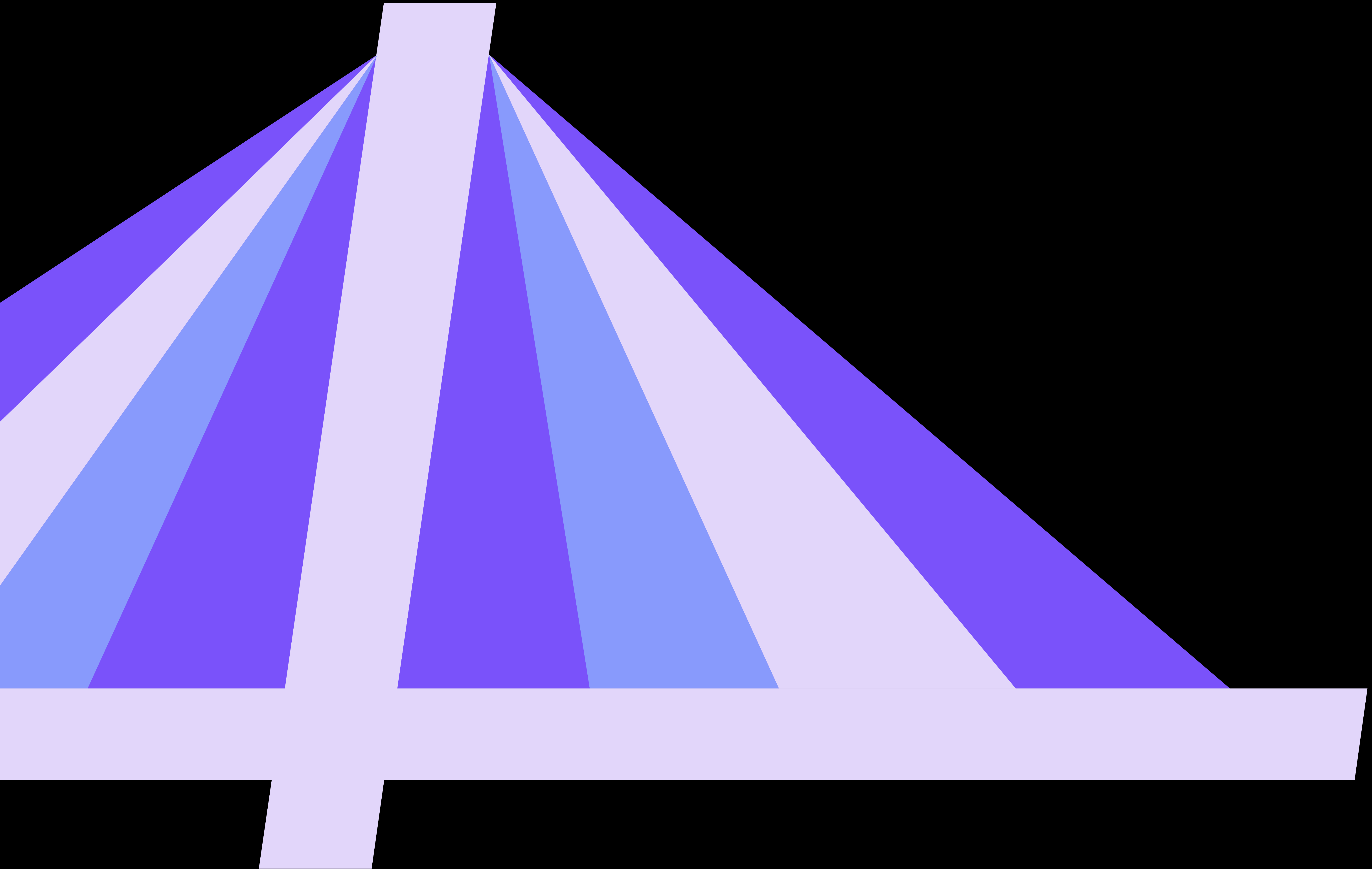
HYBRID
IDENTITY
PROTECTION
conf25
CHARLESTON



Token Hunt: Uncovering Post-Authentication Attacks in the Microsoft Cloud

Thomas Naunheim

Cyber Security Architect
@glueckkanja AG

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Thomas Naunheim

Cyber Security Architect @glueckkanja AG

- From Koblenz/Lahnstein, Germany
- Microsoft MVP (Identity & Access, Cloud Security

🦋 @naunheim.cloud

𝕏 @Thomas_Live

in /in/ThomasNaunheim

🌐 cloud-architekt.net

Token Hunt | Agenda

1. Introduction to token theft and post-authentication attacks
2. Advanced insights of Microsoft Entra ID sign-in logs
3. Correlation of sign-in events to XDR alert or anomalies
4. Correlation of user sign-in, alert, and cloud app activity logs
5. Discover exposed token artifacts with exposure management

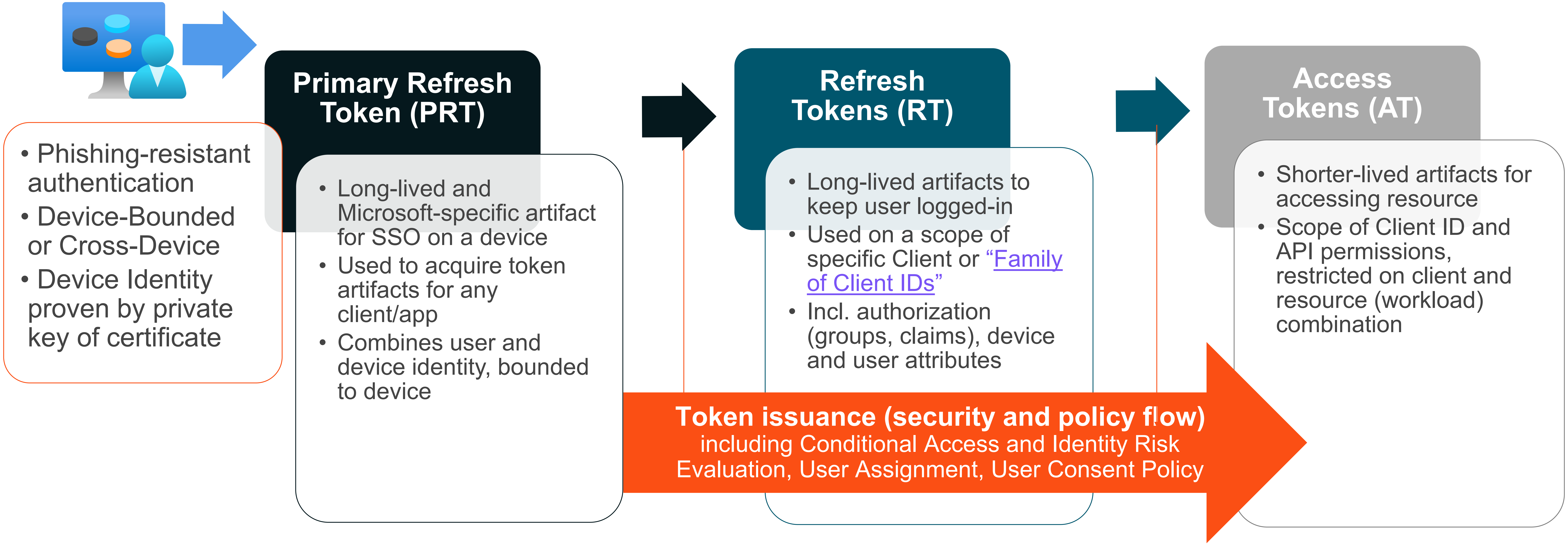
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Introduction to Token Theft and Post-Authentication Attacks

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Overview of Token Artifacts



- Phishing-resistant authentication
- Device-Bounded or Cross-Device
- Device Identity proven by private key of certificate

Primary Refresh Token (PRT)

- Long-lived and Microsoft-specific artifact for SSO on a device
- Used to acquire token artifacts for any client/app
- Combines user and device identity, bounded to device

Refresh Tokens (RT)

- Long-lived artifacts to keep user logged-in
- Used on a scope of specific Client or “Family of Client IDs”
- Incl. authorization (groups, claims), device and user attributes

Access Tokens (AT)

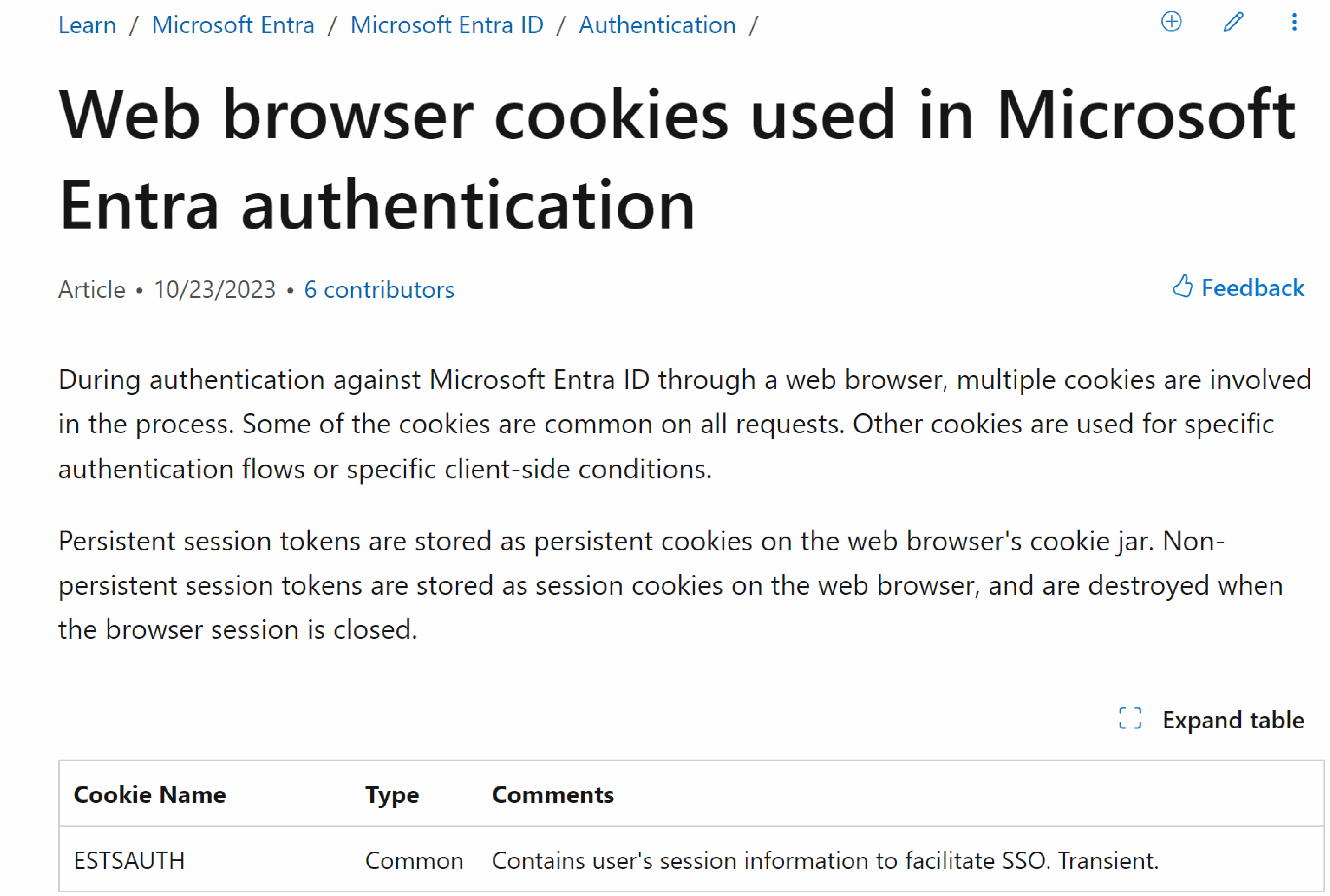
- Shorter-lived artifacts for accessing resource
- Scope of Client ID and API permissions, restricted on client and resource (workload) combination

Token issuance (security and policy flow)
including Conditional Access and Identity Risk Evaluation, User Assignment, User Consent Policy

Session Cookies

Session cookies

- Long-lived artifacts used for browser-based SSO after authentication
- Issued by IdP and service (resource owner)



Learn / Microsoft Entra / Microsoft Entra ID / Authentication /

Web browser cookies used in Microsoft Entra authentication

Article • 10/23/2023 • 6 contributors

Feedback

During authentication against Microsoft Entra ID through a web browser, multiple cookies are involved in the process. Some of the cookies are common on all requests. Other cookies are used for specific authentication flows or specific client-side conditions.

