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.

Part 1: Information Needed

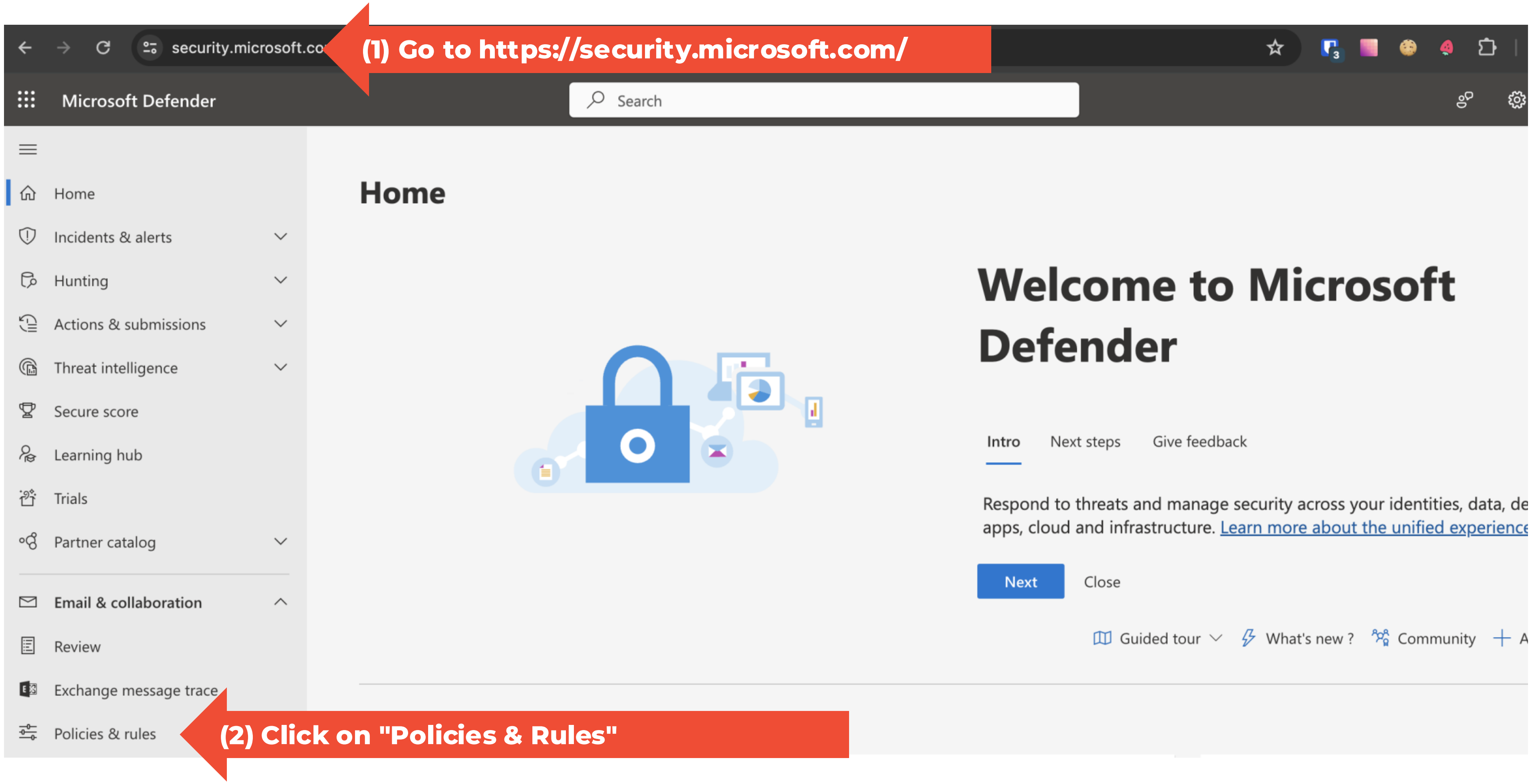
- Together with CyberPilot you have chosen a **sender domain**, which is the email address that the email will be sent from.
- IP: 3.75.105.111
- Simulation URL: link120623.dk/*
  The **sender domain** is: exemple.dk

Part 2:

Configure Advanced Delivery in Microsoft Defender

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"



(1) Go to https://security.microsoft.com/

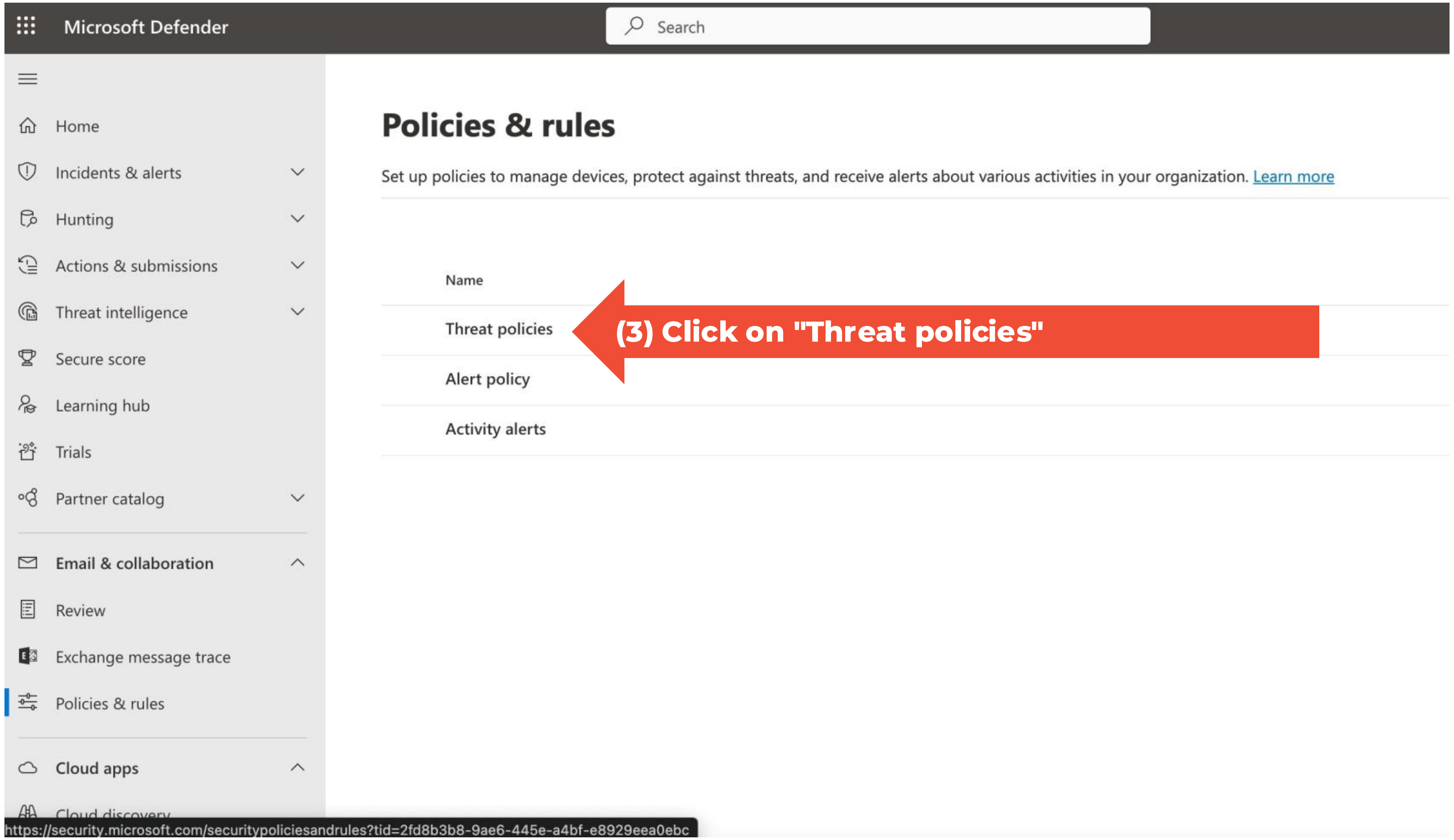
(2) Click on "Policies & Rules"

