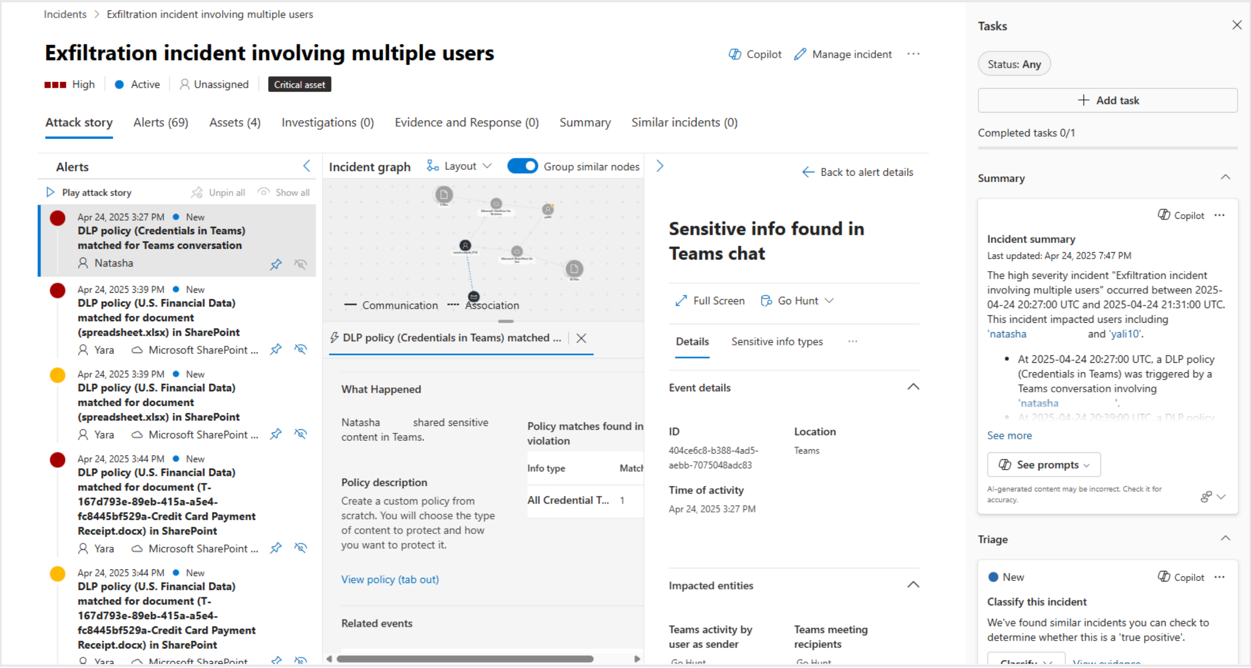
Investigate DLP alerts in Defender XDR

Step 1: Open the incidents queue

1. Go to the Microsoft Defender portal.
2. In the left navigation pane, select Incidents & alerts > Incidents.
3. Use the Service/detection source filter to select Data Loss Prevention.



Incidents > Exfiltration incident involving multiple users

Exfiltration incident involving multiple users

High | Active | Unassigned | Critical asset

Copilot | Manage incident | ···

Attack story | Alerts (69) | Assets (4) | Investigations (0) | Evidence and Response (0) | Summary | Similar incidents (0)

Alerts

Play attack story | Unpin all | Show all

- Apr 24, 2025 3:27 PM • New
  DLP policy (Credentials in Teams) matched for Teams conversation
  Natasha
- Apr 24, 2025 3:39 PM • New
  DLP policy (U.S. Financial Data) matched for document (spreadsheet.xlsx) in SharePoint
  Yara | Microsoft SharePoint ...
- Apr 24, 2025 3:39 PM • New
  DLP policy (U.S. Financial Data) matched for document (spreadsheet.xlsx) in SharePoint
  Yara | Microsoft SharePoint ...
- Apr 24, 2025 3:44 PM • New
  DLP policy (U.S. Financial Data) matched for document (T-167d793e-89eb-415a-a5e4-fc8445bf529a-Credit Card Payment Receipt.docx) in SharePoint
  Yara | Microsoft SharePoint ...
- Apr 24, 2025 3:44 PM • New
  DLP policy (U.S. Financial Data) matched for document (T-167d793e-89eb-415a-a5e4-fc8445bf529a-Credit Card Payment Receipt.docx) in SharePoint
  Yara | Microsoft SharePoint

Incident graph | Layout | Group similar nodes

— Communication ···· Association

DLP policy (Credentials in Teams) matched ...

What Happened

Natasha shared sensitive content in Teams.

