Microsoft Security

Security einfach(er) gemacht!

Hannes Schneider
Solution Engineer Security

Aktuelle Herausforderungen

Wachsende Angriffsflächen	**Regulatorik & Compliance**	**Ransomware & Malware**
Fachkräftemangel	**Supply-Chain-Risiken**	**Phishing & Social Engineering**
	Tool-Sprawl & Komplexität	

Quellen Fortra Cybersecurity Survey 2024, KPMG Cyber Security Insights 2024, Deloitte Cyber Threat Report 2024/2025, Secureframe 2025 Benchmark Report, Microsoft Digital Defense Report 2024

Lösungen

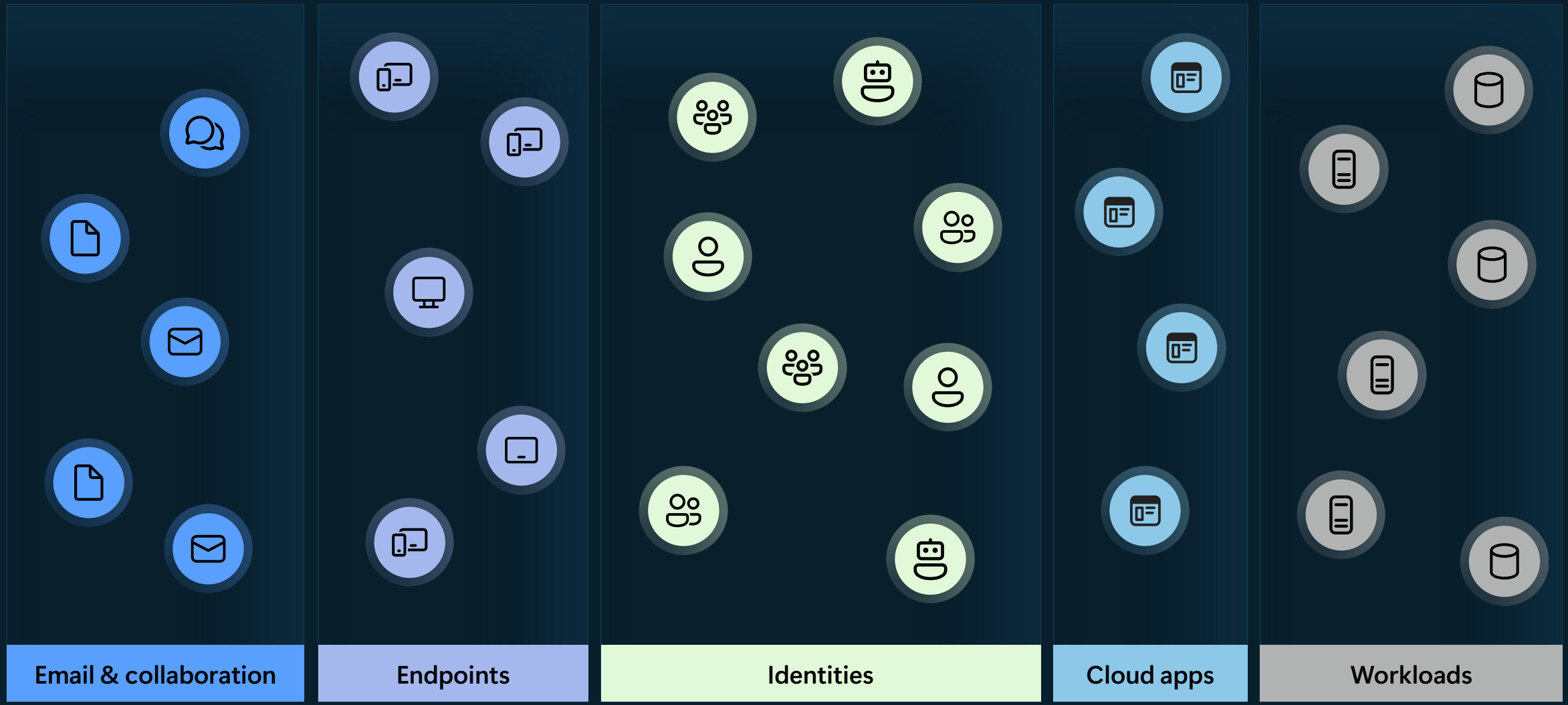
Wachsende Angriffsflächen	Sichtbarkeit
Fachkräftemangel	KI-Assistenz
Regulatorik & Compliance	Automatisierung & Nachweisbarkeit
Supply-Chain-Risiken	Zero Trust
Ransomware & Malware	Prävention & schnelle Reaktion
Phishing & Social Engineering	Identitätsschutz
Tool-Sprawl & Komplexität	Plattformisierung

Komplexität

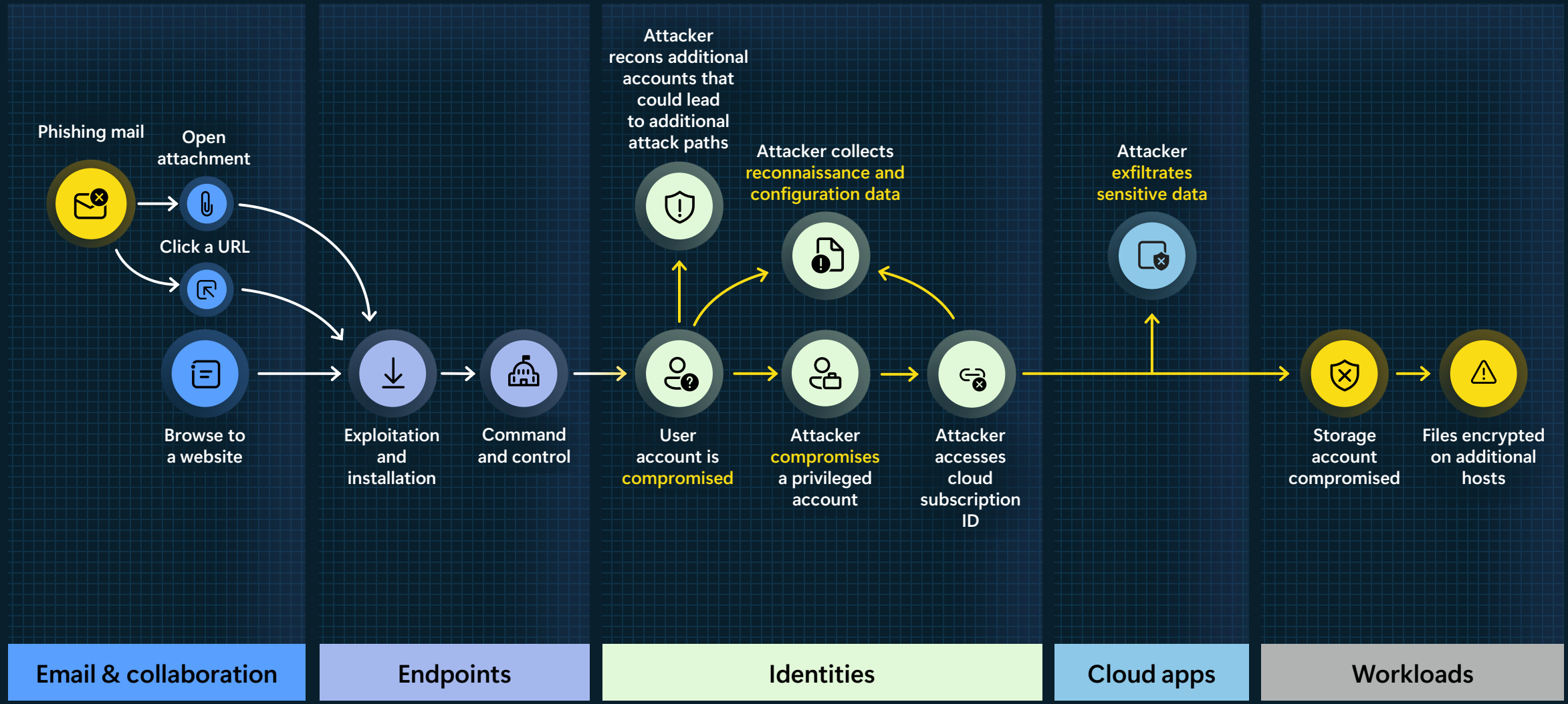
Hybride Umgebungen

Change Management

Viele Unternehmen arbeiten noch in Silos



Angreifer denken in Diagrammen und nutzen Lücken in einer Organisation aus



Microsoft Defender

Die umfassendste Cybersicherheitslösung der Branche

Security information and event management (SIEM)	→	Flexible Erkennungsreaktion auf allen Kanälen
Extended detection and response (XDR)	→	Schutz über Endpunkte, Identitäten, E-Mails, SaaS-Anwendungen, Workloads und Daten hinweg
Cloud security	→	Schutz vom Code zur Runtime
Exposure management	→	Veringerung der Angriffsfläche der gesamten Infra
Threat intelligence	→	Umfassende Bedrohungseinblicke

