CyberPilot

Guide: Whitelisting using Advanced delivery

Intro: Whitelisting guide for Phishing Simulation

- The guide relates to **Microsoft Defender**.
- This guide is for administrators to help whitelist **IP, domains and simulation urls** in **advanced delivery** in order to run phishing simulations for the organization's users.

CyberPilot

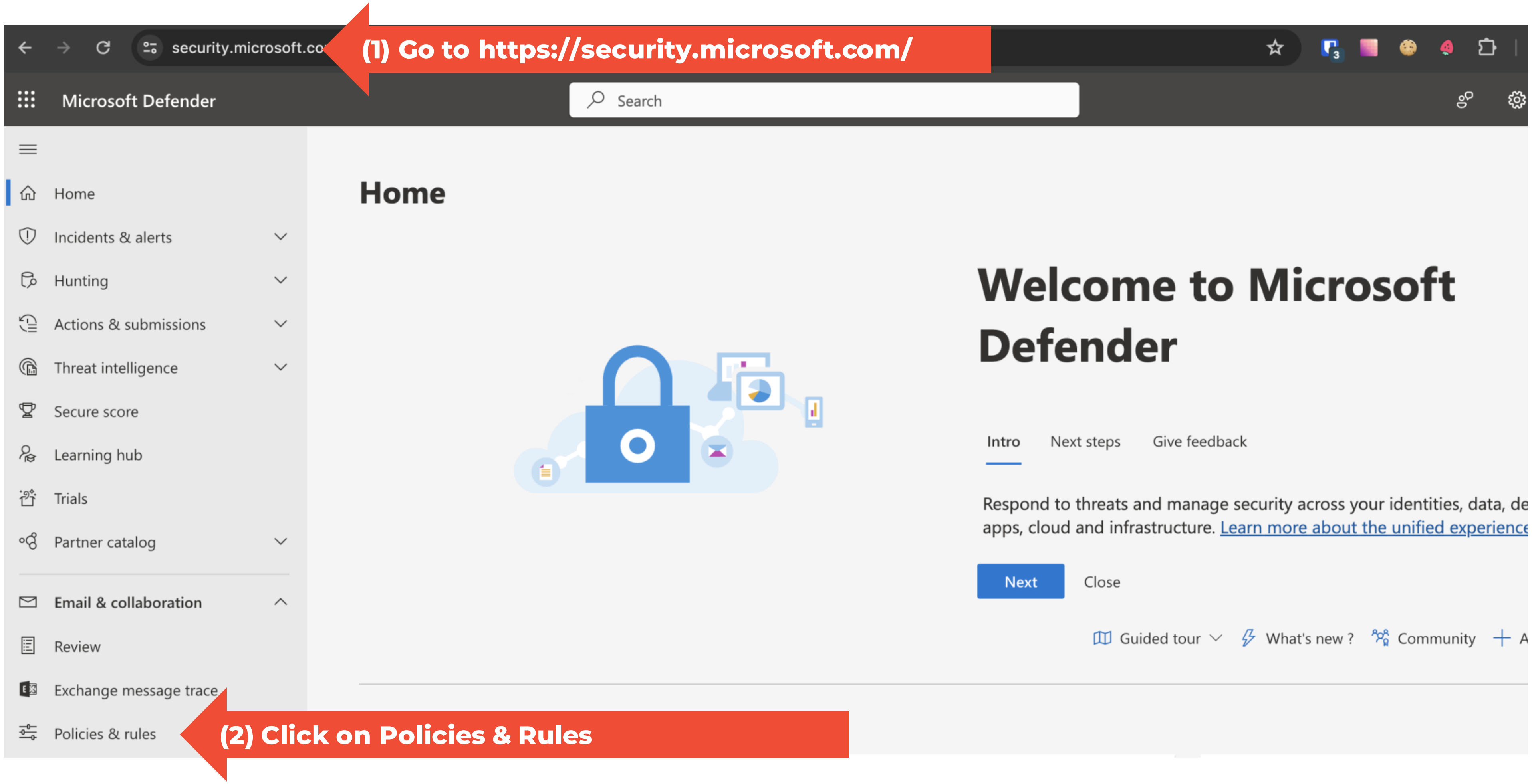
Step 1: Information needed

- Together with CyberPilot you have chosen a **sender domain**, which is the email address that the email will be sent from.
- IP: 3.75.105.111
- Simulation URL: link120623.dk and cyberdomain.com

The **sender domain** is: exemple.dk

Configure Advanced delivery in Microsoft Defender

Step 1: Go to your Defender admin in Microsoft **https://security.microsoft.com/**
Step 2: Click on "Policies & Rules"