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

Configure Advanced delivery in Microsoft Defender

Step 3: Click on "Threat policies"



Microsoft Defender

Search

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Email & collaboration
Review
Exchange message trace
Policies & rules
Cloud apps
Cloud discovery

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

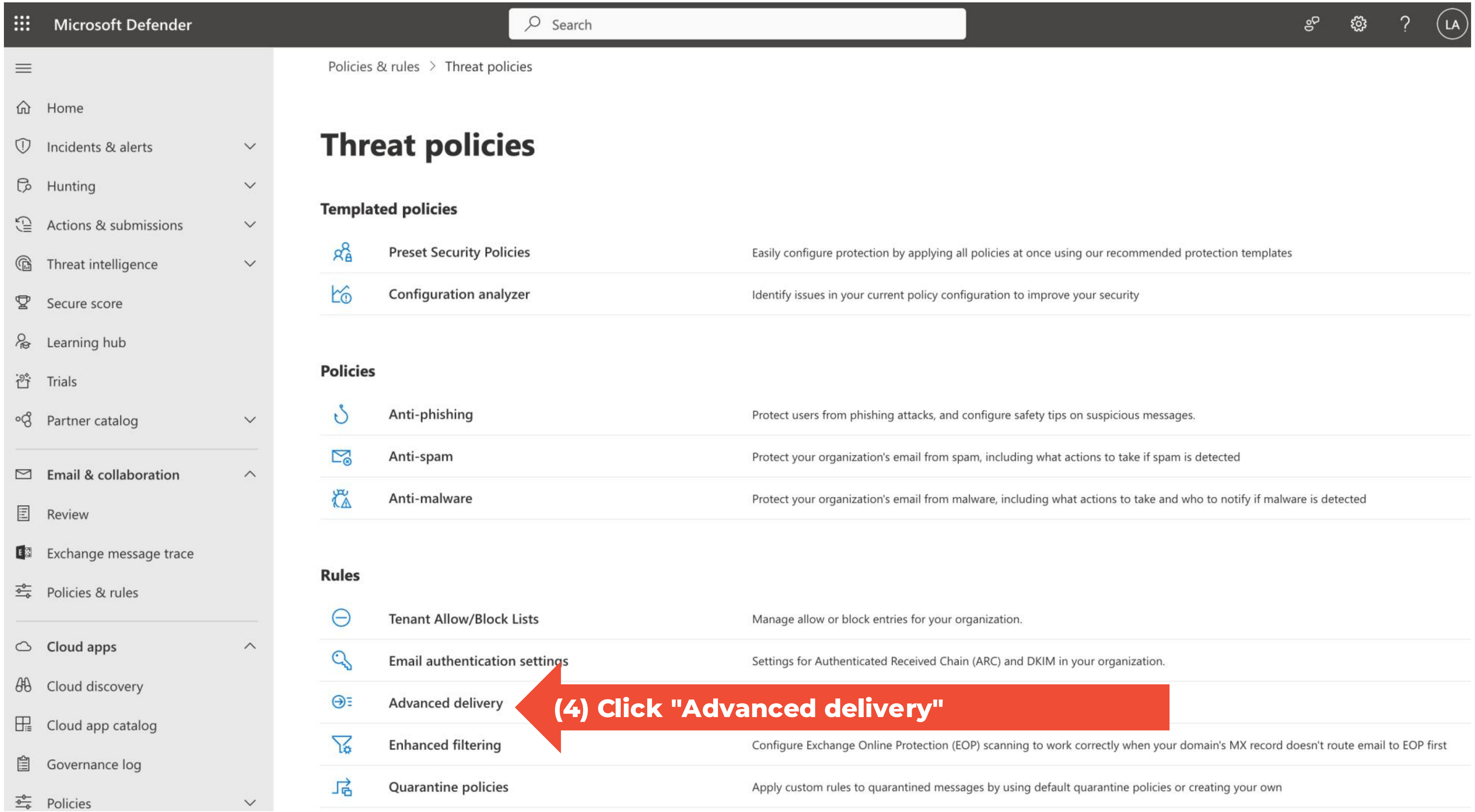
(3) Click on "Threat policies"

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

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 4: Click "Advanced delivery"



Microsoft Defender

Search

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Email & collaboration
Review
Exchange message trace
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
Governance log
Policies

