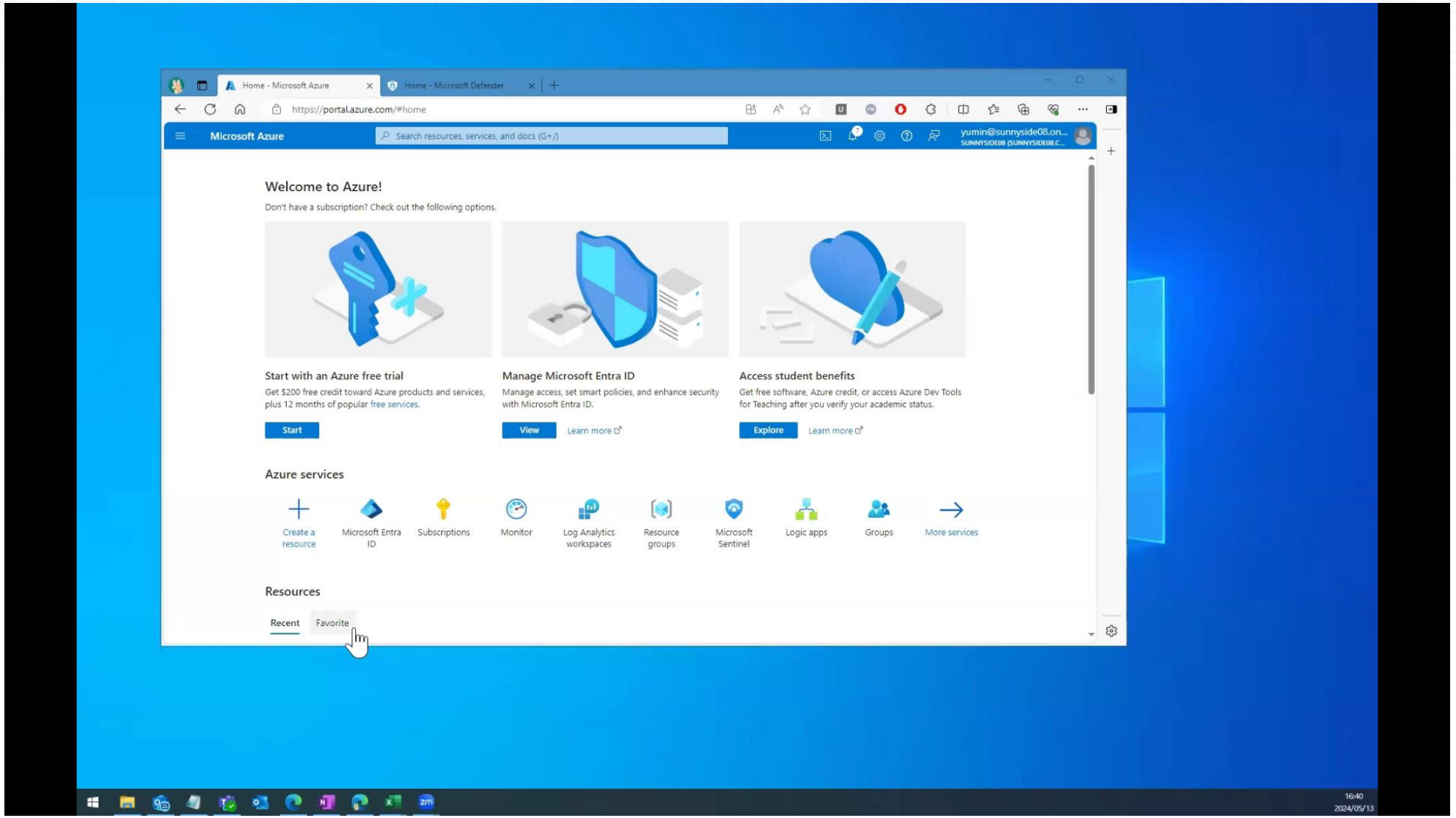
Initial response

Initial response

- What would you do?

```
Disconnect the company network
Collect and clean up Alice's computer
Delete Alice's account from the tenant
Revoke Alice's account session and reset her password
```

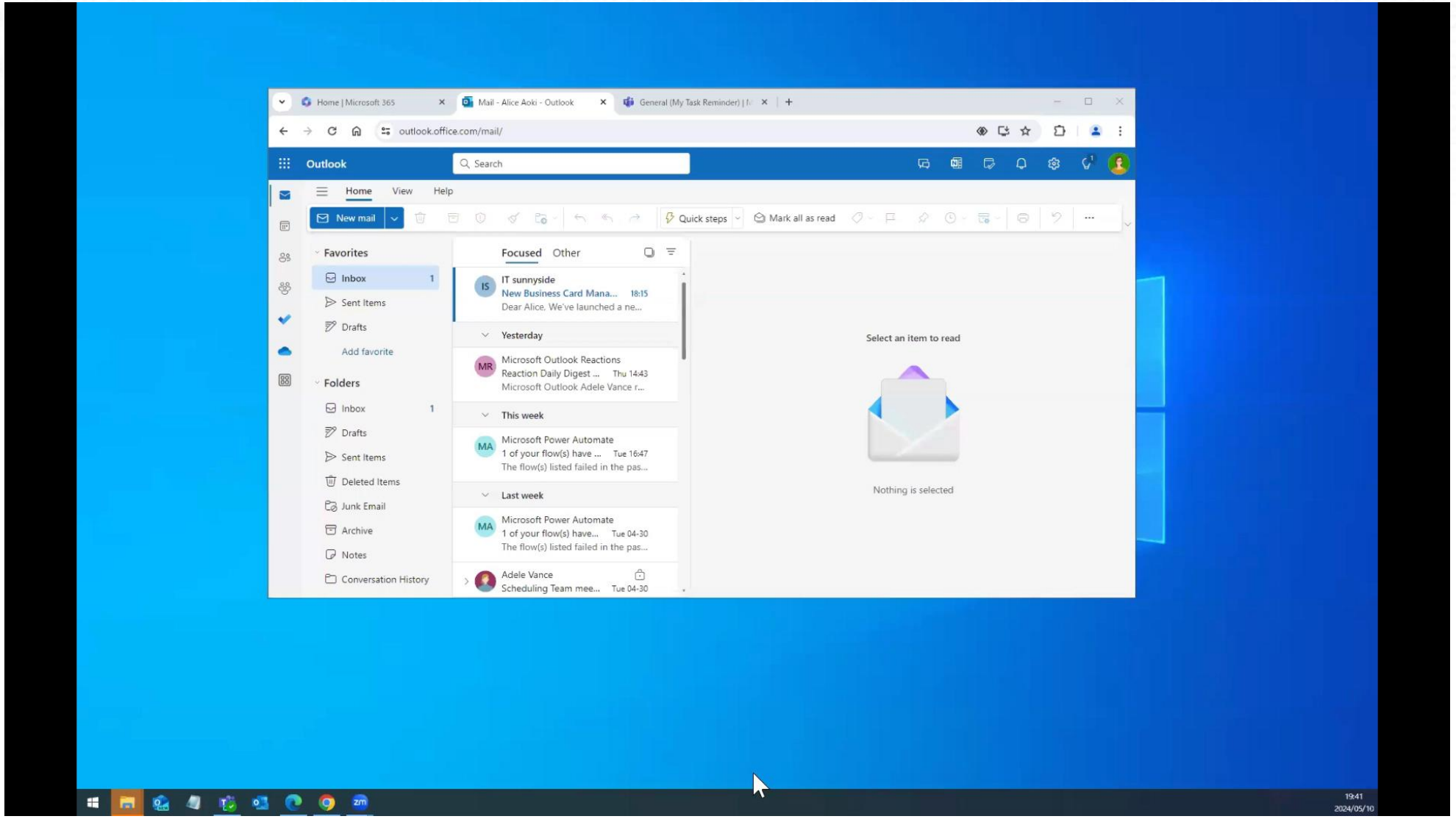
DEMO) Initial response



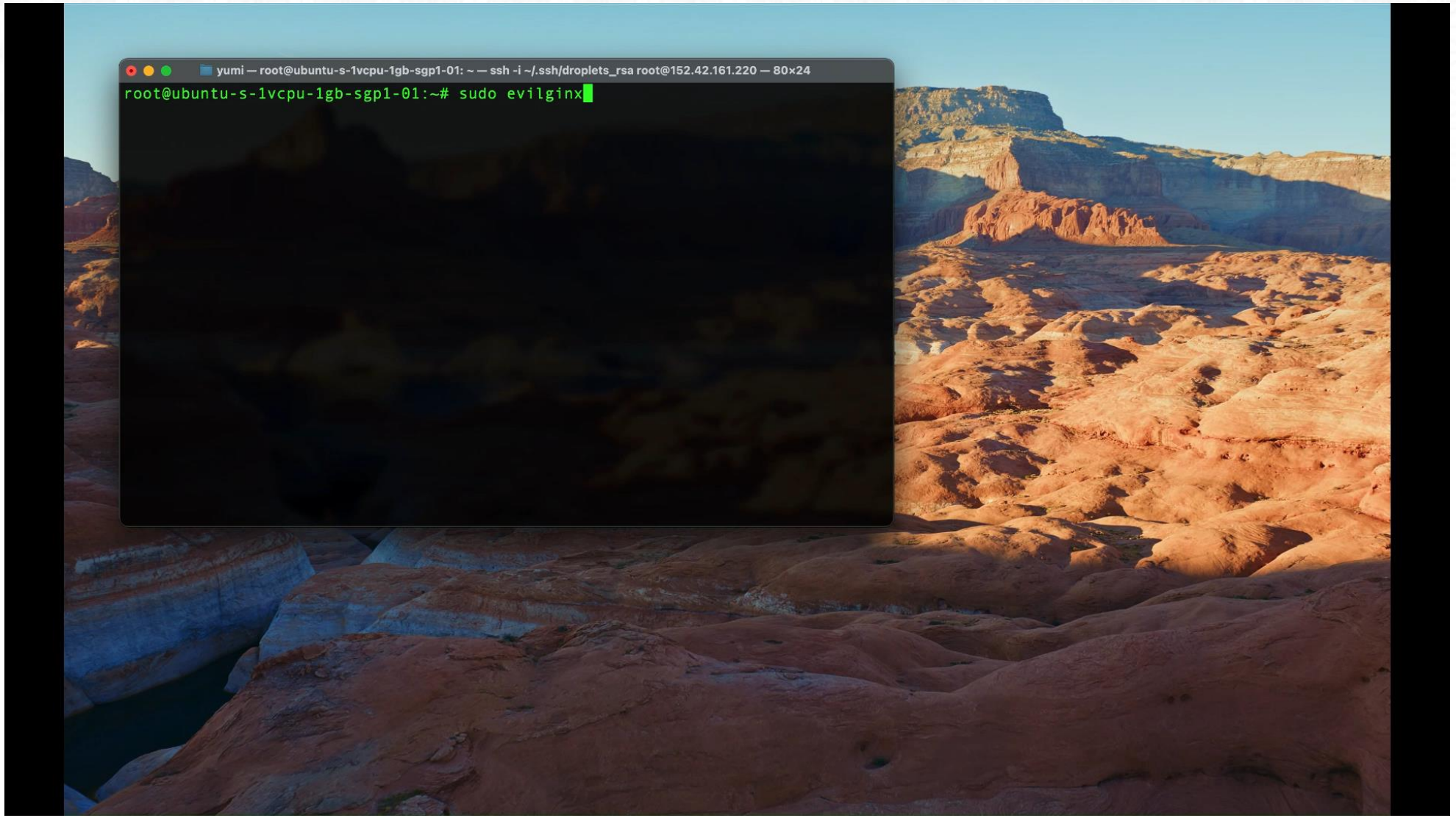
DEMO) Initial response

- ✓ **Contain the intrusion**
  - Disconnect the session
  - Remove the registered suspicious device or security info
- ✓ **Do not erase the traces**
  - Do not “delete” in general
  - Explore the “disable” option
- ✓ **Identify the scope of the intrusion**
  - Check for similar intrusion within the organization