Security platform

350+ Connectoren

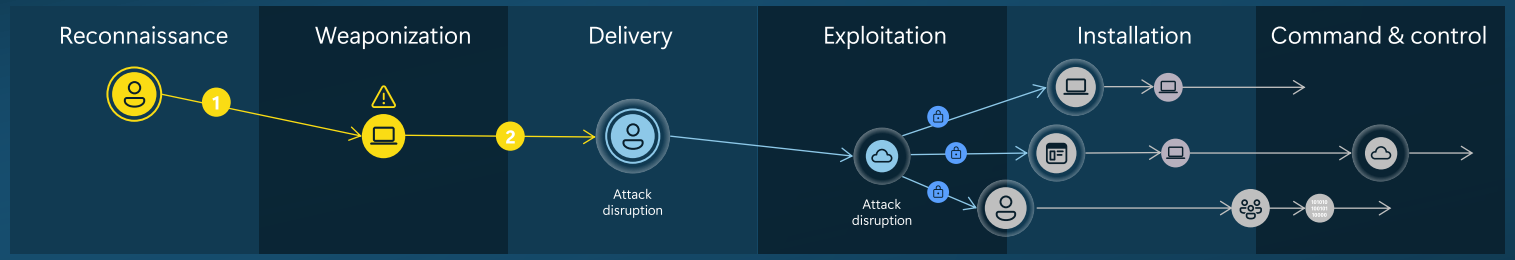
Antizipieren und Angriffe stoppen

Microsoft Defender

AI-powered SOC

Microsoft Security Copilot

Real-time, coordinated defense



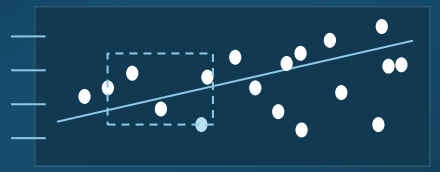
Security Copilot agents

TI Briefing Agent

Phishing Triage Agent

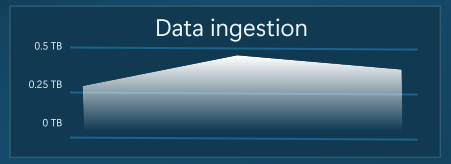
Predictive graphing

Prioritized attack paths



Attacker pivot prediction during attack

SOC optimizations

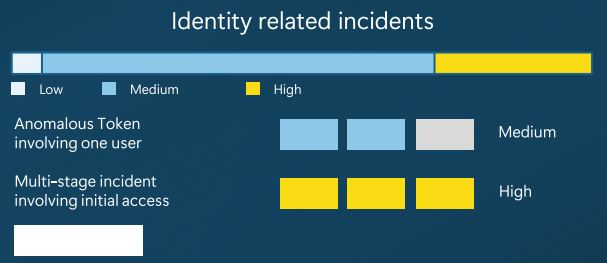


Recommended actions

Active	In progress	Completed
24	0	24

Threat intelligence

Identity threat detection and response

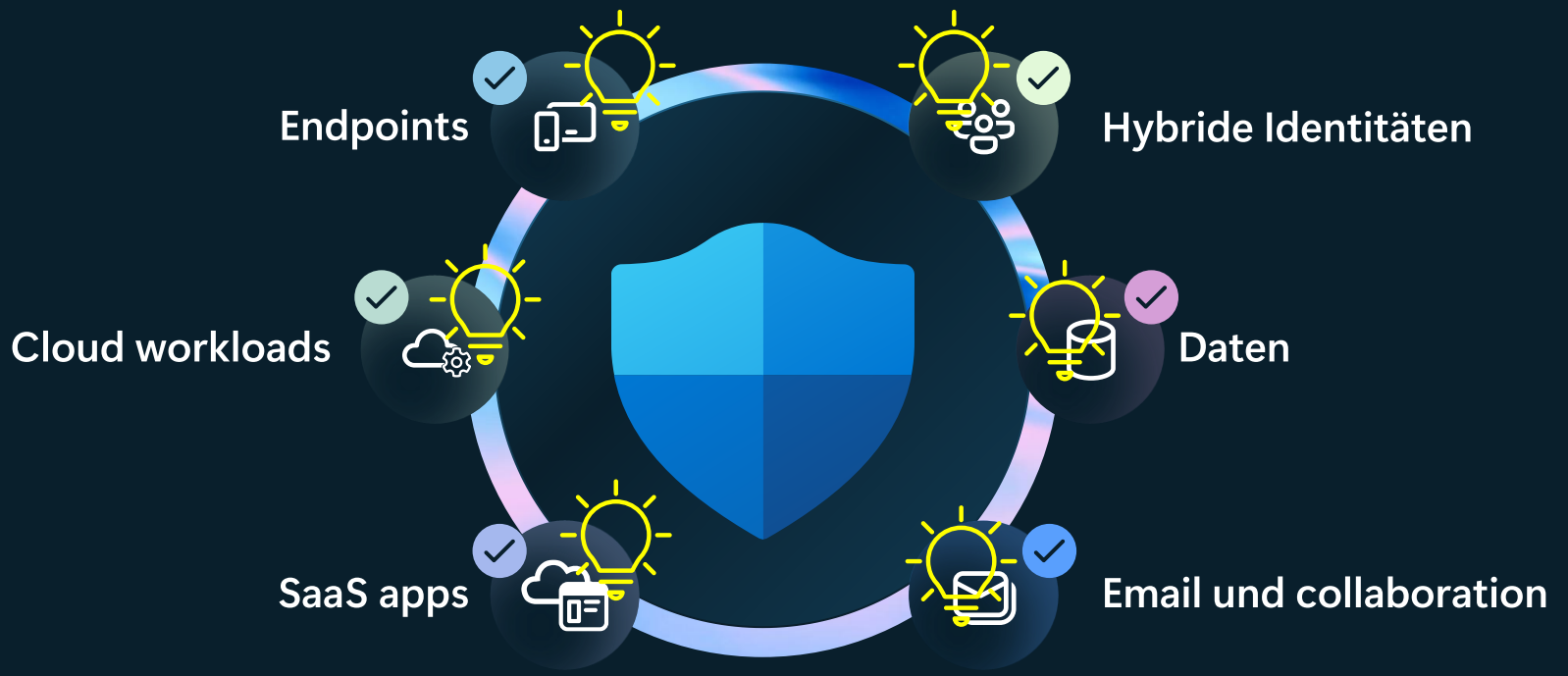


Microsoft Sentinel

Microsoft Entra

Microsoft Defender XDR

Ein domänenübergreifendes SOC-Erlebnis, das nativen Schutz auf all Ihren Geräten, Plattformen und Clouds bietet

