Trustwave®

Advanced Phishing Scanner Instructions

How to Register

Instructions for clients interested in the mailbox scanner

1 **Choose Region**

An email administrator goes to the scanner website, and chooses the applicable region (Americas, EMEA or APAC) for where their mailboxes reside

2 **Create Account**

Administrator clicks ‘Sign up now,’ creates the account, and provides their organization’s M365 Tenant ID

3 **Grant Permission**

Administrator grants permission for the tool to access mailbox and user data

4 **Email Scanning**

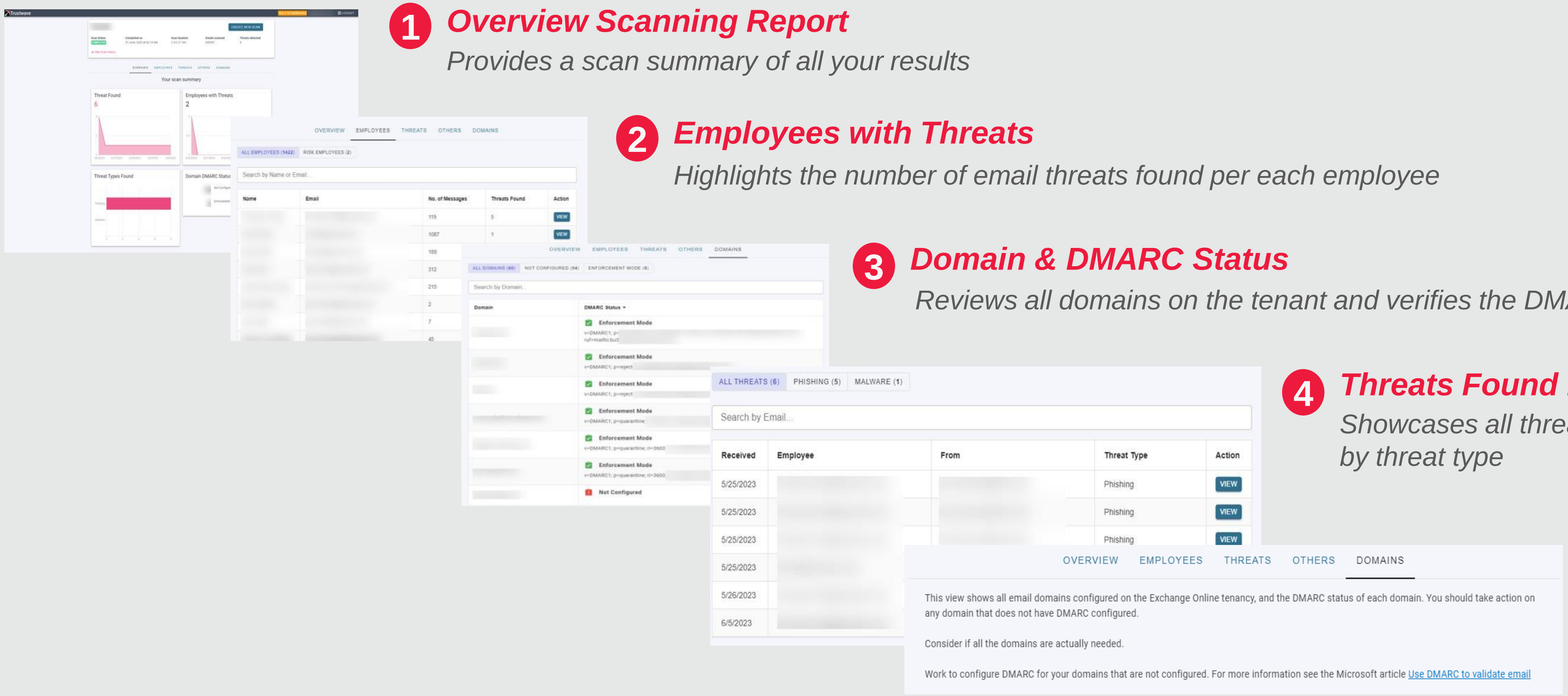
A message retrieving service is launched to gather 1 month of data. An isolated MailMarshal instance is launched, which then processes the emails gathered

5 **Delivered Results**

The results are available in the portal within ~1 business day. Mailbox data is used in transit and **not stored at rest at any time**

Sample Reports

Sample Findings



OVERVIEW EMPLOYEES THREATS OTHERS DOMAINS

ALL EMPLOYEES (1422) RISK EMPLOYEES (2)

Search by Name or Email...

