OBSIDIAN

SOLUTION BRIEF

Secure your SaaS integrations end to end with Obsidian

Shrink your attack surface, contain blast radius early and accelerate supply chain investigations

Protect all your SaaS integrations from start to finish

Identify and remove risky integrations before breaches occur, detect attacks early with full context, and investigate incidents faster to limit the blast radius and reduce time to resolution.

See every SaaS integration: Automatically inventory all SaaS integrations, including shadow apps, OAuth and APIs, without spreadsheets, guesswork or blind spots

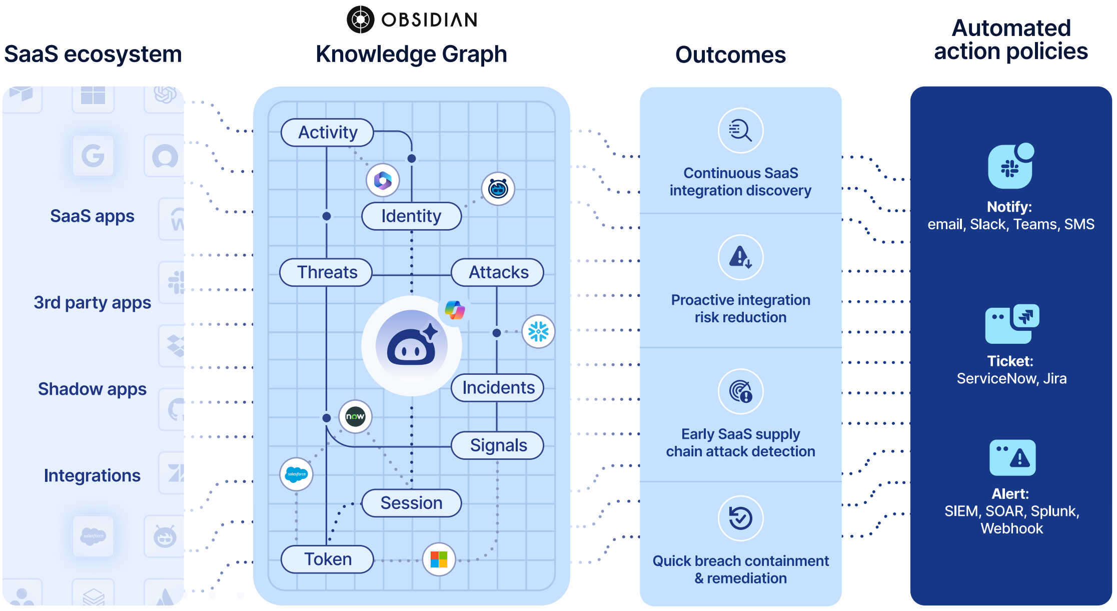
Reduce risky integrations before they're abused: Identify and prioritize high-risk integrations and proactively limit access, before attackers can abuse them

Catch supply chain compromise early: Detect compromise before delayed vendor alerts, understand what's affected, and stop lateral movement and data exposure

Contain breaches quickly and confidently: Quickly see what was accessed, limit impact fast and remediate with guided workflows built for SaaS incidents

Outcomes:

- Reduce SaaS attack surface
- Accelerate MTTI
- Accelerate MTTR
- Minimize blast radius and impact
- Improve SecOps efficiency


SaaS ecosystem
SaaS apps
3rd party apps
Shadow apps
Integrations
OBSIDIAN
Knowledge Graph
Activity
Identity
Threats
Attacks
Incidents
Signals
Session
Token
Outcomes
Continuous SaaS integration discovery
Proactive integration risk reduction
Early SaaS supply chain attack detection
Quick breach containment & remediation
Automated action policies
Notify: email, Slack, Teams, SMS
Ticket: ServiceNow, Jira
Alert: SIEM, SOAR, Splunk, Webhook

> In the absence of continuous visibility into the entire SaaS ecosystem, especially unauthorized activity between SaaS applications, we are looking at a huge data breach waiting to happen. The end-to-end SaaS Supply Chain security capabilities from Obsidian are a much-needed solution to an emerging risk most organizations are unprepared for."