Policies & rules > Threat policies

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

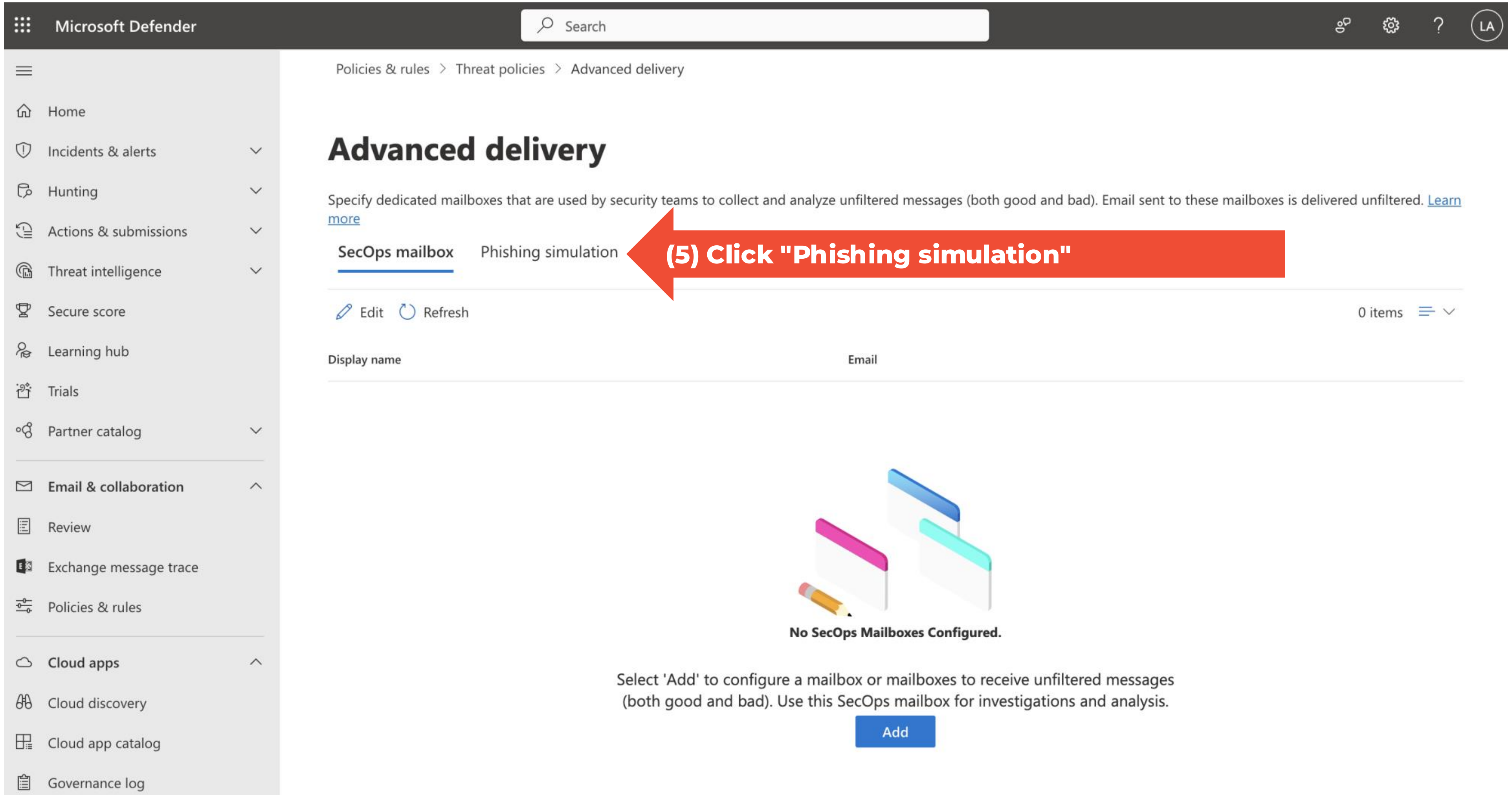
Tenant Allow/Block Lists	Manage allow or block entries for your organization.
Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
Advanced delivery	
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your 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

Display name	Email

No SecOps Mailboxes Configured.

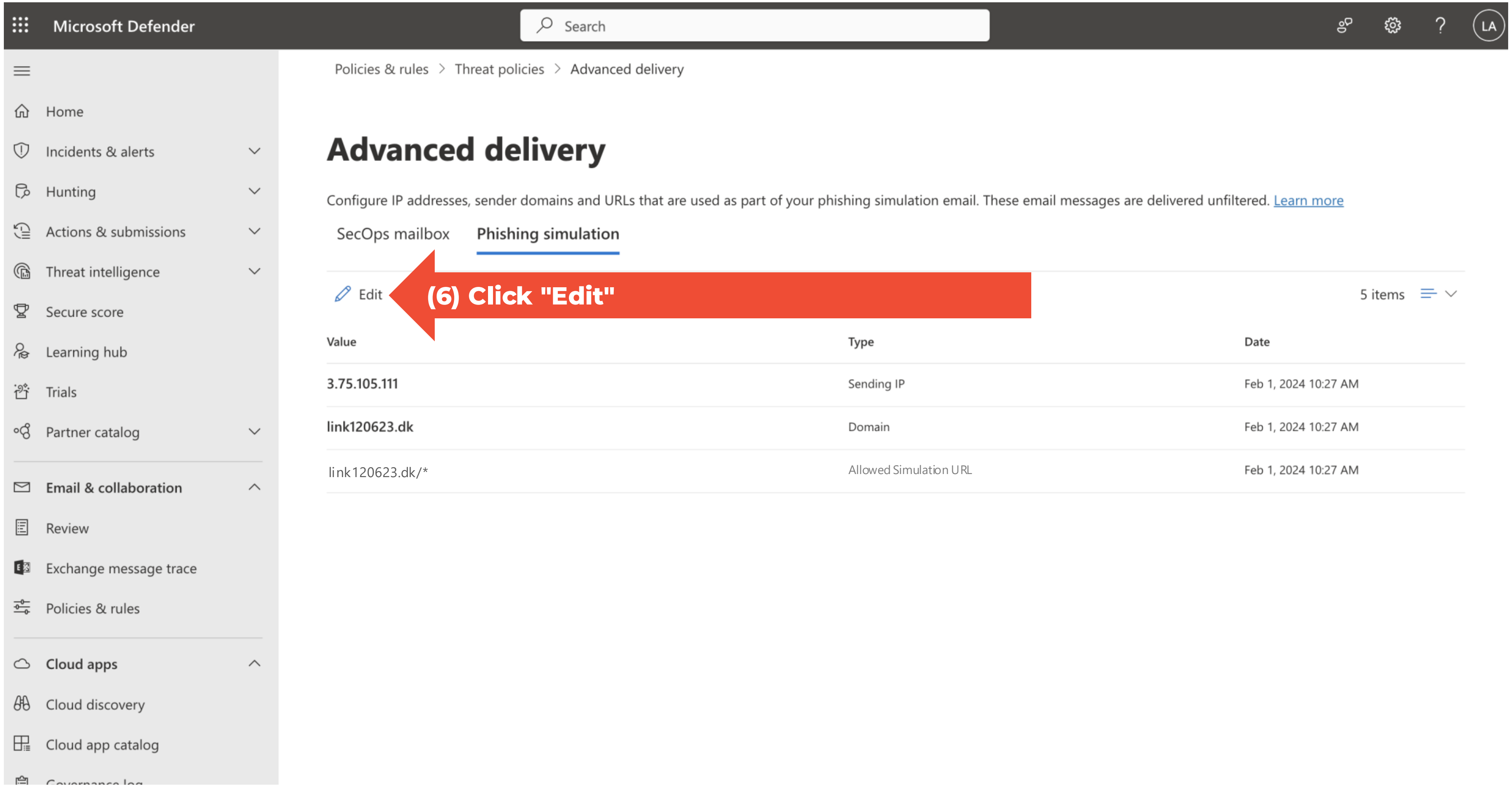
Select 'Add' to configure a mailbox or mailboxes to receive unfiltered messages (both good and bad). Use this SecOps mailbox for investigations and analysis.