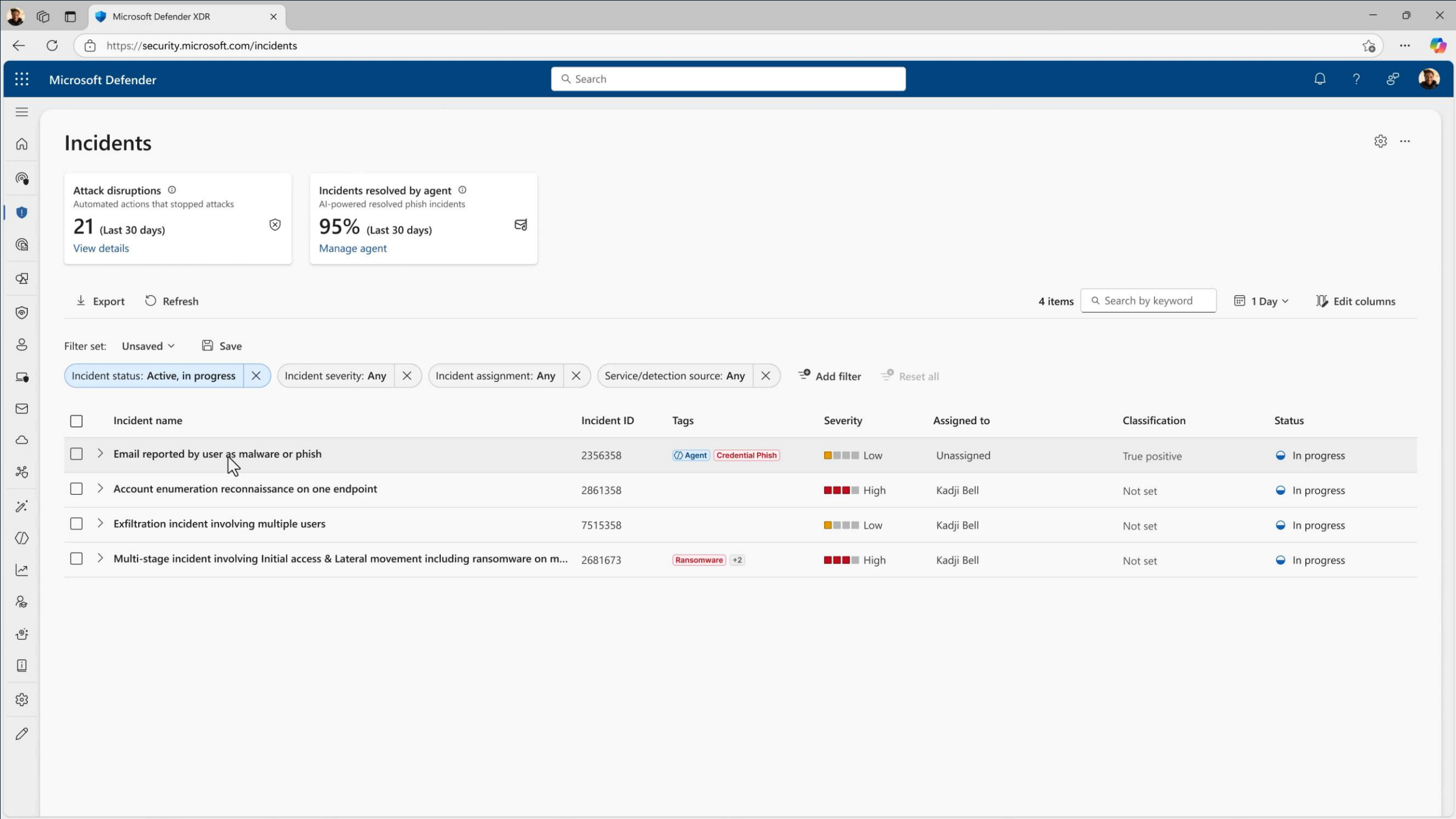


Prevent | Detect | Respond

Beispiele aus aktuellen Projekten

Demo: Security Copilot & Privilege Identity Management

Security Copilot Agenten: Phishing Triage


Microsoft Defender XDR
https://security.microsoft.com/incidents
Microsoft Defender
Search
Incidents
Attack disruptions
Automated actions that stopped attacks
21 (Last 30 days)
View details
Incidents resolved by agent
AI-powered resolved phish incidents
95% (Last 30 days)
Manage agent
Export
Refresh
4 items
Search by keyword
1 Day
Edit columns
Filter set: Unsaved
Save
Incident status: Active, in progress
Incident severity: Any
Incident assignment: Any
Service/detection source: Any
Add filter
Reset all
Incident name
Incident ID
Tags
Severity
Assigned to
Classification
Status
Email reported by user as malware or phish
2356358
Agent
Credential Phish
Low
Unassigned
True positive
In progress
Account enumeration reconnaissance on one endpoint
2861358
High
Kadji Bell
Not set
In progress
Exfiltration incident involving multiple users
7515358
Low
Kadji Bell
Not set
In progress
Multi-stage incident involving Initial access & Lateral movement including ransomware on m...
2681673
Ransomware
+2
High
Kadji Bell
Not set
In progress

ent: Any | Service/detection source: Any | Add filter | Reset all

Incident ID	Tags	Severity	Assigned to
2356358	Agent, Credential Phish	Low	Unassigned
2861358		High	Kadji Bell
7515358		Low	Kadji Bell
2681673	Ransomware +2	High	Kadji Bell

are on m...

Completed — Phishing Triage Agent

Classify phishing email attempt as 'True positive'

A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipients to click on a link due to an impending deadline. The urgency and request to click on a link are common characteristics of phishing emails. However, sandbox analysis of the email and the URLs contained within it did not identify any malicious destinations or attempts to deceive the user. Despite this, the legitimacy of the email remains unclear without further information. Therefore, out of an abundance of caution, the analyst agent decided to classify the email as a true positive pending further review.

Show less

Change classification | View agent activity

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

Incident details

Assigned to
Unassigned

Incident ID
2356358

Classification
True positive

Categories
Initial access

First activity

Last activity

Open incident page

Microsoft Defender XDR

https://security.microsoft.com/incident/2356358

Microsoft Defender

Search

Incidents > Email reported by user as malware or phish

2356358: Email reported by user as malware or phish

Low | In progress | Unassigned | True positive | Agent | Credential Phish

Attack story | Activity | Alerts (1) | Assets (2) | Evidence and response | Similar incident | Summary

Detection & categories

Active alerts
1\1

Categories
Initial access

First activity
3/18/25 at 13:18 AM

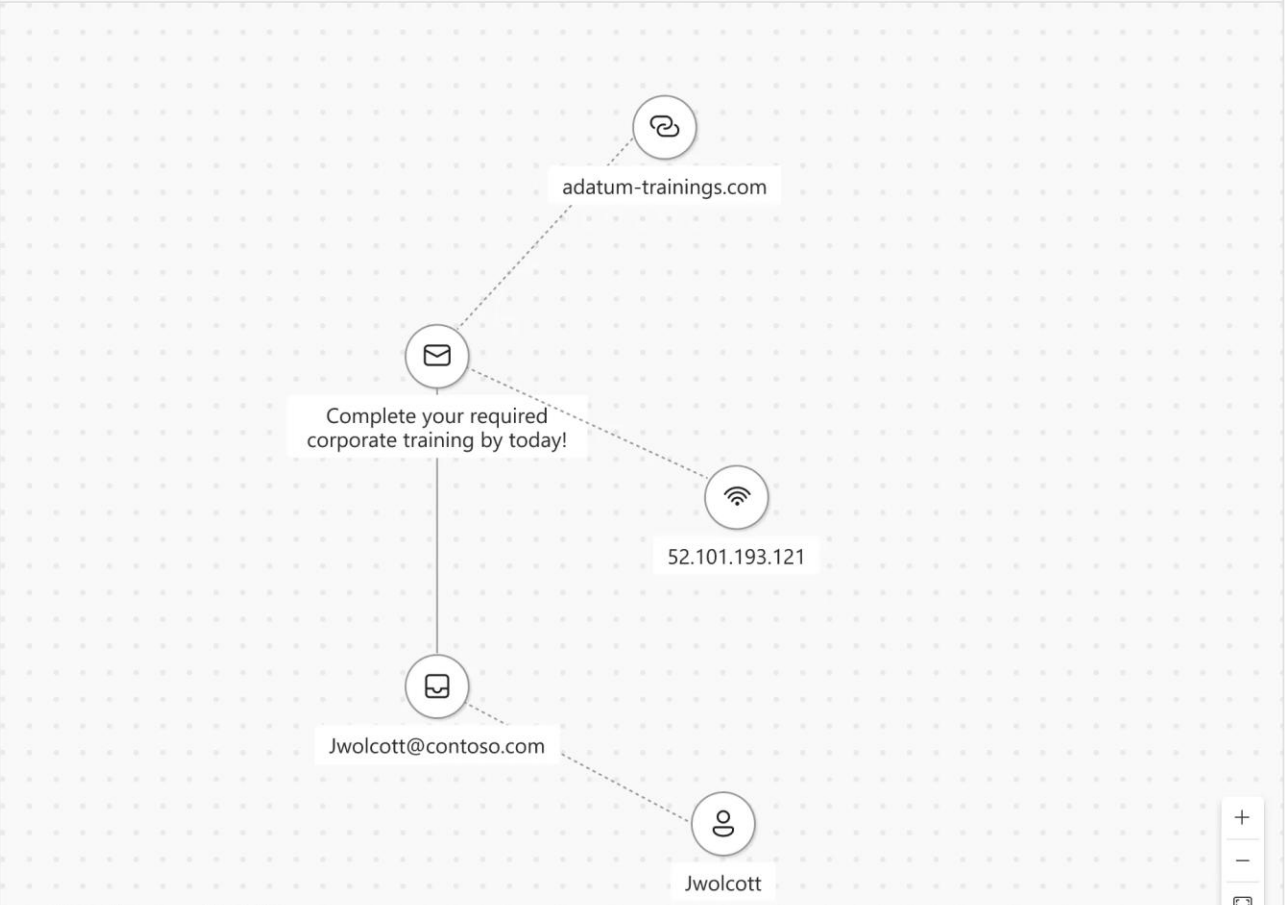
Last activity
3/18/25 at 13:32 AM

Alerts

3/18/25 at 13:18 AM | Active
Email reported by user as malware or phish
Jonathan Wolcott Jonathan Wolcott

Incident graph

Group similar entities | Layout | New query tab



Tasks

Add task

Completed tasks 4/4

Summary

Copilot

Incident summary
3/18/25 at 13:38 AM

The low severity incident "Email reported by user as malware or phish" occurred between 2025-03-18 13:18:00 UTC and 2025-03-18 13:28:00 UTC. It was tagged as Credential Phish. This incident impacted...

Show more

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

Triage

Completed | Phishing Triage Agent

Classify phishing email attempt as 'true positive'

A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipients to click on a link due to an impending deadline. The urgency and request to click on a link are common characteristics of phishing emails. However, sandbox analysis of the email and the URLs contained within it did not identify any malicious destinations or attempts to deceive the user. Despite this, the legitimacy of the email remains unclear without further information. Therefore, out of an abundance of caution, the analyst agent decided to classify the email as a true positive pending further review.