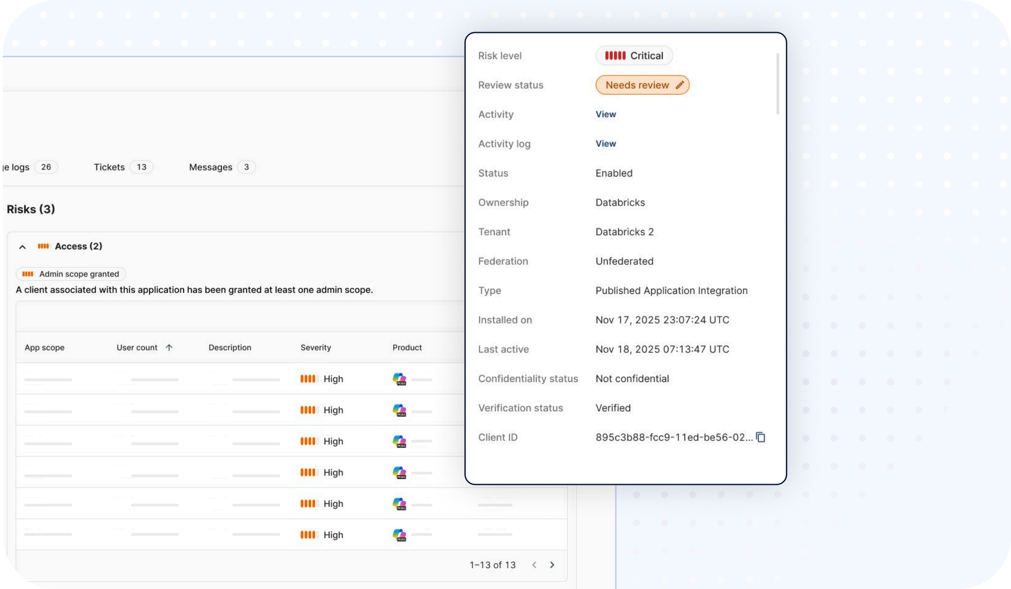
WYNDHAM
HOTELS & RESORTS

Key capabilities

Unified integration inventory

Gain a complete, always up-to-date view of all SaaS-to-SaaS integrations so you know exactly how data and access flow across your environment

- See all SaaS to SaaS integrations across core applications
- Expose hidden risk by automatically discovering shadow SaaS integrations
- Understand exactly how access and data flows across OAuth apps, APIs and non-human identities
- Eliminate blind spots with rich context on owners, permissions, authentication type, and activity



Risk level	Critical
Review status	Needs review
Activity	View
Activity log	View
Status	Enabled
Ownership	Databricks
Tenant	Databricks 2
Federation	Unfederated
Type	Published Application Integration
Installed on	Nov 17, 2025 23:07:24 UTC
Last active	Nov 18, 2025 07:13:47 UTC
Confidentiality status	Not confidential
Verification status	Verified
Client ID	895c3b88-fcc9-11ed-be56-02...

e logs 26 Tickets 13 Messages 3

Risks (3)

Access (2)

Admin scope granted

A client associated with this application has been granted at least one admin scope.

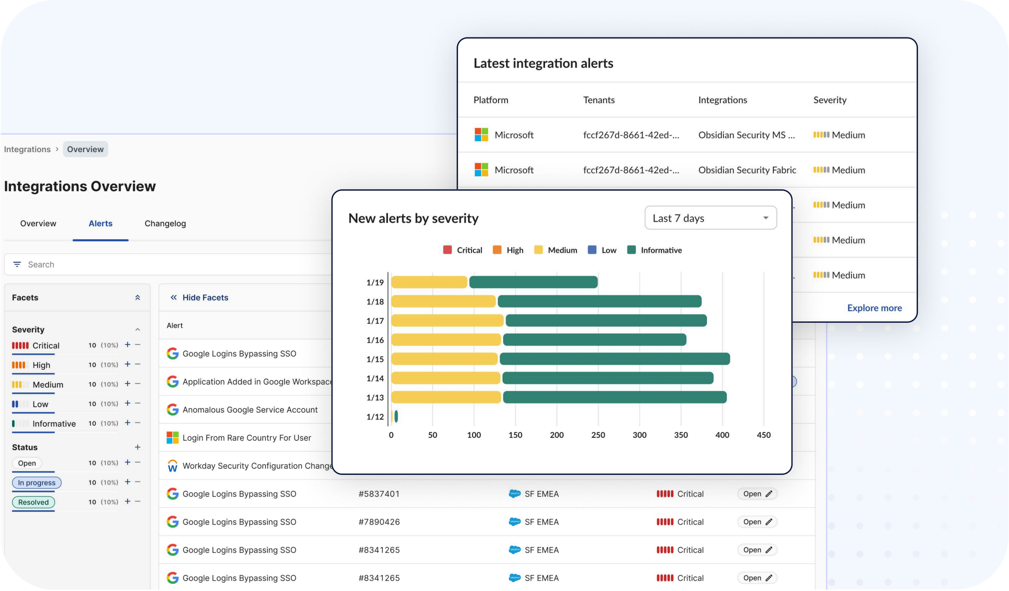
App scope	User count	Description	Severity	Product
			High	
			High	
			High	
			High	
			High	
			High	