(5) Click "Phishing simulation"

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 6: Edit simulation list



Policies & rules > Threat policies > Advanced delivery

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"

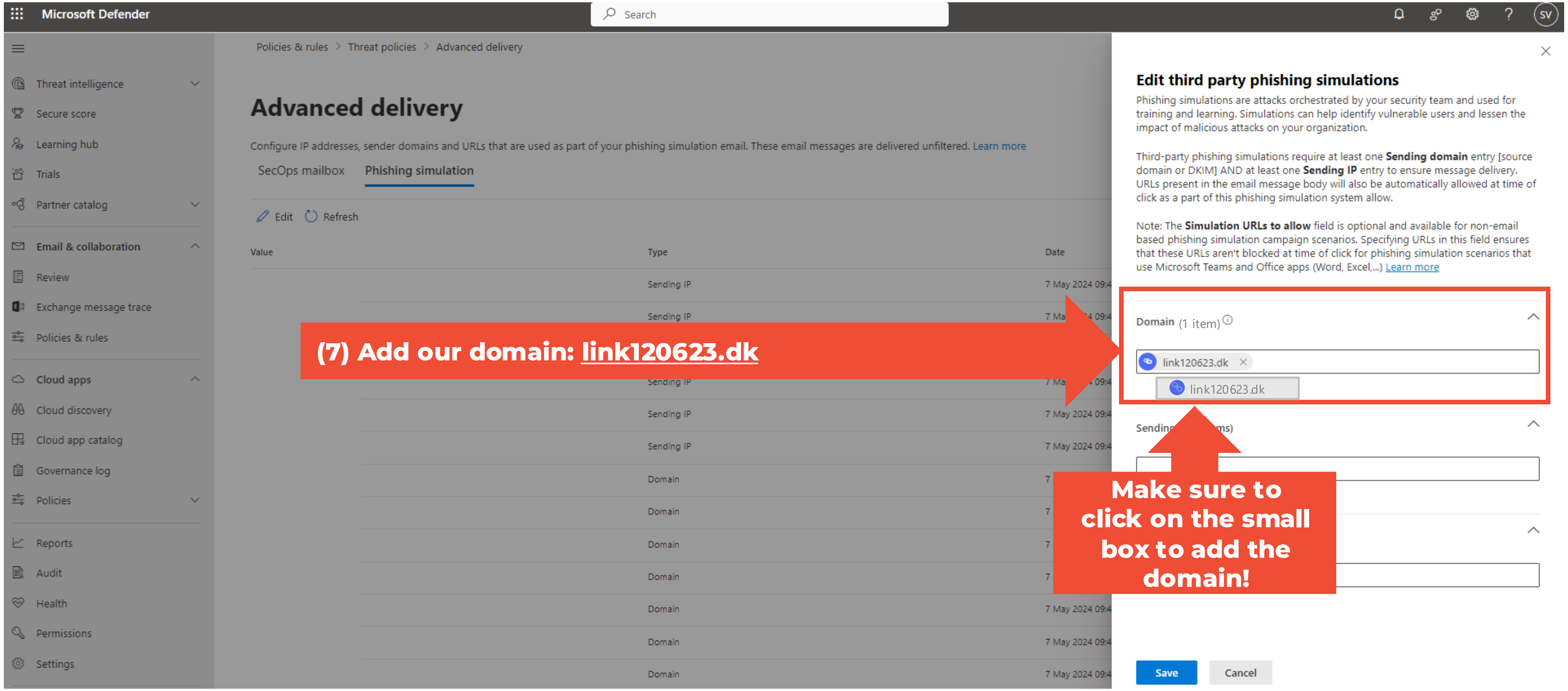
5 items

Value	Type	Date
3.75.105.111	Sending IP	Feb 1, 2024 10:27 AM
link120623.dk	Domain	Feb 1, 2024 10:27 AM
link120623.dk/*	Allowed Simulation URL	Feb 1, 2024 10:27 AM

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 7: Add our domain: link120623.dk
Always make sure you select the suggested item



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

Value	Type	Date
	Sending IP	7 May 2024 09:4
	Sending IP	7 Ma 4 09:4
	Sending IP	7 Ma 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Domain	7
	Domain	7
	Domain	7
	Domain	7
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4

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 item)

link120623.dk ×

link120623.dk

Sendin ms)