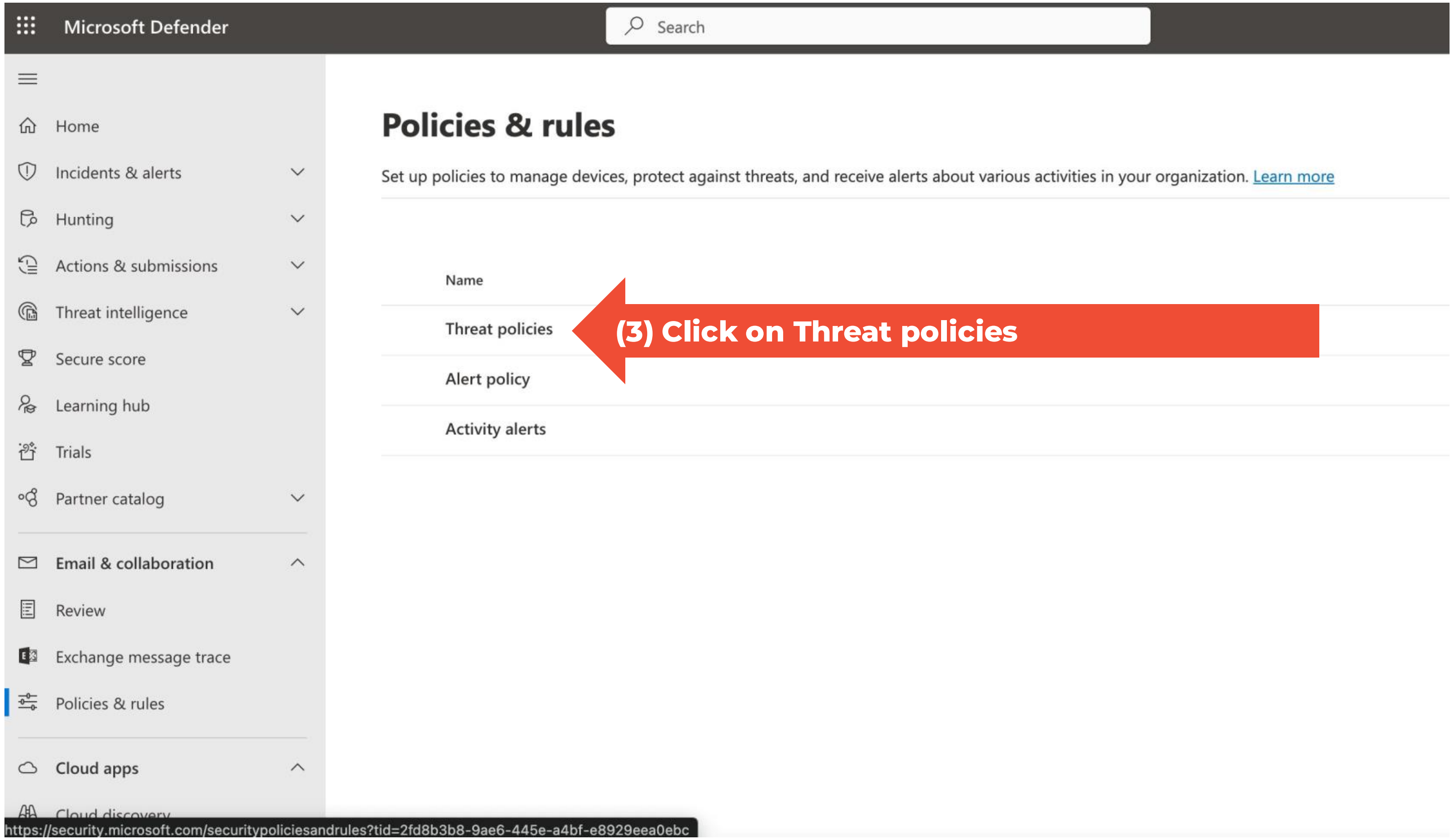
Welcome to Microsoft Defender

Respond to threats and manage security across your identities, data, de
apps, cloud and infrastructure. Learn more about the unified experience

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 3: Click on "Threat policies"



Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. Learn more

Name
Threat policies
Alert policy
Activity alerts

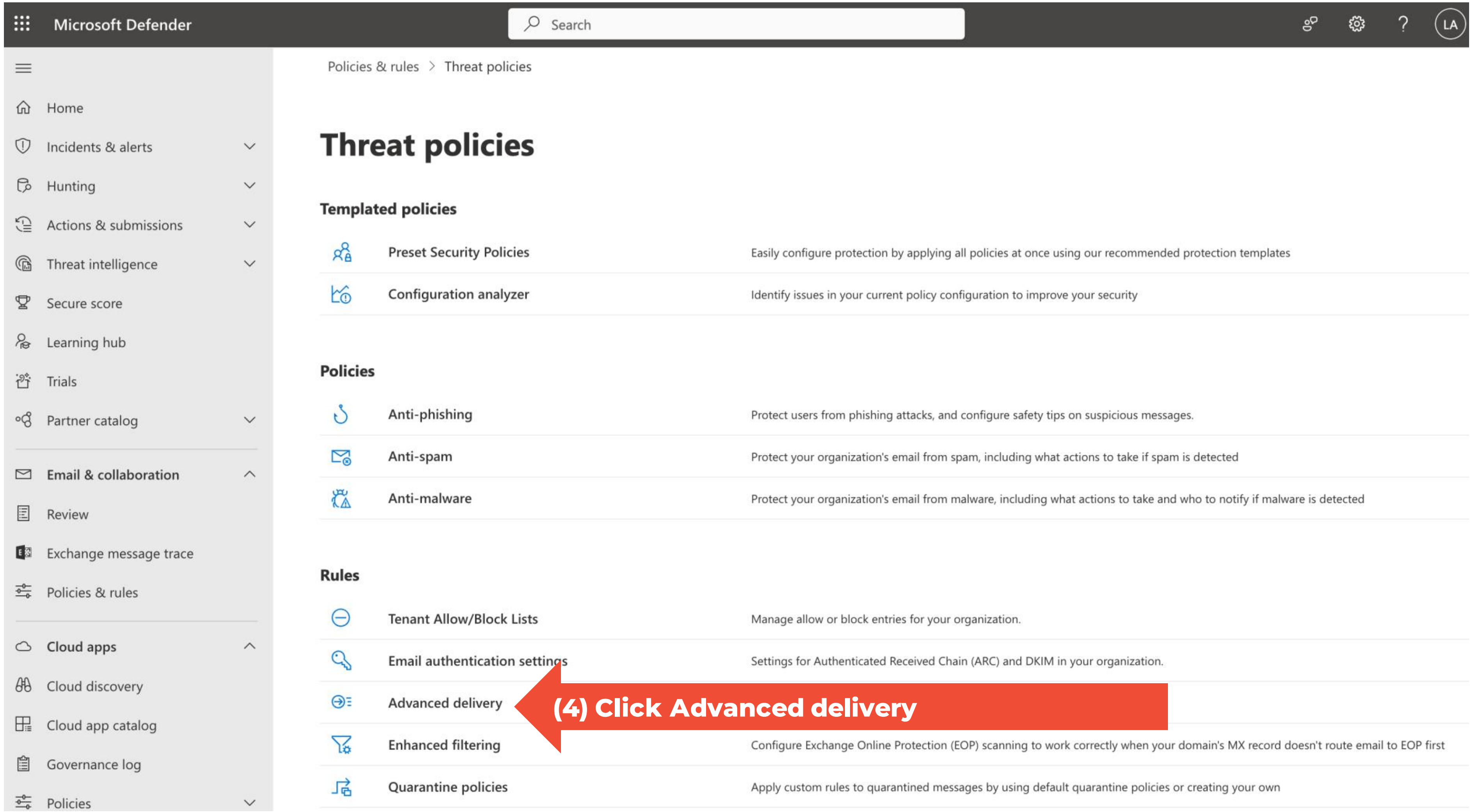
(3) Click on Threat policies

https://security.microsoft.com/securitypoliciesandrules?tid=2fd8b3b8-9ae6-445e-a4bf-e8929eea0ebc

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 4: Click Advanced delivery



Threat policies

Templated policies

Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
Configuration analyzer	Identify issues in your current policy configuration to improve your security

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected

Rules

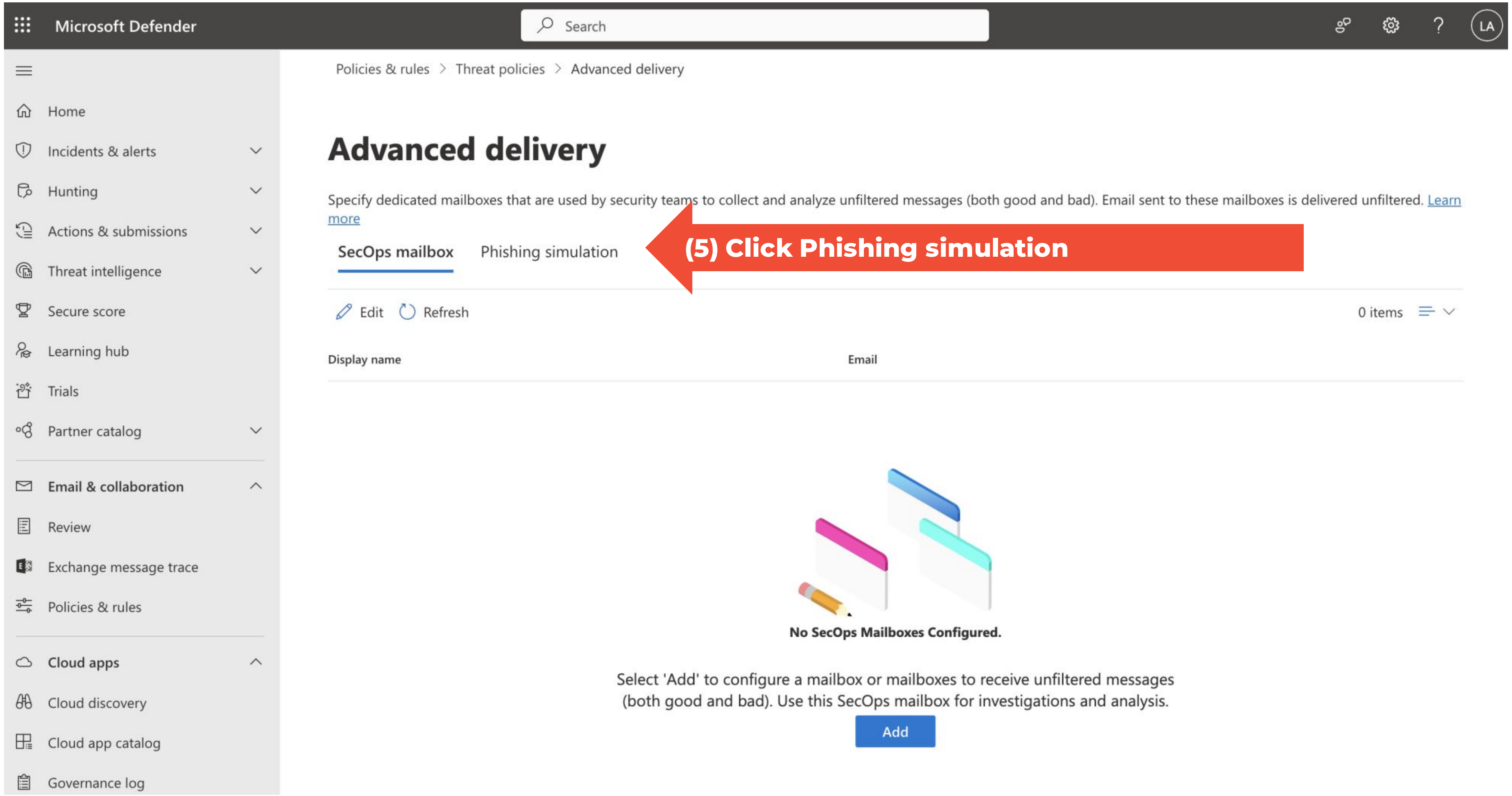
Tenant Allow/Block Lists	Manage allow or block entries for your organization.
Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
Advanced delivery	
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