See less

Change classification | View agent activity

Microsoft Defender XDR

https://security.microsoft.com/incident/2356358/activity

Microsoft Defender

Search

Incidents > Email reported by user as malware or phish

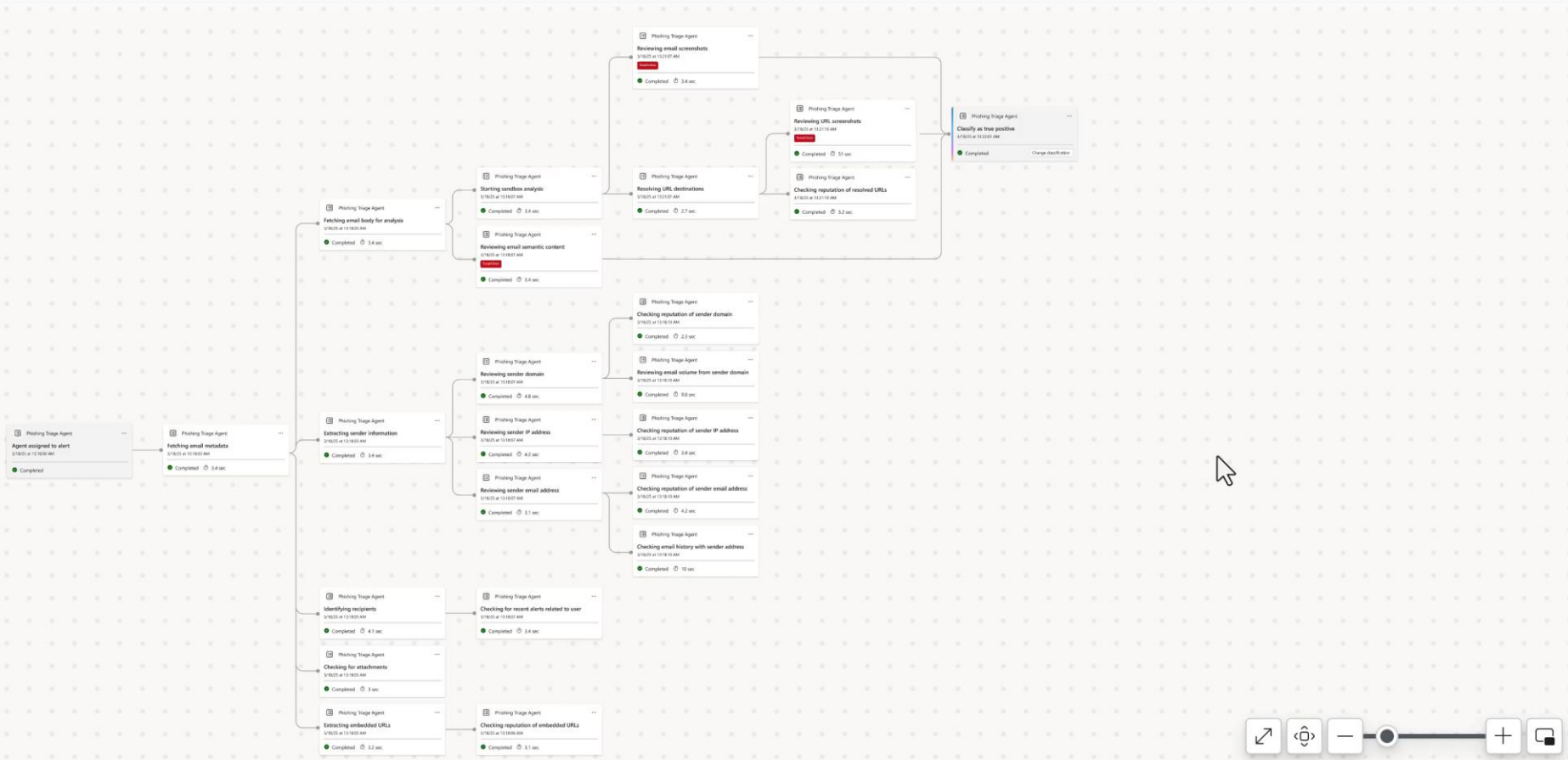
2356358: Email reported by user as malware or phish

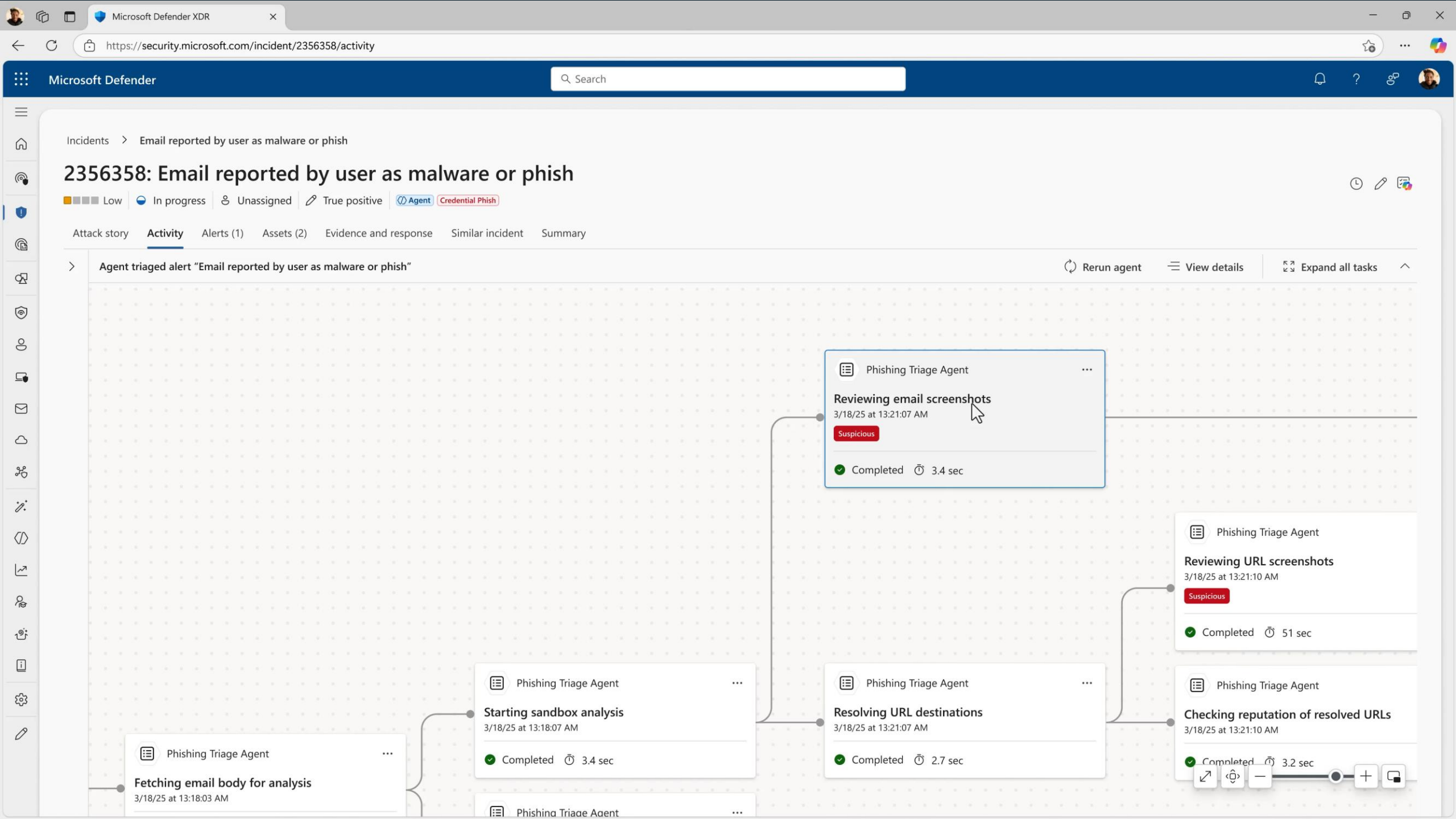
Low | In progress | Unassigned | True positive | Agent | Credential Phish

Attack story | Activity | Alerts (1) | Assets (2) | Evidence and response | Similar incident | Summary

Agent triaged alert "Email reported by user as malware or phish"

Rerun agent | View details | Expand all tasks




Microsoft Defender XDR
https://security.microsoft.com/incident/2356358/activity
Microsoft Defender
Search
Incidents
Email reported by user as malware or phish
2356358: Email reported by user as malware or phish
Low
In progress
Unassigned
True positive
Agent
Credential Phish
Attack story
Activity
Alerts (1)
Assets (2)
Evidence and response
Similar incident
Summary
Agent triaged alert "Email reported by user as malware or phish"
Rerun agent
View details
Expand all tasks
Phishing Triage Agent
Reviewing email screenshots
3/18/25 at 13:21:07 AM
Suspicious
Completed
3.4 sec
Phishing Triage Agent
Reviewing URL screenshots
3/18/25 at 13:21:10 AM
Suspicious
Completed
51 sec
Phishing Triage Agent
Starting sandbox analysis
3/18/25 at 13:18:07 AM
Completed
3.4 sec
Phishing Triage Agent
Resolving URL destinations
3/18/25 at 13:21:07 AM
Completed
2.7 sec
Phishing Triage Agent
Checking reputation of resolved URLs
3/18/25 at 13:21:10 AM
Completed
3.2 sec
Phishing Triage Agent
Fetching email body for analysis
3/18/25 at 13:18:03 AM
Phishing Triage Agent

Microsoft Defender XDR

https://security.microsoft.com/incident/2356358/activity

Microsoft Defender

Search

Incidents > Email reported by user as malware or phish

2356358: Email reported by user as malware or phish

Low | In progress | Unassigned | True positive | Agent | Credential Phish

Attack story | Activity | Alerts (1) | Assets (2) | Evidence and response | Similar incident | Summary

Agent triaged alert "Email reported by user as malware or phish"

Phishing Triage Agent
Fetching email body for analysis
3/18/25 at 13:18:03 AM

Phishing Triage Agent
Starting sandbox analysis
3/18/25 at 13:18:07 AM
Completed 3.4 sec

Phishing Triage Agent
Resolving URL destinations
3/18/25 at 13:21:07 AM
Completed 2.7 sec

Phishing Triage Agent
Reviewing email screenshots
3/18/25 at 13:21:07 AM
Suspicious
Completed 3.4 sec

Reviewing email screenshots

Completed | Suspicious

Final verdict

A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipients to click on a link due to an impending deadline. The urgency and request to click on a link are common characteristics of phishing emails. However, sandbox analysis of the email and the URLs contained within it did not identify any malicious destinations or attempts to deceive the user. Despite this, the legitimacy of the email remains unclear without further information. Therefore, out of an abundance of caution, the analyst agent decided to classify the email as a true positive pending further review.