1–13 of 13

Early behavior-based detection for SaaS supply chain compromise

Know as soon as your integrations become compromised so you can take actions before they turn into breaches

- Detect unusual or malicious integration activity using behavioral baselines and network-wide pattern modeling that's beyond the reach of traditional SIEMs and CASBs
- Identify risks based on usage patterns and data access behavior, not just static rules
- Surface subtle indicators of compromise such as unexpected access, expanded data usage, lateral movement, or behavior misaligned with an integration's intended purpose



Integrations › Overview

Integrations Overview

Severity

Critical	10	(10%)
High	10	(10%)
Medium	10	(10%)
Low	10	(10%)
Informative	10	(10%)

Status

Open	10	(10%)
In progress	10	(10%)
Resolved	10	(10%)

Alert				
Google Logins Bypassing SSO				
Application Added in Google Workspace				
Anomalous Google Service Account				
Login From Rare Country For User				
Workday Security Configuration Change				
Google Logins Bypassing SSO	#5837401	SF EMEA	Critical	Open
Google Logins Bypassing SSO	#7890426	SF EMEA	Critical	Open
Google Logins Bypassing SSO	#8341265	SF EMEA	Critical	Open
Google Logins Bypassing SSO	#8341265	SF EMEA	Critical	Open

Latest integration alerts

Platform	Tenants	Integrations	Severity
Microsoft	fccf267d-8661-42ed-...	Obsidian Security MS ...	Medium
Microsoft	fccf267d-8661-42ed-...	Obsidian Security Fabric	Medium
			Medium
			Medium
			Medium

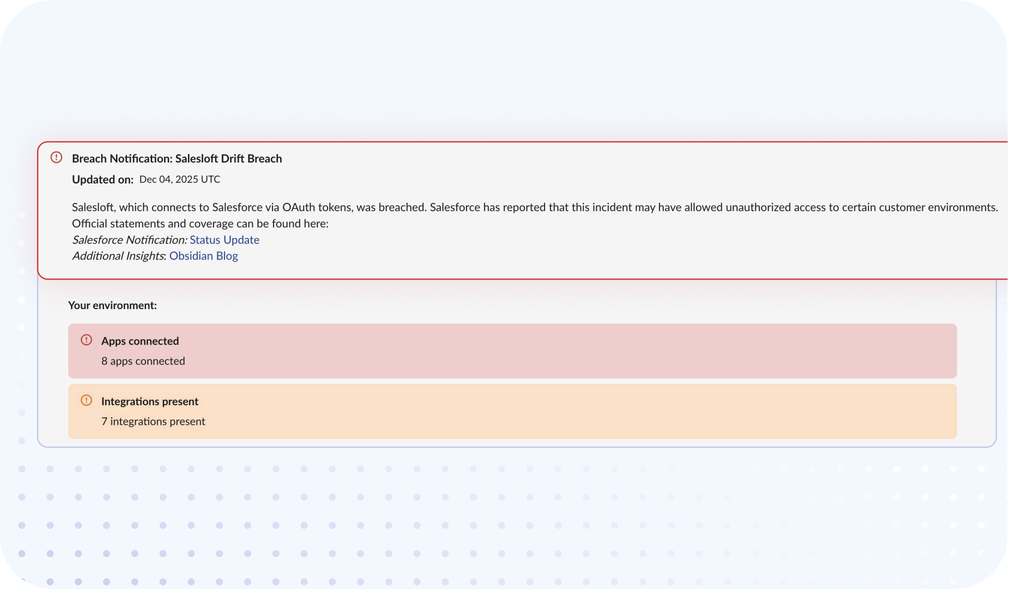
Explore more

New alerts by severity

Integration risk scoring and reduction

Reduce your attack surface by turning integration context into action and removing risky integrations before it spreads across your SaaS environment.