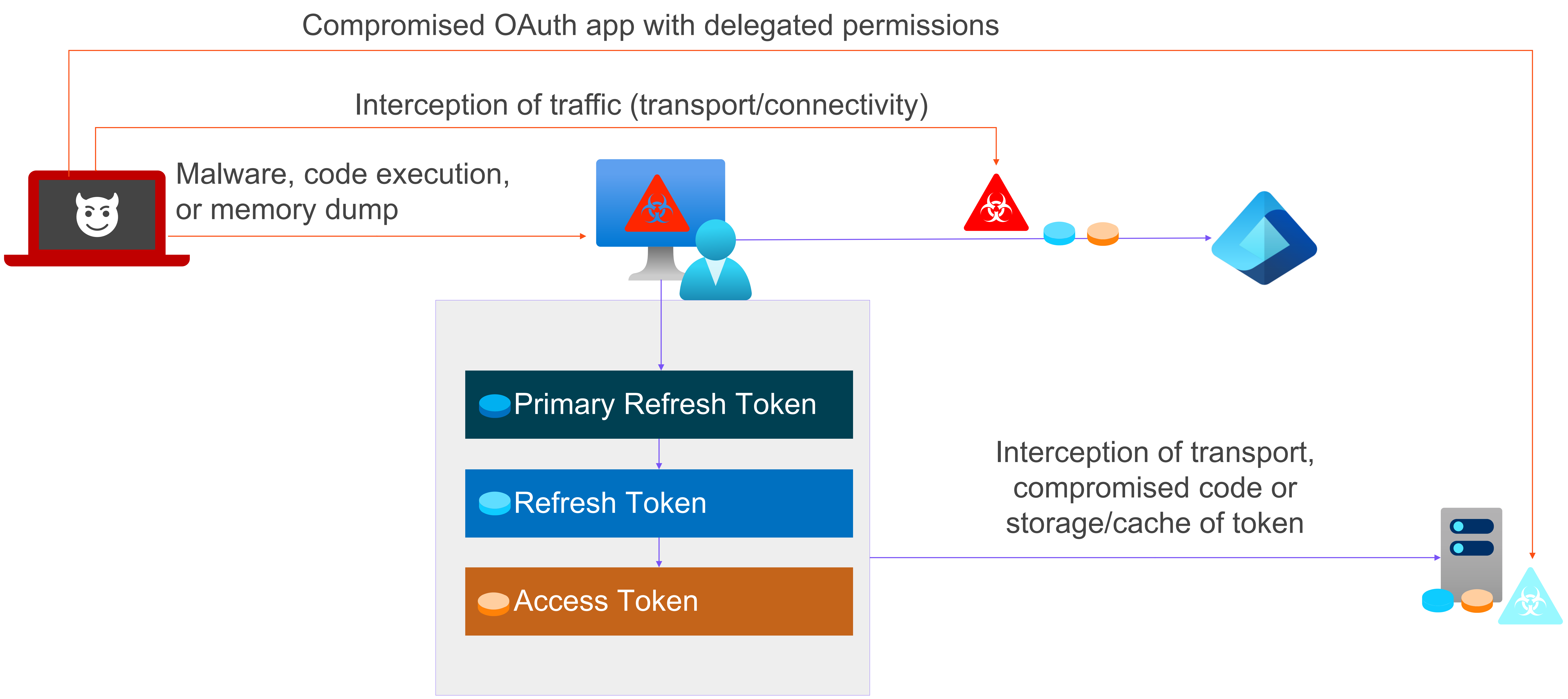
Persistent session tokens are stored as persistent cookies on the web browser's cookie jar. Non-persistent session tokens are stored as session cookies on the web browser, and are destroyed when the browser session is closed.

Expand table

Cookie Name	Type	Comments
ESTSAUTH	Common	Contains user's session information to facilitate SSO. Transient.

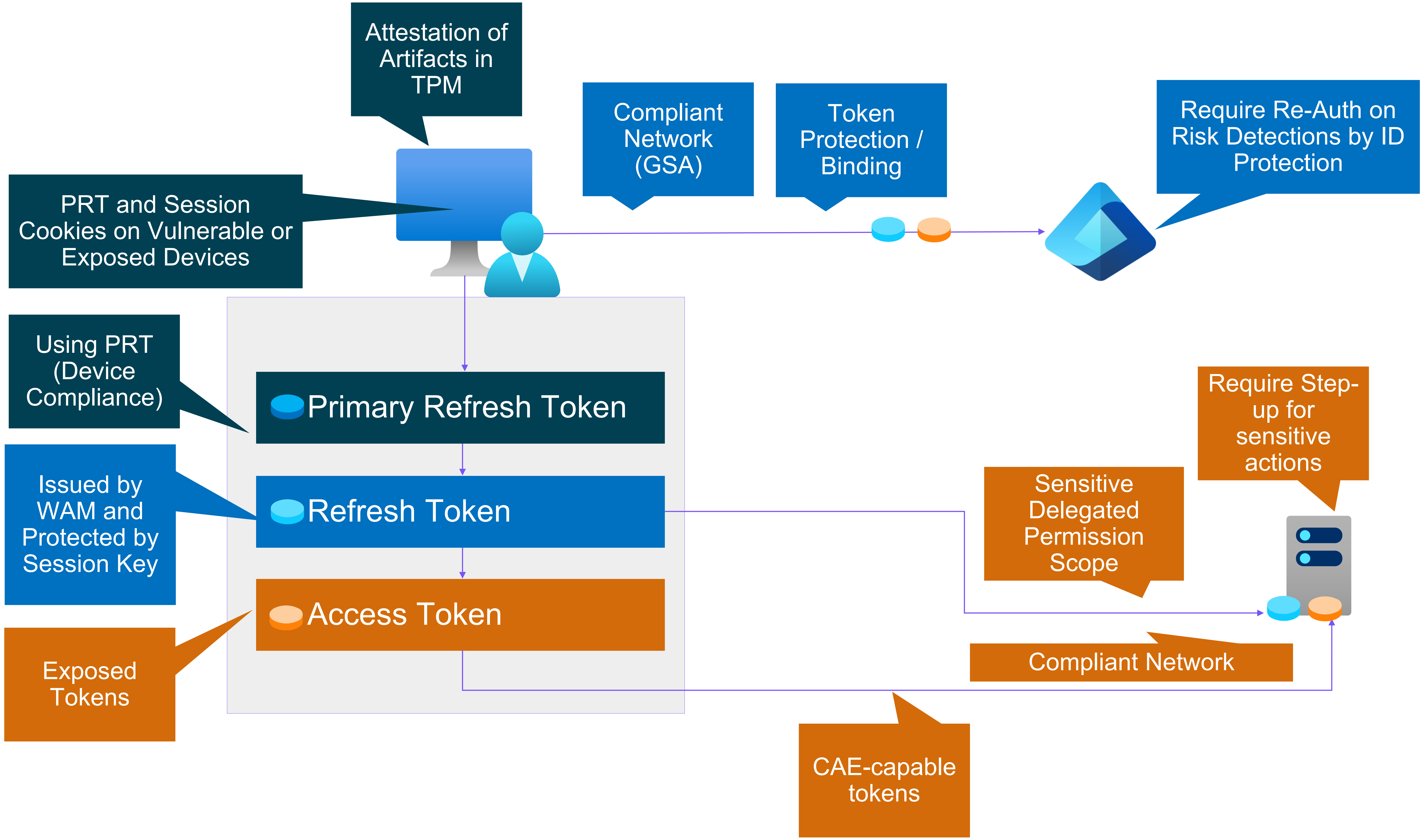
Source: Microsoft Learn | Web browser cookies used in Microsoft Entra authentication, Details about “Pass-the-cookie” attacks

Token-Related Attack Techniques


Compromised OAuth app with delegated permissions
Interception of traffic (transport/connectivity)
Malware, code execution, or memory dump
Primary Refresh Token
Refresh Token
Access Token
Interception of transport, compromised code or storage/cache of token

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Token-Related Attack Techniques



Attestation of Artifacts in TPM

PRT and Session Cookies on Vulnerable or Exposed Devices

Compliant Network (GSA)

Token Protection / Binding

Require Re-Auth on Risk Detections by ID Protection

Using PRT (Device Compliance)

Primary Refresh Token

Issued by WAM and Protected by Session Key

Refresh Token

Access Token

Exposed Tokens

Require Step-up for sensitive actions

Sensitive Delegated Permission Scope

Compliant Network

CAE-capable tokens

HIP HYBRID IDENTITY PROTECTION conf25

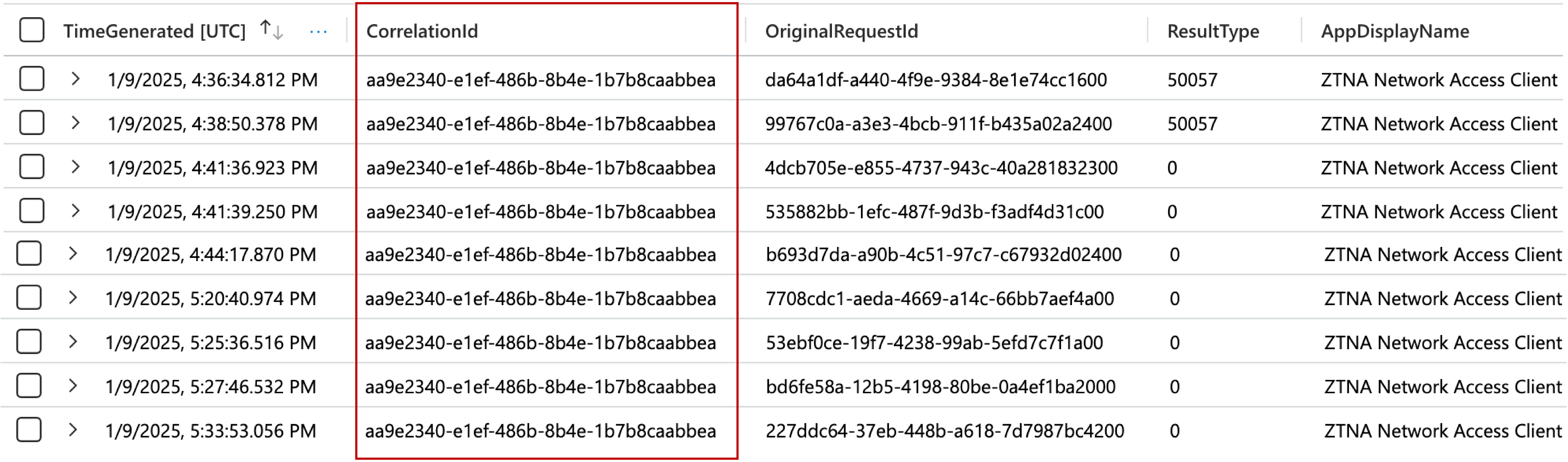
CHARLESTON

Advanced Insights of Microsoft Entra ID Sign-in Logs

Types of Sign-in Identifiers

- **Correlation ID**
  Groups sign-ins from the same sign-in session, generated by client (not IdP)