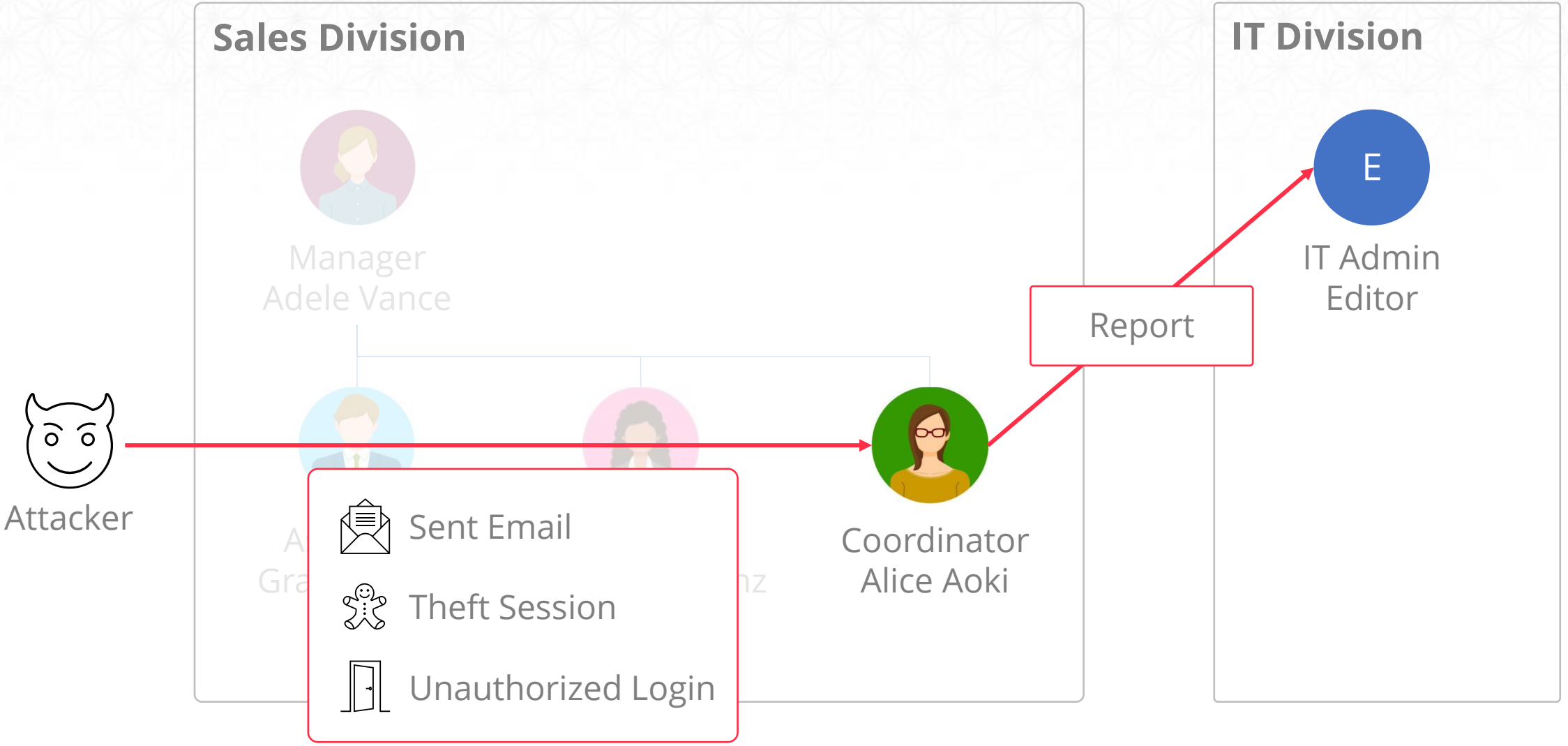
What caused the incident? – **User side**



What caused the incident? – **Attacker side**



How did the incident unfold?



Prevent unauthorized login

- ✓ Use conditional access policy to allow sign-ins only from devices that are hybrid-joined to Entra or managed by Intune and have passed compliance checks.
  License: Entra ID 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 P1, Device with string auth methods

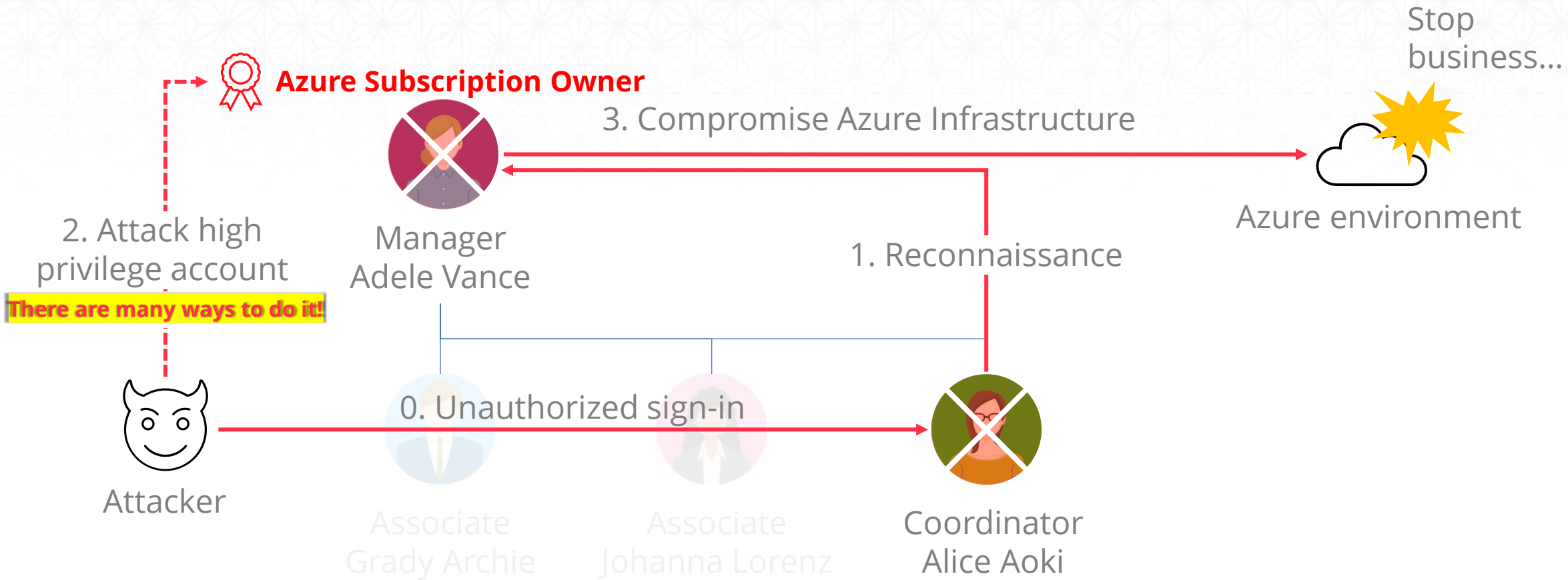
References: Conditional Access authentication strength https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths

Consider different scenario

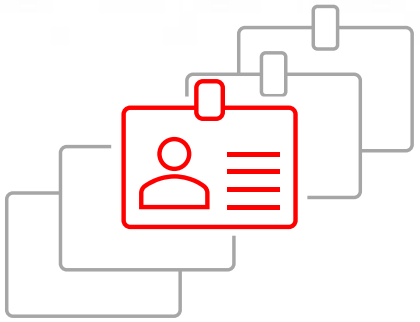
If Alice has high privileges

- ✓ Disable the account
- ✓ Examine Entra/Azure Audit Logs to identify compromises

Privilege escalation poses the greatest threat

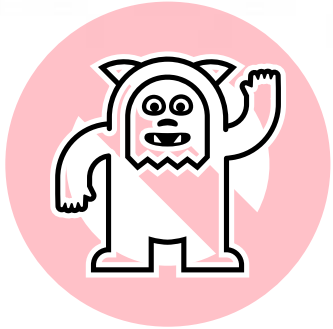


Mitigate the account intrusion attack



Implement
least privilege access

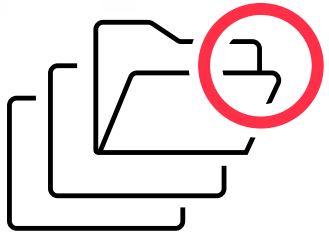
Disable
dormant accounts



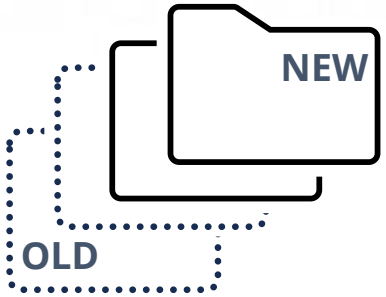
Restrict
guest accounts

Log collection & investigation

Common problems in log collection & investigation



Collect appropriate logs



Set retention periods not to lose them

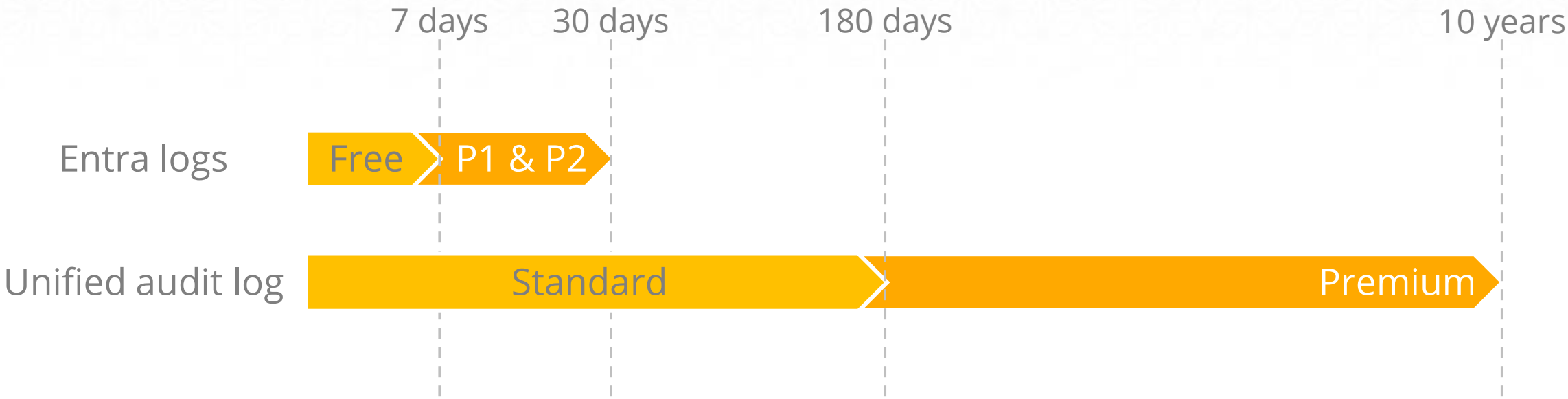
Identify attack traces

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

Logs for investigation

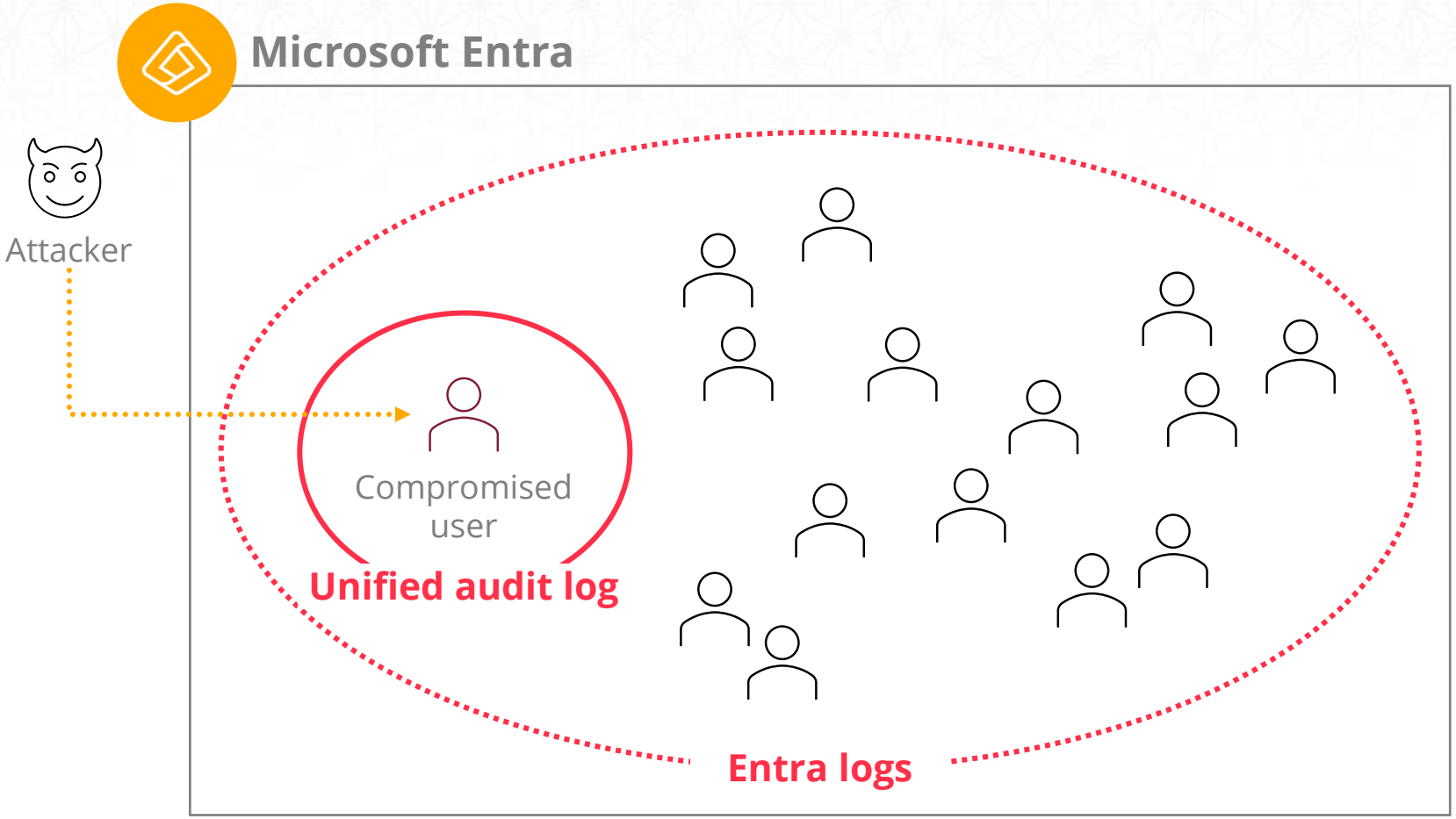
Log type	Purpose
Entra Sign-in logs	Check for suspicious sign-ins and source IP addresses.
Entra Audit logs	Check for suspicious activities. e.g. Register security information or apps
Unified audit log	Identify suspicious email and file-related activities for specific users.