(4) Click Advanced delivery

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 5: Go to Phishing simulation



Advanced delivery

Specify dedicated mailboxes that are used by security teams to collect and analyze unfiltered messages (both good and bad). Email sent to these mailboxes is delivered unfiltered. Learn more

(5) Click Phishing simulation

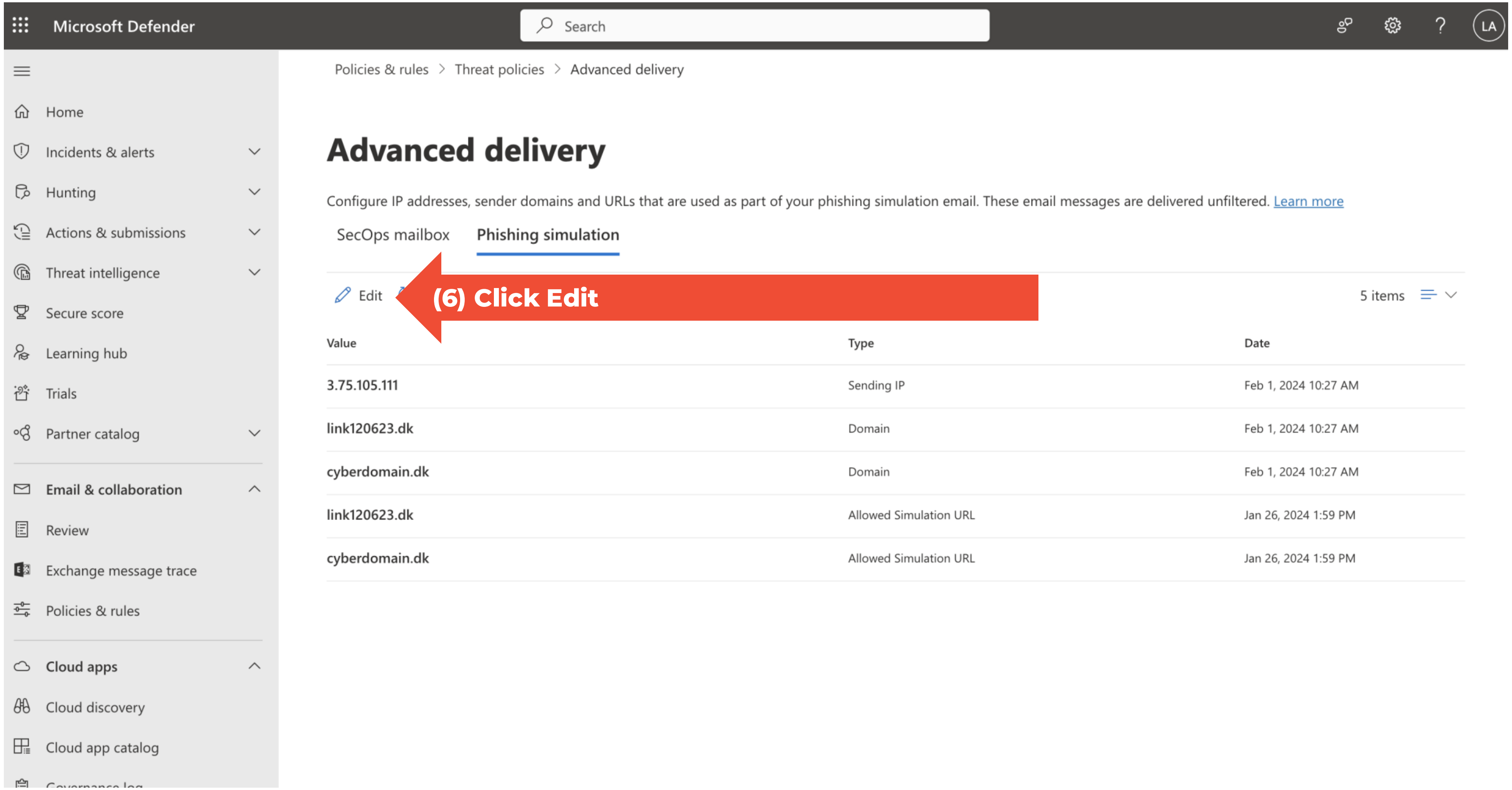
No SecOps Mailboxes Configured.