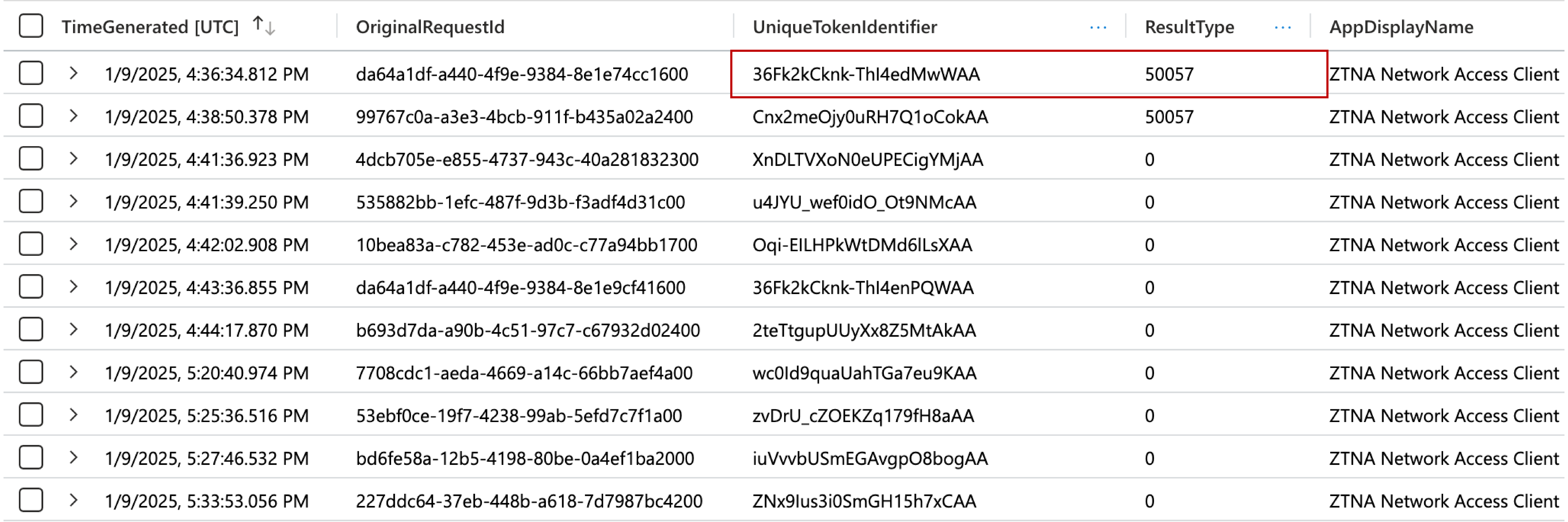
- **(Original) Request ID**
  An identifier that corresponds to an issued token
  The request identifier of the first request in the authentication sequence



□		TimeGenerated [UTC] ↑↓ ···	CorrelationId	OriginalRequestId	ResultType	AppDisplayName
□	›	1/9/2025, 4:36:34.812 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	da64a1df-a440-4f9e-9384-8e1e74cc1600	50057	ZTNA Network Access Client
□	›	1/9/2025, 4:38:50.378 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	99767c0a-a3e3-4bcb-911f-b435a02a2400	50057	ZTNA Network Access Client
□	›	1/9/2025, 4:41:36.923 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	4dcb705e-e855-4737-943c-40a281832300	0	ZTNA Network Access Client
□	›	1/9/2025, 4:41:39.250 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	535882bb-1efc-487f-9d3b-f3adf4d31c00	0	ZTNA Network Access Client
□	›	1/9/2025, 4:44:17.870 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	b693d7da-a90b-4c51-97c7-c67932d02400	0	ZTNA Network Access Client
□	›	1/9/2025, 5:20:40.974 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	7708cdc1-aeda-4669-a14c-66bb7aef4a00	0	ZTNA Network Access Client
□	›	1/9/2025, 5:25:36.516 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	53ebf0ce-19f7-4238-99ab-5efd7c7f1a00	0	ZTNA Network Access Client
□	›	1/9/2025, 5:27:46.532 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	bd6fe58a-12b5-4198-80be-0a4ef1ba2000	0	ZTNA Network Access Client
□	›	1/9/2025, 5:33:53.056 PM	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	227ddc64-37eb-448b-a618-7d7987bc4200	0	ZTNA Network Access Client

Types of Sign-in Identifiers

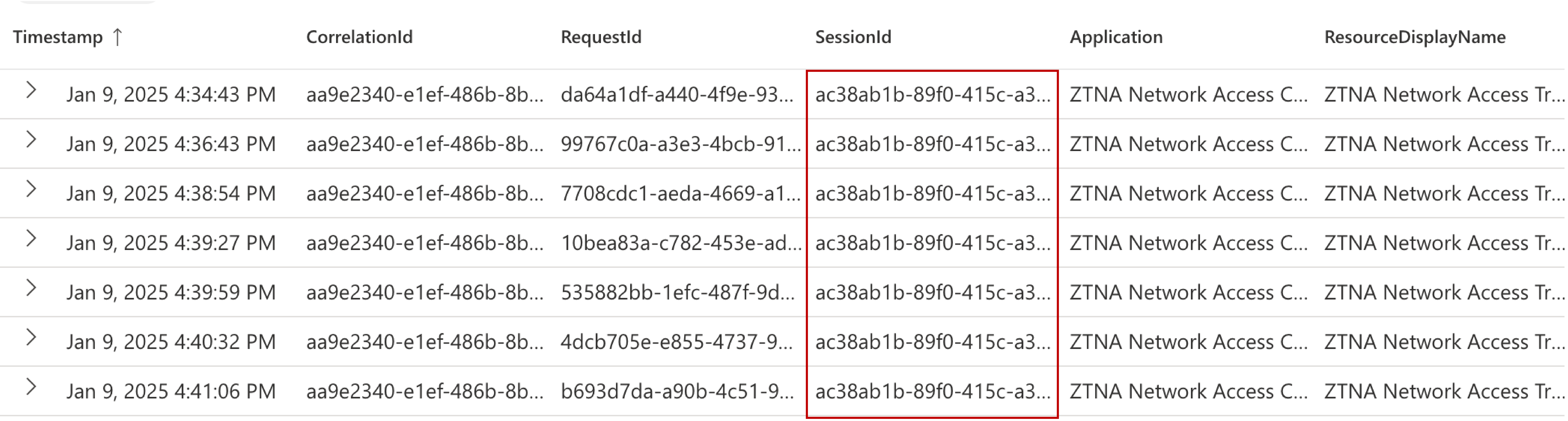
- **Unique token identifier**
  Used to correlate the sign-in with the token request (passed during the sign-in)
  Tracks tokens issued by Microsoft Entra ID as they're redeemed at resource providers



□		TimeGenerated [UTC] ↑↓	OriginalRequestId	UniqueTokenIdentifier ···	ResultType ···	AppDisplayName
□	›	1/9/2025, 4:36:34.812 PM	da64a1df-a440-4f9e-9384-8e1e74cc1600	36Fk2kCknk-Thl4edMwWAA	50057	ZTNA Network Access Client
□	›	1/9/2025, 4:38:50.378 PM	99767c0a-a3e3-4bcb-911f-b435a02a2400	Cnx2meOjy0uRH7Q1oCokAA	50057	ZTNA Network Access Client
□	›	1/9/2025, 4:41:36.923 PM	4dcb705e-e855-4737-943c-40a281832300	XnDLTVXoN0eUPECigYMjAA	0	ZTNA Network Access Client
□	›	1/9/2025, 4:41:39.250 PM	535882bb-1efc-487f-9d3b-f3adf4d31c00	u4JYU_wef0idO_Ot9NMcAA	0	ZTNA Network Access Client
□	›	1/9/2025, 4:42:02.908 PM	10bea83a-c782-453e-ad0c-c77a94bb1700	Oqi-EILHPkWtDMd6lLsXAA	0	ZTNA Network Access Client
□	›	1/9/2025, 4:43:36.855 PM	da64a1df-a440-4f9e-9384-8e1e9cf41600	36Fk2kCknk-Thl4enPQWAA	0	ZTNA Network Access Client
□	›	1/9/2025, 4:44:17.870 PM	b693d7da-a90b-4c51-97c7-c67932d02400	2teTtgupUUyXx8Z5MtAkAA	0	ZTNA Network Access Client
□	›	1/9/2025, 5:20:40.974 PM	7708cdc1-aeda-4669-a14c-66bb7aef4a00	wc0Id9quaUahTGa7eu9KAA	0	ZTNA Network Access Client
□	›	1/9/2025, 5:25:36.516 PM	53ebf0ce-19f7-4238-99ab-5efd7c7f1a00	zvDrU_cZOEKZq179fH8aAA	0	ZTNA Network Access Client
□	›	1/9/2025, 5:27:46.532 PM	bd6fe58a-12b5-4198-80be-0a4ef1ba2000	iuVvvbUSmEGAvgpO8bogAA	0	ZTNA Network Access Client
□	›	1/9/2025, 5:33:53.056 PM	227ddc64-37eb-448b-a618-7d7987bc4200	ZNx9Ius3i0SmGH15h7xCAA	0	ZTNA Network Access Client