Show less

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

Investigation details

Run by
Phishing Triage Agent

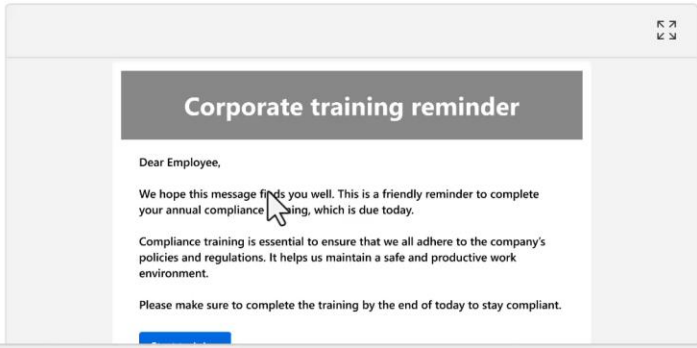
Duration
34 min

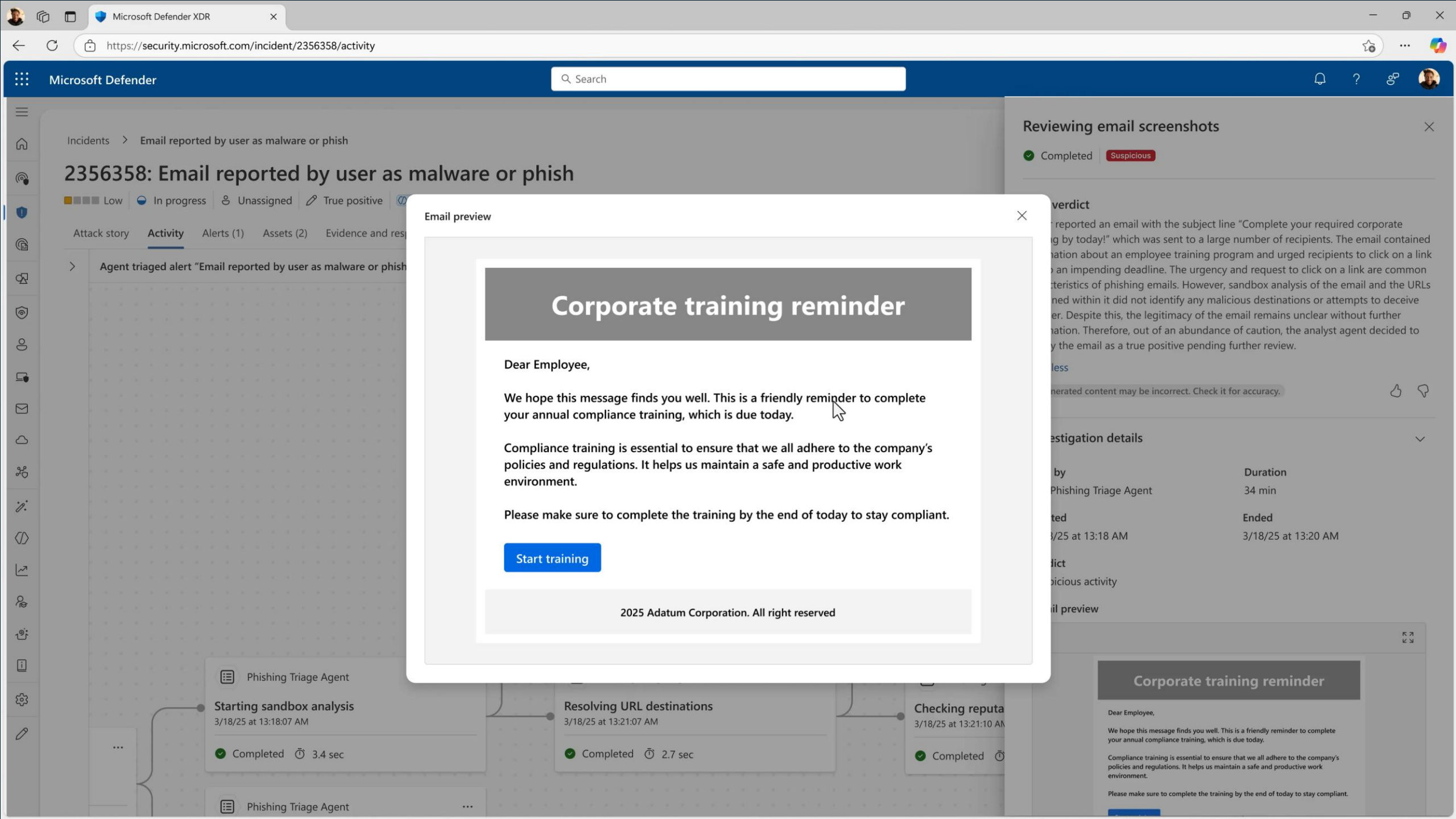
Started
3/18/25 at 13:18 AM

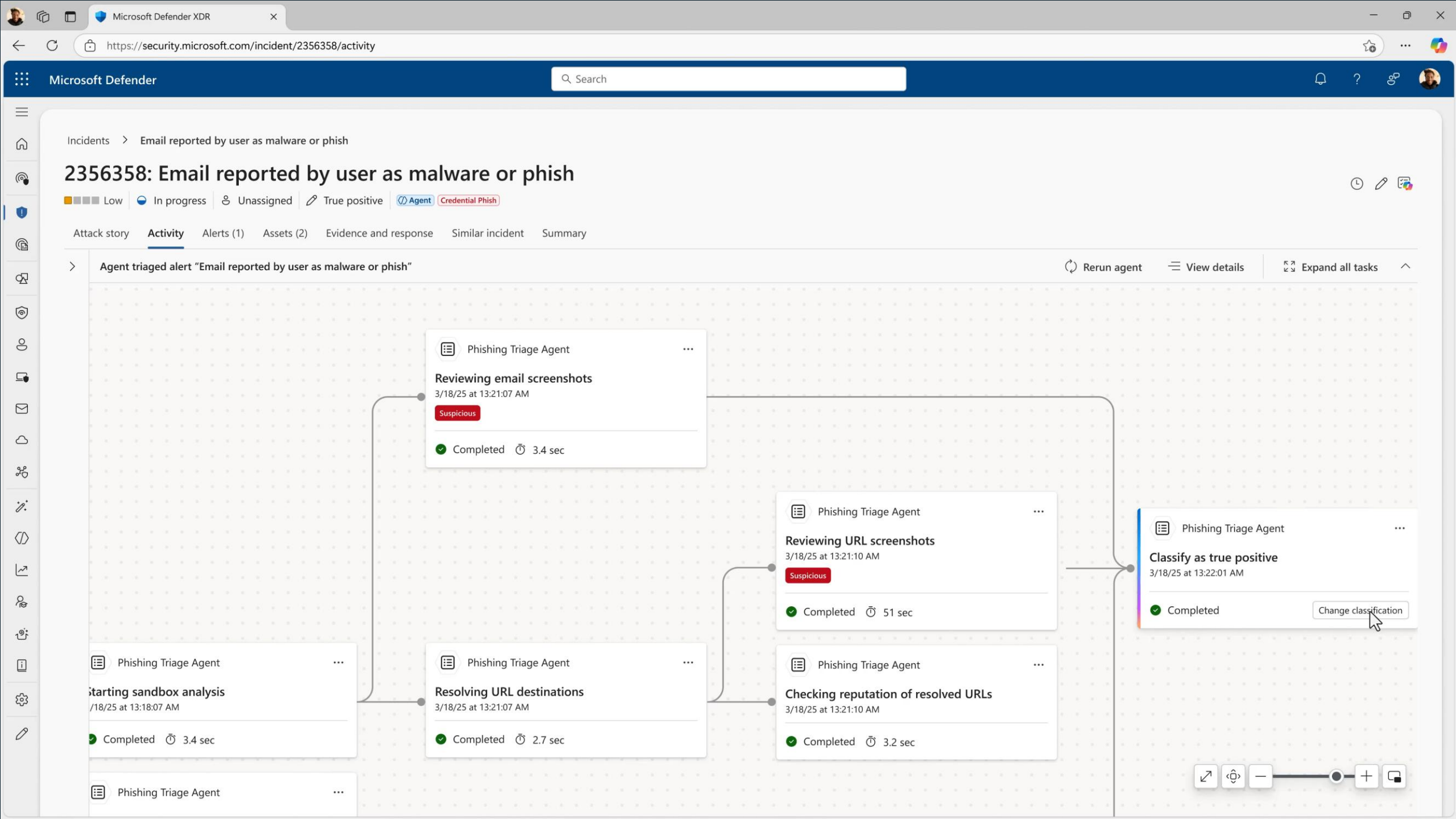
Ended
3/18/25 at 13:20 AM

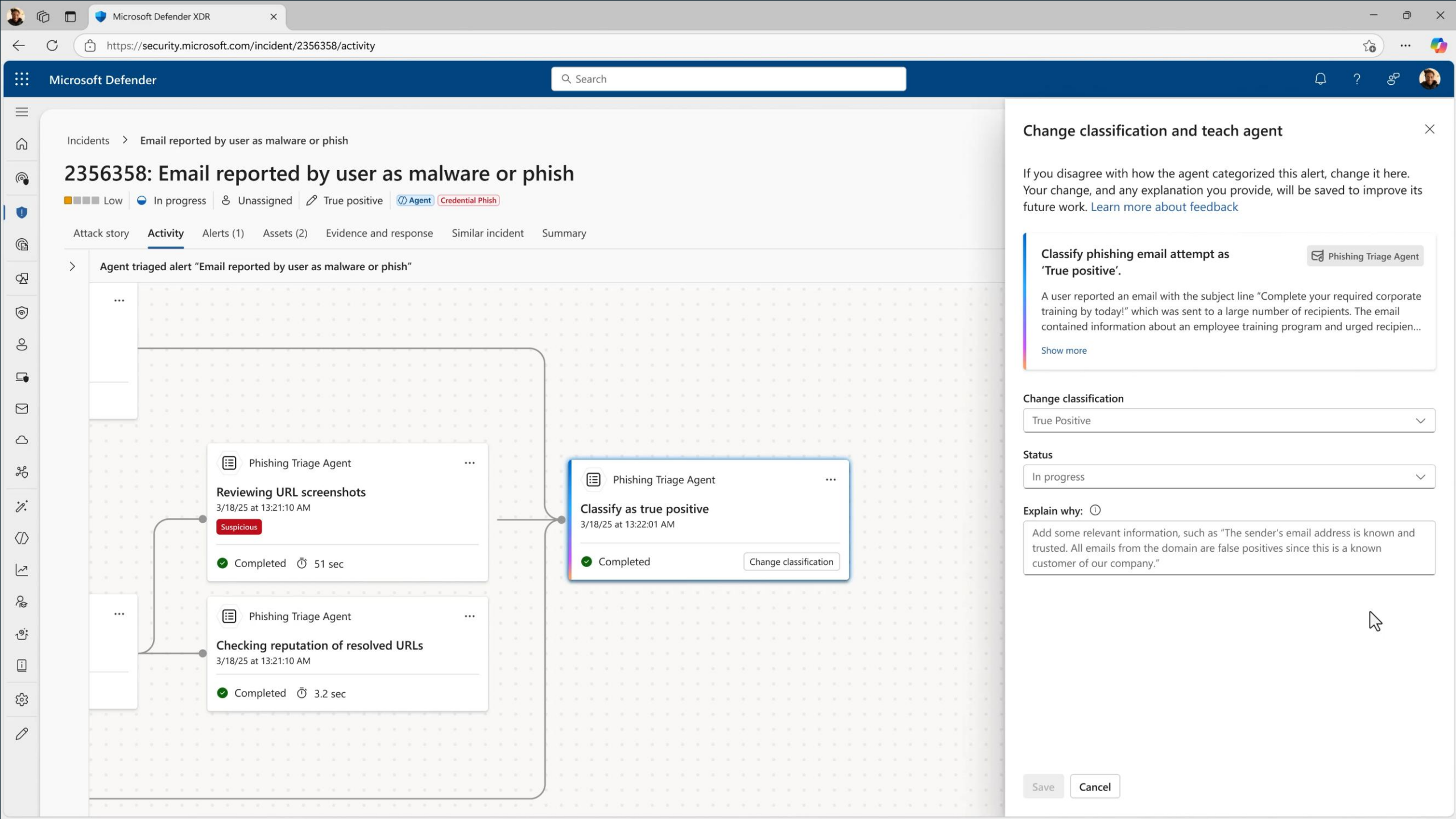
Verdict
Suspicious activity

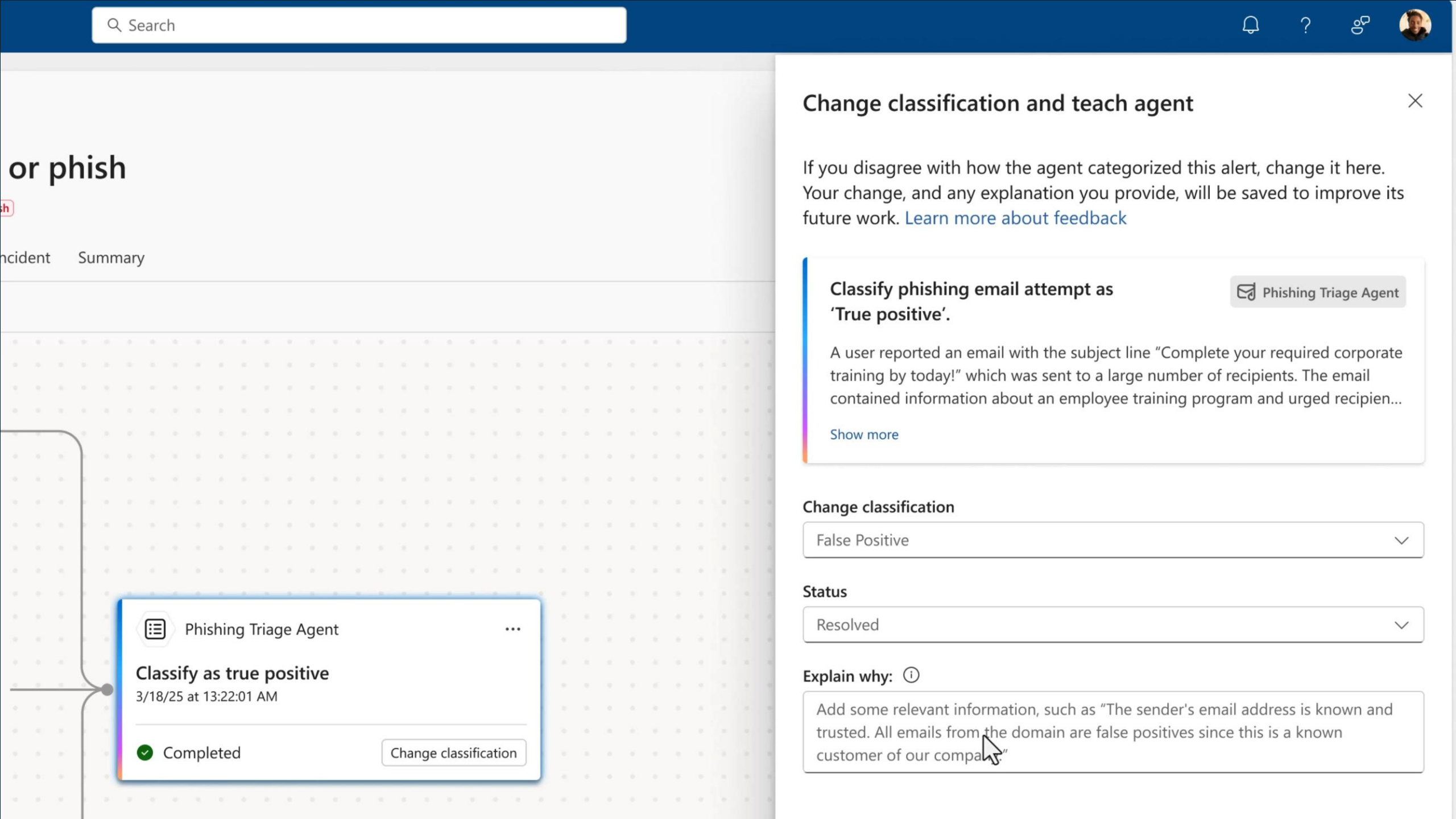
Email preview

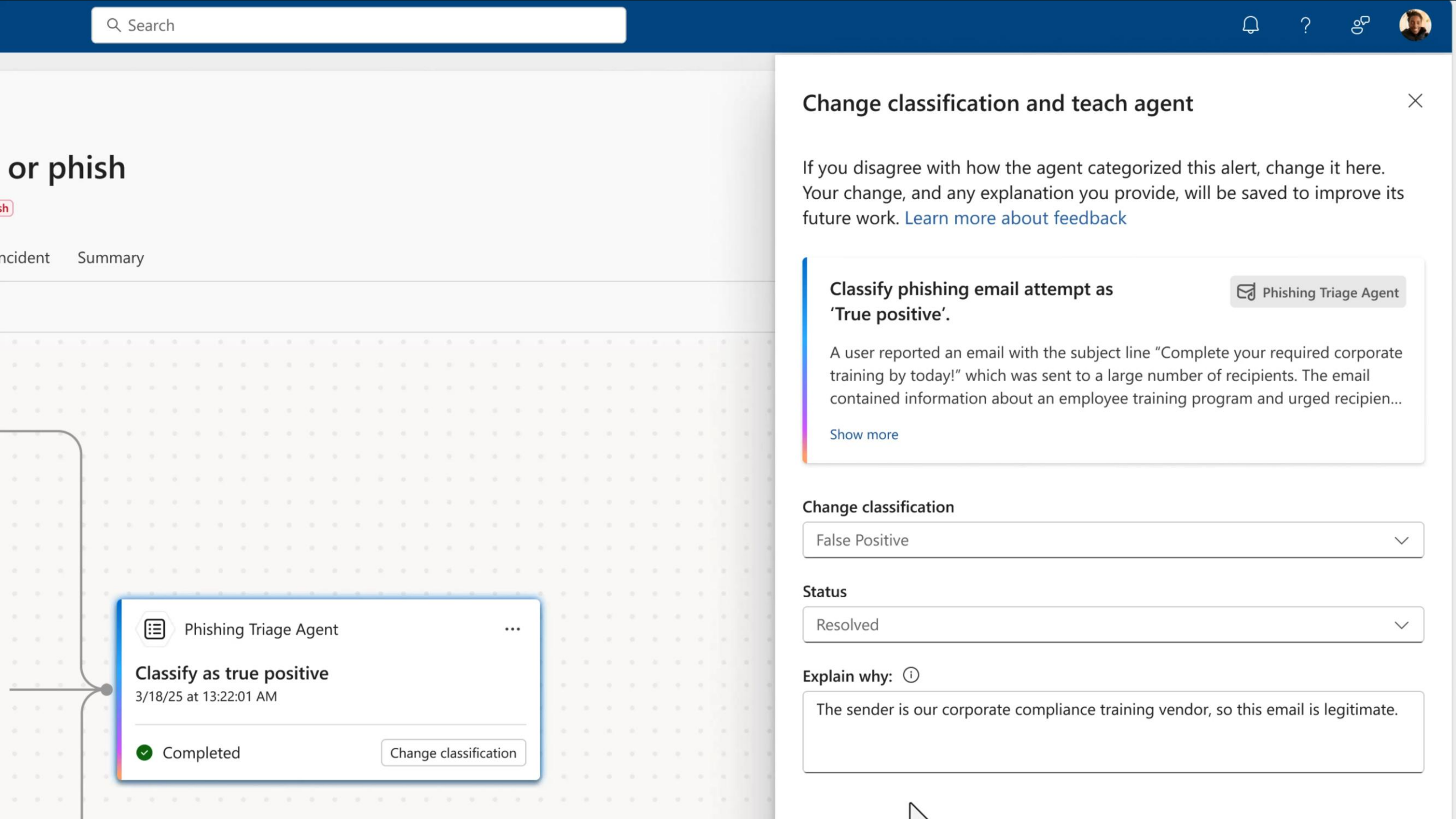


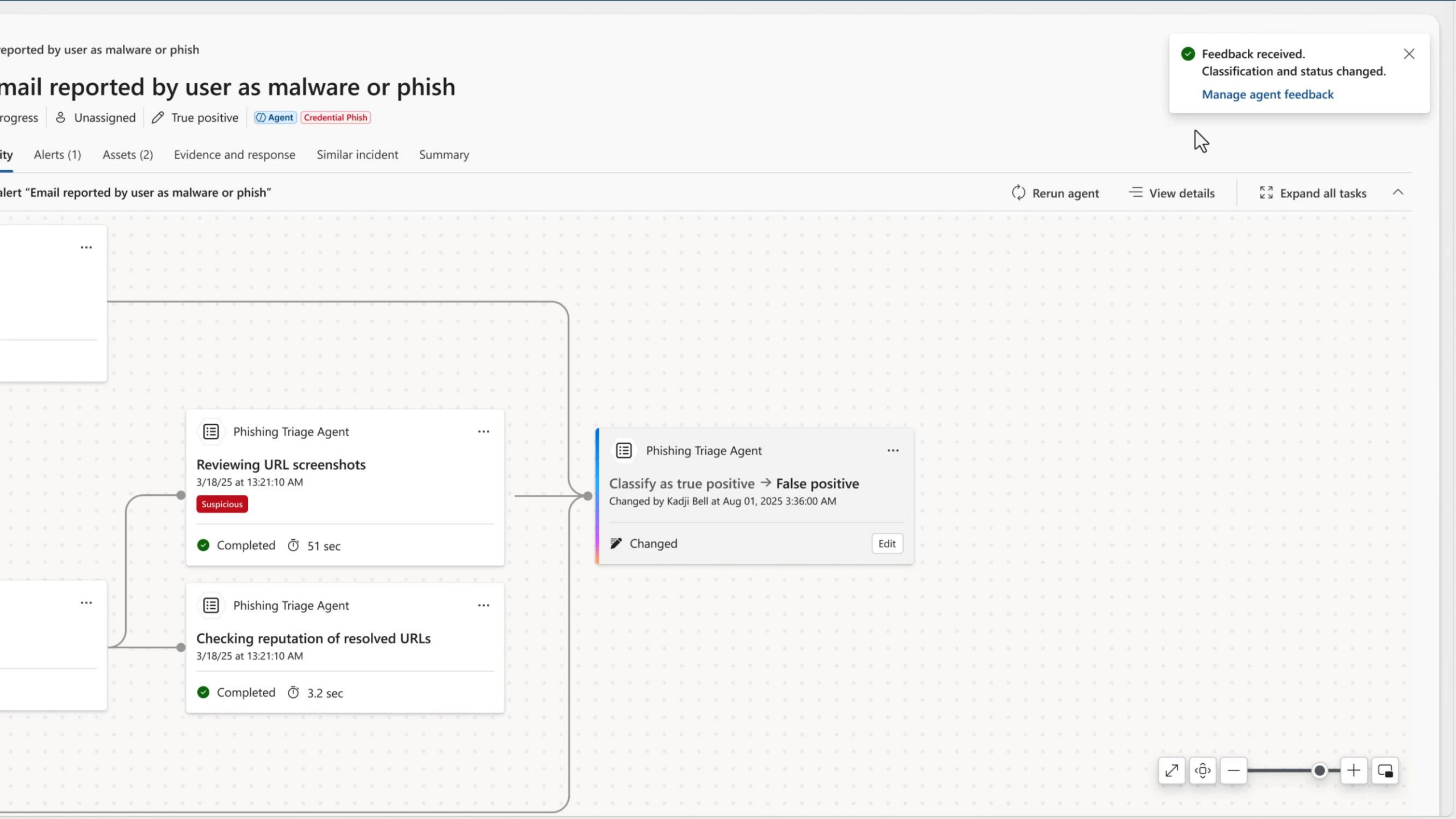

Microsoft Defender XDR
https://security.microsoft.com/incident/2356358/activity
Microsoft Defender
Search
Incidents
Email reported by user as malware or phish
2356358: Email reported by user as malware or phish
Low
In progress
Unassigned
True positive
Attack story
Activity
Alerts (1)
Assets (2)