Policy description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

View policy (tab out)

Related events

Policy matches found in violation

Info type	Match
All Credential T...	1

Back to alert details

Sensitive info found in Teams chat

Full Screen | Go Hunt

Details | Sensitive info types | ···

Event details

ID
404ce6c8-b388-4ad5-aebb-7075048adc83

Location
Teams

Time of activity
Apr 24, 2025 3:27 PM

Impacted entities

Teams activity by user as sender
Go Hunt

Teams meeting recipients
Go Hunt

Tasks

Status: Any

+ Add task

Completed tasks 0/1

Summary

Copilot ···

Incident summary

Last updated: Apr 24, 2025 7:47 PM

The high severity incident "Exfiltration incident involving multiple users" occurred between 2025-04-24 20:27:00 UTC and 2025-04-24 21:31:00 UTC. This incident impacted users including 'natasha and 'yali10'.

- At 2025-04-24 20:27:00 UTC, a DLP policy (Credentials in Teams) was triggered by a Teams conversation involving 'natasha '.
- At 2025-04-24 20:39:00 UTC, a DLP policy

See more

See prompts

AI-generated content may be incorrect. Check it for accuracy.

Triage

● New | Copilot ···

Classify this incident

We've found similar incidents you can check to determine whether this is a 'true positive'.

Classify | View evidence

This view shows incidents that include one or more DLP alerts. Each incident can contain multiple related alerts grouped together.

Step 2: Investigate a DLP alert

After an incident is identified in the queue, the next step is to examine the details of an individual alert. This helps you confirm what happened, determine whether the alert is valid, and decide what to do next.

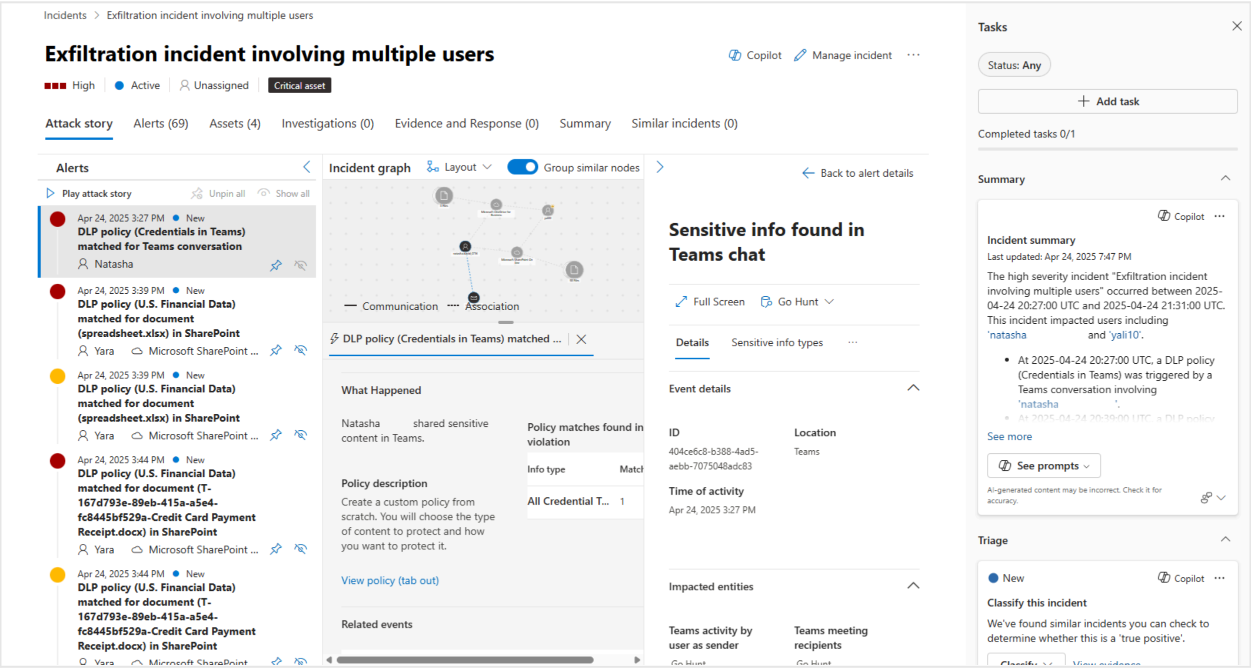
- Review the Alert story to understand what triggered the policy match.
- Use the Related events section to explore user activity like downloads, shares, or overrides.

- Open the Sensitive info types tab to see what types of sensitive content were detected.
- If permissions allow, access the Source tab to inspect the file involved in the alert.

You can copy the summary, regenerate it, or open the Security Copilot pane for deeper insights. The summary includes:

- Alert title and severity
- Matched policy and rule
- File details and access path
- User identity and associated activities

You can copy or refresh the summary, or open it in the Security Copilot pane for more context.



