



One compromised identity. No exploits. **Full access.**

Stage by stage: how ThreatDown ITDR tracks and dismantles the attack chain across Microsoft Entra ID and Okta.

Abstract

One stolen credential. Two identity platforms. No malware, no exploits — just a username, a password, and a clear path to the sensitive data behind them.

This guide walks through a realistic identity-led intrusion against a fictional organization, COMPANY, tracing how a threat actor moves from an initial credential attack to attempted data exfiltration across Microsoft Entra ID and Okta. At each stage, ThreatDown ITDR surfaces what's happening, who's doing it, and why it matters. All before the damage is done.

Table of contents

The setup	4
Stage 1 Initial access: credential attacks	5
Stage 2 Successful sign-in and tenant pivot: geo/time anomalies	7
Stage 3 Persistence and privilege escalation (Microsoft 365)	9
Stage 4 Persistence (Okta): API-based access	12
Stage 5A Exfiltration (Okta): blocked SSO access	13
Stage 5B Exfiltration (Entra ID): file and email access	14
Outcome and key takeaways	16

The setup

COMPANY runs a hybrid identity environment: Microsoft Entra ID handles O365 authentication and cloud resources, while Okta manages SSO access to business-critical SaaS applications. The two platforms are federated, meaning that Entra ID is configured as an external Identity Provider within Okta and user identities are synchronized across both environments.

In practice, when logging into Okta, the user clicks "Sign in with Microsoft" and is redirected to Microsoft's authentication portal. The user is passed back into Okta as a verified, trusted identity, no second password, no second factor. Compromising a single identity is therefore enough to gain access to both platforms and everything reachable through them. It's a common, practical configuration. It's also exactly what the attacker is counting on.

Stage 1 - Initial access: credential attacks

What happened

The attack begins quietly. The threat actor, operating from South Korea, runs automated credential attacks against both identity providers simultaneously. Against Okta, the attempts fail: no valid credentials are found. Against Entra ID, the spray succeeds. After cycling through a list of common passwords across multiple accounts, the attacker lands on a working credential pair tied to matthew@company.com.

Why it matters

Password spraying is deliberately slow and distributed to avoid lockout thresholds. Individual failed logins look like noise. The signal only emerges when you correlate volume, timing, and source across the entire authentication stream, on both platforms, simultaneously.

ITDR surfaces the spray pattern before the attacker has done anything with the credential. **That’s the highest-value intervention point in the entire attack chain.**

Multiple Users Login with invalid credentials from Agent/Proxy

Severity	Identity	TimeStamp	Attack technique	Source	Status
Low	paolo@company.com	2026-04-28T15:00:43Z	Valid Accounts	Okta	Open



Actor

Actor ID	00utwiv4ag0Kukiois97
Actor Type	User
Actor Roles	User
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
OS	Mac OS X
Browser	CHROME
Device	Computer



Geolocation Network

IP Address	43.155.216.204
City	Seoul
State	Gangwon
Country	Korea

1.1 Brute-force attack (Okta): paolo@company.com is the first user targeted in this brute-force attack. The incident is associated with this identity.

```

{
  "ip": [ 1 item
    0: "43.155.216.204"
  ]
  "meta_id": [...] 6 items
  "distinct_user_id_count": 6
  "distinct_principal_userid": [ 6 items
    0: "emma@company.com"
    1: "leonardo@company.com"
    2: "lucas@company.com"
    3: "maria@company.com"
    4: "paolo@company.com"
    5: "ryan@company.com"
  ]
}

```

1.2 Brute-force attack (Okta): this view shows the targeted usernames and the originating IP address of the brute-force attempts.

Severity

Medium

Identity

emma@company.com

TimeStamp

2026-04-28T15:00:11Z

Attack technique

Valid Accounts, Valid Accounts: Cloud Accounts

Source

Entra

Status

Open

Identity

Email

emma@company.com

Display Name

emma

Identity Type

user

User Type

Member

Identity Context

Admin

No

Risk Level

Medium

Last Password Change

Apr 27, 2026 5:01 PM

Sign in Context

IP Address

43.155.216.204

City

Seoul

State

Gangwon

1.3 Password spray attack (Entra): emma@company.com is the first account targeted in this attack. The overall incident is linked to this identity.

```

{
  "meta_id": [...] 64 items
  "affected_users": { 11 items
    "emma@company.com": 6
    "ryan@company.com": 6
    "lucas@company.com": 6
    "marco@company.com": 6
    "maria@company.com": 5
    "paolo@company.com": 6
    "matthew@company.com": 6
    "leonardo@company.com": 6
    "mohammed@company.com": 6
    "patrizio@company.com": 3
    "alexander@company.com": 6
  }
}

```

1.4 Password spray attack activity (Entra): the incident Context displays the attempted usernames.

In the above views, ITDR surfaces everything an analyst needs to understand the spray attempts at a glance: the accounts targeted, the geographic origin of the attack, and the contextual details that make the difference between an alert and an actionable lead.