Name	Email	No. of Messages	Threats Found	Action
[redacted]	[redacted]	119	5	VIEW
[redacted]	[redacted]	1087	1	VIEW
[redacted]	[redacted]	189		
[redacted]	[redacted]	312		
[redacted]	[redacted]	215		
[redacted]	[redacted]	2		
[redacted]	[redacted]	7		
[redacted]	[redacted]	45		

OVERVIEW EMPLOYEES THREATS OTHERS DOMAINS

ALL DOMAINS (60) NOT CONFIGURED (54) ENFORCEMENT MODE (6)

Search by Domain...

Domain	DMARC Status ▾

[redacted]	✓ Enforcement Mode
	v=DMARC1; p= [redacted]
	ruf=mailto:bu3 [redacted]

[redacted]	✓ Enforcement Mode v=DMARC1; p=reject [redacted]
[redacted]	✓ Enforcement Mode v=DMARC1; p=reject
[redacted]	✓ Enforcement Mode v=DMARC1; p=quarantine
[redacted]	✓ Enforcement Mode v=DMARC1; p=quarantine; ri=3600
[redacted]	✓ Enforcement Mode v=DMARC1; p=quarantine; ri=3600
[redacted]	! Not Configured

ALL THREATS (6) PHISHING (5) MALWARE (1)

Search by Email...

Received	Employee	From	Threat Type	Action
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]			
5/26/2023	[redacted]			
6/5/2023	[redacted]			

OVERVIEW EMPLOYEES THREATS OTHERS DOMAINS

This view shows all email domains configured on the Exchange Online tenancy, and the DMARC status of each domain. You should take action on any domain that does not have DMARC configured.

Consider if all the domains are actually needed.

Work to configure DMARC for your domains that are not configured. For more information see the Microsoft article Use DMARC to validate email