(7) Add our domain: link120623.dk

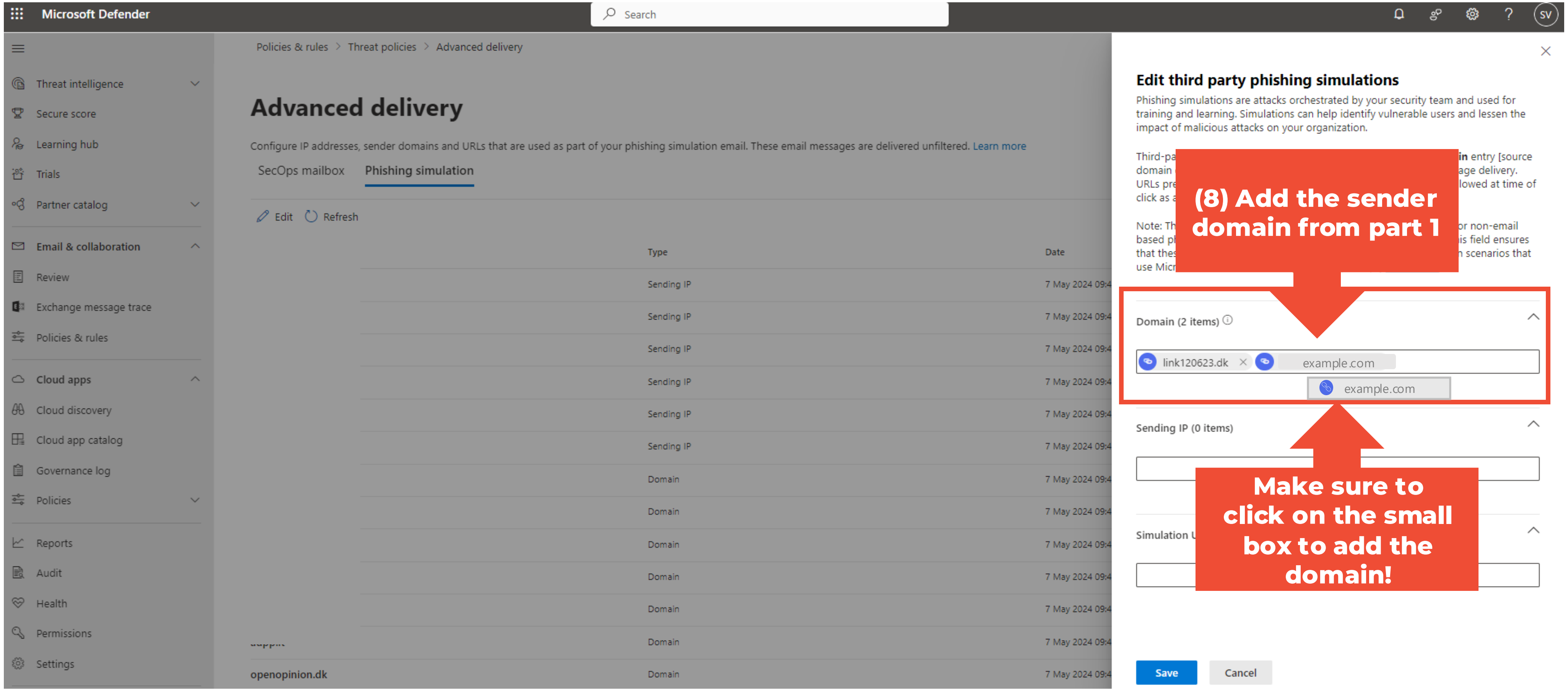
Make sure to click on the small box to add the domain!

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 8: Add the sender domain for the campaign - see **Part 1**. *If you are unsure what this is, your Customer Success Manager can help you.*

- Always make sure you select the suggested item



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

	Type	Date
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
[illegible]	Domain	7 May 2024 09:4
openopinion.dk	Domain	7 May 2024 09:4

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-pa in entry [source domain age delivery. URLs pre lowed at time of click as a

Note: Th or non-email based pl is field ensures that thes n scenarios that use Micr

Domain (2 items)

link120623.dk × example.com

example.com

Sending IP (0 items)

Simulation U

(8) Add the sender domain from part 1

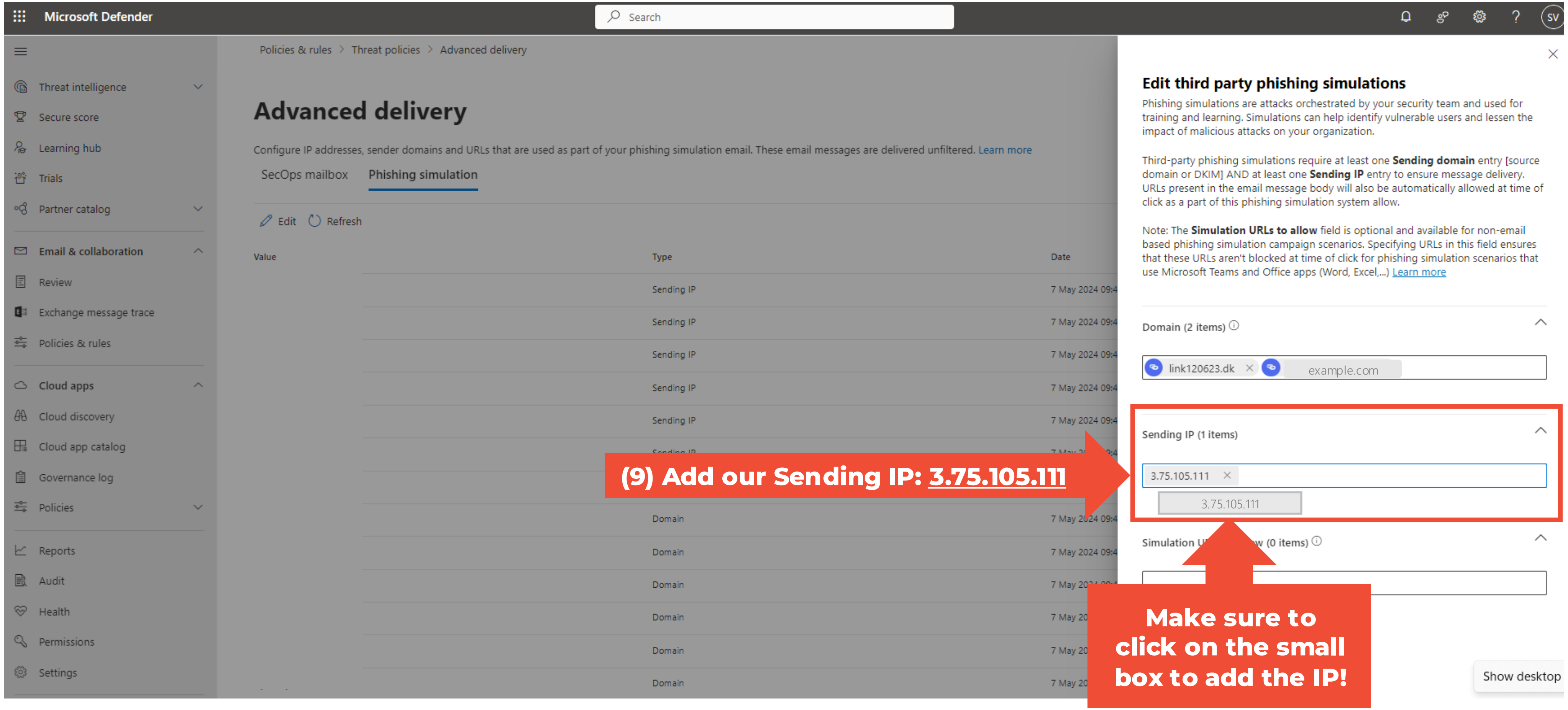
Make sure to click on the small box to add the domain!