Stage 2 - Successful sign-in and tenant pivot: geo/time anomalies

What happened

With valid Entra ID credentials in hand, the attacker logs in. The session originates from a Korean IP address at an hour that falls well outside Matthew’s normal working pattern. From there, the attacker leverages the Entra ID / Okta federation to pivot directly into Okta without requiring additional credentials.

To the individual platform, each login looks like a single event. To ITDR, the picture is different: two sign-ins, two platforms, the same anomalous origin, close anomalous timing, and a clear lateral movement pattern connecting them.

How ITDR builds confidence

Neither the geographic anomaly nor the time-of-access deviation alone would be enough to raise a high-confidence alert. However, when evaluated against Matthew’s established behavioral baseline across both platforms, they tell a consistent story. This is where behavioral context transforms weak signals into actionable detections.

Two platforms, one view. ITDR centralizes the Entra ID login and the Okta pivot into a single dashboard, eliminating the blind spot that exists when platforms are monitored in isolation.

Sign-In from Location Outside Allowed Area

Severity

Medium

Identity

matthew@company.com

TimeStamp

2026-04-28T23:00:50Z

Attack technique

Valid Accounts: Domain Accounts

Source

Okta

Status

Open

Actor

Actor ID

00u10z74ke1z4e0U698

Actor Type

User

Actor Roles

User

User Agent

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

OS

Mac OS X

Browser

CHROME

Device

Computer

Geolocation Network

IP Address

43.155.216.204

City

Seoul

State

Gangwon

Country

Korea

2.1 Suspicious sign-in: red boxes show the geo/time anomalies (sign-in after 6:00 PM from Korean IP).

```
√ { 3 items
  "user": "matthew@company.com"
  √ "action": [ 1 item
    0: "ALLOW"
  ]
  > "summary": [...] 1 item
}
```

2.2 Suspicious sign-in: the Context shows the sign-in was allowed for user matthew.

In this view, ITDR captures the suspicious sign-in originating from an unexpected location and occurring outside the user's normal working hours, two signals that give analysts immediate confidence the session is compromised.

Stage 3 - Persistence and privilege escalation (Microsoft 365)

What happened

The attacker knows that compromised credentials are temporary, passwords get reset, and sessions expire. The priority now is establishing a foothold that survives detection and response. The chosen method is straightforward: abuse legitimate tenant collaboration features.

First, the attacker, exploiting several account misconfigurations, invites an external identity (support@company-secure.com) into the COMPANY tenant. An external invite is a routine operation in most M365 environments, easy to overlook. Then, that guest account is converted from guest to member status, quietly expanding its access scope. Finally, an administrative role is assigned, completing the escalation from outside visitor to privileged insider in three steps.

Why this is a common real-world tactic

External user invitations and role assignments are normal administrative activities. Individually, each action is defensible as routine. The threat only becomes visible when these actions are preceded by the suspicious authentication context from Stage 2, the same session, the same anomalous origin, minutes apart.

External invitations and role assignments are normal admin activity. What makes them visible here is the session context that preceded them. The same anomalous origin, minutes apart. **ITDR connects those dots.**

External User invited to Tenant

Severity	Identity	TimeStamp	Attack technique	Source	Status
Medium	matthew@company.com	2026-04-28T23:08:50Z	Valid Accounts	Entra	Open
Identity					
Email		matthew@company.com			
Display Name		matthew			
User ID		matthew@company.com			
Identity Type		user			
User Type		Member			
Identity Context					
Admin		No			

Admin	No
Risk Level	unknown
Last Password Change	Apr 29, 2026 11:10 AM
Sign In Context	
IP Address	43.155.216.204
Country Name	Korea
Action	
Event Type	GENERIC_EVENT
Display Message	Invite external user
Product Event Type	Invite external user
Security Result Action	ALLOW
Security Result Summary	success