Exfiltration incident involving multiple users

Apr 24, 2025 3:27 PM • New
DLP policy (Credentials in Teams) matched for Teams conversation
Natasha

Apr 24, 2025 3:39 PM • New
DLP policy (U.S. Financial Data) matched for document (spreadsheet.xlsx) in SharePoint
Yara · Microsoft SharePoint ...

Apr 24, 2025 3:39 PM • New
DLP policy (U.S. Financial Data) matched for document (spreadsheet.xlsx) in SharePoint
Yara · Microsoft SharePoint ...

Apr 24, 2025 3:44 PM • New
DLP policy (U.S. Financial Data) matched for document (T-167d793e-89eb-415a-a5e4-fc8445bf529a-Credit Card Payment Receipt.docx) in SharePoint
Yara · Microsoft SharePoint ...

Apr 24, 2025 3:44 PM • New
DLP policy (U.S. Financial Data) matched for document (T-167d793e-89eb-415a-a5e4-fc8445bf529a-Credit Card Payment Receipt.docx) in SharePoint
Yara · Microsoft SharePoint

DLP policy (Credentials in Teams) matched ...

What Happened

Natasha shared sensitive content in Teams.

Policy matches found in violation

Info type	Matcl
All Credential T...	1

Policy description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

View policy (tab out)

Related events

Sensitive info found in Teams chat

Event details

ID: 404ce6c8-b388-4ad5-aebb-7075048adc83
Location: Teams
Time of activity: Apr 24, 2025 3:27 PM

Impacted entities

Teams activity by user as sender: Go Hunt
Teams meeting recipients: Go Hunt

Completed tasks 0/1

Incident summary
Last updated: Apr 24, 2025 7:47 PM

The high severity incident "Exfiltration incident involving multiple users" occurred between 2025-04-24 20:27:00 UTC and 2025-04-24 21:31:00 UTC. This incident impacted users including 'natasha and 'yali10'.

- At 2025-04-24 20:27:00 UTC, a DLP policy (Credentials in Teams) was triggered by a Teams conversation involving 'natasha '.
- At 2025-04-24 20:39:00 UTC, a DLP policy

AI-generated content may be incorrect. Check it for accuracy.

New

Classify this incident

We've found similar incidents you can check to determine whether this is a 'true positive'.

Step 3: Take response actions

Based on your investigation, you can take action directly from the alert view:

- Download email (for Exchange alerts)
- Apply sensitivity label, Unshare, Delete, or Download (for SharePoint or OneDrive files)
- Apply retention label

- Send email notification
- Withdraw feedback if the alert was marked incorrectly

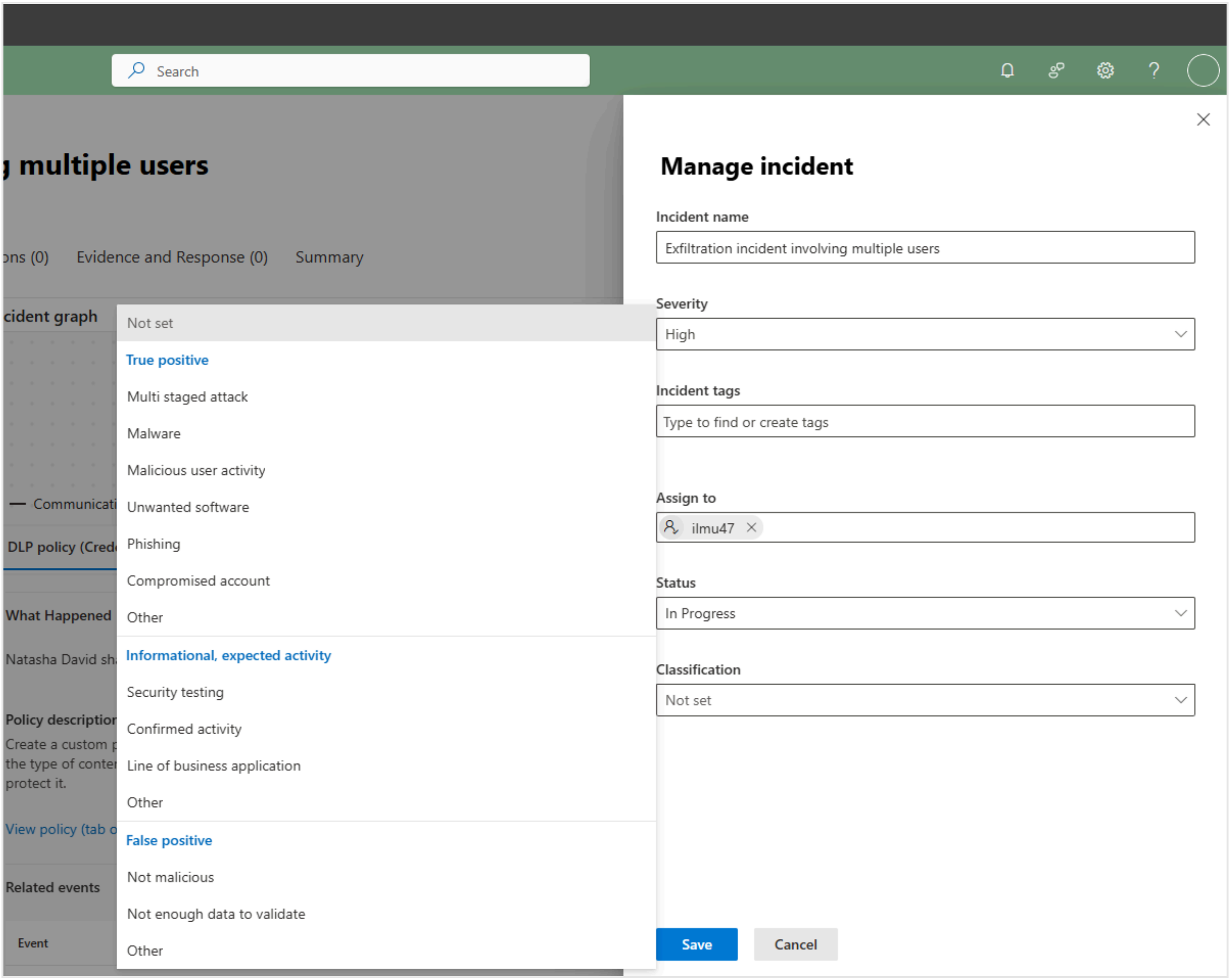
To respond at the user level, select the User card to view profile details and take actions like resetting passwords or disabling accounts.