- Instantly understand which integrations pose the greatest risk with dynamic app-specific risk scoring based on custom risk factors
- Prioritize remediation based on real exposure so the riskiest integrations are addressed first
- Enforce least privilege by eliminating inactive or over-permissioned integrations



Breach Notification: Salesloft Drift Breach

Updated on: Dec 04, 2025 UTC

Salesloft, which connects to Salesforce via OAuth tokens, was breached. Salesforce has reported that this incident may have allowed unauthorized access to certain customer environments. Official statements and coverage can be found here:
Salesforce Notification: Status Update
Additional Insights: Obsidian Blog

Your environment:

Apps connected
8 apps connected

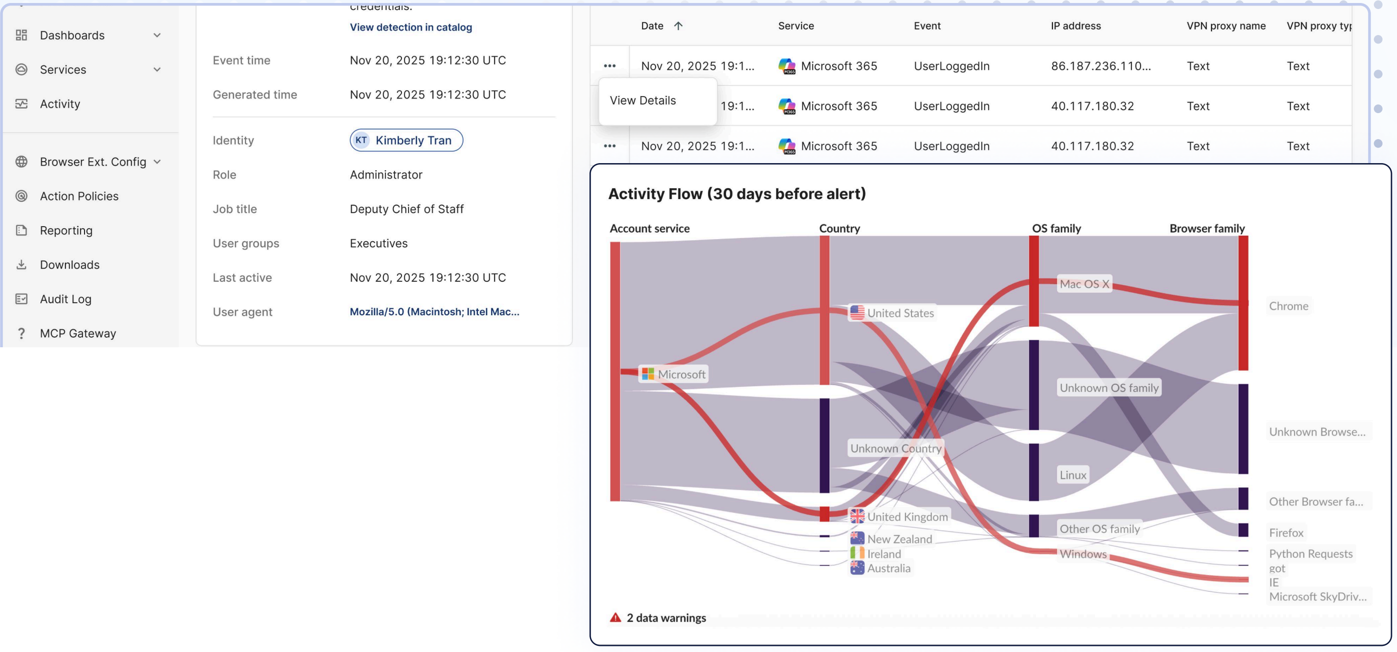
Integrations present
7 integrations present

End to end SaaS Supply Chain Security with Obsidian

Full breach blast radius and impact visualization

Get a complete picture of impact across your SaaS with full context

- Correlate activity across the entire SaaS environment using the Obsidian Knowledge Graph
- Instantly visualize blast radius with cross-SaaS applications context, integrations, tokens, users and service accounts
- Trace the full attack path, including users or services, actions taken, locations, tenants, sessions, and permissions, leveraging historic activity of identity and app
- Quickly determine what data was accessed, which integrations were affected, and the downstream business impact



credentials.