3.1 External user invited: the alert shows the details of the user who performed the invitation (matthew).

3.2 External user invited: details of the invitation action are shown inside the red box.

```

v{ 2 items
  "user": "matthew@company.com"
  "target_user_display_name": "support@company-secure.com"
}

```

3.3 External user invited: the context shows the inviting user (matthew) and the invited external account (support).

Here, ITDR surfaces the full picture of the external user invitation: the compromised internal account used to send it and the external identity being onboarded, a pairing that, set against the suspicious session context already established, immediately signals deliberate persistence rather than routine collaboration.

Guest Account converted to member

Severity

Medium

Identity

matthew@company.com

TimeStamp

2026-04-28T23:13:50Z

Attack technique

Modify Authentication Process

Source

Entra

Status

Open

Identity

Email

matthew@company.com

Display Name

matthew

User ID

matthew@company.com

Identity Type

user

User Type

Member

Identity Context

Admin

Yes

Directory Roles

Global Administrator

PIM Managed

Yes

3.4 External identity converted to member: the alert shows who initiated the account update (matthew).

Sign In Context

IP Address

43.155.216.204

Country Name

Korea

App Device

User Agent

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleW

Action

Event Type

GENERIC_EVENT

Display Message

Update user

Product Event Type

Update user

Security Result Action

ALLOW

Security Result Summary

success

3.5 External identity converted to member: the account update action details are shown in the red box.

```

v{ 1 item
  "user": "support@company-secure.com"
}

```

3.6 External identity converted to member: the context reveals the account update target identity (support).

ITDR tracks the next step in the same attack sequence. The external identity has now been successfully converted to a member. The compromised account driving these actions remains consistently identified in the Identity tab, giving analysts a single, unbroken line of attribution from the initial sign-in anomaly to this point in the intrusion.

User elevated to Admin Role

Severity	Identity	TimeStamp	Attack technique
Medium	matthew@company.com	2026-04-28T23:15:50Z	Account Manipulation,Account Manipulation: Additional Cloud Roles

 Identity

Email	matthew@company.com
Display Name	matthew
User ID	matthew@company.com
Identity Type	user
User Type	Member
O 365 User Type	Regular

 Identity Context

Admin	Yes
-------	-----

3.7 Admin role assignment: this section displays the user who carried out the privilege escalation (matthew).

App Device	
User Agent	O365AdminPortal
Action	
Operation	Add member to role.
Result Status	Success
Workload	AzureActiveDirectory
Event Type	USER_UNCATEGORIZED
Product Event Type	Add member to role.
Security Result Action	ALLOW
Security Result Summary	Added a user to an admin role successfully
Target Action	
Target App ID	User_ad386d40-fa08-4712-8eff-3072932ed39b

3.8 Admin role assignment: this section details the role assignment action and its resulting outcome (Success).

```
{ 2 items
  "user": "matthew@company.com"
  "target_user": "support@company-secure.com"
}
```

3.9 Admin role assignment: the context shows which user initiated the elevation (matthew) and which user has been elevated (support).

ITDR captures the final step of the persistence chain: the external identity, invited in, converted to member, and now granted administrative privileges. The compromised account driving each of these actions remains consistently attributed throughout, giving analysts a clear, sequential view of how an outsider became a privileged insider in three deliberate steps.