Select 'Add' to configure a mailbox or mailboxes to receive unfiltered messages (both good and bad). Use this SecOps mailbox for investigations and analysis.

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 6: Edit simulation list



Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulation email. These email messages are delivered unfiltered. Learn more

SecOps mailbox | Phishing simulation

Edit

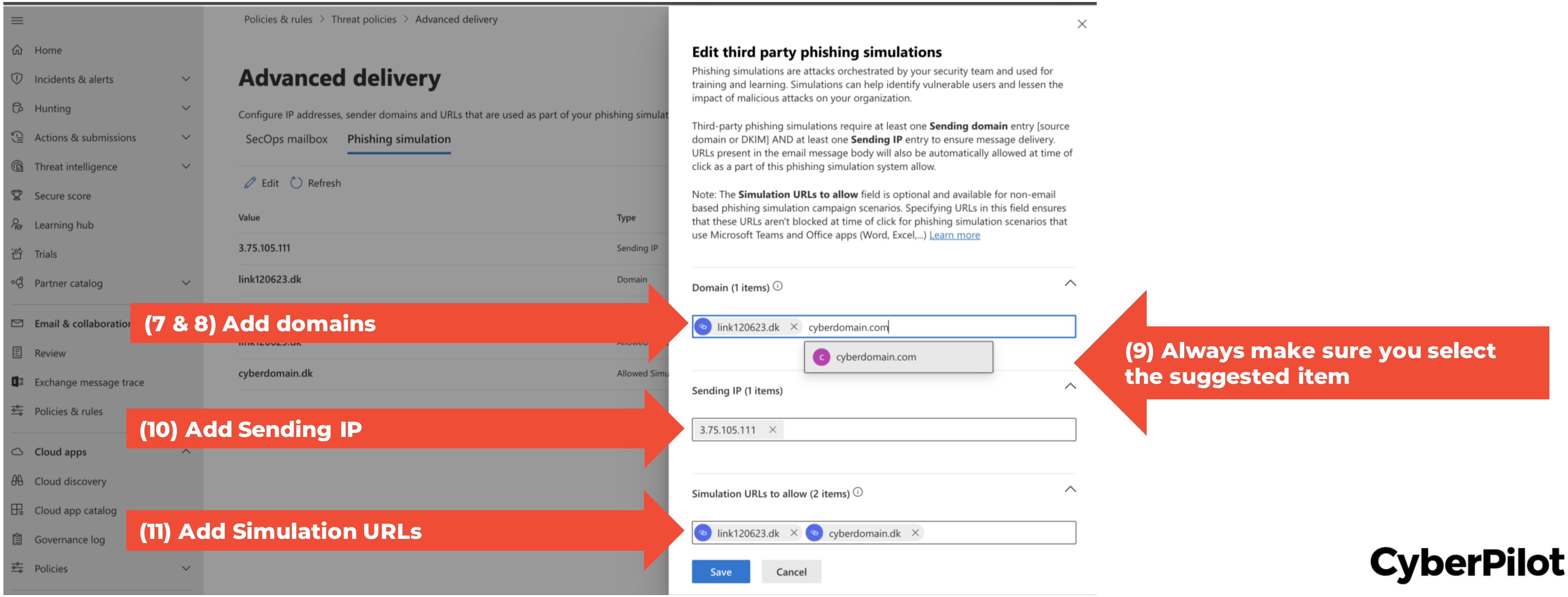
(6) Click Edit

5 items

Value	Type	Date
3.75.105.111	Sending IP	Feb 1, 2024 10:27 AM
link120623.dk	Domain	Feb 1, 2024 10:27 AM
cyberdomain.dk	Domain	Feb 1, 2024 10:27 AM
link120623.dk	Allowed Simulation URL	Jan 26, 2024 1:59 PM
cyberdomain.dk	Allowed Simulation URL	Jan 26, 2024 1:59 PM

Configure Advanced delivery in Microsoft Defender

Step 7: Add our domains: link120623.dk and cyberdomain.com
Step 8: Add the sender domain for the campaign see **Step 1**.
Step 9: Always make sure you select the suggested item
Step 10: Add sending IP. Our IP is 3.75.105.111
Step 11: Add simulation URLs. Our URLs are: link120623.dk and cyberdomain.com



Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulat

Value	Type
3.75.105.111	Sending IP
link120623.dk	Domain
link120623.dk	Allowed
cyberdomain.dk	Allowed Simu

Edit third party phishing simulations

Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one **Sending domain** entry [source domain or DKIM] AND at least one **Sending IP** entry to ensure message delivery. URLs present in the email message body will also be automatically allowed at time of click as a part of this phishing simulation system allow.