Data retention periods

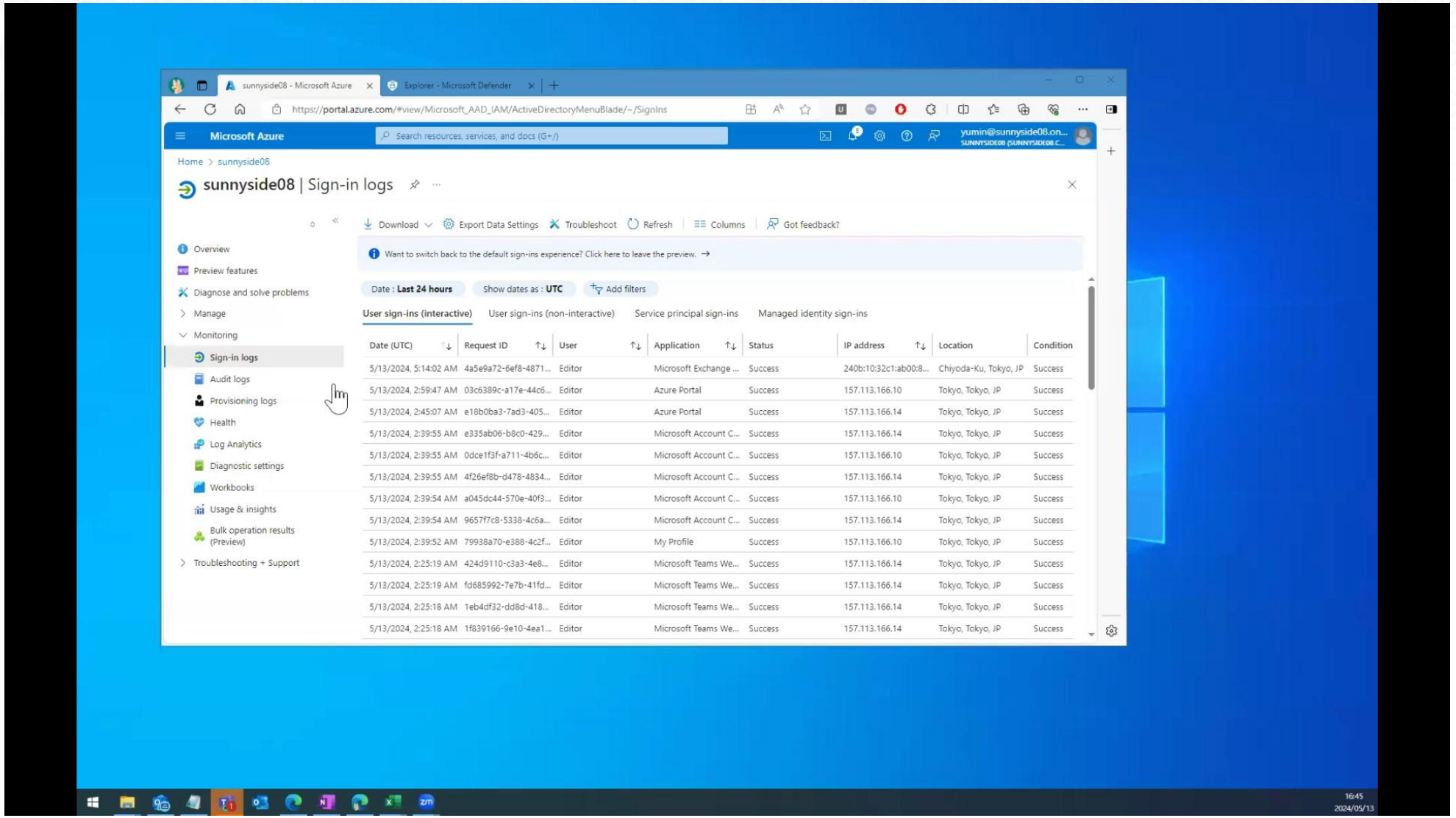


References:
Microsoft Entra data retention: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention#activity-reports
Default audit log retention policy: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies#default-audit-log-retention-policy

Investigation scope for log types



DEMO) Entra audit logs investigation



Points for collecting and investigating logs

- ✓ Be aware of the licenses and log retention periods beforehand!
- ✓ Start the exploration from known intrusions.
- ✓ Identify and respond to the intrusion to prevent further compromises.
    - Detect a suspicious application → disable it, check this contents

Attack traces) Add an application

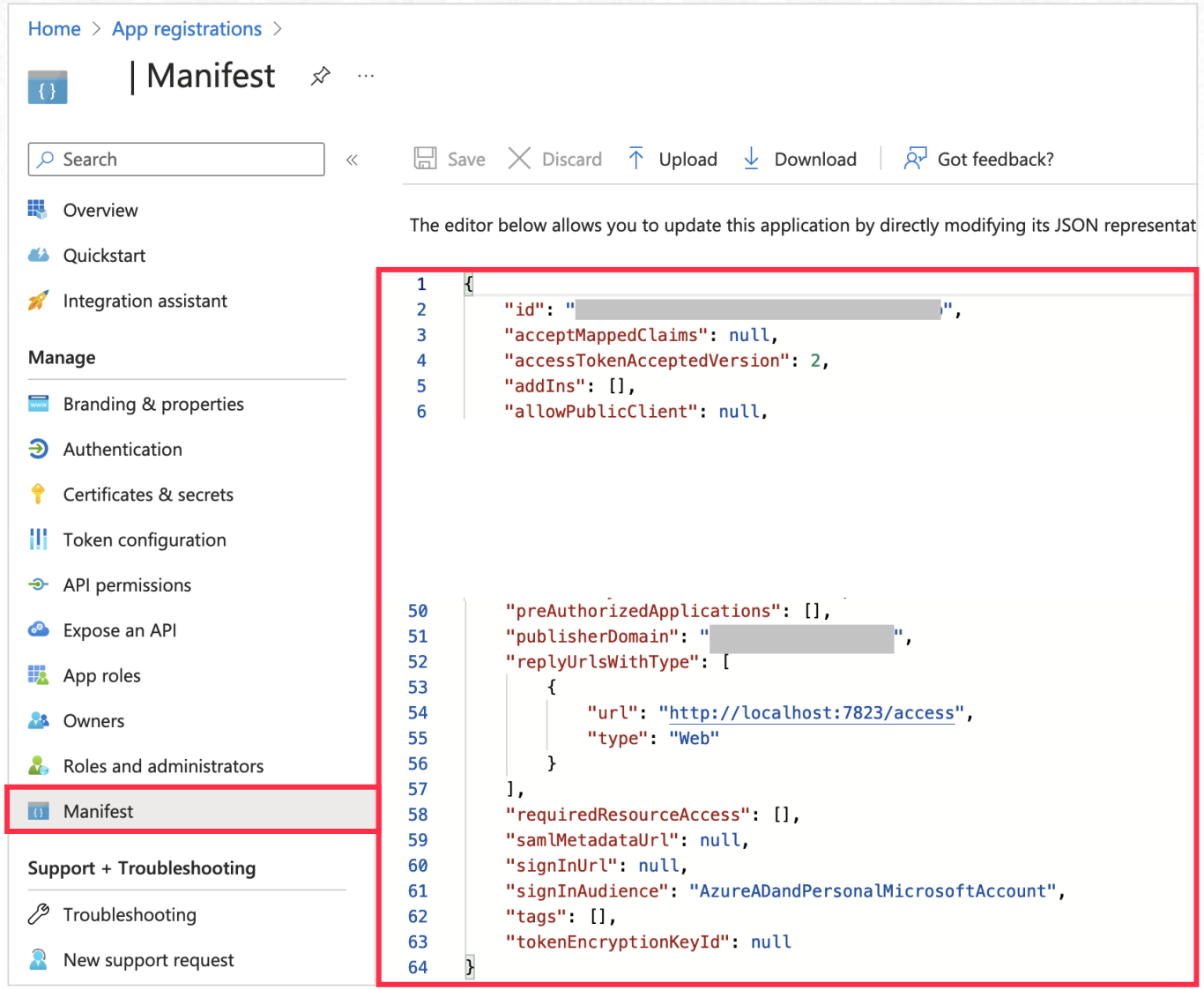
The actual incident have shown the following attacks:

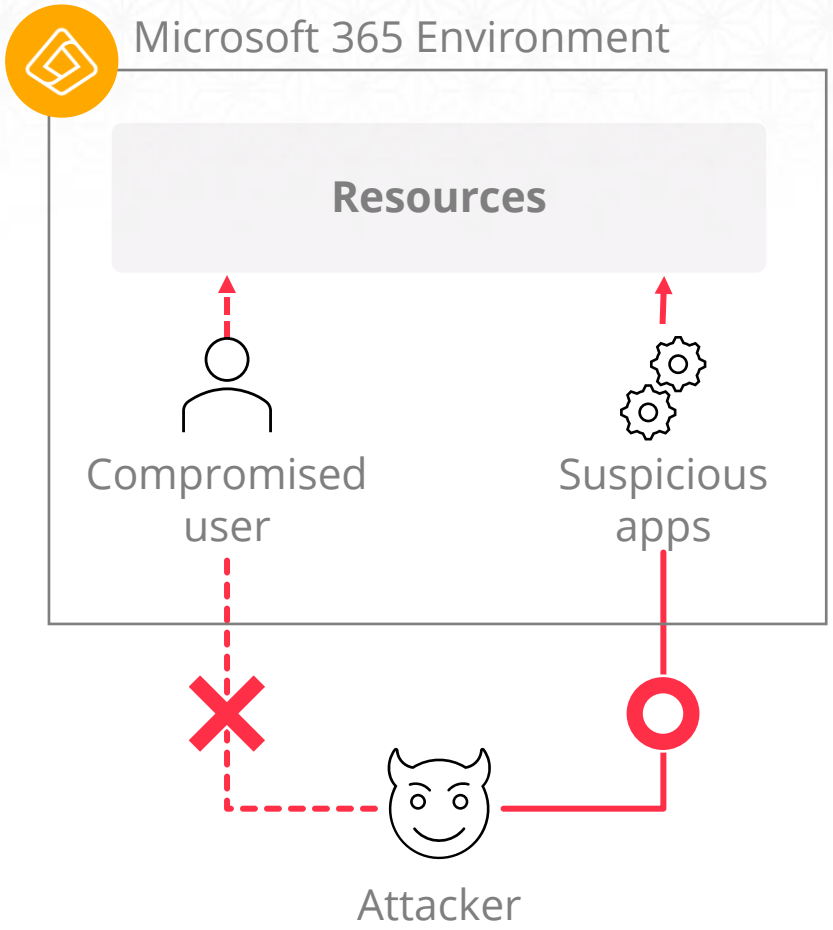
*We only collected Unified Audit Log in this real incident due to data retention period.