Stage 4 - Persistence (Okta): API-based access

What happened

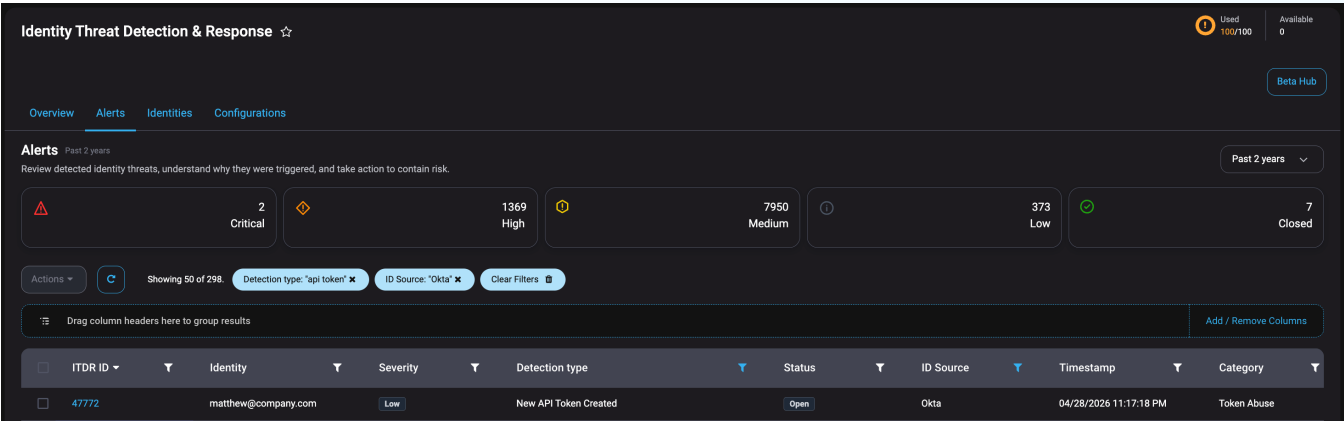
On the Okta side, the attacker takes a different approach. Rather than creating new identities, they create a long-lived API token from within the compromised session. API tokens in Okta are powerful: they enable programmatic access to tenant administration, survive interactive session termination, and can persist indefinitely unless explicitly revoked.

The token is created outside normal business hours, a detail that, combined with the risk context already established in this session, makes the intent clear.

Why defenders should care

An API token in the wrong hands is a silent skeleton key. It enables the attacker to enumerate users, inspect application assignments, and interact with the Okta API, all without triggering interactive login events.

An API token created outside business hours, in a high-risk session, is a **skeleton key in the wrong hands**. ITDR flags it immediately, turning a routine-looking admin action into a confirmed persistence indicator.



4.1 API token created: this view shows matthew created a new Okta API token.

Stage 5A - Exfiltration (Okta): blocked SSO access

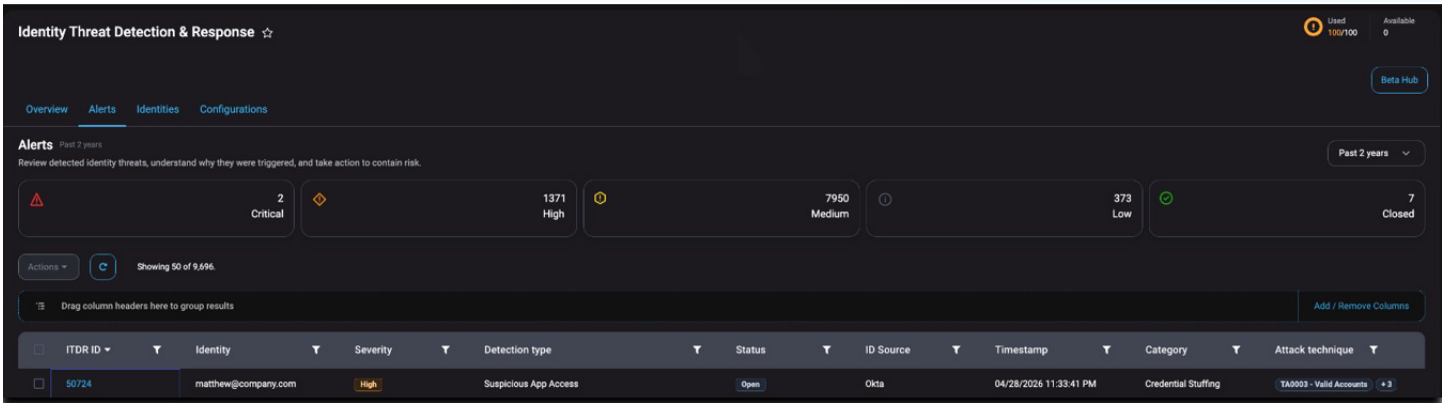
What happened

The attacker enumerates the applications assigned to Matthew’s account, mapping which SaaS services are reachable via SSO. A cloud storage application is identified as the target. The attacker attempts to launch it through Okta SSO to access and exfiltrate stored documents, but the attempt is blocked by Okta's own enforcement engine.