1 *Overview Scanning Report*

Provides a scan summary of all your results

2 *Employees with Threats*

Highlights the number of email threats found per each employee

3 *Domain & DMARC Status*

Reviews all domains on the tenant and verifies the DMARC status

4 *Threats Found in Environment*

Showcases all threats found and categorizes by threat type

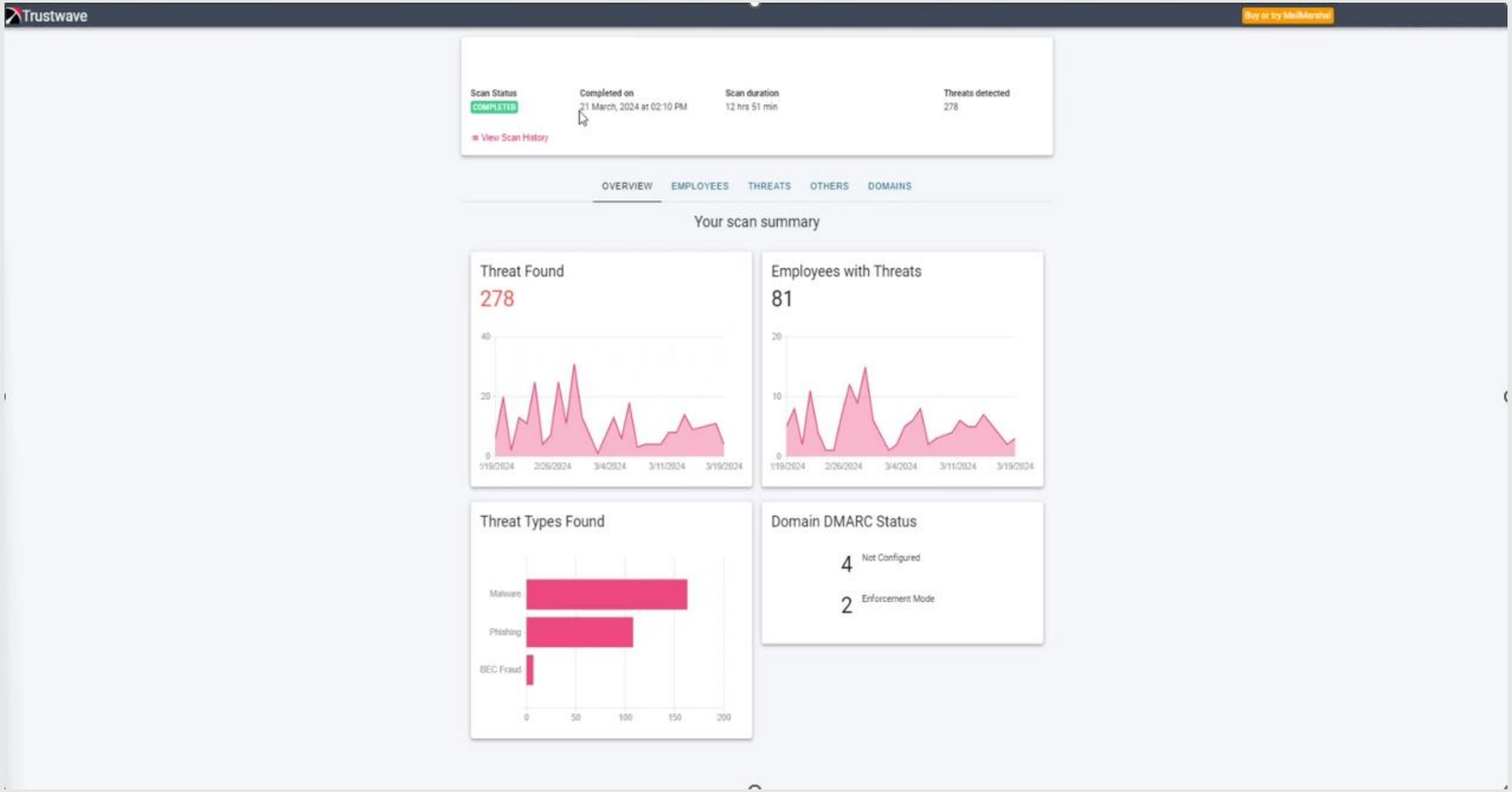
5 *Actions to Improve Security Posture*

Displays actions that should be taken to improve security posture

Scan summary

Summary view of:

- Threats found
- Employees with threats
- Threat types
- Domain DMARC status



Scan Status: COMPLETED
Completed on: 21 March, 2024 at 02:10 PM
Scan duration: 12 hrs 51 min
Threats detected: 278