	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	{"CreationTime":"2023-08-29						
43	8/29/2023 8:43:00 PM	8	Add app role assignment grar	{"CreationTi						
44	8/29/2023 8:43:00 PM	15	UserLoggedIn	{"CreationTi						
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						

The flow of adding application

Attack traces) Add an application





Prevent adding applications

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

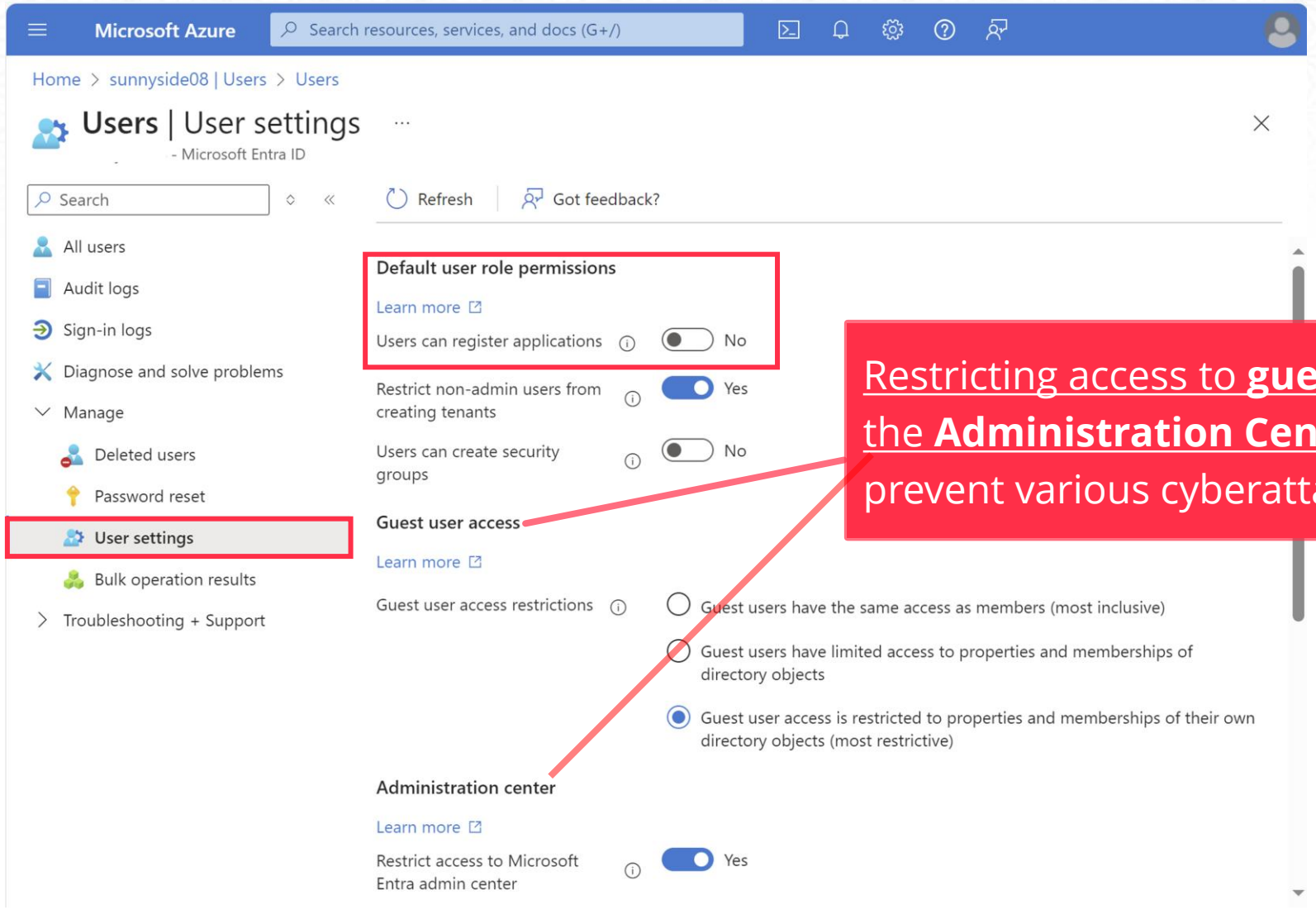
  License: Entra ID Free

- ✓ Do not allow general users from “Consent to applications”
  - 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 / Applications that are not known to administrators are added to enterprise applications!

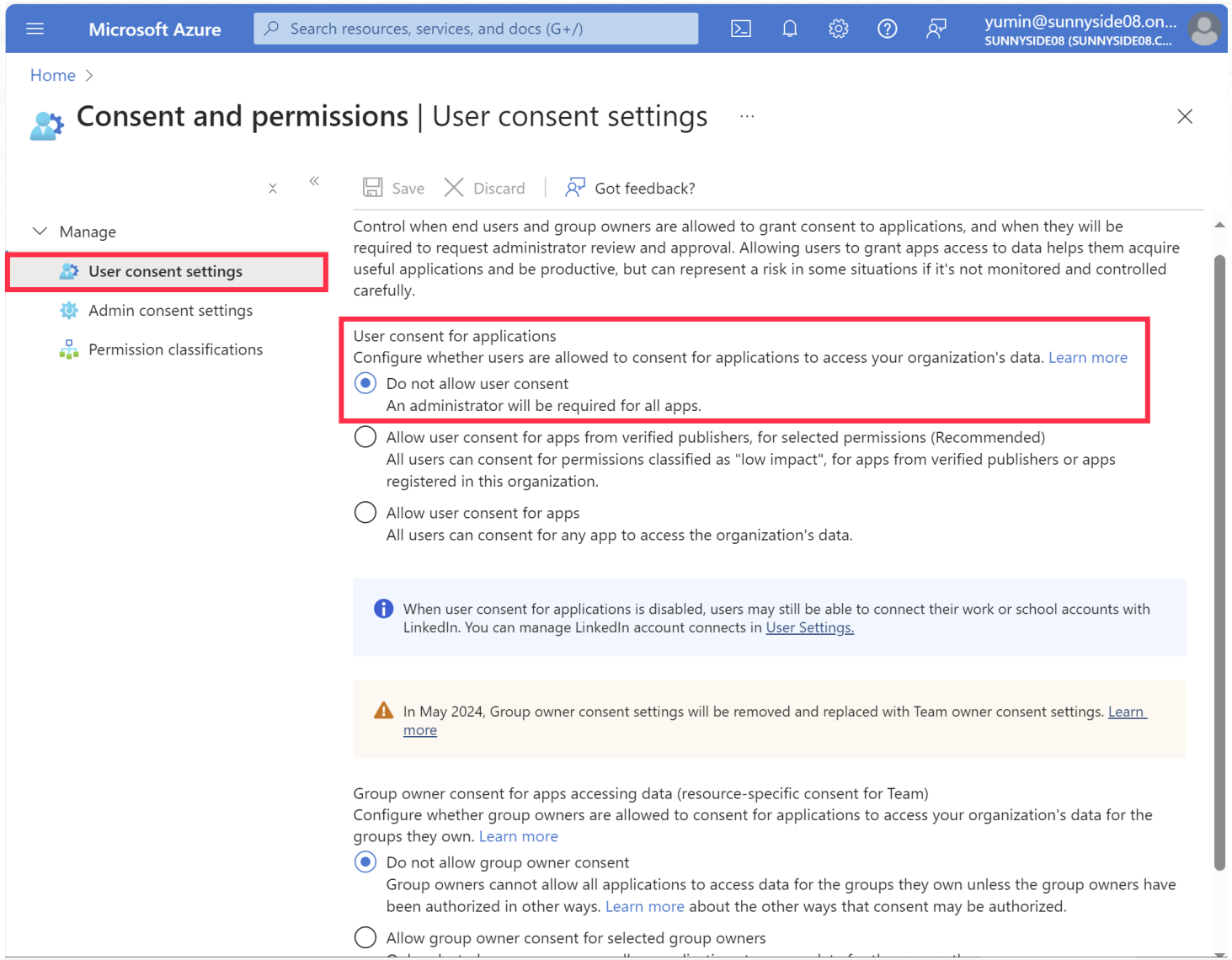
Prevent adding applications



Restricting access to **guest users** and the **Administration Center** can help prevent various cyberattacks.

Users - Microsoft Azure

Prevent the user from consenting to the application



[Consent and permissions - Microsoft Azure]

Attack traces) User registered security info, device

The following attacks in the actual incidents:

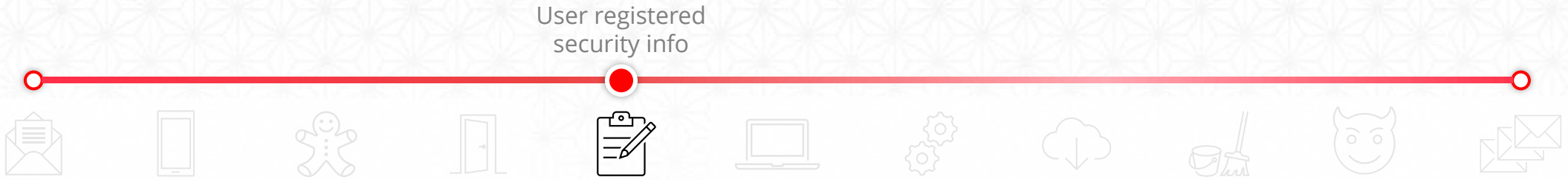
*Device registration is not covered in this demo, but it has been seen in the past.

	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		
6	2023-06-23T16:19:41.7904811+00:0	Core Directory	UserManagement	Update user	Success		cation
7	2023-06-23T16:19:52.496551+00:00	Core Directory	Device	Add registered owner to device	Success		cation
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

Prevent the 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 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

Log collection & investigation

- Unified audit logs

RecordTypes for unified audit log *Extract

#	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.
30	MicrosoftFlow	Microsoft Power Automate (formerly called Microsoft Flow) events.