What made the difference

By this point in the session, Okta has accumulated enough risk signals to act: the anomalous sign-in origin, the behavioral deviations, and the API token creation have collectively raised the session risk score above the enforcement threshold. Okta blocks the application launch before any data is reached, and ITDR receives and surfaces that block event, contextualizing it within the broader attack chain already under investigation.

ITDR doesn’t replace the enforcement capabilities of the identity provider. It makes them visible, and meaningful, by connecting the block event to the full attack chain already under investigation.



5.1 Suspicious app access blocked: incident overview

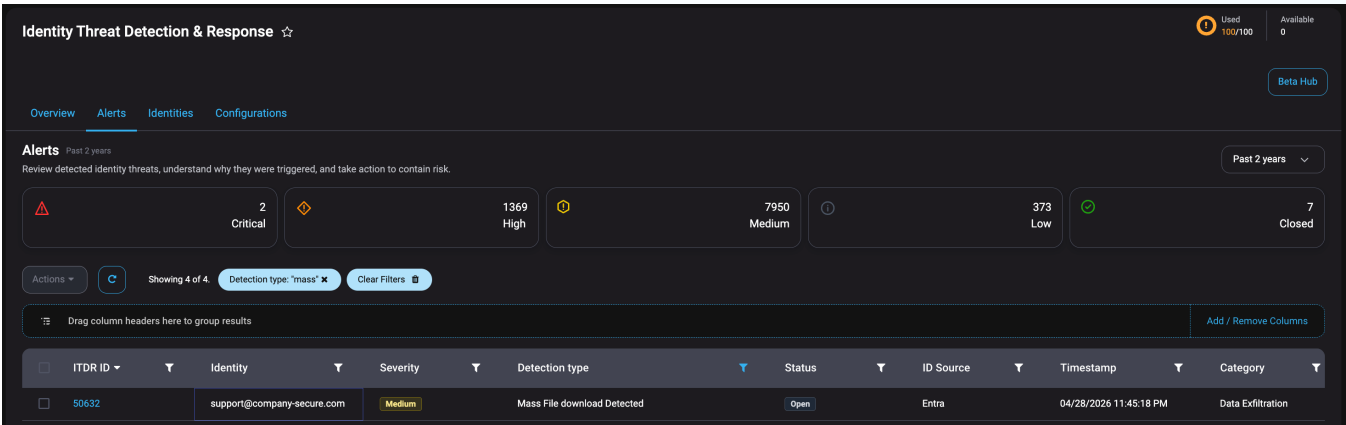
Stage 5B - Exfiltration (Entra ID): file and email access

What happened

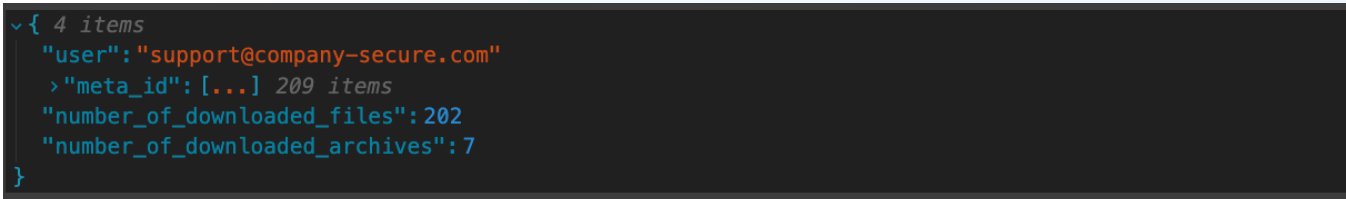
In parallel, the attacker pursues a second exfiltration path through Entra ID. Using the original compromised session, they access Matthew's OneDrive and download a large volume of documents in a short time window. They then access the mailbox, reviewing email content likely in search of sensitive business information, internal credentials, or privileged conversations.

How ITDR surfaces the activity

Both actions, bulk file download and mailbox access, are detected through a combination of volume anomalies and access pattern deviation from baseline. Neither activity is inherently impossible for a legitimate user. The combination of unusual volume, unusual timing, and the high-risk session context that preceded them is what elevates these events into confirmed exfiltration indicators.