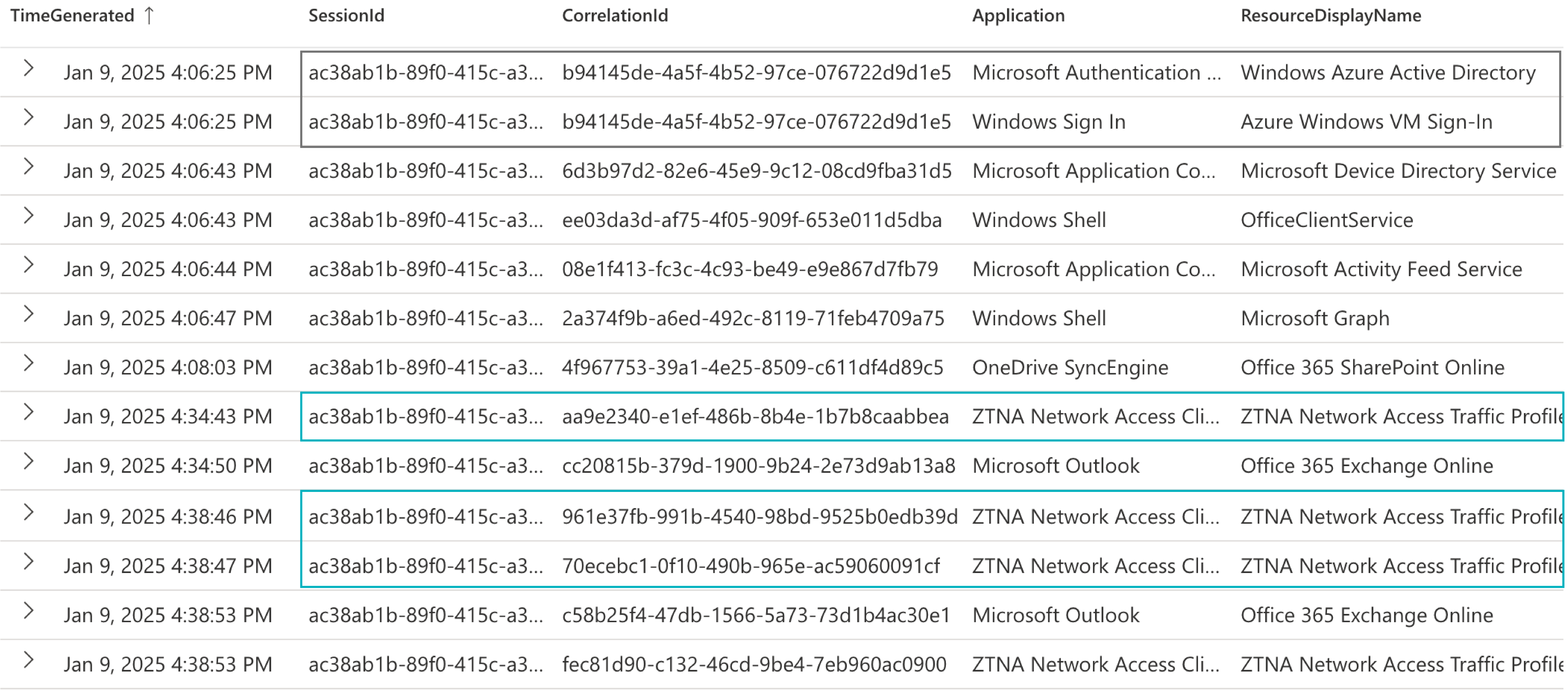
Types of Sign-in Identifiers

- **SessionId**
  Identifies and matches the session (cookie) that was generated during the sign-in between the client and the IdP



Timestamp ↑	CorrelationId	RequestId	SessionId	Application	ResourceDisplayName
Jan 9, 2025 4:34:43 PM	aa9e2340-e1ef-486b-8b...	da64a1df-a440-4f9e-93...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:36:43 PM	aa9e2340-e1ef-486b-8b...	99767c0a-a3e3-4bcb-91...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:38:54 PM	aa9e2340-e1ef-486b-8b...	7708cdc1-aeda-4669-a1...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:39:27 PM	aa9e2340-e1ef-486b-8b...	10bea83a-c782-453e-ad...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:39:59 PM	aa9e2340-e1ef-486b-8b...	535882bb-1efc-487f-9d...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:40:32 PM	aa9e2340-e1ef-486b-8b...	4dcb705e-e855-4737-9...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...
Jan 9, 2025 4:41:06 PM	aa9e2340-e1ef-486b-8b...	b693d7da-a90b-4c51-9...	ac38ab1b-89f0-415c-a3...	ZTNA Network Access C...	ZTNA Network Access Tr...

SessionId vs CorrelationId



TimeGenerated ↑	SessionId	CorrelationId	Application	ResourceDisplayName
Jan 9, 2025 4:06:25 PM	ac38ab1b-89f0-415c-a3...	b94145de-4a5f-4b52-97ce-076722d9d1e5	Microsoft Authentication ...	Windows Azure Active Directory
Jan 9, 2025 4:06:25 PM	ac38ab1b-89f0-415c-a3...	b94145de-4a5f-4b52-97ce-076722d9d1e5	Windows Sign In	Azure Windows VM Sign-In
Jan 9, 2025 4:06:43 PM	ac38ab1b-89f0-415c-a3...	6d3b97d2-82e6-45e9-9c12-08cd9fba31d5	Microsoft Application Co...	Microsoft Device Directory Service
Jan 9, 2025 4:06:43 PM	ac38ab1b-89f0-415c-a3...	ee03da3d-af75-4f05-909f-653e011d5dba	Windows Shell	OfficeClientService
Jan 9, 2025 4:06:44 PM	ac38ab1b-89f0-415c-a3...	08e1f413-fc3c-4c93-be49-e9e867d7fb79	Microsoft Application Co...	Microsoft Activity Feed Service
Jan 9, 2025 4:06:47 PM	ac38ab1b-89f0-415c-a3...	2a374f9b-a6ed-492c-8119-71feb4709a75	Windows Shell	Microsoft Graph
Jan 9, 2025 4:08:03 PM	ac38ab1b-89f0-415c-a3...	4f967753-39a1-4e25-8509-c611df4d89c5	OneDrive SyncEngine	Office 365 SharePoint Online
Jan 9, 2025 4:34:43 PM	ac38ab1b-89f0-415c-a3...	aa9e2340-e1ef-486b-8b4e-1b7b8caabbea	ZTNA Network Access Cli...	ZTNA Network Access Traffic Profile
Jan 9, 2025 4:34:50 PM	ac38ab1b-89f0-415c-a3...	cc20815b-379d-1900-9b24-2e73d9ab13a8	Microsoft Outlook	Office 365 Exchange Online
Jan 9, 2025 4:38:46 PM	ac38ab1b-89f0-415c-a3...	961e37fb-991b-4540-98bd-9525b0edb39d	ZTNA Network Access Cli...	ZTNA Network Access Traffic Profile
Jan 9, 2025 4:38:47 PM	ac38ab1b-89f0-415c-a3...	70ecebc1-0f10-490b-965e-ac59060091cf	ZTNA Network Access Cli...	ZTNA Network Access Traffic Profile
Jan 9, 2025 4:38:53 PM	ac38ab1b-89f0-415c-a3...	c58b25f4-47db-1566-5a73-73d1b4ac30e1	Microsoft Outlook	Office 365 Exchange Online
Jan 9, 2025 4:38:53 PM	ac38ab1b-89f0-415c-a3...	fec81d90-c132-46cd-9be4-7eb960ac0900	ZTNA Network Access Cli...	ZTNA Network Access Traffic Profile

Other Token-Related Properties

- **Incoming token types**
  Token type that were presented to Microsoft Entra ID to authenticate the actor in the sign in

  For example:
  PrimaryRefreshToken, RefreshToken, SAML or
  None (= Browser SSO / Direct Auth. via Creds)

- **Token Protection - Sign In Session**
  Indicator if sign-in token (PRT/RT) was cryptographically bound to the device (or not)

- **AuthenticationProcessingDetails**
  - Is CAE Token
  - OAuth Scope Info

HYBRID IDENTITY PROTECTION
conf25
CHARLESTON

Graph, Diagnostic, & XDR Logs (2025-01)

Entra Portal (Sign-in events)	Microsoft Graph Beta	Diagnostic Logs	AADSignInEventsBeta
Date	createdDateTime	CreatedDateTime	Timestamp
Correlation ID	correlationId	CorrelationId	CorrelationId (= ReportId)
Request ID	id (beta-Endpoint with empty OriginalRequestId)	id, OriginalRequestId	RequestId
Unique token identifier	uniqueTokenIdentifier	UniqueTokenIdentifier	**N/A**
Session ID	sessionId	**N/A**	SessionId
Token Protection Status	signInTokenProtectionStatus	**N/A**	**N/A**
Incoming token type	incomingTokenType	**N/A**	**N/A**
GlobalSecureAccessIpAddress	GlobalSecureAccessIpAddress	**N/A**	**N/A**
Through Global Secure Access	isThroughGlobalSecureAccess	**N/A**	**N/A**
Is CAE Token	Is CAE Token	Is CAE Token	**N/A**
Oauth Scope Info	Oauth Scope Info	Oauth Scope Info	**N/A**

Graph, Diagnostic, & XDR Logs (>2025-03)

Entra Portal (Sign-in events)	Microsoft Graph Beta	Diagnostic Logs	AADSignInEventsBeta
Date	createdDateTime	CreatedDateTime	Timestamp
Correlation ID	correlationId	CorrelationId	CorrelationId (= ReportId)
Request ID	id (beta-Endpoint with empty OriginalRequestId)	id, OriginalRequestId	RequestId
Unique token identifier	uniqueTokenIdentifier	UniqueTokenIdentifier	**N/A**
Session ID	sessionId	**SessionId**	SessionId
Token Protection Status	signInTokenProtectionStatus	**signInTokenProtectionStatus**	**N/A**
Incoming token type	incomingTokenType	**incomingTokenType**	**N/A**
GlobalSecureAccessIpAddress	GlobalSecureAccessIpAddress	**GlobalSecureAccessIpAddress**	**N/A**
Through Global Secure Access	isThroughGlobalSecureAccess	**isThroughGlobalSecureAccess**	**N/A**
Is CAE Token	Is CAE Token	Is CAE Token	**N/A**
Oauth Scope Info	Oauth Scope Info	Oauth Scope Info	**N/A**

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Advanced Insights of Microsoft Entra ID Sign-in Logs

Enrichment of sign-in data with mitigation capabilities for token theft and detection of unusual token issuance