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

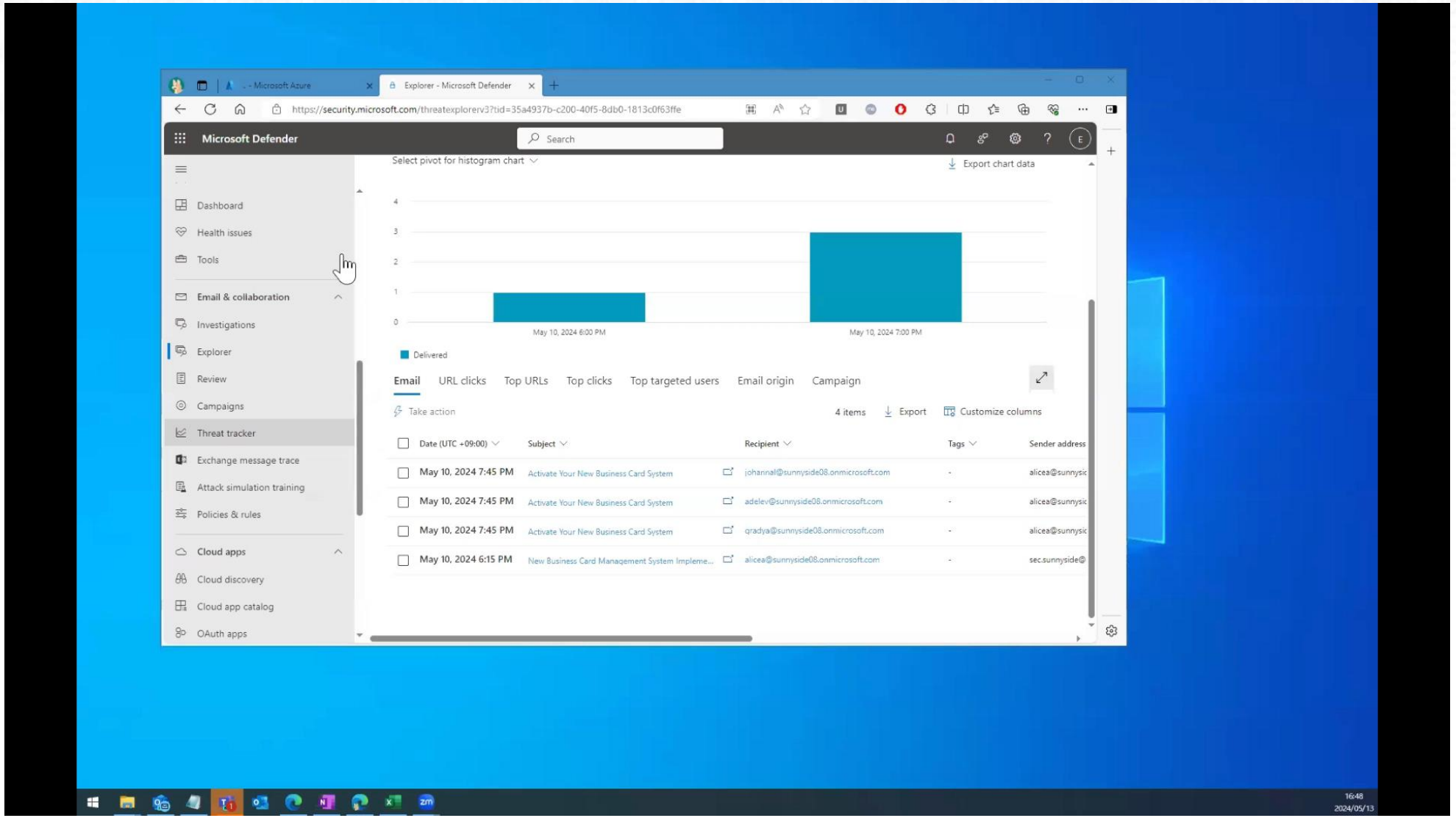
Data Scheme for unified audit log

	A	B	C	D	E	F	G	H	I
1	RecordId	CreationDate	RecordType	Operation	UserId	AuditData	AssociatedAdminUnits	AssociatedAdminUnitsNames	
31	f86b46ba-0	2024-05-10T10:54:07.	15	UserLoginFailed	AliceA@sunnyside08.onmicrosof	{"CreationTime":"2024-05-10T10:54:07","Id":"f86b46ba-06e1-4eb1-b042-29b26fd53600","Operation":"UserLoginFailed","OrganizationId":"35a4937b-c200-40f5-8db0-1813c0f63ffe","RecordType":15,"ResultStatus":"Success","UserKey":"1f2ff6f0-1c1a-4b24-aaba-8ce906bea318","UserType":0,"Version":1,"Workload":"AzureActiveDirectory","ClientIP":"240b:10:32c1:ab00:857:889:3734:e93","ObjectId":"00000003-0000-0000-c000-000000000000","UserId":"AliceA@sunnyside08.onmicrosoft.com","AzureActiveDirectoryEventType":1,"ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Success"},{"Name":"UserAgent","Value":"Mozilla¥/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko¥/20100101 Firefox¥/125.0"},{"Name":"RequestType","Value":"OAuth2:Authorize"}],"ModifiedProperties":[],"Actor":[{"ID":"1f2ff6f0-1c1a-4b24-aaba-8ce906bea318","Type":0},{"ID":"AliceA@sunnyside08.onmicrosoft.com","Type":5}],"ActorContextId":"35a4937b-c200-40f5-8db0-1813c0f63ffe","ActorIpAddress":"240b:10:32c1:ab00:857:889:3734:e93","InterSystemsId":"f8a7a023-903c-41d5-8cea-907eaed82cfa","IntraSystemId":"f86b46ba-06e1-4eb1-b042-29b26fd53600","SupportTicketId":"","Target":[{"ID":"00000003-0000-0000-c000-000000000000","Type":0}],"TargetContextId":"35a4937b-c200-40f5-8db0-1813c0f63ffe","ApplicationId":"3f691a1c-cb53-41e5-a56e-acfb23ae6ca5","DeviceProperties":[{"Name":"OS","Value":"MacOs"},{"Name":"BrowserType","Value":"Firefox"},{"Name":"SessionId","Value":"74775ea8-85c5-4d6a-b962-ecf66684a895"}],"ErrorNumber":"90094","LogonError":"AdminConsentRequired"}		
32	d77fdff9-de	2024-05-10T10:45:44.	2	Send	AliceA@sunnyside08.onmicrosof				
			2	Create	AliceA@sunnyside08.onmicrosof				
			15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
			15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
			15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
			15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
121	18b4564c-9	2024-05-10T10:44:05.	1	New-InboxRule	AliceA@sunnyside08.onmicrosof				
150	6eb5c540-8	2024-05-10T10:43:16.	50	MailItemsAccessed	AliceA@sunnyside08.onmicrosof				
154	8391fc22-5(	2024-05-10T10:43:16.	50	MailItemsAccessed	AliceA@sunnyside08.onmicrosof				
161	80a2375e-5	2024-05-10T10:43:16.	50	MailItemsAccessed	AliceA@sunnyside08.onmicrosof				
185	bba891d1-c	2024-05-10T10:43:05.	15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
240	a6f47778-b	2024-05-10T10:43:00.	15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
282	01088291-5	2024-05-10T10:41:55.	15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
287	37b153fc-c:	2024-05-10T10:41:50.	15	UserLoggedIn	AliceA@sunnyside08.onmicrosof				
324	54d4b1bf-a	2024-05-10T10:41:41.	15	UserLoginFailed	AliceA@sunnyside08.onmicrosof				
349									
350									
351									

Many UALs have the following common fields:

AuditData is JSON.
PowerQuery is useful for parsing them.

DEMO) Unified audit logs investigation



Points to investigate unified audit logs

- ✓ Analyze typical attack patterns.

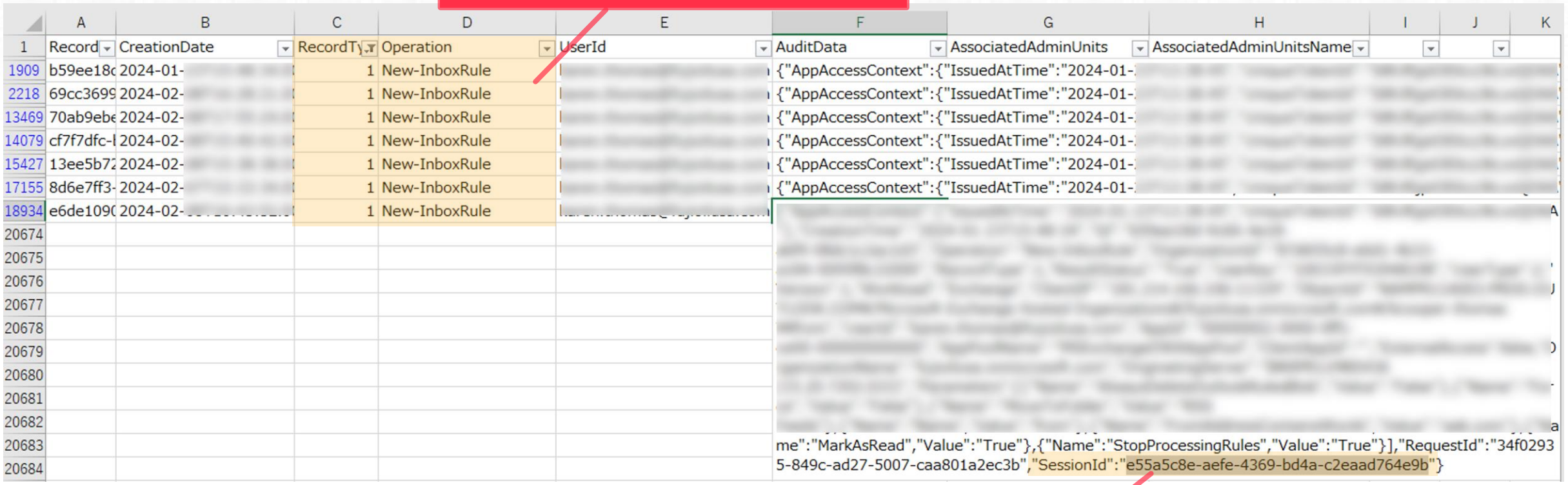
Priority	RecordType	Verification
1	ExchangeAdmin	Inbox-Rule created or deleted?
1	MicrosoftFlow	Unusual Microsoft Power Automate events created?
2	ExchangeItem	Unusual email reading/deletion activities?
2	SharePointFileOperation	Unusual file (SharePoint, OneDrive) reading/deletion activities?

- ✓ Interview the user and delete suspicious activity.

- ✓ Expand the investigation scope based on “SessionId”

SessionId is useful for investigation

Filtered to “New-InboxRule”



	A	B	C	D	E	F	G	H	I	J	K
1	Record	CreationDate	RecordTy	Operation	UserId	AuditData	AssociatedAdminUnits	AssociatedAdminUnitsName			
1909	b59ee18c	2024-01-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
2218	69cc3699	2024-02-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
13469	70ab9ebe	2024-02-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
14079	cf7f7dfc-l	2024-02-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
15427	13ee5b72	2024-02-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
17155	8d6e7ff3-	2024-02-	1	New-InboxRule		{"AppAccessContext":{"IssuedAtTime":"2024-01-					
18934	e6de1090	2024-02-	1	New-InboxRule							
20674											
20675											
20676											
20677											
20678											
20679											
20680											
20681											
20682											
20683						me":"MarkAsRead","Value":"True"},{"Name":"StopProcessingRules","Value":"True"}],"RequestId":"34f0293					
20684						5-849c-ad27-5007-caa801a2ec3b","SessionId":"e55a5c8e-aefe-4369-bd4a-c2eaad764e9b"}					