View detection in catalog

Event time	Nov 20, 2025 19:12:30 UTC
Generated time	Nov 20, 2025 19:12:30 UTC
Identity	KT Kimberly Tran
Role	Administrator
Job title	Deputy Chief of Staff
User groups	Executives
Last active	Nov 20, 2025 19:12:30 UTC
User agent	Mozilla/5.0 (Macintosh; Intel Mac...

	Date ↑	Service	Event	IP address	VPN proxy name	VPN proxy typ
•••	Nov 20, 2025 19:1...	Microsoft 365	UserLoggedIn	86.187.236.110...	Text	Text
	19:1...	Microsoft 365	UserLoggedIn	40.117.180.32	Text	Text
•••	Nov 20, 2025 19:1...	Microsoft 365	UserLoggedIn	40.117.180.32	Text	Text

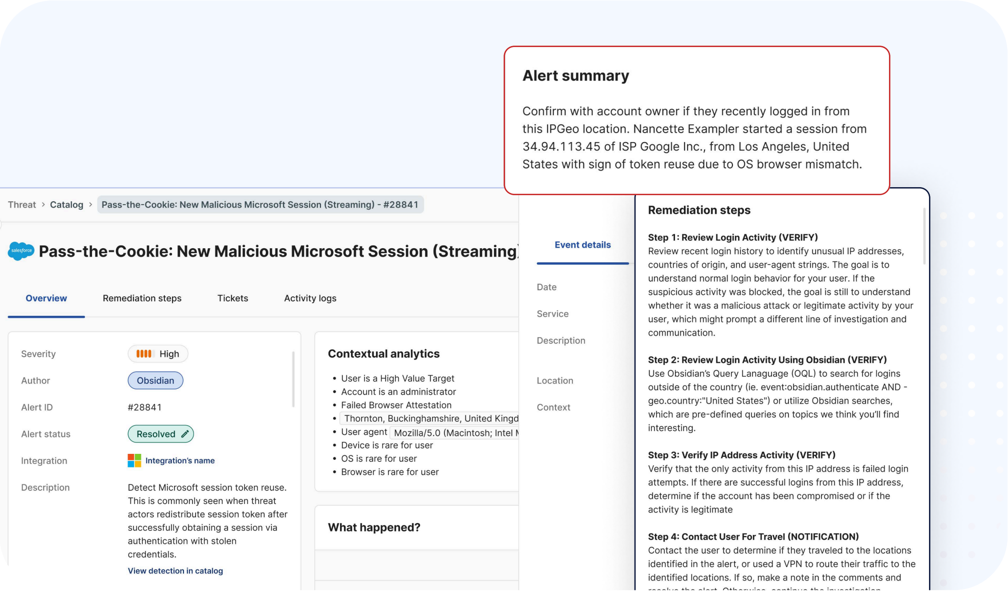
Activity Flow (30 days before alert)

2 data warnings

Guided recommendations to contain breaches

Respond quickly and confidently when breaches happen

- In-product alert explanations show what's risky, why it matters, and how to reduce exposure
- Step-by-step guided investigation and remediation during incidents, from review and validation to token revocation and integration removal
- Get faster, more confident containment to limit blast radius and prevent further impact



Alert summary

Confirm with account owner if they recently logged in from this IPGeo location. Nancette Exampler started a session from 34.94.113.45 of ISP Google Inc., from Los Angeles, United States with sign of token reuse due to OS browser mismatch.