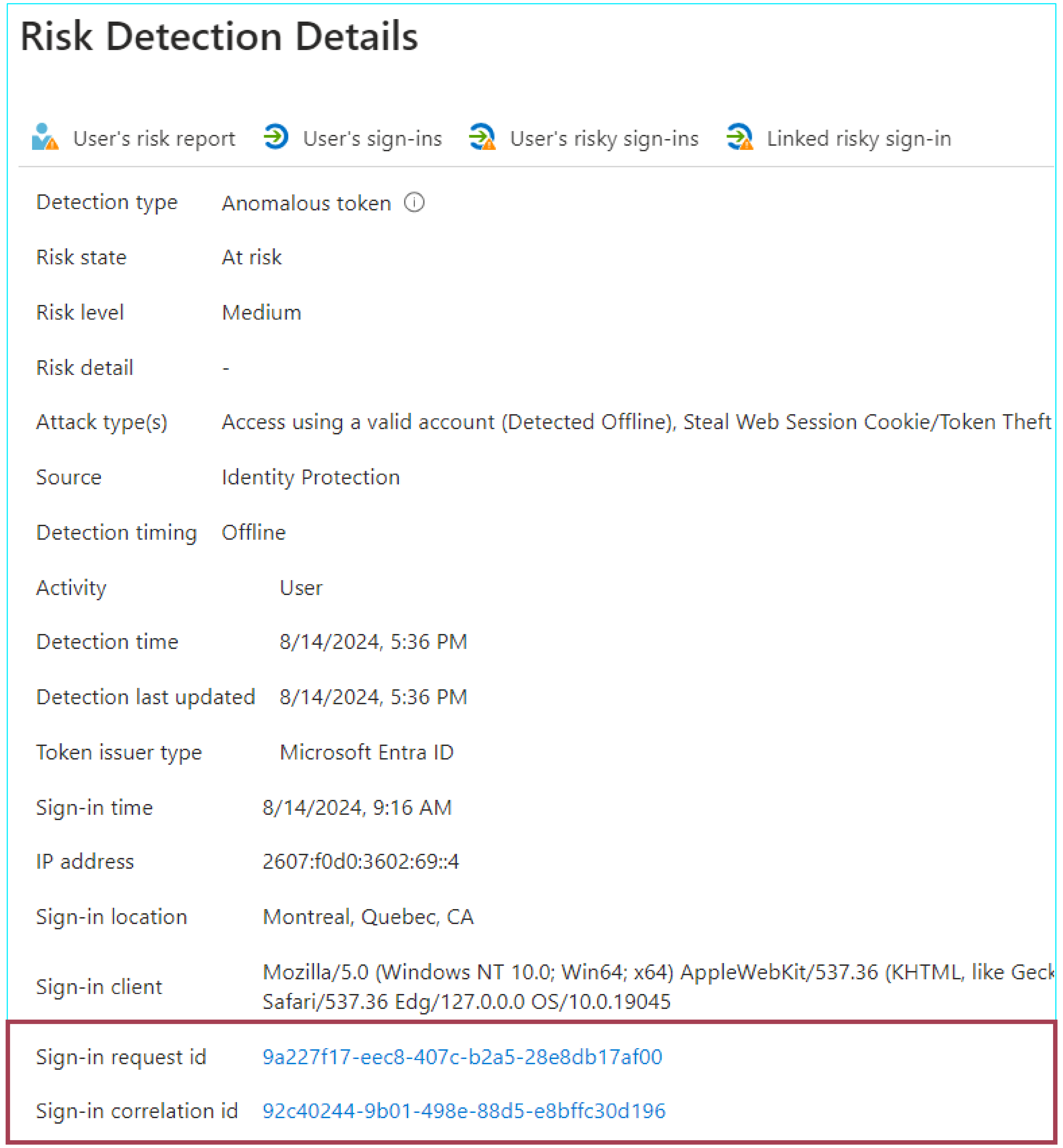
Demo

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Correlation of Sign-in Events to XDR Alert or Anomalies

Risk Detection in Entra ID Protection



Risk Detection Details

User's risk report · User's sign-ins · User's risky sign-ins · Linked risky sign-in

Detection type	Anomalous token ⓘ
Risk state	At risk
Risk level	Medium
Risk detail	-
Attack type(s)	Access using a valid account (Detected Offline), Steal Web Session Cookie/Token Theft
Source	Identity Protection
Detection timing	Offline
Activity	User
Detection time	8/14/2024, 5:36 PM
Detection last updated	8/14/2024, 5:36 PM
Token issuer type	Microsoft Entra ID
Sign-in time	8/14/2024, 9:16 AM
IP address	2607:f0d0:3602:69::4
Sign-in location	Montreal, Quebec, CA
Sign-in client	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck Safari/537.36 Edg/127.0.0.0 OS/10.0.19045
Sign-in request id	9a227f17-eec8-407c-b2a5-28e8db17af00
Sign-in correlation id	92c40244-9b01-498e-88d5-e8bffc30d196

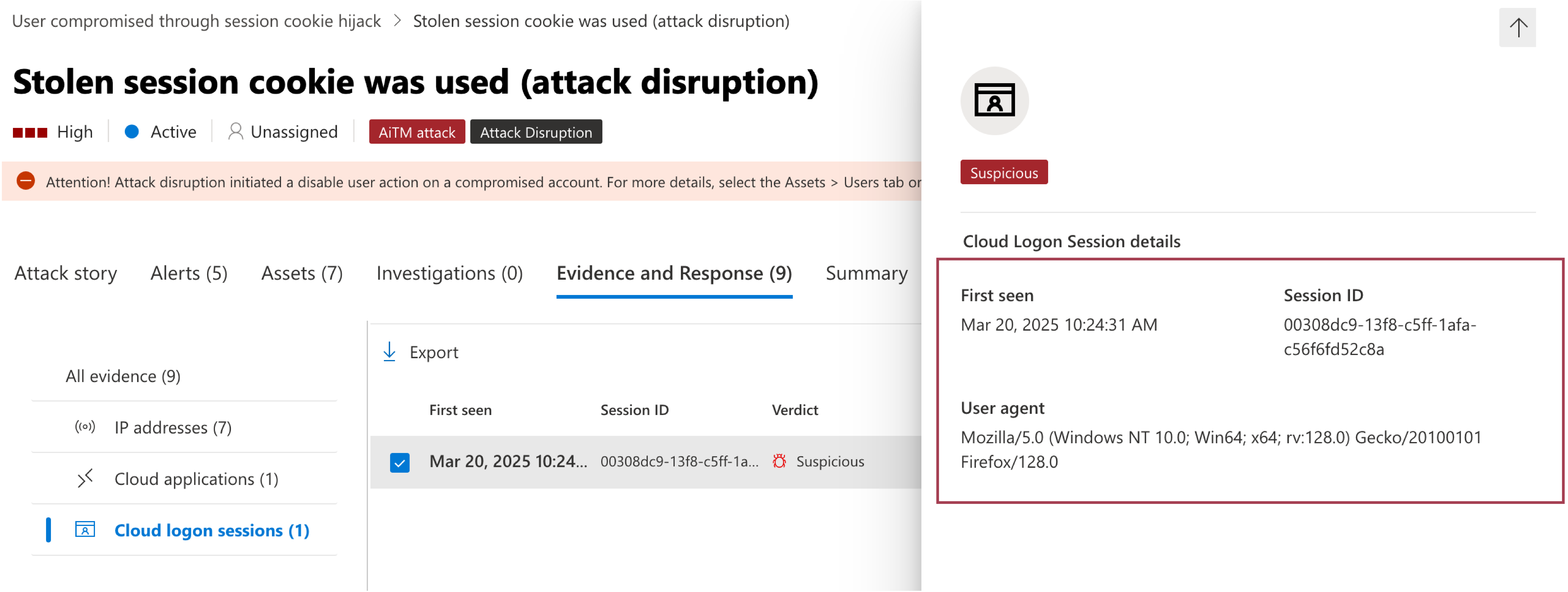
Risk Detections in relation to sign-in/token:

- Anomalous token (offline detection)
- Attempted access of PRT (by MDE)
- Unfamiliar sign-in properties
- Unfamiliar sign-in

Risk Detections by post-auth. activity:

- Mass Access to Sensitive Files
- Suspicious API traffic
- ...

Suspicious Session Cookie



User compromised through session cookie hijack > Stolen session cookie was used (attack disruption)

Stolen session cookie was used (attack disruption)

High | Active | Unassigned | AiTM attack | Attack Disruption

Attention! Attack disruption initiated a disable user action on a compromised account. For more details, select the Assets > Users tab or

	First seen	Session ID	Verdict
☑	Mar 20, 2025 10:24...	00308dc9-13f8-c5ff-1a...	Suspicious

Suspicious

Cloud Logon Session details

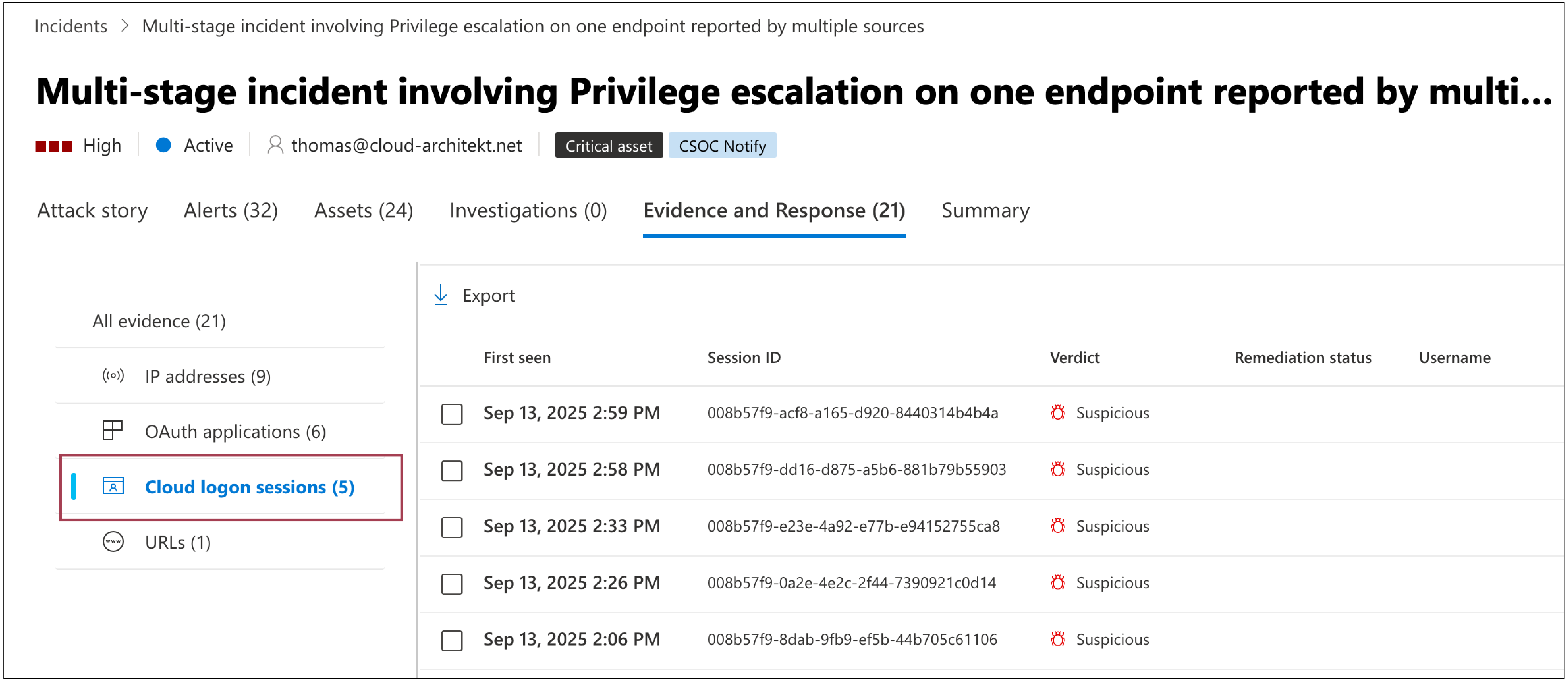
First seen
Mar 20, 2025 10:24:31 AM

Session ID
00308dc9-13f8-c5ff-1afa-c56f6fd52c8a

User agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Defender XDR Incident Evidence



Incidents > Multi-stage incident involving Privilege escalation on one endpoint reported by multiple sources

Multi-stage incident involving Privilege escalation on one endpoint reported by multi...