All entries have the SAME SessionId
e55a5c8e-aefe-4369-bd4a-c2eaad764e9b

SessionId is useful for investigation

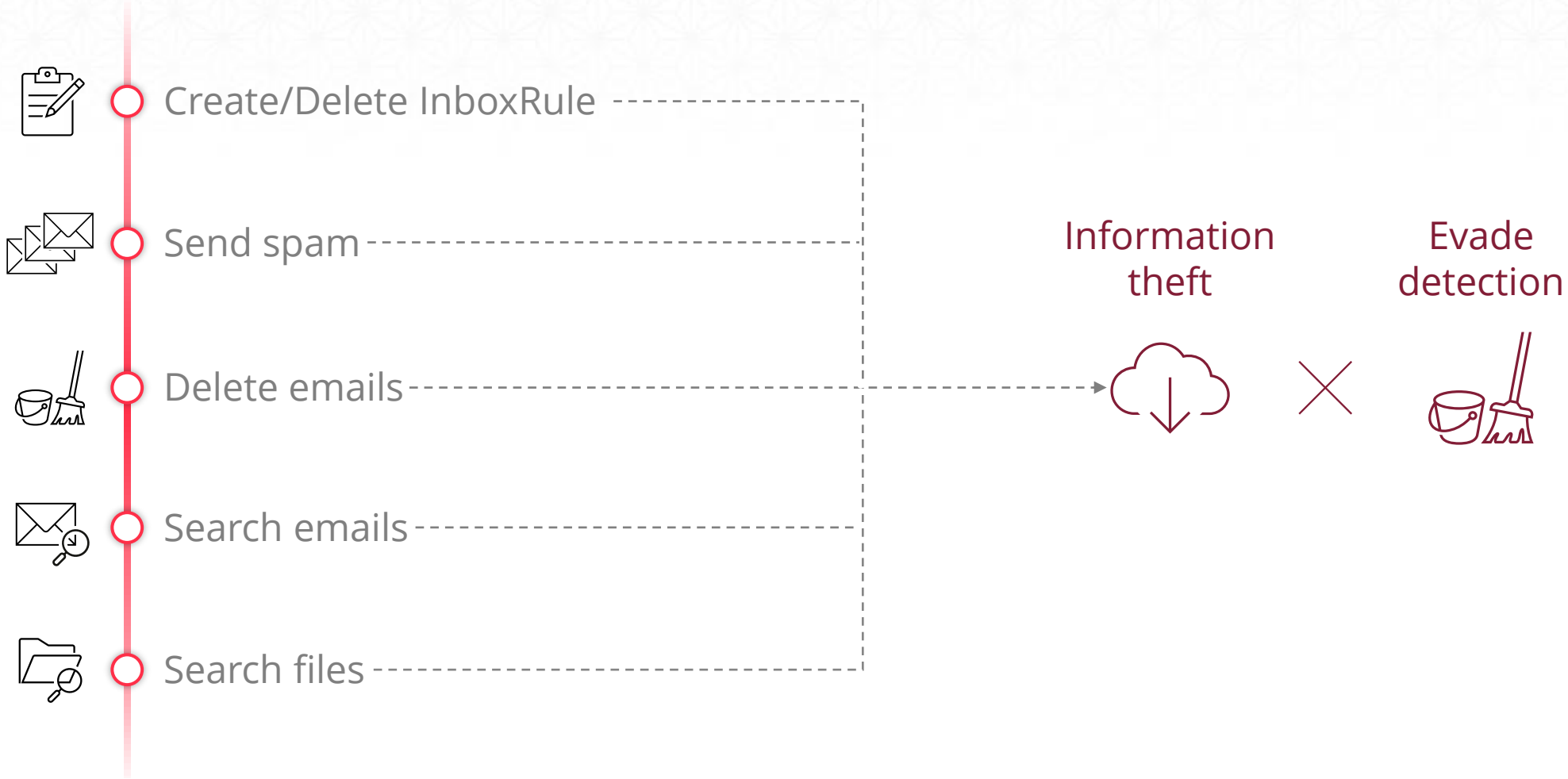
	A	B	C	D	E	F	G	H
1	Record	CreationDate	RecordTy	Operation	UserId	AuditData	AssociatedAdminUnits	AssociatedAdminUnitsName
495	a45f64ba	2024-02-	15	UserLoginFailed		{"CreationTime":"2024-02-1		
625	1b677d34	2024-02-	3	SoftDelete		{"CreationTime":"2024-02-0		
1048	bb87ecf4	2024-02-	3	SoftDelete		{"CreationTime":"2024-02-0		
1130	971dc01b	2024-02-	3	SoftDelete		{"CreationTime":"2024-02-0		
1214	f78e3a01	2024-02-	3	SoftDelete		{"C		
1268	f1ca58e9	2024-02-	3	SoftDelete		{"C		
1909	45c6faf9-	2024-02-	3	MoveToDeletedItems		{"C		
2218	ec6f0fc3-	2024-02-	3	MoveToDeletedItems		{"C		
2321	e2dfd23c	2024-02-	3	MoveToDeletedItems		{"C		
2870	780667b4	2024-02-	3	MoveToDeletedItems		{"CreationTime":"2024-02-0		
2928	70ab9eb6	2024-02-	1	New-InboxRule		{"AppAccessContext":{"Issue		
3025	a07b15a1	2024-02-	2	Create		tionTime":"2024-02-0		
3726	4ec14f41	2024-02-	3	MoveToDeletedItems		tionTime":"2024-02-0		
3868	812585b9	2024-02-	2	Create		tionTime":"2024-02-0		
3998	e6de109(	2024-02-	1	New-InboxRule		AccessContext":{"Issue		
4015	6ccbf74a	2024-02-	2	Create		tionTime":"2024-02-0		
4156	b09bcea1	2024-02-	3	SoftDelete		{"CreationTime":"2024-02-0		
4157	af31f814-	2024-02-	3	SoftDelete		{"CreationTime":"2024-02-0		
4514	f3cf7014-	2024-02-	3	MoveToDeletedItems		{"CreationTime":"2024-02-0		
4579	4860215b	2024-02-	2	Create		{"CreationTime":"2024-02-0		
5549	cdf4ac4f-	2024-02-	2	Create		{"CreationTime":"2024-02-0		
5703	69cc3699	2024-02-	1	New-InboxRule		{"AppAccessContext":{"Issue		
5827	49ccfde6	2024-02-	3	MoveToDeletedItems		{"CreationTime":"2024-02-0		
6098	e1d1899f	2024-02-	2	Create		{"CreationTime":"2024-02-0		
6176	228d81e8	2024-02-	2	Create		{"CreationTime":"2024-02-0		
6685	cf7f7dfc-l	2024-02-	1	New-InboxRule		{"AppAccessContext":{"Issue		
6789	13ee5b72	2024-02-	1	New-InboxRule		{"AppAccessContext":{"Issue		

Filterd to SessionId:
e55a5c8e-aefe-4369-bd4a-c2eaad764e9b

The attack flow is easy to follow

Attack traces revealed in unified audit logs

By analyzing actual incidents, we found the following attack traces in the unified audit log:



Attack traces revealed in unified audit logs

- Create/Delete Inbox-Rule
- Send spam
- Delete email
- Search emails
- Search files

	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 revealed in unified audit logs

- Create/Delete Inbox-Rule
- Send spam
- Del
- Search emails
- Search files

	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	MailboxLo					
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-In					
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-In					
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					

Automatically forward replies to spam emails sent by attackers to the deleted folder

```
"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 revealed in unified audit logs

- Create/Delete Inbox-Rule
- Send spam
- Delete email
- Search emails
- Search files

	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 revealed in unified audit logs

Create/Delete Inbox-Rule

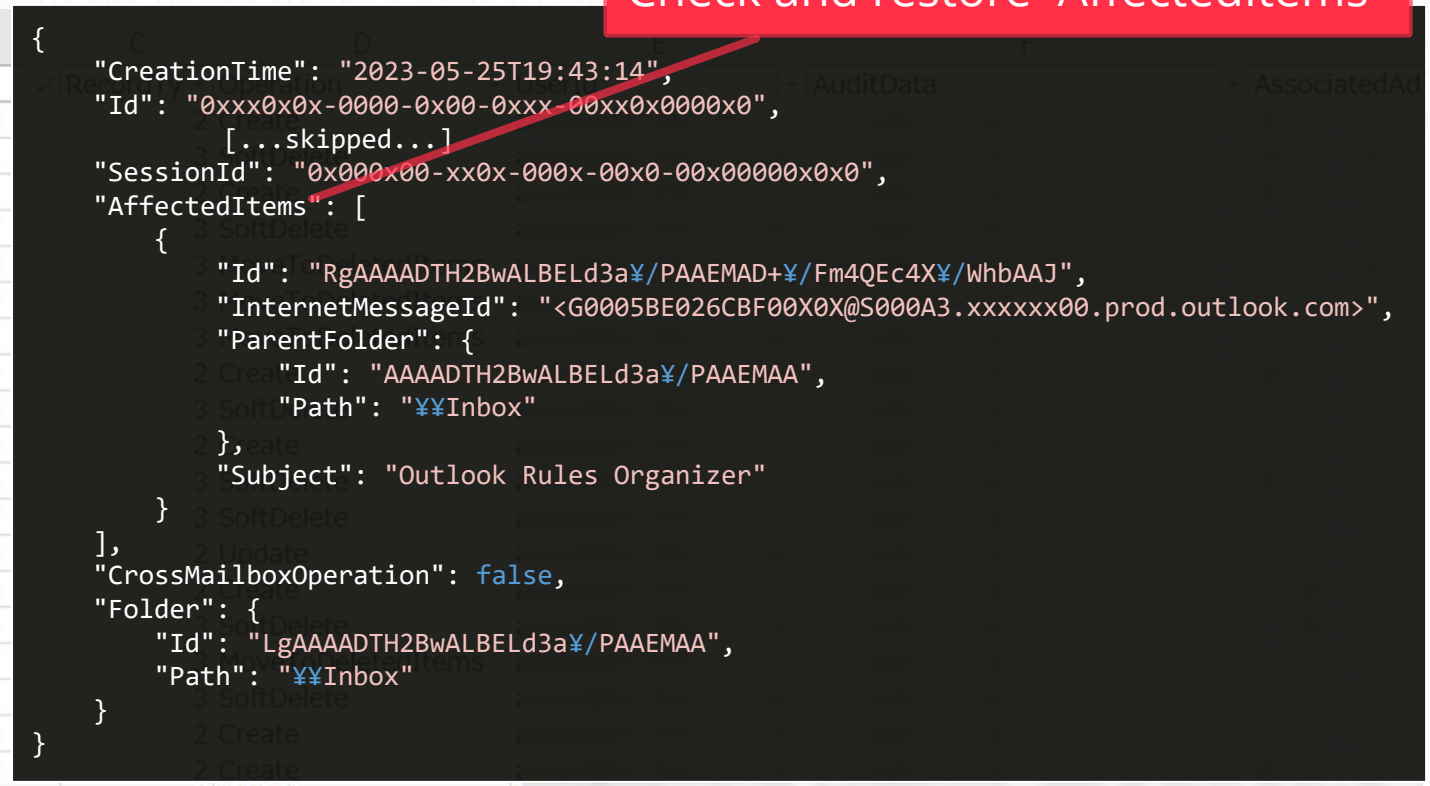
Send spam

Delete email

Search emails

Search files

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			
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

Attack traces revealed in unified audit logs

- Create/Delete Inbox-Rule
- Send spam
- Delete email
- Search emails
- Search files

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

Attack traces revealed in unified audit logs

- Create/Delete Inbox-Rule
- Send spam
- Delete email
- Search emails
- Search files

	A	B	C	D	E	F	G	H	I
1	CreationDate	RecordTyp	Operation	UserId	AuditD	Associa	Associa	dAdminUnitsNames	
9	6/16/2023 7:51:04 PM	2	MailboxLogin	[redacted]					
10	6/16/2023 7:54:02 PM	1	New-InboxRule	[redacted]					
11	6/17/2023 6:05:22 PM	2	MailboxLogin	[redacted]					
12	6/17/2023 6:05:22 PM	2	MailboxLogin	[redacted]					
13	6/19/2023 11:15:08 A	2	MailboxLogin	[redacted]					
14	6/19/2023 2:19:52 PM	2	Create	[redacted]					
15	6/19/2023 2:29:32 PM	2	Create	[redacted]					
16	6/19/2023 2:32:22 PM	1	New-InboxRule	[redacted]					
17	6/19/2023 2:34:28 PM	2	Update	[redacted]					
18	6/19/2023 2:43:59 PM	2	Update	[redacted]					

Log Excerpt