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 9: Add sending IP. Our IP is 3.75.105.111

- Always make sure you select the suggested item



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

Value	Type	Date
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Sending IP	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 2024 09:4
	Domain	7 May 20
	Domain	7 May 20
	Domain	7 May 20

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 ×   example.com

Sending IP (1 items)

3.75.105.111 ×

3.75.105.111

Simulation U... w (0 items)

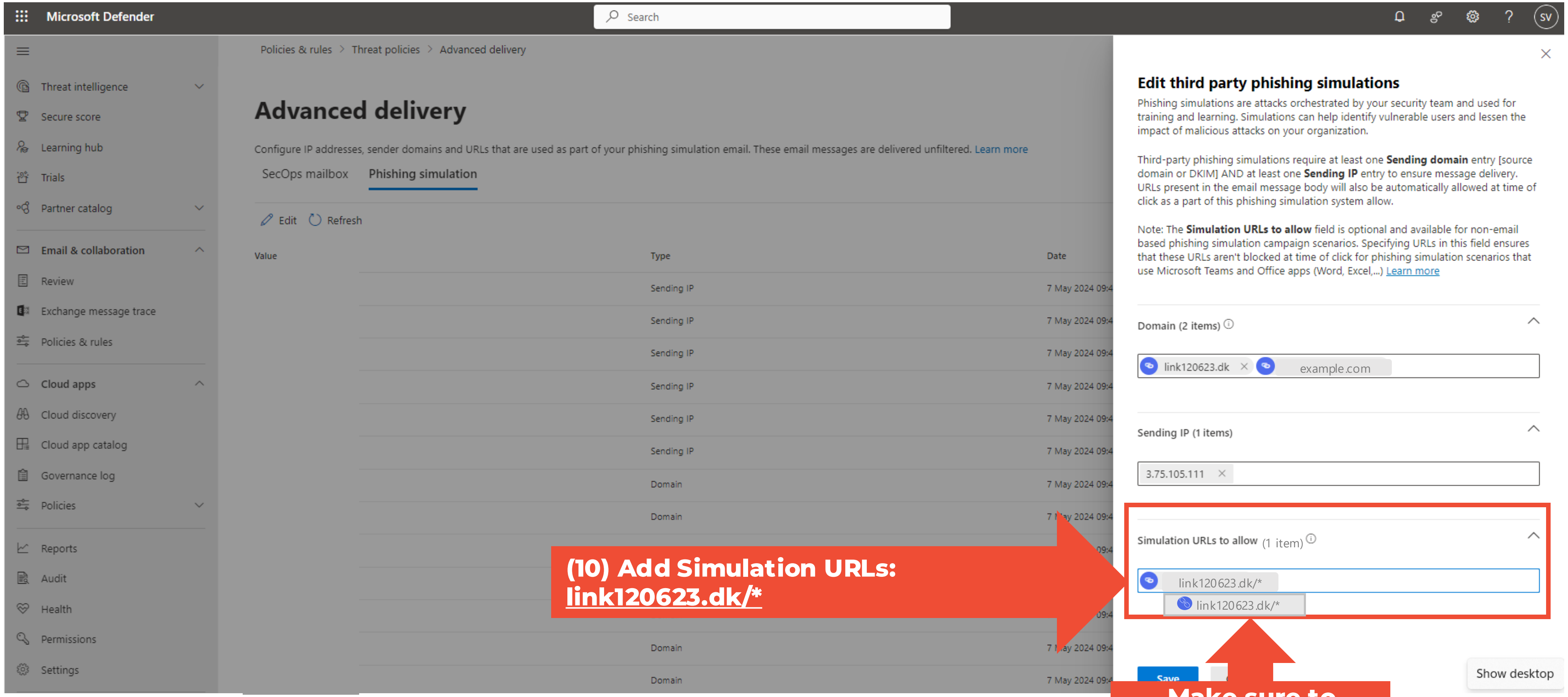
(9) Add our Sending IP: 3.75.105.111

Make sure to click on the small box to add the IP!

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 10: Add simulation URLs. Our URLs are: link120623.dk/*
Always make sure you select the suggested item