Your scan summary

Threat Found
278

Employees with Threats
81

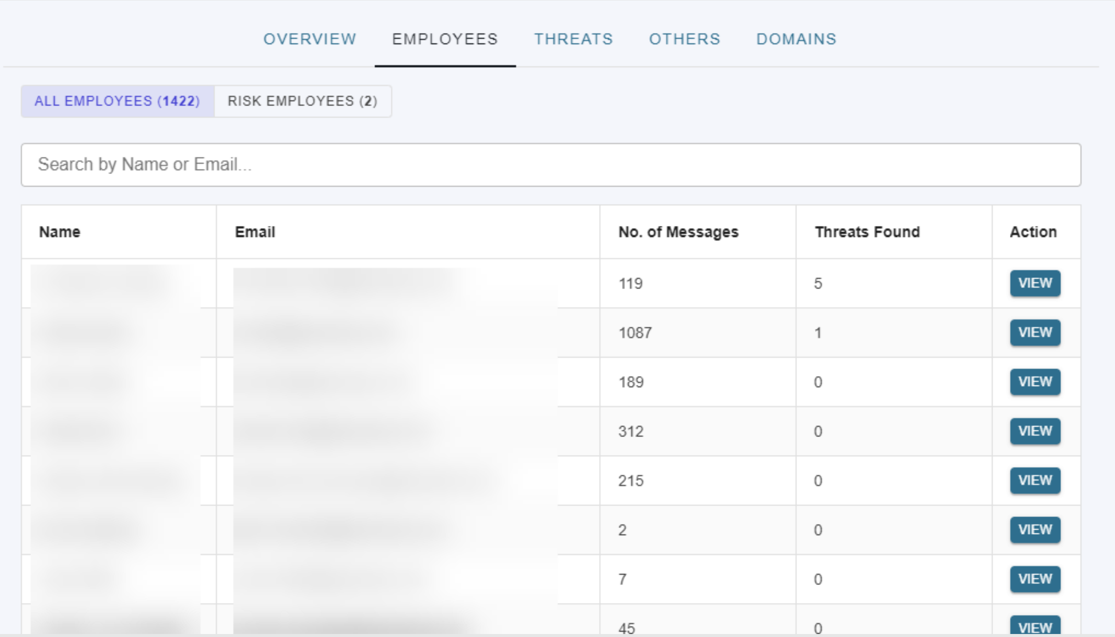
Threat Types Found

Domain DMARC Status

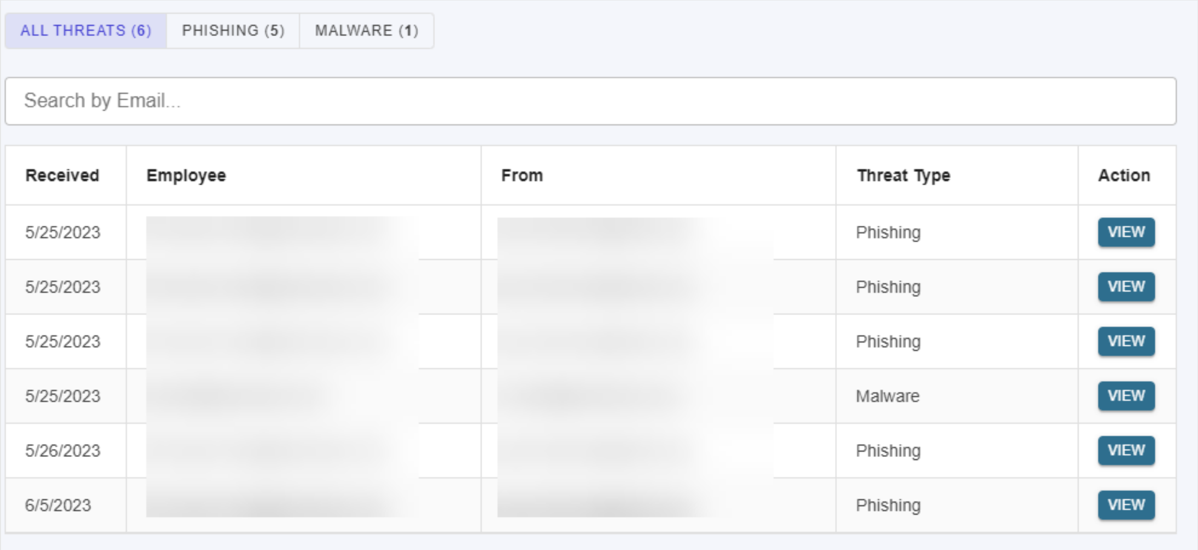
4 Not Configured
2 Enforcement Mode

Employee Information

Highlights the number of email threats found per each employee

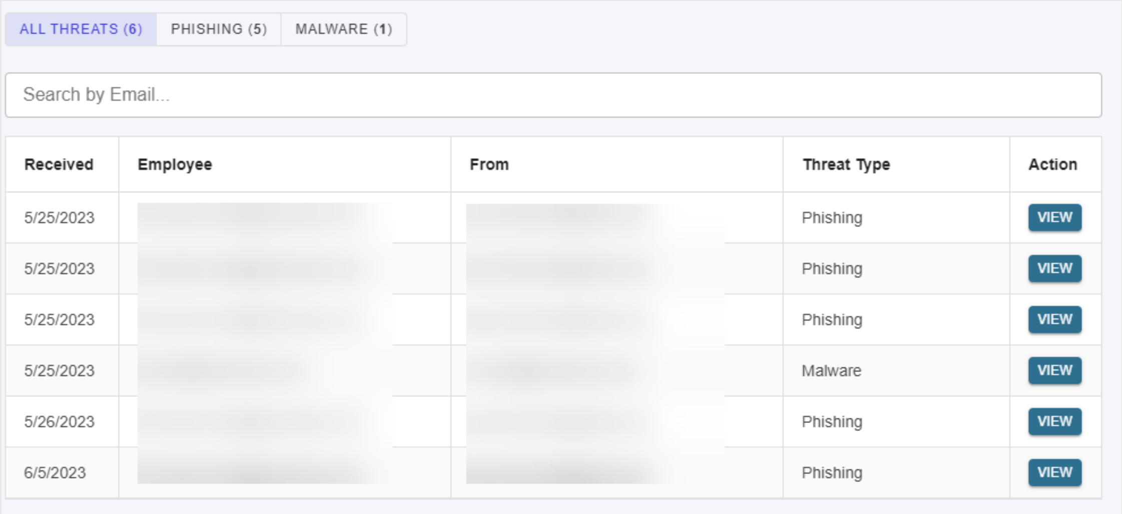


Name	Email	No. of Messages	Threats Found	Action
[redacted]	[redacted]	119	5	VIEW
[redacted]	[redacted]	1087	1	VIEW