For device-based DLP alerts, select the Device card to view device details and isolate or manage the device.

Step 4: Manage the incident

To complete incident handling, return to the incident summary page and select Manage incident. You can:

- Set the incident Severity
- Add or create Incident tags
- Assign the incident to an analyst or response team
- Update the Status to reflect progress (for example: In Progress, Resolved)
- Choose a Classification, such as True Positive or False Positive, and specify a reason (like Malicious user activity or Security testing)



Manage incident

Incident name: Exfiltration incident involving multiple users

Severity: High

Incident tags: Type to find or create tags

Assign to: ilmu47

Status: In Progress

Classification: Not set

These fields help organize and close out the investigation for future reference and auditing.

Use advanced hunting for deeper investigation

Advanced hunting lets you query user, file, and activity data across workloads using the CloudAppEvents table. This table contains audit logs from across Microsoft 365 workloads, including:

- Exchange
- SharePoint
- OneDrive
- Devices

To start hunting:

1. In the Defender portal, select Advanced hunting.
2. Use a built-in query, or select Go Hunt from an event in the alert details.
3. Defender provides contextual queries based on the event source, such as:
    - File shared with
    - File activities
    - Site activity
    - User DLP violations (last 30 days)

You can run, customize, or save the query to track related activity.

Extend your investigation with Microsoft Sentinel

While Defender XDR offers deep alert-level investigation, Microsoft Sentinel adds cross-platform correlation and automation. Microsoft Sentinel can bring DLP insights into broader investigations and workflows alongside other Microsoft and non-Microsoft data sources.

If your organization uses Microsoft Sentinel, you can integrate DLP alerts from Microsoft Defender XDR into Microsoft Sentinel for:

- Cross-platform investigation
- Custom correlation rules
- Automated response using SOAR (security orchestration, automation, and response)

To get started:

1. Use the Microsoft Defender XDR connector in Microsoft Sentinel to import DLP alerts and incidents.
2. Enable the CloudAppEvents connector to ingest audit logs.
3. Use KQL queries in Microsoft Sentinel to correlate alerts and investigate root causes.

Example query:

Kusto

Copy

```
let Alert = SecurityAlert
| where TimeGenerated > ago(30d)
| where SystemAlertId == "INSERT_ALERT_ID"; // insert the
systemAlertID here
CloudAppEvents
| extend correlationId1 =
parse_json(tostring(RawEventData.Data)).cid
| extend correlationId = tostring(correlationId1)
| join kind=inner Alert on $left.correlationId ==
$right.AlertType
| where RawEventData.CreationTime > StartTime and
RawEventData.CreationTime < EndTime
```

This query identifies activity related to a specific alert using the CloudAppEvents table.

Microsoft Defender XDR helps security teams respond to data loss incidents by grouping alerts, enriching them with context, and enabling fast investigation. With integrated advanced hunting and response actions, DLP alert handling becomes part of a broader security operations workflow.

Whether you're managing alerts in Microsoft Defender or extending your investigation with Microsoft Sentinel, these tools help bring clarity to complex data loss events. With capabilities for alert correlation, activity analysis, and automated response, security teams can act faster and with greater confidence to reduce data risk.