■■■ High | ● Active | thomas@cloud-architekt.net | Critical asset | CSOC Notify

Attack story | Alerts (32) | Assets (24) | Investigations (0) | **Evidence and Response (21)** | Summary

- All evidence (21)
- IP addresses (9)
- OAuth applications (6)
- **Cloud logon sessions (5)**
- URLs (1)

Export

	First seen	Session ID	Verdict	Remediation status	Username
□	**Sep 13, 2025 2:59 PM**	008b57f9-acf8-a165-d920-8440314b4b4a	Suspicious		
□	**Sep 13, 2025 2:58 PM**	008b57f9-dd16-d875-a5b6-881b79b55903	Suspicious		
□	**Sep 13, 2025 2:33 PM**	008b57f9-e23e-4a92-e77b-e94152755ca8	Suspicious		
□	**Sep 13, 2025 2:26 PM**	008b57f9-0a2e-4e2c-2f44-7390921c0d14	Suspicious		
□	**Sep 13, 2025 2:06 PM**	008b57f9-8dab-9fb9-ef5b-44b705c61106	Suspicious		

Samples of Behavior-Based Detections

- **Behaviors in Microsoft Defender XDR**
  Mass download (OneDrive), Unusual addition of credentials to an OAuth app,...
- **User Entity Behavior Analytics (UEBA) in Microsoft Sentinel**
  ML-based anomalies on activities but also sign-ins
  Suspicious number of protected documents accessed
- **Alerts in Microsoft Defender for Cloud (e.g., Resource Manager)**
  Suspicious management session using Azure Portal/PowerShell detected,...
- ...

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Correlation of Sign-in Events to XDR Alert or Anomalies

Enrichment of sign-in data with related alerts from Microsoft Defender XDR

Demo

HYBRID
IDENTITY
PROTECTION
conf25
CHARLESTON

Correlation of User Sign-in, Alert, and Cloud App Activity Logs

Sign-in, Alert, and Activity Log Mapping

Correlation XDR/SIEM Incident to suspicious sign-in
Correlation of token/session to activity
AADUserRiskEvent
RequestId
SecurityAlert
cloud-logon-request
cloud-logon-session
SignInLogs AADNonInteractiveUserSignInLogs
Time, IP, Actor and TargetObject
API or Cloud App Activity Logs
Mapping to sign-in event by Time window join & other entities
User/DeviceId URL, UniqueTokenId/ Token3PUniqueId*
UniqueToken Identifier
SessionId
NetworkAccessTraffic
AzureActivity
OfficeActivity
MicrosoftGraphActivityLogs
CloudAppEvents
Microsoft Azure
Microsoft Exchange Online
Microsoft SharePoint, OneDrive & Teams**

* limited to traffic for Entra ID token endpoint and Private Access Traffic

** limited to specific ActionTypes of M365 workloads

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Linkable Token Identifier

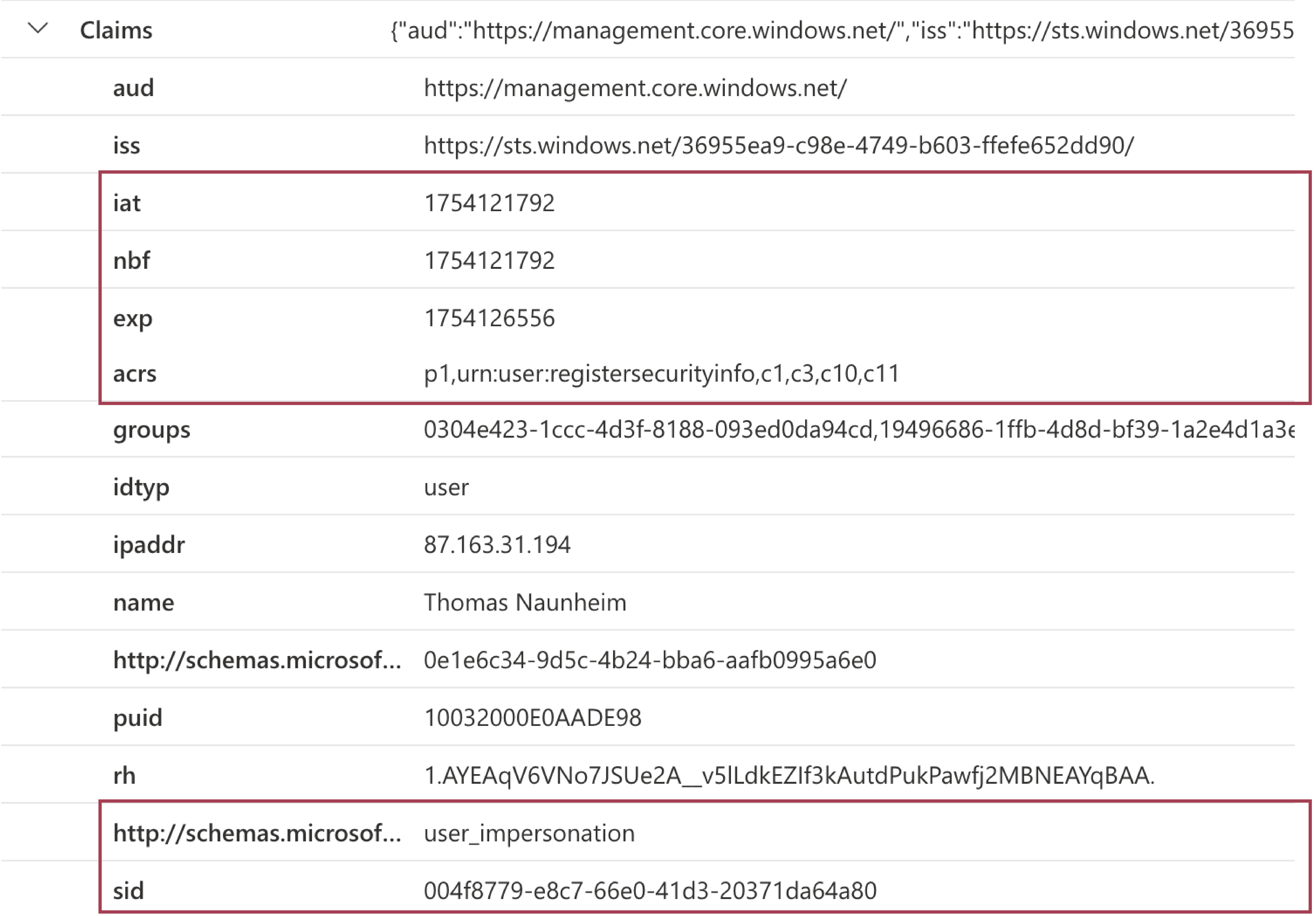
- **GA “feature” since July 2025, identifier “SessionId” across log sources**
  - Microsoft Entra sign-in logs
  - Microsoft Exchange Online audit logs
  - Microsoft Graph activity logs
  - Microsoft Teams audit logs
  - Microsoft SharePoint Online audit logs

- **“Limitation”: Device Code Flow shares same session ID**

Linkable Token Identifier in Claims

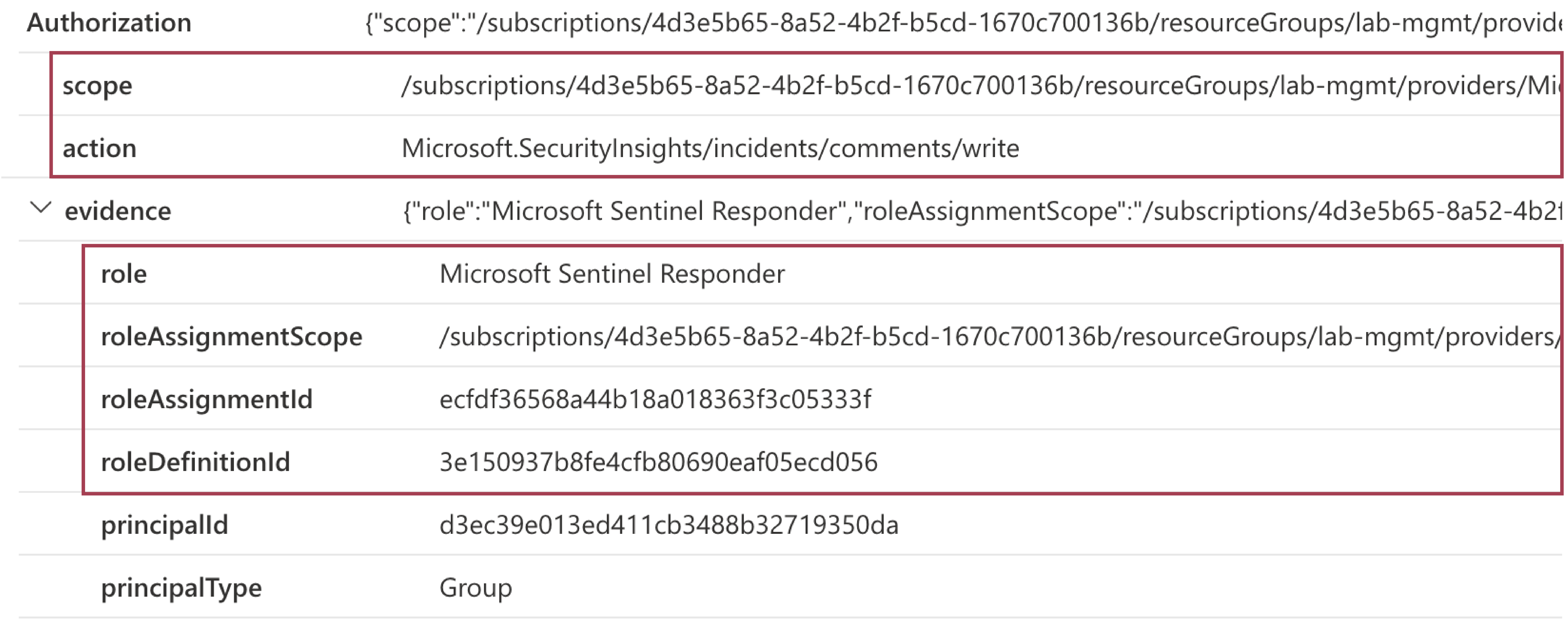
Claim	Description
`oid`	Immutable identifier identity of the user or service principal
`tid`	Tenant ID that the user is signing in to
`sid`	Identifier for entire session which has been generated when a user does interactive authentication. ID links all authentication artifacts
`deviceid`	Unique identifier for the device
`uti`	Token identifier
`iat`	Timestamp when the authentication for this token occurred.