```
    "Item": {
        "Attachments": "PO-11103.pdf (103475b); image001.png (2843b); image002.png (1111b); image003.png
(3964b); image004.png (4144b)",
        "Id": "XXXX¥/xxxx",
        "InternetMessageId": "<XXXXXXX.namprd11.prod.outlook.com>",
        "IsRecord": false,
        "ParentFolder": {
            "Id": "XXXX¥/xxxx",
            "Path": "¥¥Sent Items"
        },
        "SizeInBytes": 152295,
        "Subject": "RE: APPS - need new section created - Urgent"
    },
    "ModifiedProperties": [
        "AttachmentCollection"
    ]
```

Reporting

Report writing

We have detected the following suspicious activity in your logs.

Please confirm whether these were expected and review the following action items.

■ Summary

- Between 09:25:56 and 10:55:45 UTC on May 10, 2024, we observed suspicious sign-ins and activities to Alice's account.
- Phishing email was sent to Alice's colleague but they did not click on the phishing link.
- The mail InboxRule was created for evading spam email from the user.
- The application ".." was added to tenant with several permission limited to the user scope.

We recommend taking the following actions to prevent further compromise.

■ Response Actions

- Revoke Alice's account session
- Reset Alice's account password.
- Disable or remove the application.
- Remove the InboxRule.

1. Summary of the intrusion

2. Recommended response actions

Report writing

Here are the detailed information of compromise.

■ Suspicious IP Addresses

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0

152.42.161.220

240b:10:32c1:ab00:857:889:3734:e93

■ The added Application

Application.DisplayName: ..

AppId:3f691a1c-cb53-41e5-a56e-acfb23ae6ca5

DelegatedPermissionGrant

Scope:

email

Mail.ReadWrite.Shared

Mail.Send.Shared

openid

TeamsActivity.Read

TeamsActivity.Send

User.Read

ConsentType:Principal

3. Detailed information of compromise (optional)

■ Mail forwarding rules

Name: .

Action: Move to deleted forder

Rule:"SubjectContainsWords","Value":"Activate Your New Business Card System"

If you have any questions, feel freely ask us.

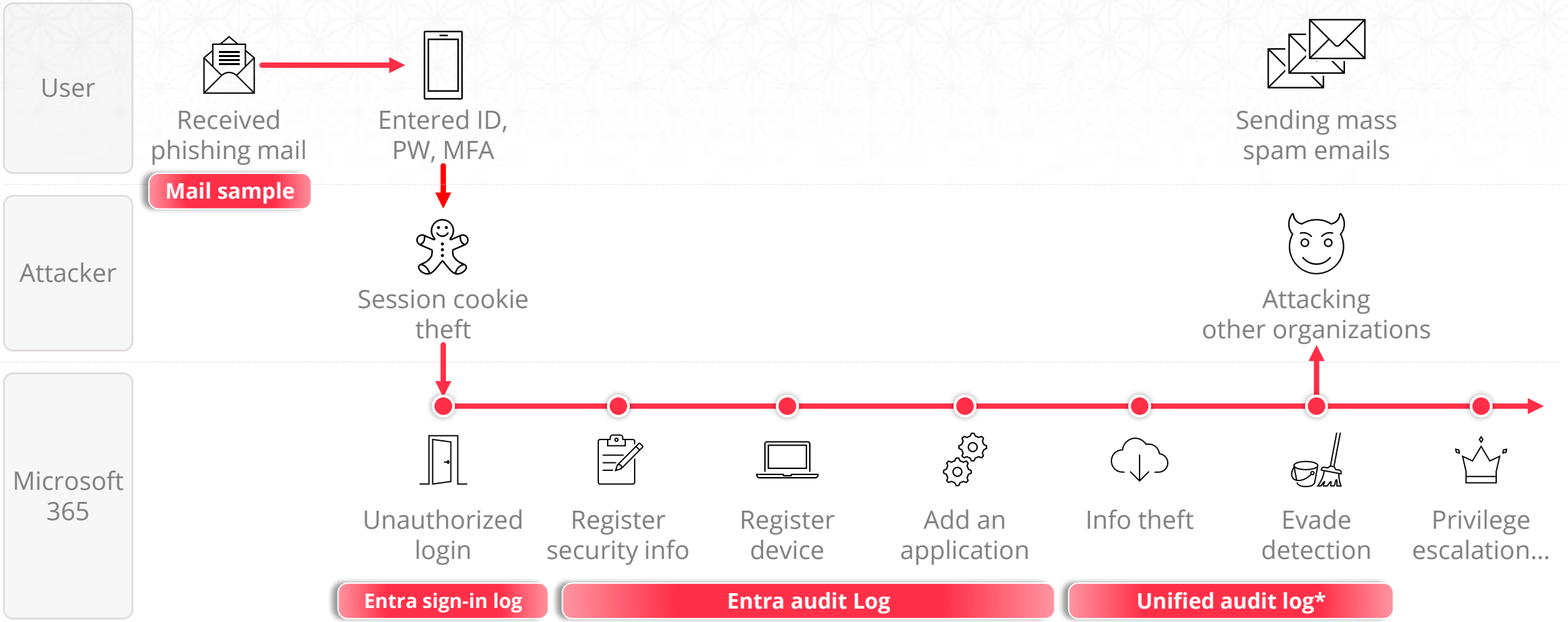
Thank you for your time and attention.

Incident timeline

	A	C	D	E	F	G	H	I	J
1	Time(UTC)	Action	Details	UPN	IP Address	UA	App	Artifact	Note
2	2024-05-10T10:55:45.02	Consent to applicatior	ConsentContext	AliceA@sunnyside08.or	20.39.192.224	EvoSTS	..	AuditLogs_2024-05-13	ConsentContext.IsAdminConsent "False" ConsentContext.IsAppOnly "False"
3	2024-05-10T10:55:45.02	Add app role assignm	AppRole.Id	AliceA@sunnyside08.or	20.39.192.224	EvoSTS	..	AuditLogs_2024-05-13	AppRole.Id "00000000-0000-0000-0000-000000000000"
4	2024-05-10T10:55:45Z	Success		alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	InteractiveSignIns_202	same Application Id
5	2024-05-10T10:55:44.98	Add delegated permis	DelegatedPermissionGrant.Scc	AliceA@sunnyside08.or	20.39.192.224	EvoSTS	..	AuditLogs_2024-05-13	DelegatedPermissionGrant.Scope "email Mail.ReadWrite.Shared Mail.Send.Shared openid TeamsActivity.Read TeamsActivity.Send User.Read" DelegatedPermissionGrant.ConsentType "Principal"
6	2024-05-10T10:55:41Z	Interrupted	The user or administrator has r	alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	InteractiveSignIns_202	same Application Id
7	2024-05-10T10:55:06.47	Update application	RequiredResourceAccess	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"ResourceAppId":"00000003-0000-0000-c
8	2024-05-10T10:55:06.33	Update service princip	Included Updated Properties	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
9	2024-05-10T10:55:02.89	Update application	RequiredResourceAccess	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"ResourceAppId":"00000003-0000-0000-c
10	2024-05-10T10:55:02.76	Update service princip	Included Updated Properties	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
11	2024-05-10T10:54:59.19	Update application	RequiredResourceAccess	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"ResourceAppId":"00000003-0000-0000-c
12	2024-05-10T10:54:59.05	Update service princip	Included Updated Properties	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
13	2024-05-10T10:54:54.86	Update application	RequiredResourceAccess	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"ResourceAppId":"00000003-0000-0000-c
14	2024-05-10T10:54:54.72	Update service princip	Included Updated Properties	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
15	2024-05-10T10:54:34Z	Failure	Admin consent is required for t	alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	InteractiveSignIns_202	same Application Id
16	2024-05-10T10:54:19Z	Failure	Admin consent is required for t	alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	InteractiveSignIns_202	same Application Id
17	2024-05-10T10:54:07.00	UserLoginFailed		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	same sessionid
18	2024-05-10T10:54:07Z	Failure	Admin consent is required for t	alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	InteractiveSignIns_202	Application Id: 3f691a1c-cb53-41e5-a56e-ac
19	2024-05-10T10:50:00.24	Update application		AliceA@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
20	2024-05-10T10:50:00.24	Update application – (	KeyDescription	AliceA@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	["[KeyIdentifier=01a70d19-0336-45ff-8db2-e
21	2024-05-10T10:49:59.97	Update service princip	Included Updated Properties	AliceA@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
22	2024-05-10T10:49:47.06	Update application	RequiredResourceAccess	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"ResourceAppId":"00000003-0000-0000-c
23	2024-05-10T10:49:46.93	Update service princip	Included Updated Properties	AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
24	2024-05-10T10:47:56.46	Update application		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"AddressType":0,"Address":"https://oauth
25	2024-05-10T10:47:56.32	Update service principal		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	[{"AddressType":0,"Address":"https://oauth
26	2024-05-10T10:45:44.00	Send		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	same sessionid
27	2024-05-10T10:45:42.00	Create		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	same sessionid
28	2024-05-10T10:45:05.08	Add owner to service principal		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	ServicePrincipal.ObjectID "f2183b1b-a75d-45
29	2024-05-10T10:45:04.94	Add service principal		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13.xlsx	
30	2024-05-10T10:45:04.33	Add owner to application		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	Application.ObjectID "c902dbd3-8886-4314-88be-f61a8ae17b41" Application.DisplayName ".."
31	2024-05-10T10:45:04.20	Add application		AliceA@sunnyside08.onmicrosoft.com		Mozilla/5.0 (Macintosh	..	AuditLogs_2024-05-13	AppId ["3f691a1c-cb53-41e5-a56e-acfb23ae
32	2024-05-10T10:44:25.00	TeamsSessionStarted		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	300-9683-f53c931d836d.xlsx
33	2024-05-10T10:44:20.00	UserLoggedIn		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	same sessionid
34	2024-05-10T10:44:20Z	Success		alicea@sunnyside08.or	240b:10:32c1:ab00	Mozilla/5.0 (Macintosh	Azure Portal	InteractiveSignIns_2024-04-13_2024-05-13.xlsx	
35	2024-05-10T10:44:18.00	UserLoggedIn		AliceA@sunnyside08.or	240b:10:32c1:ab00:857:889:3734:e93			UAL_528c685b-9367-4	same sessionid

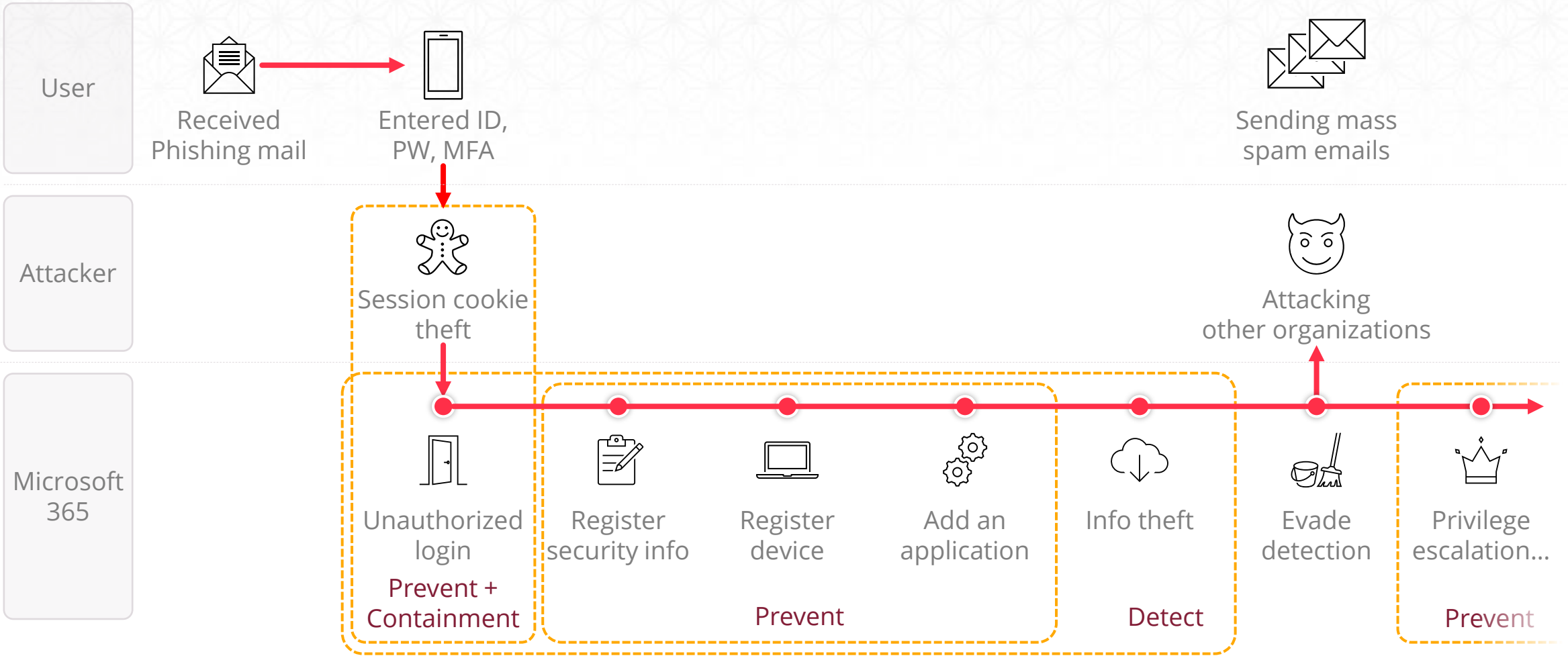
Defensive measures

Incident flow



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

Defensive measures



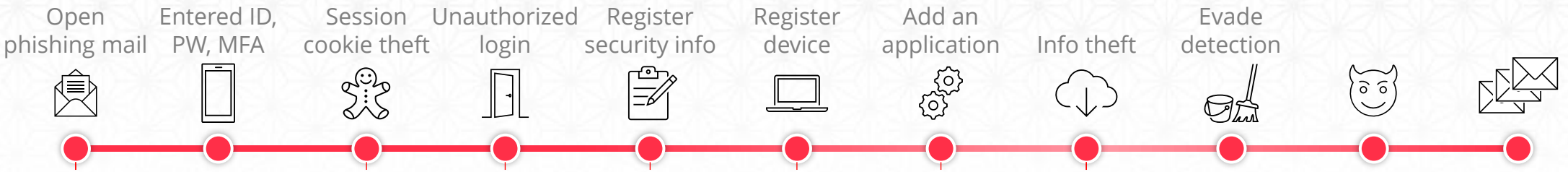
Summary

Summary

Following is this presentation covered:

- ✓ The key points of incident response for quickly and effectively
  - Initial Response
  - Log collection & investigation
  - Detailed attack traces
- ✓ Effective defense measures

Initial response is important



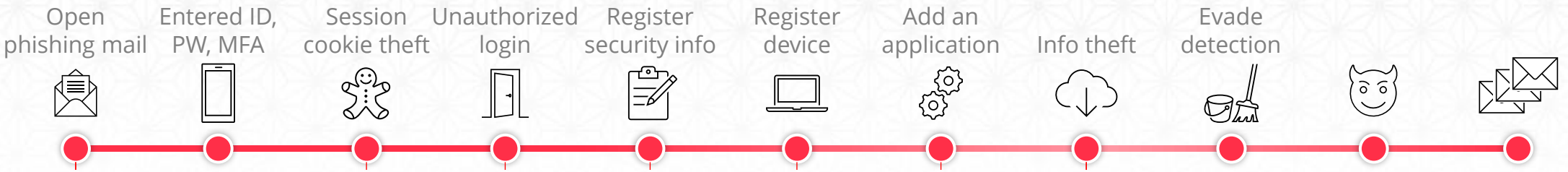
1. Disable sessions if they are still active.
2. Reset the password of the compromised user.
3. Delete suspicious security info from the compromised user.
4. Disable suspicious registered devices.
5. Delete suspicious mail forwarding rules.
6. Delete suspicious Power Automate flows
7. Disable Entra apps that were registered before or after the intrusion.
8. Request, collect, and investigate logs.
9. Investigate other recipients of the intrusion-starting email.
10. Investigate suspicious sign-ins before and after receiving the email to identify other compromised users.

Thank you!

Appendix

Reference of initial response

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.

5. Delete suspicious Power Automate flows

6. Disable Entra 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/) using an account that has user administrator or higher permissions..
   Search for the compromised user in [Microsoft Entra ID] - [Manage|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 [Manage|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 [Manage|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 user1@example.com
   ```

   Remove suspicious InboxRules about compromised user.