Threat › Catalog › Pass-the-Cookie: New Malicious Microsoft Session (Streaming) - #28841

Pass-the-Cookie: New Malicious Microsoft Session (Streaming

Severity	High
Author	Obsidian
Alert ID	#28841
Alert status	Resolved
Integration	Integration's name
Description	Detect Microsoft session token reuse. This is commonly seen when threat actors redistribute session token after successfully obtaining a session via authentication with stolen credentials. View detection in catalog

Contextual analytics

- User is a High Value Target
- Account is an administrator
- Failed Browser Attestation
- Thornton, Buckinghamshire, United Kingd
- User agent Mozilla/5.0 (Macintosh; Intel M
- Device is rare for user
- OS is rare for user
- Browser is rare for user

What happened?

Remediation steps

Step 1: Review Login Activity (VERIFY)
Review recent login history to identify unusual IP addresses, countries of origin, and user-agent strings. The goal is to understand normal login behavior for your user. If the suspicious activity was blocked, the goal is still to understand whether it was a malicious attack or legitimate activity by your user, which might prompt a different line of investigation and communication.

Step 2: Review Login Activity Using Obsidian (VERIFY)
Use Obsidian's Query Lanaguage (OQL) to search for logins outside of the country (ie. event:obsidian.authenticate AND -geo.country:"United States") or utilize Obsidian searches, which are pre-defined queries on topics we think you'll find interesting.

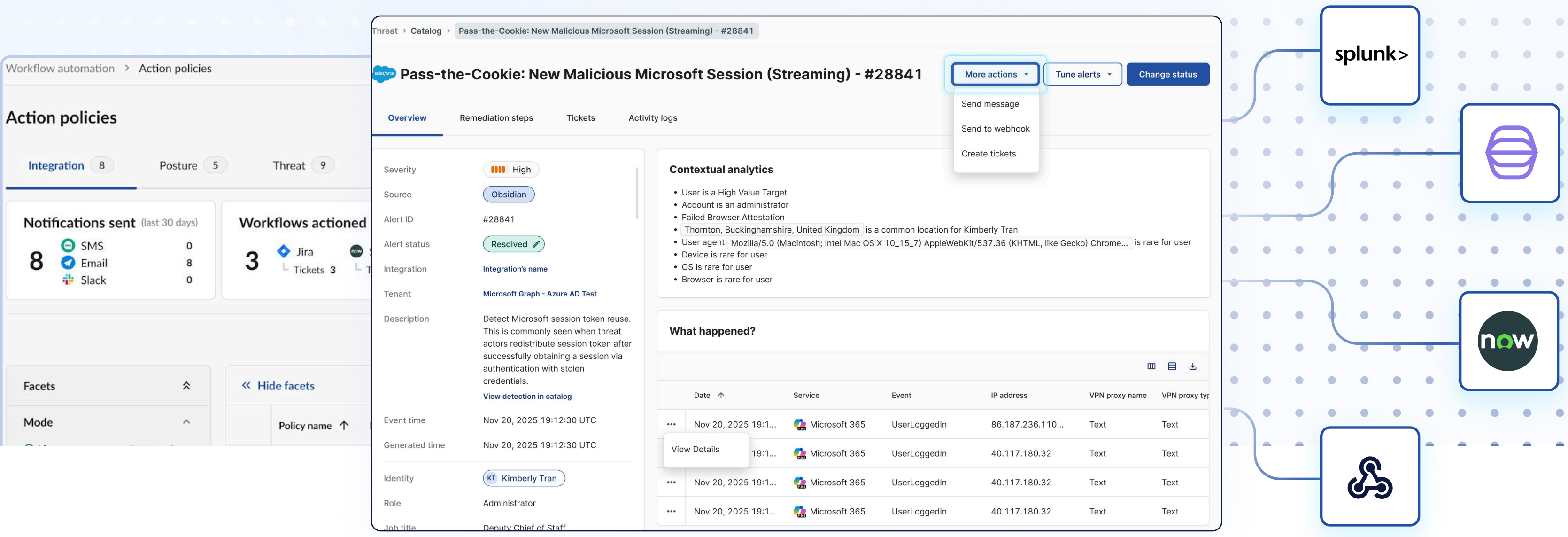
Step 3: Verify IP Address Activity (VERIFY)
Verify that the only activity from this IP address is failed login attempts. If there are successful logins from this IP address, determine if the account has been compromised or if the activity is legitimate