Azure Activity Log



Claims	{"aud":"https://management.core.windows.net/","iss":"https://sts.windows.net/36955
aud	https://management.core.windows.net/
iss	https://sts.windows.net/36955ea9-c98e-4749-b603-ffefe652dd90/
iat	1754121792
nbf	1754121792
exp	1754126556
acrs	p1,urn:user:registersecurityinfo,c1,c3,c10,c11
groups	0304e423-1ccc-4d3f-8188-093ed0da94cd,19496686-1ffb-4d8d-bf39-1a2e4d1a3
idtyp	user
ipaddr	87.163.31.194
name	Thomas Naunheim
http://schemas.microsof...	0e1e6c34-9d5c-4b24-bba6-aafb0995a6e0
puid	10032000E0AADE98
rh	1.AYEAqV6VNo7JSUe2A__v5lLdkEZIf3kAutdPukPawfj2MBNEAYqBAA.
http://schemas.microsof...	user_impersonation
sid	004f8779-e8c7-66e0-41d3-20371da64a80

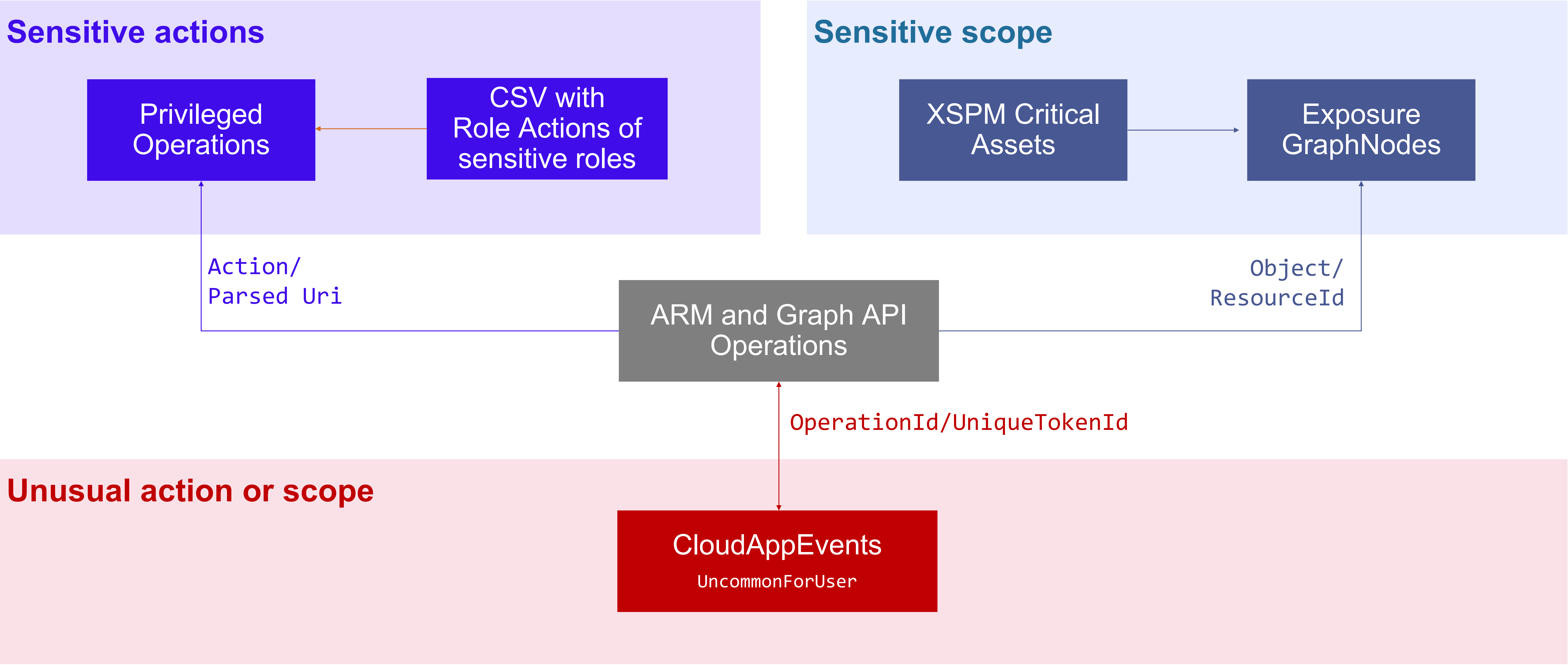
Azure Activity Log



Authorization	{"scope":"/subscriptions/4d3e5b65-8a52-4b2f-b5cd-1670c700136b/resourceGroups/lab-mgmt/provid
scope	/subscriptions/4d3e5b65-8a52-4b2f-b5cd-1670c700136b/resourceGroups/lab-mgmt/providers/Mi
action	Microsoft.SecurityInsights/incidents/comments/write
evidence	{"role":"Microsoft Sentinel Responder","roleAssignmentScope":"/subscriptions/4d3e5b65-8a52-4b2f
role	Microsoft Sentinel Responder
roleAssignmentScope	/subscriptions/4d3e5b65-8a52-4b2f-b5cd-1670c700136b/resourceGroups/lab-mgmt/providers/
roleAssignmentId	ecfdf36568a44b18a018363f3c05333f
roleDefinitionId	3e150937b8fe4cfb80690eaf05ecd056
principalId	d3ec39e013ed411cb3488b32719350da
principalType	Group

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Enrichment of Sensitive Actions/Scope



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Correlation of User Sign-in, Alert, and Cloud App Activity Logs

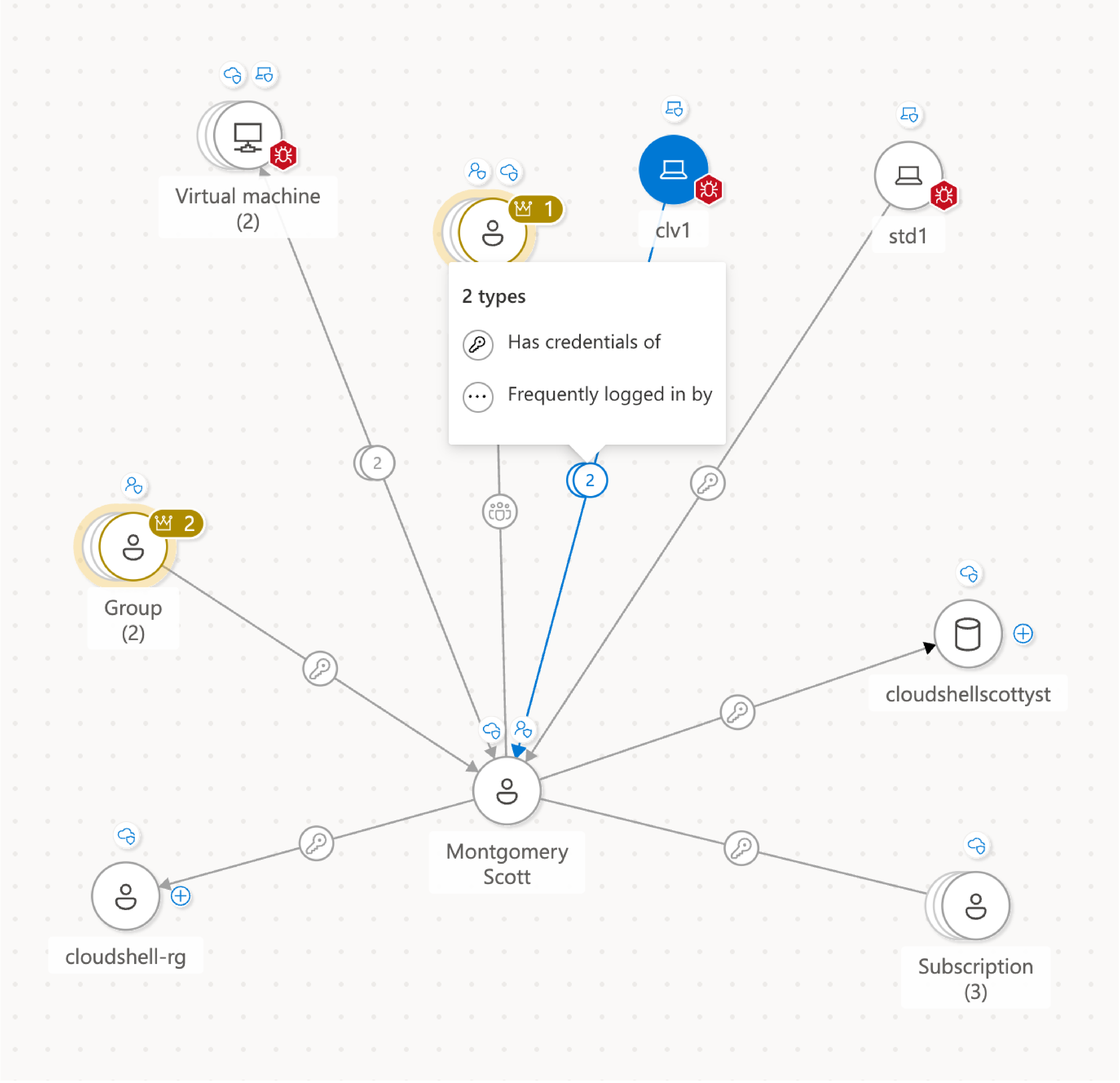
Tracking sign-in events and issued tokens, correlated to cloud app access (post-authentication events)

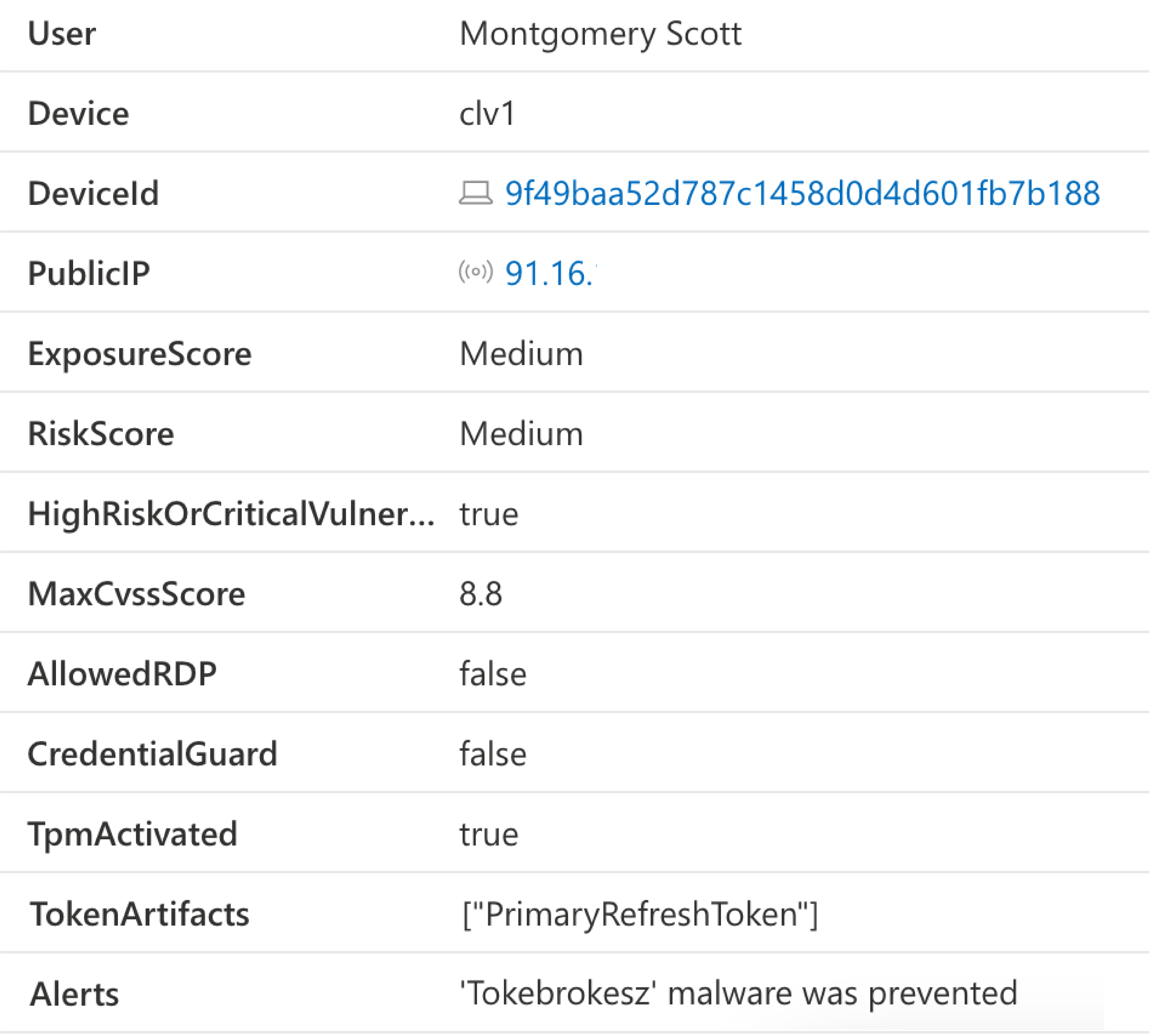
Demo

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Discover Exposed Token Artifacts with Exposure Management