[redacted]	[redacted]	189	0	VIEW
[redacted]	[redacted]	312	0	VIEW
[redacted]	[redacted]	215	0	VIEW
[redacted]	[redacted]	2	0	VIEW
[redacted]	[redacted]	7	0	VIEW
[redacted]	[redacted]	45	0	VIEW

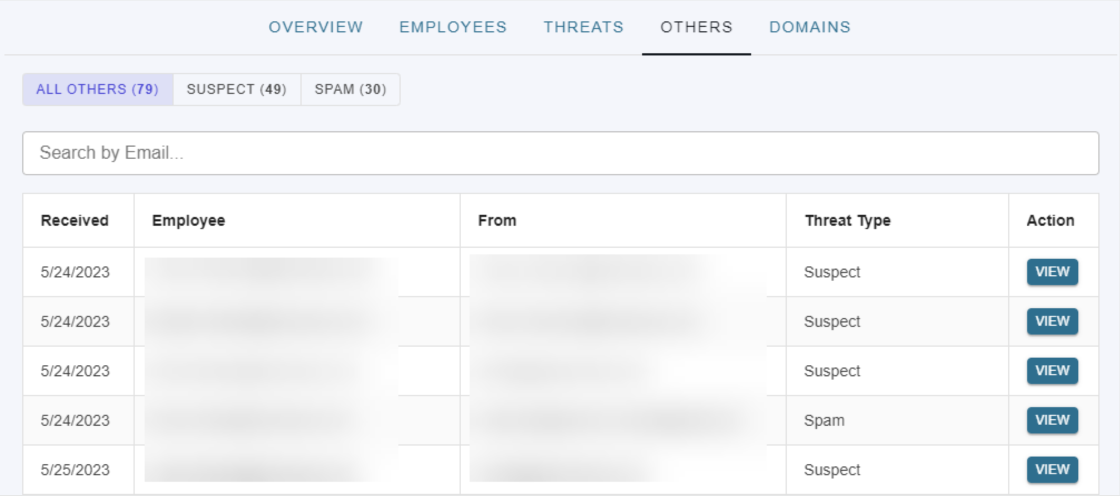


Received	Employee	From	Threat Type	Action
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Malware	VIEW
5/26/2023	[redacted]	[redacted]	Phishing	VIEW
6/5/2023	[redacted]	[redacted]	Phishing	VIEW