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

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 ×   example.com

Sending IP (1 items)
3.75.105.111 ×

Simulation URLs to allow (1 item)
link120623.dk/*
link120623.dk/*

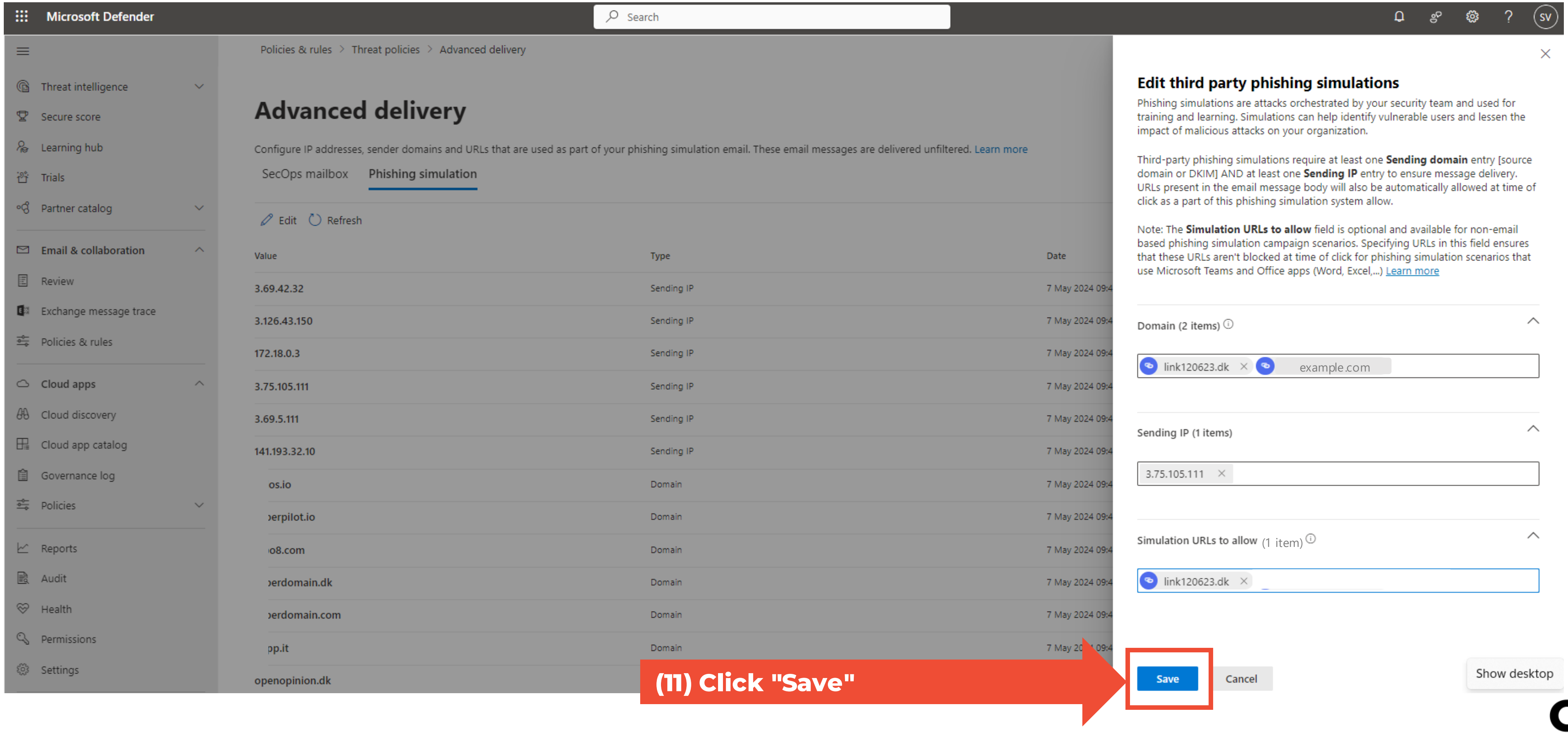
(10) Add Simulation URLs: link120623.dk/*

Make sure to click on the small box to add the URL!

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 11: Click "Save"



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

Value	Type	Date
3.69.42.32	Sending IP	7 May 2024 09:4
3.126.43.150	Sending IP	7 May 2024 09:4
172.18.0.3	Sending IP	7 May 2024 09:4
3.75.105.111	Sending IP	7 May 2024 09:4
3.69.5.111	Sending IP	7 May 2024 09:4
141.193.32.10	Sending IP	7 May 2024 09:4
os.io	Domain	7 May 2024 09:4
erpilot.io	Domain	7 May 2024 09:4
o8.com	Domain	7 May 2024 09:4
erdomain.dk	Domain	7 May 2024 09:4
erdomain.com	Domain	7 May 2024 09:4
pp.it	Domain	7 May 20 09:4
openopinion.dk		

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 × example.com

Sending IP (1 items)

3.75.105.111 ×

Simulation URLs to allow (1 item)