Agent triaged alert "Email reported by user as malware or phish
Email preview
Corporate training reminder
Dear Employee,
We hope this message finds you well. This is a friendly reminder to complete your annual compliance training, which is due today.
Compliance training is essential to ensure that we all adhere to the company's policies and regulations. It helps us maintain a safe and productive work environment.
Please make sure to complete the training by the end of today to stay compliant.
Start training
2025 Adatum Corporation. All right reserved
Reviewing email screenshots
Completed
Suspicious
verdict
reported an email with the subject line "Complete your required corporate
by today!" which was sent to a large number of recipients. The email contained
nation about an employee training program and urged recipients to click on a link
an impending deadline. The urgency and request to click on a link are common
teristics of phishing emails. However, sandbox analysis of the email and the URLs
ned within it did not identify any malicious destinations or attempts to deceive
er. Despite this, the legitimacy of the email remains unclear without further
nation. Therefore, out of an abundance of caution, the analyst agent decided to
the email as a true positive pending further review.
less
nerated content may be incorrect. Check it for accuracy.
estigation details
by
Phishing Triage Agent
Duration
34 min
ted
/25 at 13:18 AM
Ended
3/18/25 at 13:20 AM
dict
icious activity
il preview
Phishing Triage Agent
Starting sandbox analysis
3/18/25 at 13:18:07 AM
Completed
3.4 sec
Resolving URL destinations
3/18/25 at 13:21:07 AM
Completed
2.7 sec
Checking reputa
3/18/25 at 13:21:10 AM
Completed
Phishing Triage Agent