Vulnerable Device and MDE Alerts



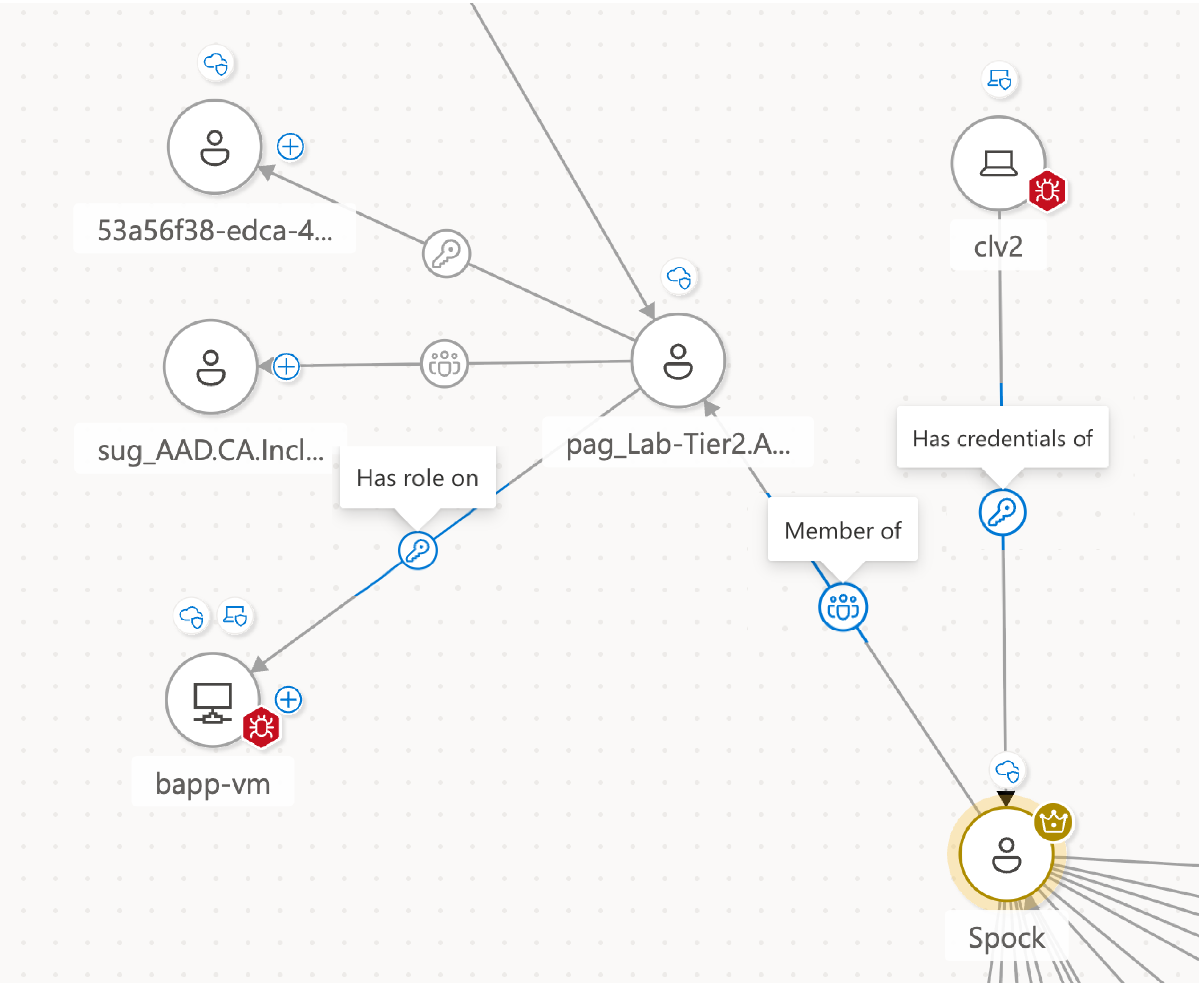


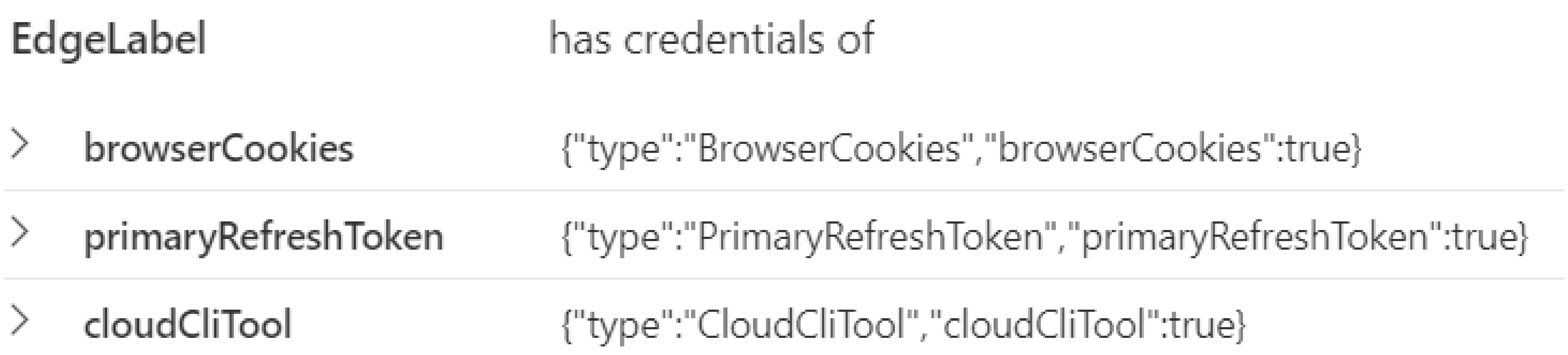
User	Montgomery Scott
Device	clv1
DeviceId	9f49baa52d787c1458d0d4d601fb7b188
PublicIP	91.16.
ExposureScore	Medium
RiskScore	Medium
HighRiskOrCriticalVulner...	true
MaxCvssScore	8.8
AllowedRDP	false
CredentialGuard	false
TpmActivated	true
TokenArtifacts	["PrimaryRefreshToken"]
Alerts	'Tokebrokesz' malware was prevented

But What About Session...?

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

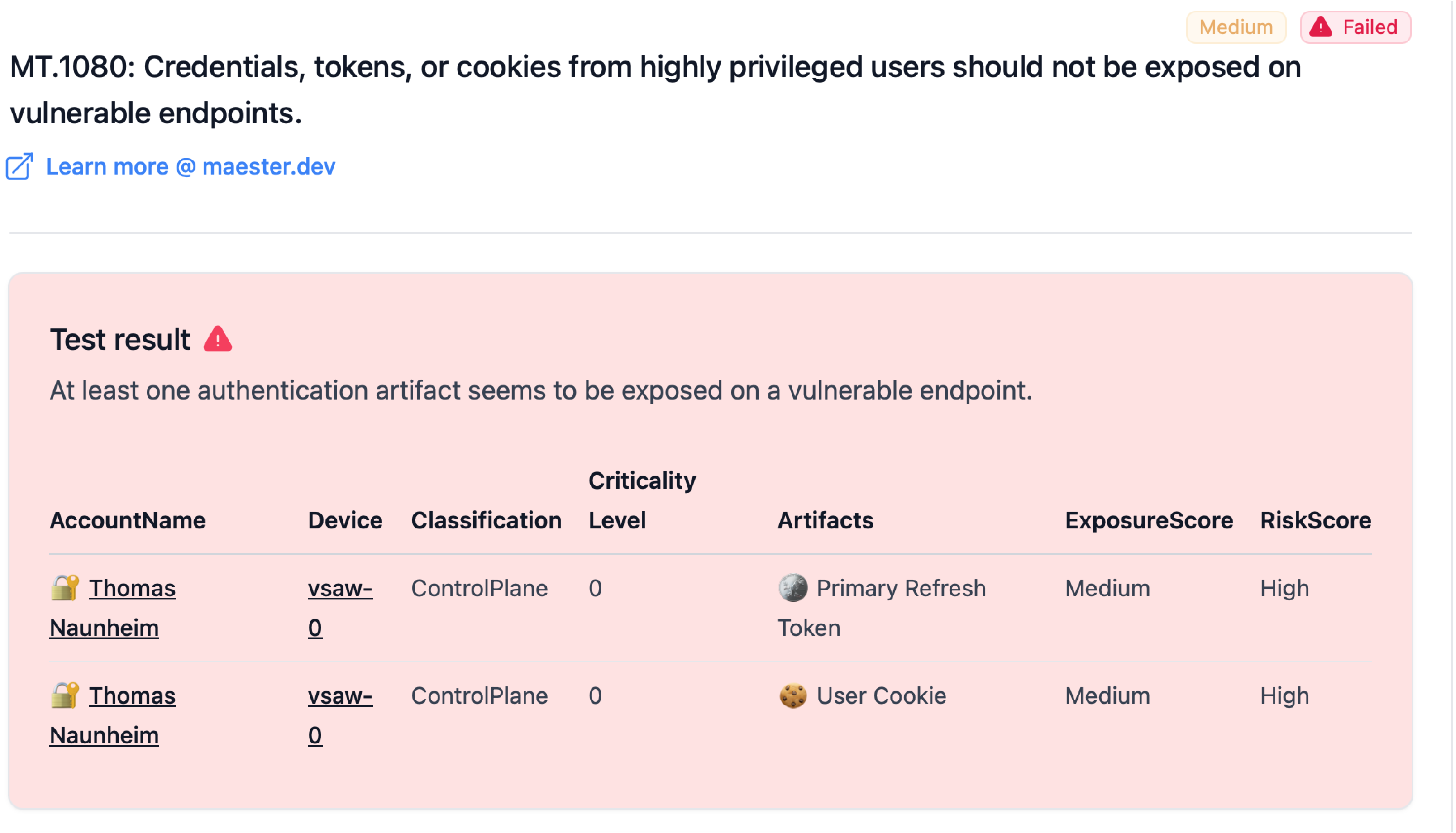
Smart Analysis of Browser Artifacts





EdgeLabel	has credentials of
browserCookies	{"type":"BrowserCookies","browserCookies":true}
primaryRefreshToken	{"type":"PrimaryRefreshToken","primaryRefreshToken":true}
cloudCliTool	{"type":"CloudCliTool","cloudCliTool":true}

Maester Check



Medium ⚠ Failed

MT.1080: Credentials, tokens, or cookies from highly privileged users should not be exposed on vulnerable endpoints.

Learn more @ maester.dev

Test result ⚠

At least one authentication artifact seems to be exposed on a vulnerable endpoint.

AccountName	Device	Classification	Criticality Level	Artifacts	ExposureScore	RiskScore
🔐 Thomas Naunheim	vsaw-0	ControlPlane	0	Primary Refresh Token	Medium	High
🔐 Thomas Naunheim	vsaw-0	ControlPlane	0	🍪 User Cookie	Medium	High

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Get hunting queries from my demos

This is not a phishing link 😇

Questions?

hip

CHARLESTON

HYBRID
IDENTITY
PROTECTION

conf25