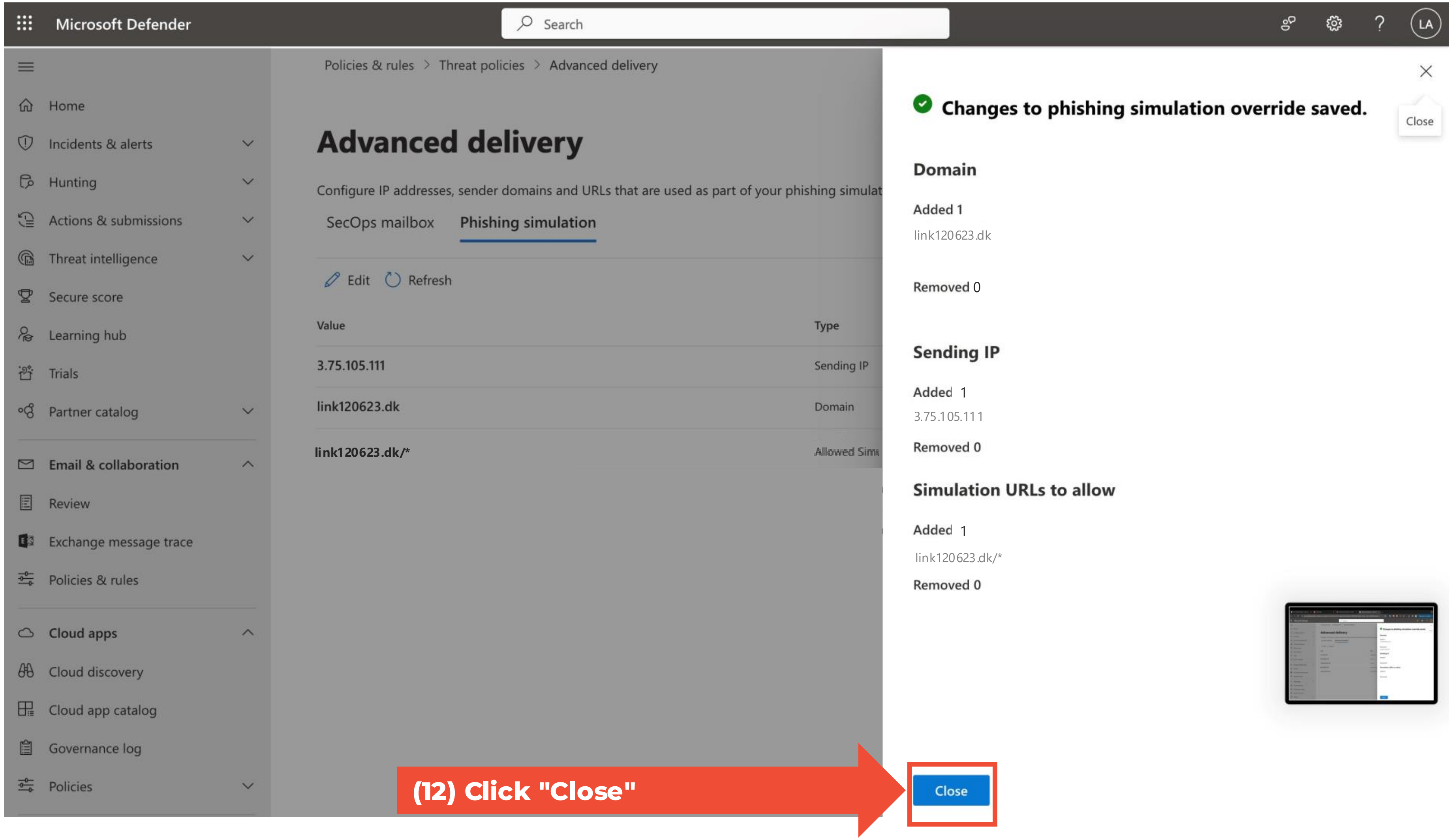
link120623.dk ×

(11) Click "Save"

CyberPilot

Configure Advanced delivery in Microsoft Defender

Step 12: 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
link120623.dk/*	Allowed Simu

Changes to phishing simulation override saved.

Domain

Added 1

link120623.dk

Removed 0

Sending IP

Added 1

3.75.105.111

Removed 0

Simulation URLs to allow

Added 1

link120623.dk/*

Removed 0

(12) Click "Close"

CyberPilot

Part 3:

Tell your Customer Success Manager you have whitelisted.

Then you will get a test email to check that the whitelisting worked.

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.

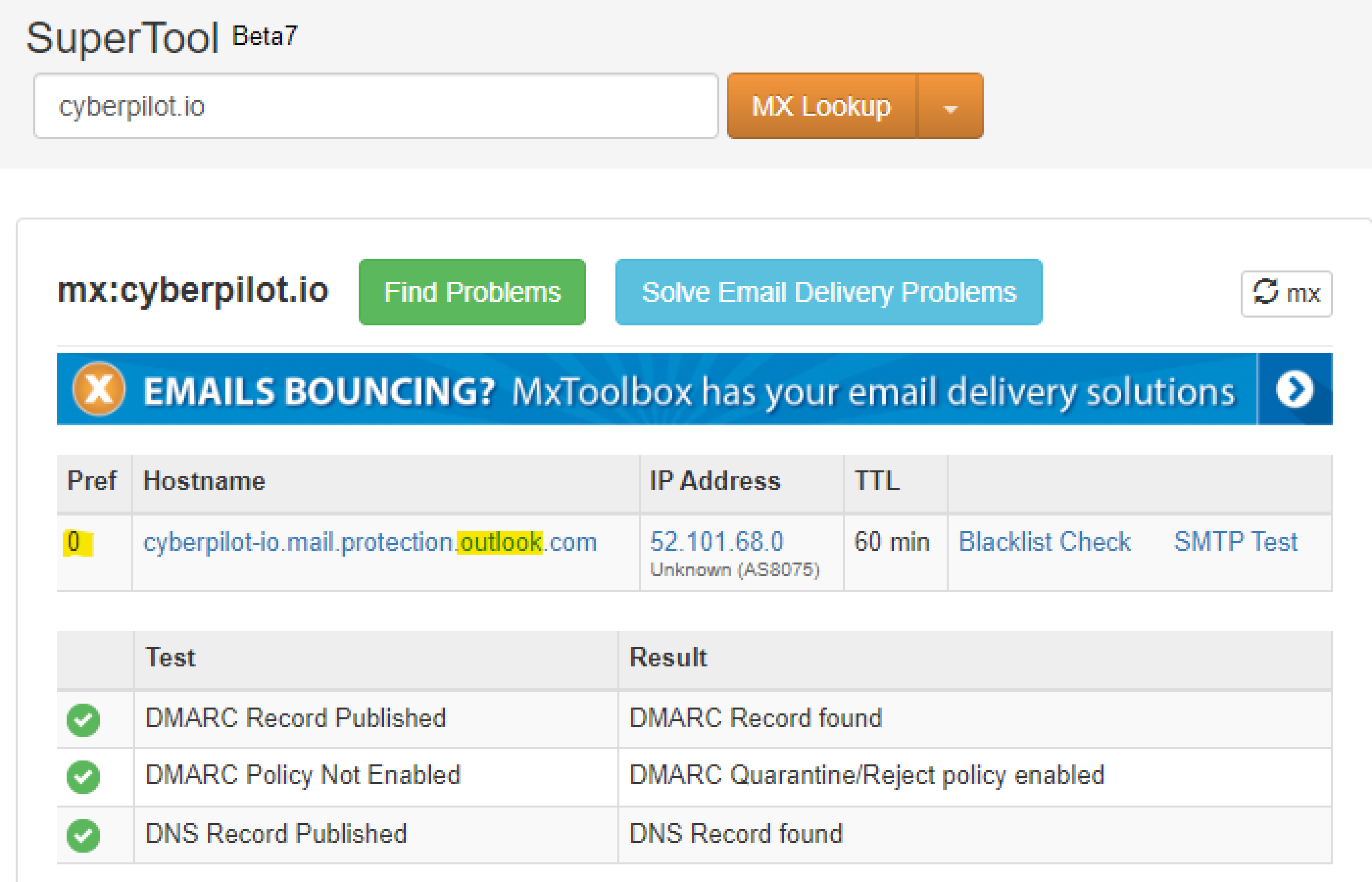
If this is the case, then you can configure a "partner connector" in addition to the steps in this guide. See the guide on connectors.

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
mx:cyberpilot.io
Find Problems
Solve Email Delivery Problems
mx
EMAILS BOUNCING? MxToolbox has your email delivery solutions

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

CyberPilot