   ```
   Remove-InboxRule -Mailbox user1@example.com -Identity "ProjectA-MoveToFolderA"
   ```

6. Disable Entra apps that were registered before or after the intrusion.

   Access the Azure Portal (https://portal.azure.com/) using an account that has application viewer or higher permissions.

   【Enterprise applications】

   a. Navigate to [Microsoft Entra ID] - [Manage|Enterprise applications] - [Manage|All applications].
   b. 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.
   c. Switch to the [Manage|Properties] section and set “Enable for users to sign-in?" to "No".
   d. Delete apps after the incident response is complete. (Cont.)

Details of initial response

6. (Cont.) Disable Entra apps that were registered before or after the intrusion.

   Access the Azure Portal (https://portal.azure.com/) using an account that has application viewer or higher permissions.

   【App registrations】

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

7. Request, collect, and investigate logs.

   【 Entra ID logs 】

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

   【 Unified audit log - GUI】

   a. Access the Microsoft Purview (https://compliance.microsoft.com/).
   b. Navigate to [Audit]. Select time range, users, and record types that you need. Click [Search].
   c. Once the search is completed, click [Completed] and select [Export].

Details of initial response

7. (Cont.) Request, collect, and investigate logs.

   【Unified Audit Log】

   a. Connect to Exchange Online using PowerShell.

   b. Use `Search-UnifiedAuditLog` to get logs. The following is a reference.

```
Search-UnifiedAuditLog -UserIds "user1@example.com" -StartDate 4/1/2024 -EndDate 5/26/2024 |
Export-Csv -Path C:¥<Folder path>¥Auditlog.csv -NoTypeInformation
```

8. Investigate other recipients of the intrusion-starting email.

   Access Microsoft Defender (https://security.microsoft.com/).

   Navigate to [Email & collaboration] - [Explorer].

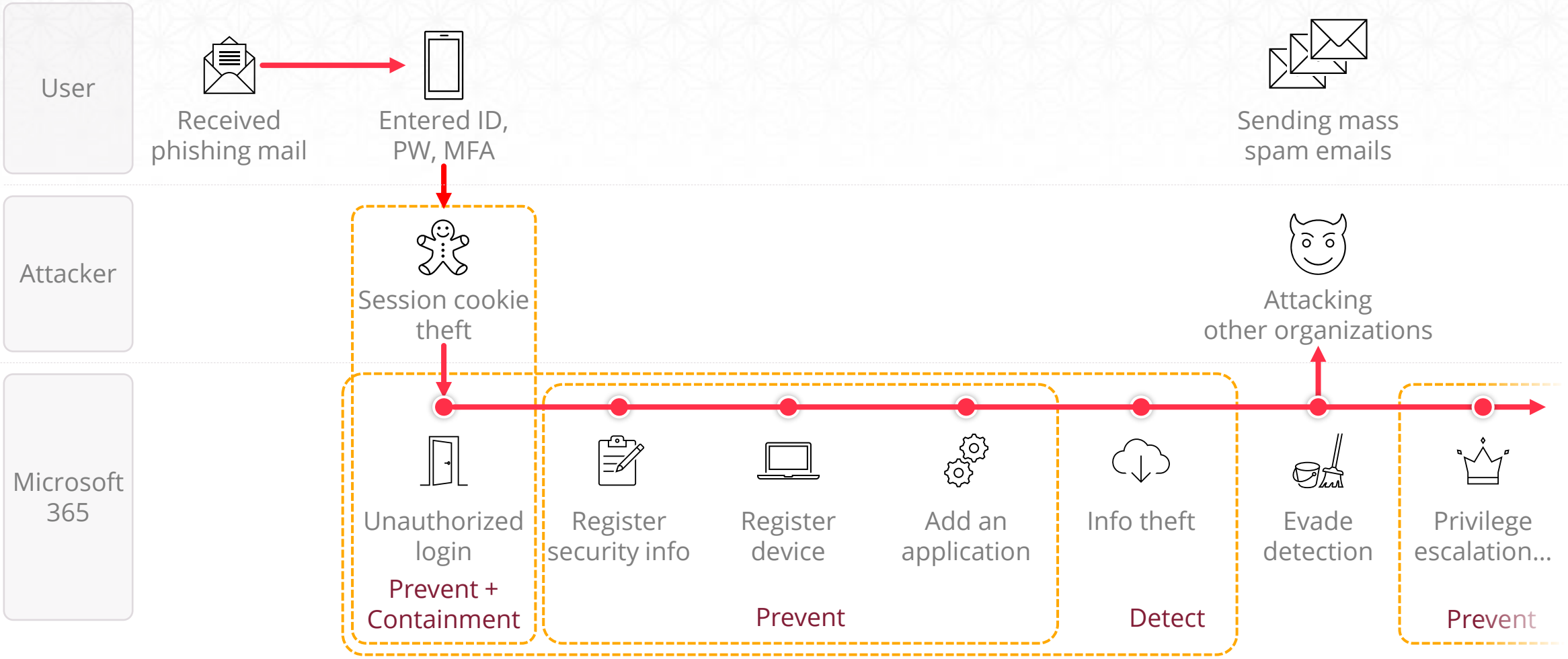
   Investigate whether there are any users who have received similar emails to the compromised user.

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

List of defensive measures

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

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 P2

  Policy settings:

  - [Assignments]
    - [Users]: [Include] “All users” or “Select users and groups” *Exclude break glass accounts.
    - [Target resources] - [Cloud apps]: Select any Office 365 application
  - [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 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 or managed by Intune and have passed compliance checks.

License: Entra ID 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 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 (Phishing-resistant MFA)”

References: 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 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 Protection.

  License: Entra ID P2

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

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 P1

Policy settings:

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

Microsoft Entra Internet Access is also good for this defender measure.

References: 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

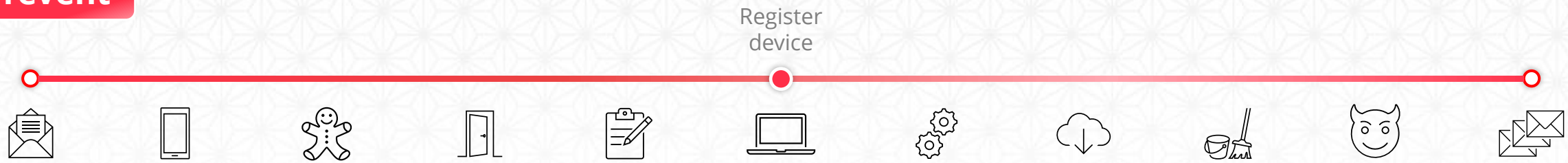
✓ Export Entra audit logs to SIEM and monitor the following attributes.

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 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 P1

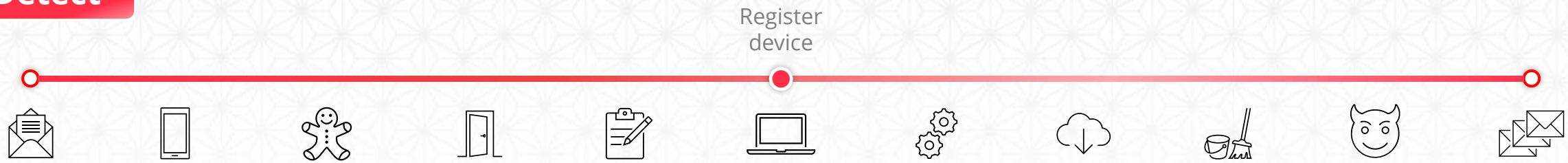
Policy settings:

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

Microsoft Entra Internet Access is also good for this defender measure.

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

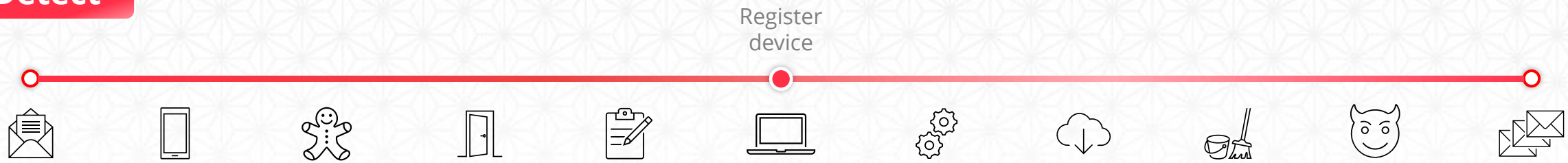
Detect



- ✓ 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 P1 + Intune

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

Detect



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

License: Entra ID P1+ SIEM

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

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

References:
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/

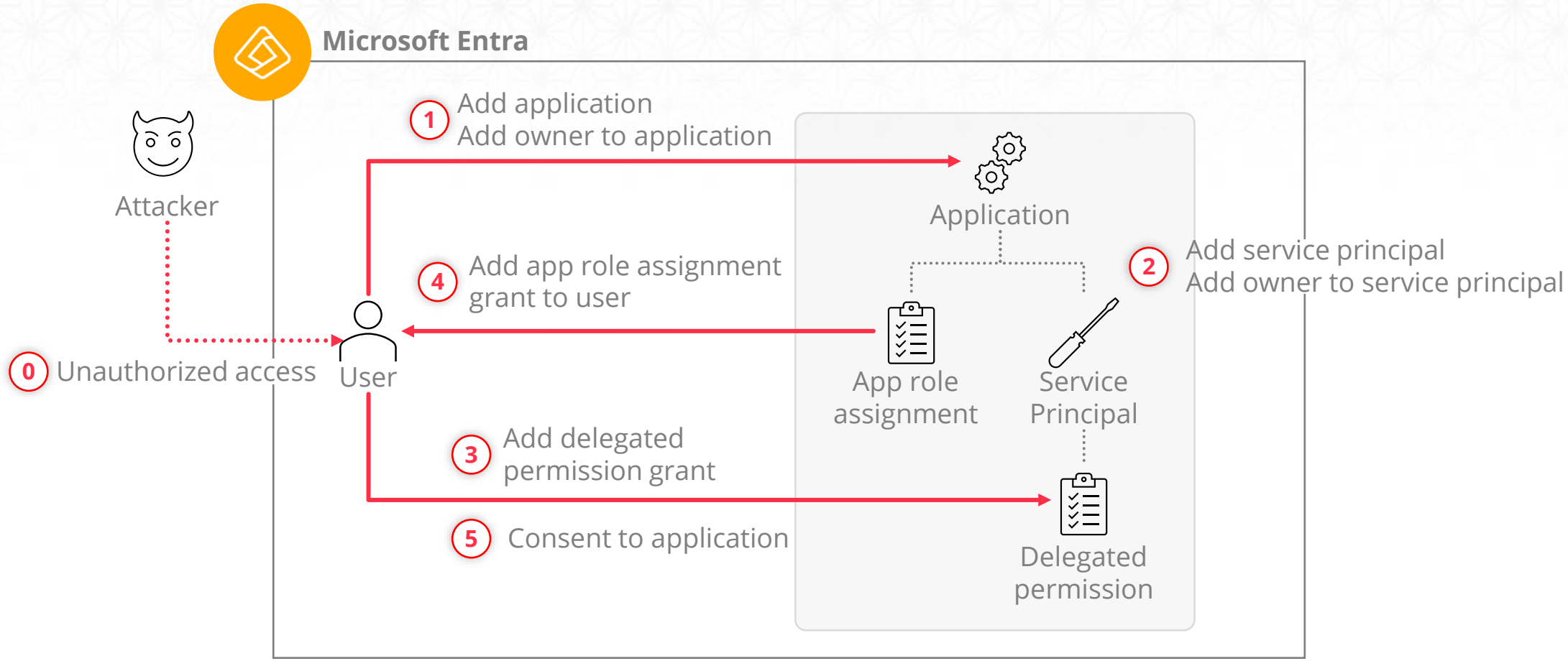
Detect

✓ Export Entra 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

The flow of adding an application



*This process is based on logs from May 10, 2024, and is subject to future changes.

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)