Note: The **Simulation URLs to allow** field is optional and available for non-email based phishing simulation campaign scenarios. Specifying URLs in this field ensures that these URLs aren't blocked at time of click for phishing simulation scenarios that use Microsoft Teams and Office apps (Word, Excel,...) Learn more

Domain (1 items): link120623.dk × cyberdomain.com — suggested: cyberdomain.com

Sending IP (1 items): 3.75.105.111 ×

Simulation URLs to allow (2 items): link120623.dk × cyberdomain.dk ×

(7 & 8) Add domains

(9) Always make sure you select the suggested item

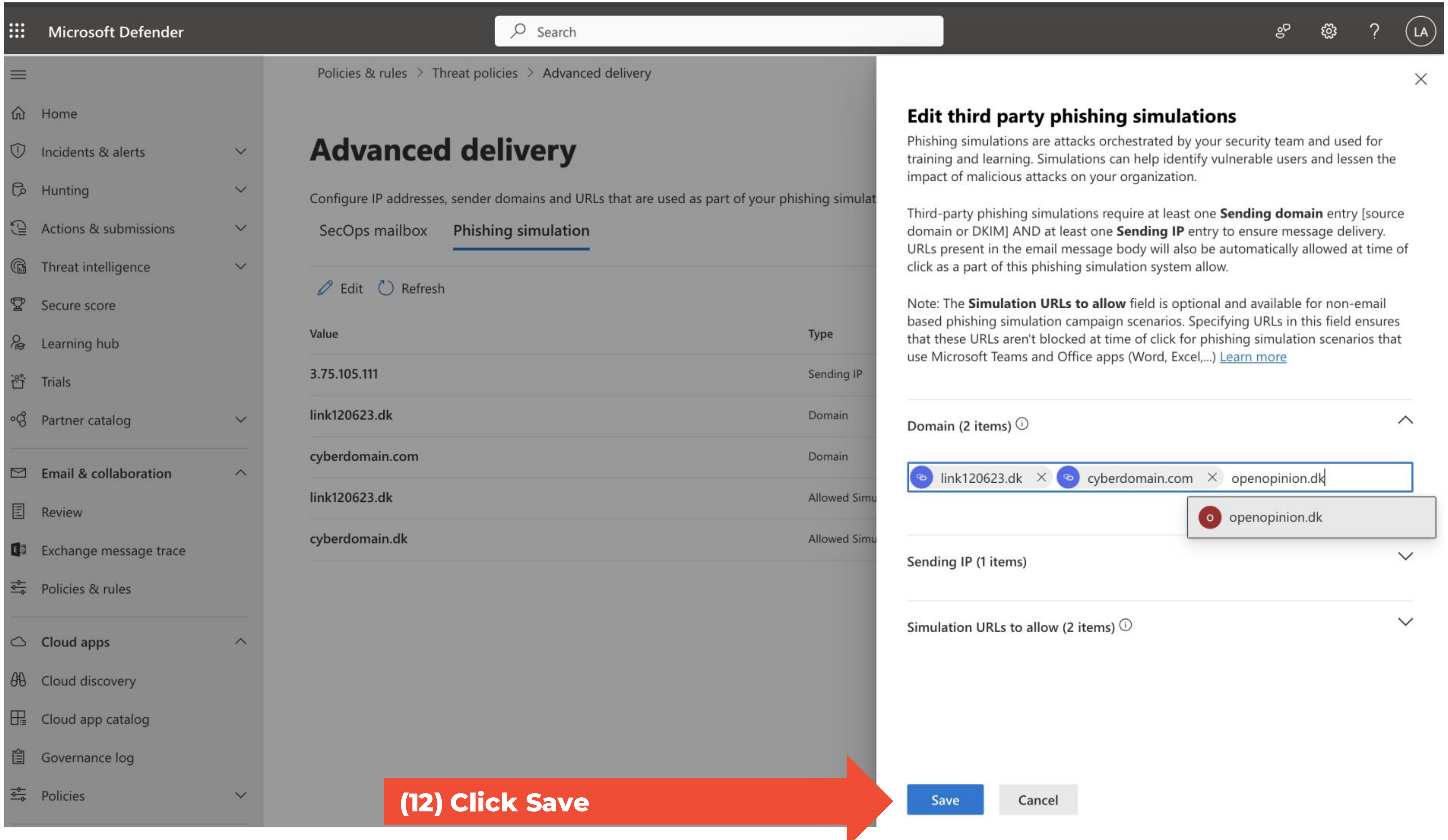
(10) Add Sending IP

(11) Add Simulation URLs

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 12: Click Save



Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulat

SecOps mailbox | Phishing simulation

Value	Type
3.75.105.111	Sending IP
link120623.dk	Domain
cyberdomain.com	Domain
link120623.dk	Allowed Simu
cyberdomain.dk	Allowed Simu

Edit third party phishing simulations

Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one **Sending domain** entry [source domain or DKIM] AND at least one **Sending IP** entry to ensure message delivery. URLs present in the email message body will also be automatically allowed at time of click as a part of this phishing simulation system allow.