Threats



Received	Employee	From	Threat Type	Action
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Phishing	VIEW
5/25/2023	[redacted]	[redacted]	Malware	VIEW
5/26/2023	[redacted]	[redacted]	Phishing	VIEW
6/5/2023	[redacted]	[redacted]	Phishing	VIEW

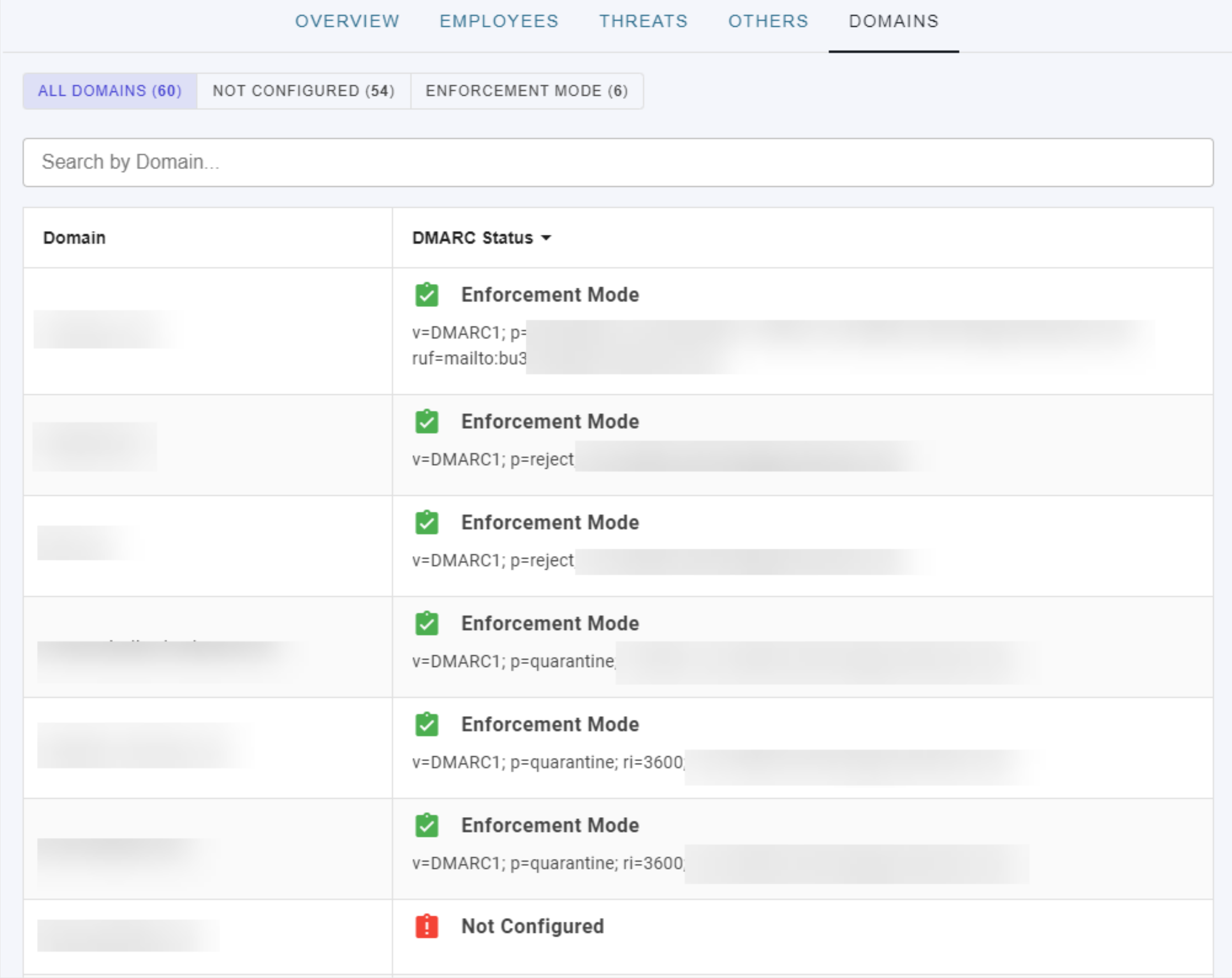


Received	Employee	From	Threat Type	Action
5/24/2023	[redacted]	[redacted]	Suspect	VIEW
5/24/2023	[redacted]	[redacted]	Suspect	VIEW
5/24/2023	[redacted]	[redacted]	Suspect	VIEW
5/24/2023	[redacted]	[redacted]	Spam	VIEW
5/25/2023	[redacted]	[redacted]	Suspect	VIEW

Showcases all threats found and categorizes by threat type, including:

- *Phishing*
- *Malware*
- *Suspect attachments*
- *Spam*
- *Others*

Domains



Domain	DMARC Status ▾

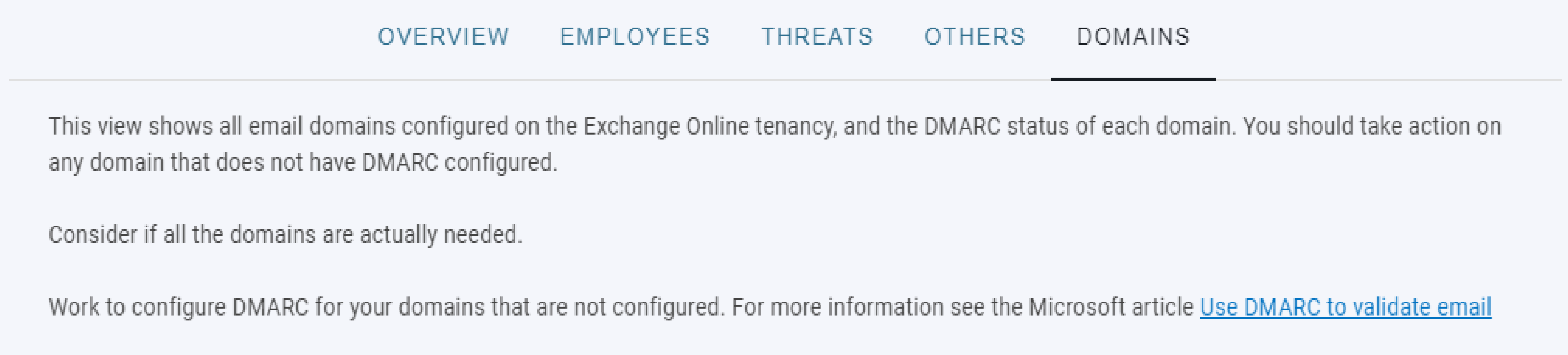
[redacted]	✓ **Enforcement Mode**
	v=DMARC1; p=[redacted]
	ruf=mailto:bu3[redacted]

[redacted]	✓ **Enforcement Mode** v=DMARC1; p=reject[redacted]
[redacted]	✓ **Enforcement Mode** v=DMARC1; p=reject[redacted]
[redacted]	✓ **Enforcement Mode** v=DMARC1; p=quarantine[redacted]
[redacted]	✓ **Enforcement Mode** v=DMARC1; p=quarantine; ri=3600[redacted]
[redacted]	✓ **Enforcement Mode** v=DMARC1; p=quarantine; ri=3600[redacted]
[redacted]	! **Not Configured**

Reviews all domains on the tenant and verifies the DMARC status

Recommended Actions

Displays actions that should be taken to improve email security posture



This view shows all email domains configured on the Exchange Online tenancy, and the DMARC status of each domain. You should take action on any domain that does not have DMARC configured.

Consider if all the domains are actually needed.

Work to configure DMARC for your domains that are not configured. For more information see the Microsoft article Use DMARC to validate email