Step 4: Contact User For Travel (NOTIFICATION)
Contact the user to determine if they traveled to the locations identified in the alert, or used a VPN to route their traffic to the identified locations. If so, make a note in the comments and

Automate response for faster remediation

Create automated action policies triggered by integration risk or suspicious behavior, reducing manual triage and ensuring consistent response

- Notify the right users and responders instantly via email, Slack, Microsoft Teams, or SMS to take action before exposure spreads
- Automatically launch response workflows by creating Jira or ServiceNow tickets, triggering webhooks, or updating Obsidian Security Review states, eliminating delays and handoffs
- Build custom integrations using well-documented APIs to create tailored workflows
- Stream alerts and enriched context to SIEMs such as Splunk, improving correlation, auditability, and centralized incident management



Pass-the-Cookie: New Malicious Microsoft Session (Streaming) - #28841

Severity	High
Source	Obsidian
Alert ID	#28841
Alert status	Resolved
Integration	Integration's name
Tenant	Microsoft Graph - Azure AD Test
Description	Detect Microsoft session token reuse. This is commonly seen when threat actors redistribute session token after successfully obtaining a session via authentication with stolen credentials. View detection in catalog
Event time	Nov 20, 2025 19:12:30 UTC
Generated time	Nov 20, 2025 19:12:30 UTC
Identity	Kimberly Tran
Role	Administrator
Job title	Deputy Chief of Staff

Contextual analytics

- User is a High Value Target
- Account is an administrator
- Failed Browser Attestation
- Thornton, Buckinghamshire, United Kingdom is a common location for Kimberly Tran
- User agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome... is rare for user
- Device is rare for user
- OS is rare for user
- Browser is rare for user

What happened?

Date	Service	Event	IP address	VPN proxy name	VPN proxy typ
Nov 20, 2025 19:1...	Microsoft 365	UserLoggedIn	86.187.236.110...	Text	Text
19:1...	Microsoft 365	UserLoggedIn	40.117.180.32	Text	Text
Nov 20, 2025 19:1...	Microsoft 365	UserLoggedIn	40.117.180.32	Text	Text
Nov 20, 2025 19:1...	Microsoft 365	UserLoggedIn	40.117.180.32	Text	Text

Why Obsidian

Obsidian Security is built for SaaS supply chain security from day one

It is not a SIEM pipeline retrofitted for SaaS, and it is not a point in time audit. Obsidian gives you continuous visibility into what actually creates supply chain risk in SaaS: integrations, non-human identities, and the effective access they end up with across connected apps.

Obsidian then ties that access to real activity

That matters because most SaaS supply chain attacks do not look like malware. They look like normal OAuth use, normal API calls, and normal third-party behavior until you connect the dots. By correlating access context with behavior, Obsidian surfaces abuse that blends in as legitimate and closes the gap where these attacks usually succeed.

Powered by the Obsidian Knowledge Graph

Informed by the largest SaaS breach repository, and real-world SaaS security telemetry, Obsidian helps teams detect compromise earlier, determine blast radius fast, and reduce supply chain exposure before it turns into an incident.

End to end SaaS Supply Chain Security with Obsidian

Capability	Traditional Tools	With Obsidian
Comprehensive integration visibility	**Fragmented visibility:** Integrations discovered manually across SaaS UIs, shadow access often goes unnoticed.	**Complete visibility:** Continuous discovery of all SaaS integrations, OAuth tokens, APIs, and non-human identities.
Integration Risk Management	**Manual, static reviews:** Risk assessed app-by-app using disconnected tools like IdPs, individual SaaS consoles, and spreadsheets.	**Continuous, risk-based prioritization:** Risks ranked based on real usage, permissions, and business impact.
Breach Detection	**Delayed, reactive detection:** Relies on vendor disclosures, public TTPs, or custom SIEM rules after exposure has already occurred.	**Early, behavior-based detection:** Detects compromised integrations using behavioral baselines and contextual analysis.
Investigation and Impact	**Slow, manual reconstruction:** Incident analysis stitched together from partial SaaS logs, exports, and spreadsheets.	**Instant attack-path visibility:** Full blast-radius and impact visualization across SaaS apps, integrations, identities, and data.

Get a demo