Note: The **Simulation URLs to allow** field is optional and available for non-email based phishing simulation campaign scenarios. Specifying URLs in this field ensures that these URLs aren't blocked at time of click for phishing simulation scenarios that use Microsoft Teams and Office apps (Word, Excel,...) Learn more

Domain (2 items)

link120623.dk ✕ cyberdomain.com ✕ openopinion.dk

openopinion.dk

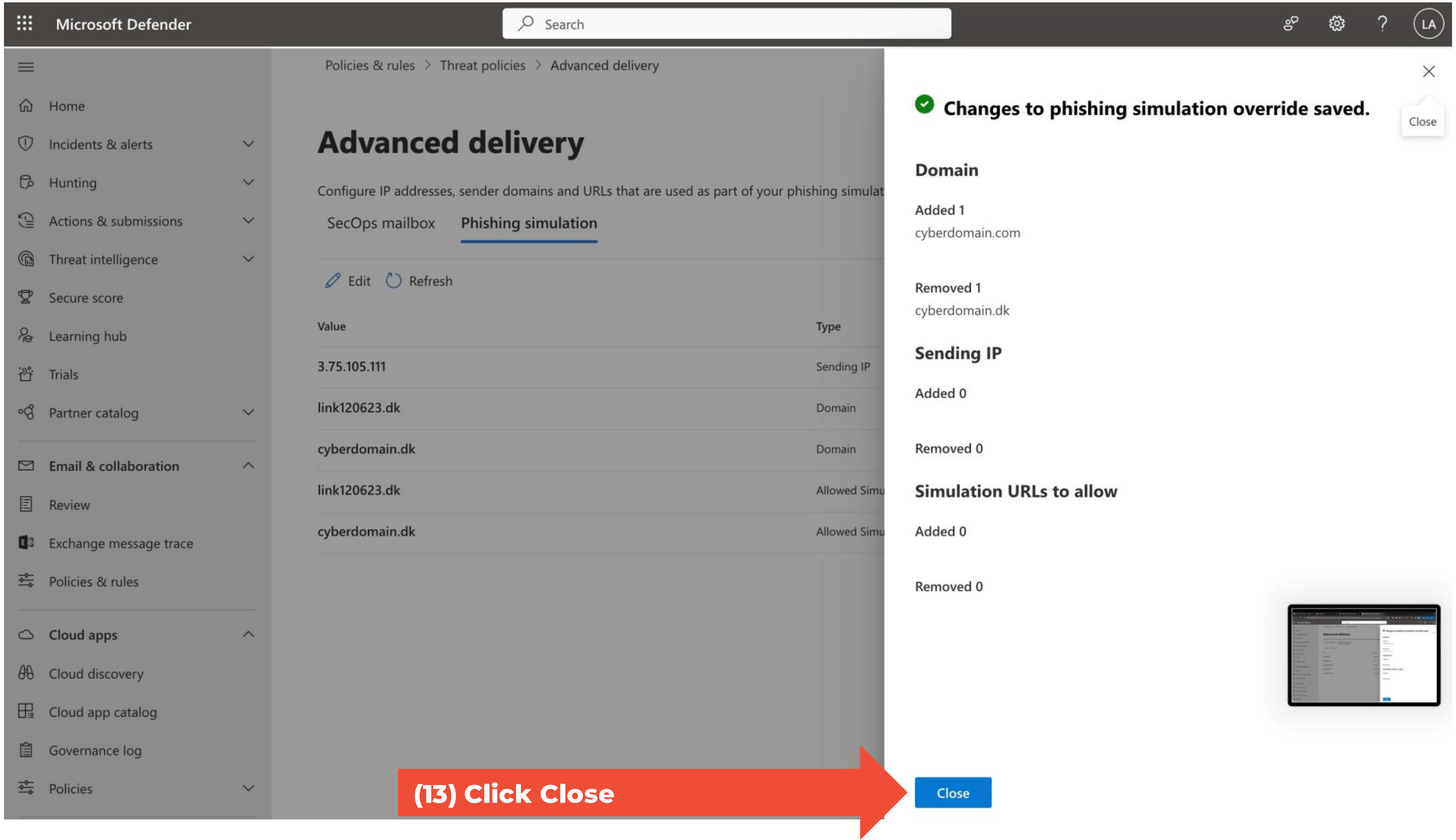
Sending IP (1 items)

Simulation URLs to allow (2 items)

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 13: Click Close



Advanced delivery

Configure IP addresses, sender domains and URLs that are used as part of your phishing simulat

Value	Type
3.75.105.111	Sending IP
link120623.dk	Domain
cyberdomain.dk	Domain
link120623.dk	Allowed Simu
cyberdomain.dk	Allowed Simu

Changes to phishing simulation override saved.

Domain

Added 1
cyberdomain.com

Removed 1
cyberdomain.dk

Sending IP

Added 0

Removed 0

Simulation URLs to allow

Added 0

Removed 0

CyberPilot

For those of you who have additional levels of anti-spam security

You may find that you have whitelisted according to the steps above, but the phishing simulation test emails still are not getting through.