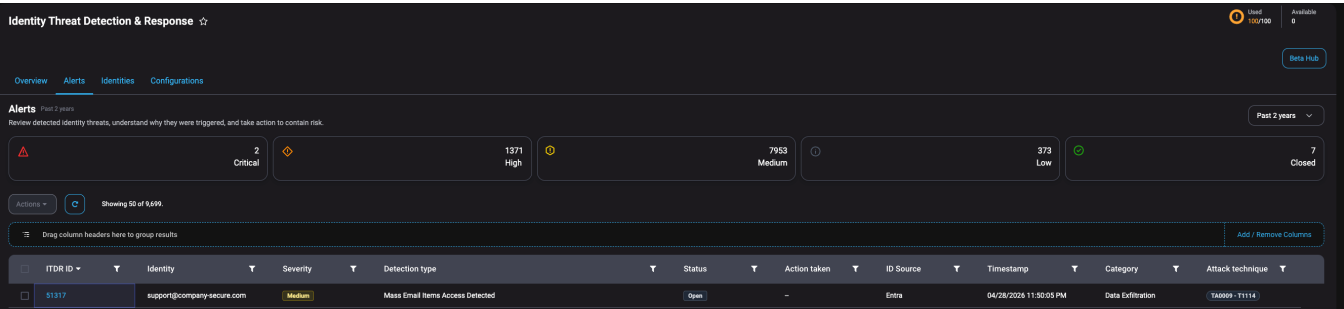


6.1 Massive file download: incident overview

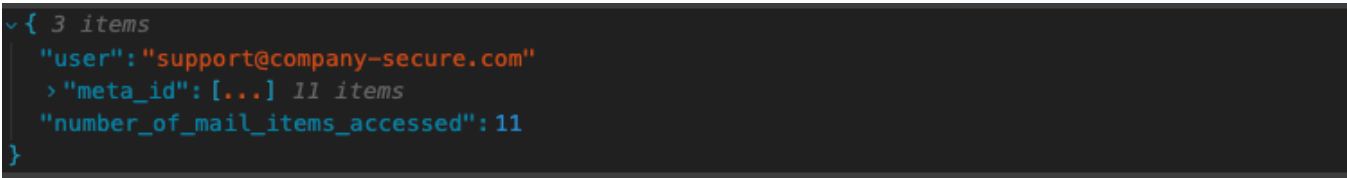


6.2 Massive file download: the Context displays the exfiltration volume, detailing the number of files and archives downloaded and the identity who performed the exfiltration (support).

Here, ITDR surfaces the exfiltration attempt in measurable terms: the account performing the downloads is clearly attributed, and the download statistics give analysts an immediate sense of scale, turning what could look like routine file access into a quantifiable data theft event.



6.3 Massive mail access: incident overview



6.4 Massive mail access: this section displays the mail exfiltration volume, detailing the number of accessed mails and the identity who accessed them (support).

Finally, ITDR shows the mailbox access in full: the compromised account behind it and the volume of emails reviewed. In the context of everything that preceded this moment, these are not routine access events. They are the final stage of a deliberate data collection effort.

Outcome and key takeaways

The attacker touched two identity platforms, created two independent persistence mechanisms, and attempted exfiltration through two separate paths. At no point did they use malware or exploit a vulnerability. Every action was performed through legitimate platform features with stolen credentials and abused functionality.

Stage	Action	ITDR Response
Initial access	Password spray across Entra ID and Okta	Spray pattern detected across both platforms
Sign-in and pivot	Login from anomalous geo/time, federation pivot	Behavioral deviation identified across both platforms
Persistence (M365)	External invite → guest-to-member → admin role	Admin actions following suspicious session context identified
Persistence (Okta)	API token created outside business hours	Token creation flagged within high-risk session
Exfiltration (Okta)	SSO app access attempt	Okta block reported based on accumulated session risk
Exfiltration (Entra ID)	Bulk file download and mailbox access	Detected via volume anomaly and session context

For security teams

- **Detect the spray, stop the chain.** Credential attacks are the starting line. Catching them before persistence is established is the highest-value intervention point in the entire kill chain. Everything that follows depends on getting that first foothold.
- **Federation is a lateral movement path.** A compromised Entra ID credential is a compromised Okta credential when the platforms are linked and monitoring is siloed. One identity, two attack surfaces.
- **The attacker's best tools are already in the environment.** External invites, role assignments, and API tokens are all normal operations. Context is what separates routine admin activity from a deliberate intrusion. Without it, each action looks defensible. With it, the intent is unmistakable.

Shut down identity-based attacks before they become breaches.

[Learn more today](#)



 threatdown.com

 sales@threatdown.com