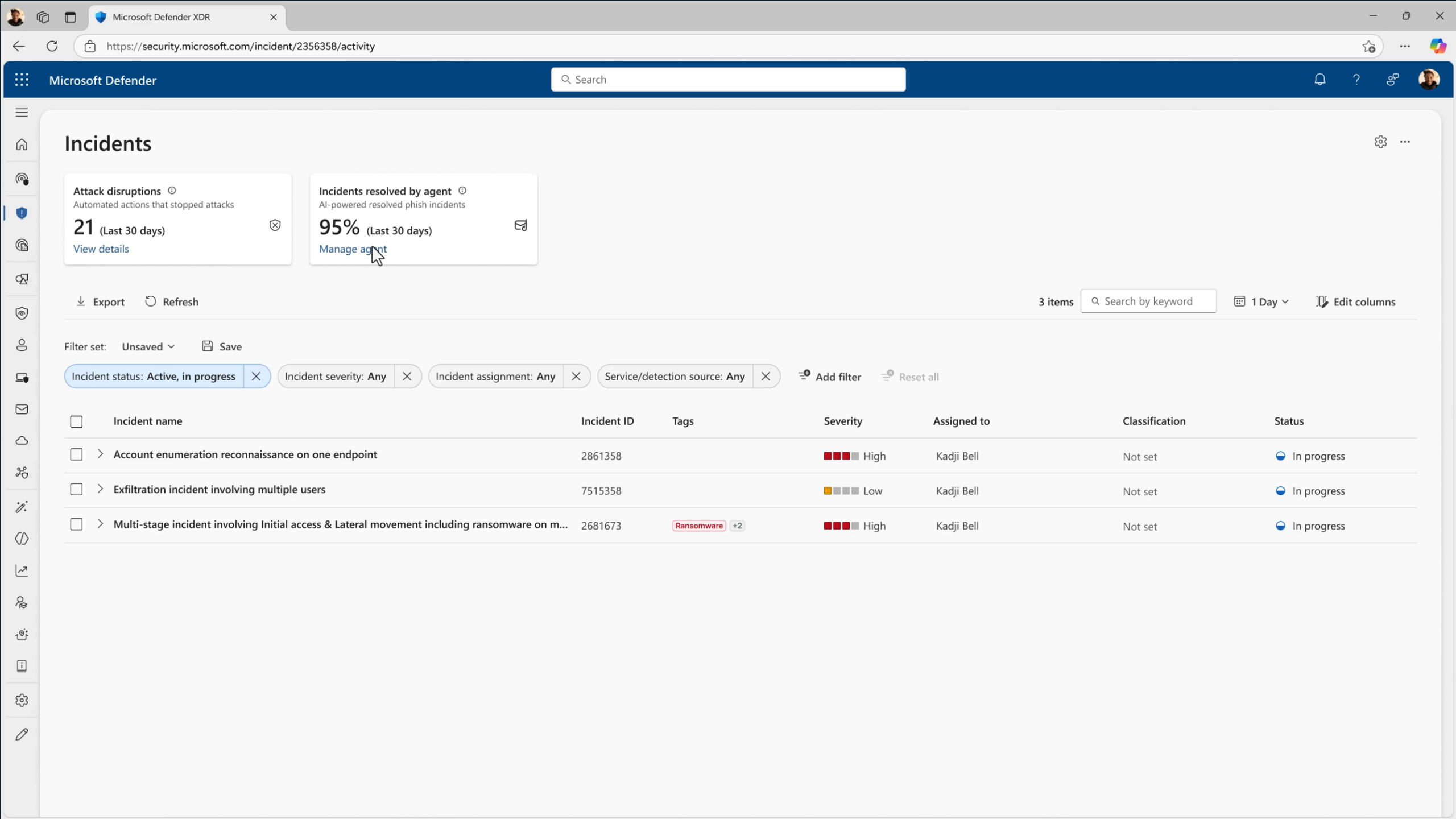

Microsoft Defender XDR
https://security.microsoft.com/incident/2356358/activity
Microsoft Defender
Search
Incidents
Email reported by user as malware or phish
2356358: Email reported by user as malware or phish
Low
In progress
Unassigned
True positive
Agent
Credential Phish
Attack story
Activity
Alerts (1)
Assets (2)
Evidence and response
Similar incident
Summary
Agent triaged alert "Email reported by user as malware or phish"
Rerun agent
View details
Expand all tasks
Phishing Triage Agent
Reviewing email screenshots
3/18/25 at 13:21:07 AM
Suspicious
Completed
3.4 sec
Phishing Triage Agent
Reviewing URL screenshots
3/18/25 at 13:21:10 AM
Suspicious
Completed
51 sec
Phishing Triage Agent
Classify as true positive
3/18/25 at 13:22:01 AM
Completed
Change classification
Phishing Triage Agent
Starting sandbox analysis
/18/25 at 13:18:07 AM
Completed
3.4 sec
Phishing Triage Agent
Resolving URL destinations
3/18/25 at 13:21:07 AM
Completed
2.7 sec
Phishing Triage Agent
Checking reputation of resolved URLs
3/18/25 at 13:21:10 AM
Completed
3.2 sec
Phishing Triage Agent


Microsoft Defender XDR
https://security.microsoft.com/incident/2356358/activity
Microsoft Defender
Search
Incidents
Email reported by user as malware or phish
2356358: Email reported by user as malware or phish
Low
In progress
Unassigned
True positive
Agent
Credential Phish
Attack story
Activity
Alerts (1)
Assets (2)
Evidence and response
Similar incident
Summary
Agent triaged alert "Email reported by user as malware or phish"
Phishing Triage Agent
Reviewing URL screenshots
3/18/25 at 13:21:10 AM
Suspicious
Completed
51 sec
Phishing Triage Agent
Checking reputation of resolved URLs
3/18/25 at 13:21:10 AM
Completed
3.2 sec
Phishing Triage Agent
Classify as true positive
3/18/25 at 13:22:01 AM
Completed
Change classification
Change classification and teach agent
If you disagree with how the agent categorized this alert, change it here. Your change, and any explanation you provide, will be saved to improve its future work. Learn more about feedback
Classify phishing email attempt as 'True positive'.
Phishing Triage Agent
A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipien...
Show more
Change classification
True Positive
Status
In progress
Explain why:
Add some relevant information, such as "The sender's email address is known and trusted. All emails from the domain are false positives since this is a known customer of our company."
Save
Cancel


Search
or phish
ncident
Summary
Phishing Triage Agent
Classify as true positive
3/18/25 at 13:22:01 AM
Completed
Change classification
Change classification and teach agent
If you disagree with how the agent categorized this alert, change it here. Your change, and any explanation you provide, will be saved to improve its future work. Learn more about feedback
Classify phishing email attempt as 'True positive'.
Phishing Triage Agent
A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipien...
Show more
Change classification
False Positive
Status
Resolved
Explain why:
Add some relevant information, such as "The sender's email address is known and trusted. All emails from the domain are false positives since this is a known customer of our compa..."


Search
or phish
ncident
Summary
Phishing Triage Agent
Classify as true positive
3/18/25 at 13:22:01 AM
Completed
Change classification
Change classification and teach agent
If you disagree with how the agent categorized this alert, change it here. Your change, and any explanation you provide, will be saved to improve its future work. Learn more about feedback
Classify phishing email attempt as 'True positive'.
Phishing Triage Agent
A user reported an email with the subject line "Complete your required corporate training by today!" which was sent to a large number of recipients. The email contained information about an employee training program and urged recipien...
Show more
Change classification
False Positive
Status
Resolved
Explain why:
The sender is our corporate compliance training vendor, so this email is legitimate.


reported by user as malware or phish
mail reported by user as malware or phish
rogress
Unassigned
True positive
Agent
Credential Phish
ity
Alerts (1)
Assets (2)
Evidence and response
Similar incident
Summary
Feedback received.
Classification and status changed.
Manage agent feedback
alert "Email reported by user as malware or phish"
Rerun agent
View details
Expand all tasks
Phishing Triage Agent
Reviewing URL screenshots
3/18/25 at 13:21:10 AM
Suspicious
Completed
51 sec
Phishing Triage Agent
Checking reputation of resolved URLs
3/18/25 at 13:21:10 AM
Completed
3.2 sec
Phishing Triage Agent
Classify as true positive → False positive
Changed by Kadji Bell at Aug 01, 2025 3:36:00 AM
Changed
Edit


Microsoft Defender XDR
https://security.microsoft.com/incident/2356358/activity
Microsoft Defender
Search
Incidents
Attack disruptions
Automated actions that stopped attacks
21 (Last 30 days)
View details
Incidents resolved by agent
AI-powered resolved phish incidents
95% (Last 30 days)
Manage agent
Export
Refresh
3 items
Search by keyword
1 Day
Edit columns
Filter set:
Unsaved
Save
Incident status: Active, in progress
Incident severity: Any
Incident assignment: Any
Service/detection source: Any
Add filter
Reset all
Incident name
Incident ID
Tags
Severity
Assigned to
Classification
Status
Account enumeration reconnaissance on one endpoint
2861358
High
Kadji Bell
Not set
In progress
Exfiltration incident involving multiple users
7515358
Low
Kadji Bell
Not set
In progress
Multi-stage incident involving Initial access & Lateral movement including ransomware on m...
2681673
Ransomware
+2
High
Kadji Bell
Not set
In progress

Erweiterter Entra / Zero Trust Usecase

Moderne Authentifizierung an “alten” Applikationen

Sicherer Zugang für jeden Mitarbeiter, überall, zu jeder App oder Ressource

Jeder Mitarbeiter
Cloudbasierte und lokale Identitäten, Gruppen und Rollen

Irgendein Ort
Hauptsitz, Zweigstelle, Zuhause, remote

Jede Plattform
Android, iOS, Linux, MacOS, Windows

Jedes Gerät
Corporate oder persönlich

Alle Daten, Apps oder Ressourcen

IaaS, PaaS, Datacenter

Microsoft 365

SaaS, Websites

On-premises

Microsoft-Entra-Ansatz

Schützen, verwalten und sichern Sie den Zugang der Arbeitskräfte zu den Ressourcen der Organisation

Onboard users

- Employee onboarding
- Guest onboarding

Microsoft Entra Verified ID

Govern access

- Access rights to resources
- Self-service access
- Just-in-time access
- Access recertification
- Lifecycle automation

Microsoft Entra ID Governance

Secure access

- Continuous risk assessment and automation
- Threat intelligence and telemetry
- Zero Trust, adaptive risk-based access policy

Microsoft Entra ID Protection

Microsoft Entra Internet Access

Microsoft Entra Private Access

Internet resources

- Microsoft 365 apps
- Internet & SaaS apps

Private resources

- Apps hosted in cloud infra
- On-premises apps

Ongoing auditing and reporting

Microsoft Security

Danke