This is likely because your organization has **additional levels of anti-spam security** from third party providers, e.g., Vipre, Sophos, Crowdstrike, etc.

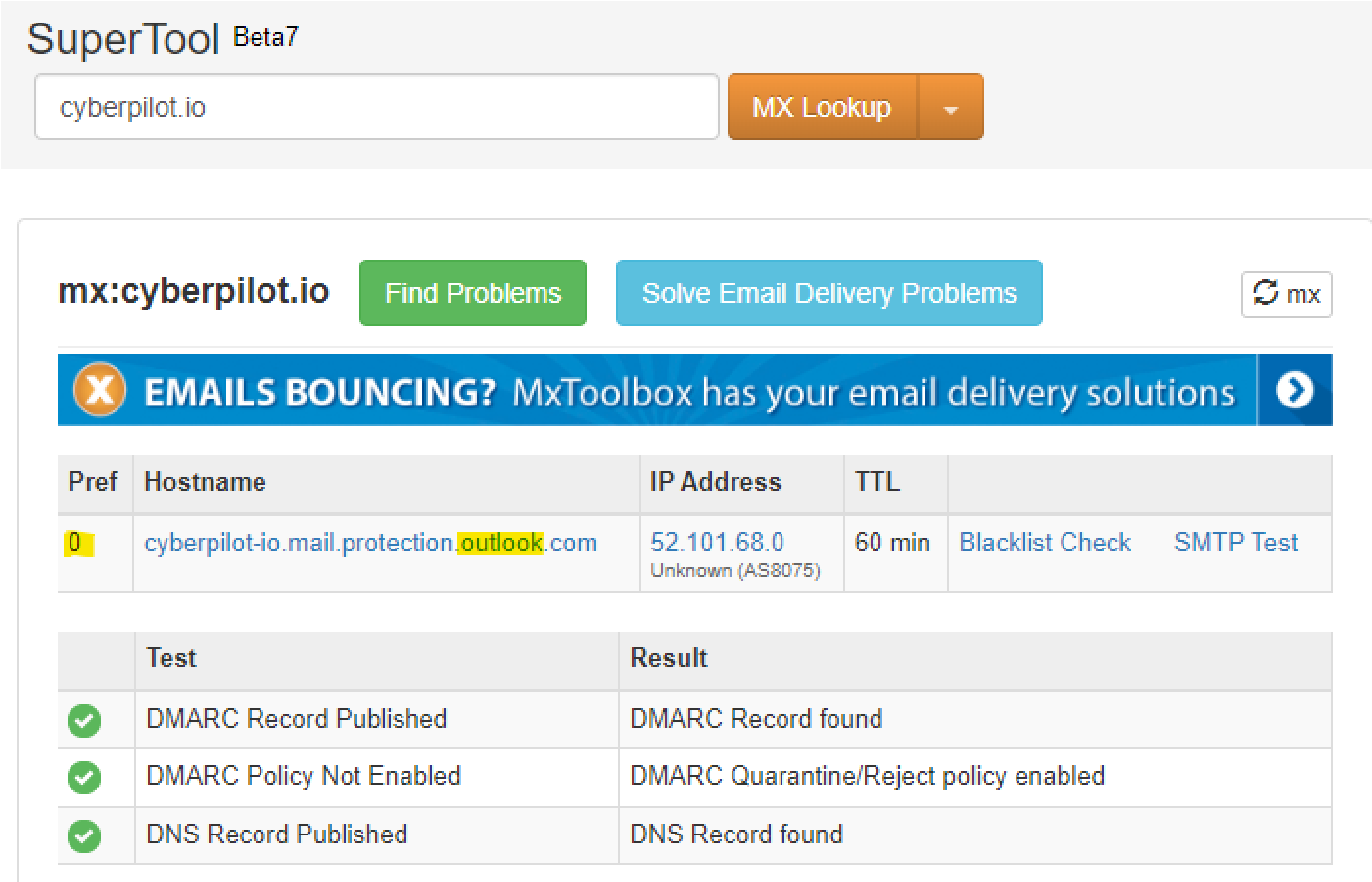
If this is the case, then you can configure a "partner connector" in addition to the steps in this guide. See the guide on connectors.

Next step (only if phishing simulation test emails still don’t get through): **Check your domain**

There are several tools that you can use to check the various layers of anti-spam filtering that your organization uses. Here’s a tool that we like.

Check with [mx toolbox]() to learn more about which security measures you organization uses by typing your email domain.

Example: “Pref 0” is the first touchpoint of an email, and you can see that “outlook” is the protection before going to CyberPilot. This means that we only need to follow the steps in this guide.


SuperTool Beta7
cyberpilot.io
MX Lookup
Find Problems
Solve Email Delivery Problems
mx
EMAILS BOUNCING? MxToolbox has your email delivery solutions

mx:cyberpilot.io

Pref	Hostname	IP Address	TTL		
0	cyberpilot-io.mail.protection.outlook.com	52.101.68.0 Unknown (AS8075)	60 min	Blacklist Check	SMTP Test

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DNS Record Published	DNS Record found