

Thanks for your interest in Harmony Email & Collaboration CheckUp.

Please note that Harmony Email & Collaboration is designed to be non-intrusive and does not require any changes to your MX records. By default, you will be onboarded into monitor/detect only. Onboarding requires a global admin to perform the setup process but can be reduced to an exchange admin after onboarding.

We will provide a high-level overview of the email and security health check steps during the discovery call. The dependencies and deliverables after each will also be highlighted.

The next few slides will go over the CheckUp process and what you can expect in the coming days and weeks, followed by a sample of the report you will receive once the CheckUp is over.

Harmony Email & Collaboration CheckUp - 14 Day Overview



The First Meeting

Objective: Establish a first call with the customer to provide a high-level overview of what is offered during the health check and the different steps

Dependencies: Signed up for the health check. Having the global admin or Exchange admin present will be beneficial. Also, (assuming) approval is needed for any change control on the customer side to proceed with the installation and start the health checks

Deliverable: Agree on the installation date and start date of the health check and cover the installation process and sample report, offer assistance with any change control approval preparation needed, and cover any questions raised from the customer side.

The Installation

Objective: Installation of the Harmony email and collaboration product with the assistance of the Global/exchange admin present

Dependencies: Having the global admin or Exchange admin present and approval for change control on the customer side. Checkpoint and partner technical resources are present and assisting with the installation.

Deliverable: Baseline report after installation, and contact details on the partner and checkpoint side for any questions during the health check and/or support needed.

Harmony Email & Collaboration Deployment - Just a Few Clicks

1

Welcome to Check Point

georgep@avanan.com

Please follow this short wizard to activate Check Point's Cloud-Security platform.
In this short wizard you will choose the SaaS you wish to secure as well as the security issues you wish to resolve.
Your selection can be modified later from our app-store.
Ready? Let's get started!

Let's Get Started

2

SaaS Selection

In this screen you need to select the cloud-service. You will be required to authorize access to Check Point using a SAML admin-level authentication to your SAAS. To chose - click on "Start" below the SAAS icon, and follow the authentication instructions.
Please note - without proper admin-level authentication Check Point will not be able to secure that service. You can choose multiple SAAS products to have Check Point secure all of them and you can change this selection later on.

Office 365 Mail

Top-of-the-line set of productivity tools

Start

Gmail

Gmail is built on the idea that email can be more efficient and useful

Start

Office 365 OneDrive

Designed for business—access, share, and collaborate on all your files from anywhere

Start

Office 365 SharePoint

SharePoint empowers teamwork with dynamic and productive team sites for every project team, department, and division

Start

Microsoft Teams

Microsoft Teams is a hub for teamwork in Office 365

Start

Google Drive

Get access to files anywhere through secure cloud storage

Start

Slack

A messaging app for teams

Start

Dropbox

Safe, simple way to access your files on any device

Start

3

Installation Mode

☒ Automatic: The initial setup and future configuration changes in the Exchange admin center will be performed by the Check Point application.

☐ Manual: The initial setup and any future configuration changes must be done manually in the Exchange admin center. Check Point will not take any action with the application. Please contact support@checkpoint.com for assistance.

☐ Restrict inspection to a specific group (group filter)

☐ I Accept [Terms Of Service](#)

Cancel

OK

4

Pick an account

Admin User
admin@avanandemo3.onmicrosoft.com
Signed in

user1@avanandemo1.onmicrosoft.com

Use another account

5

Microsoft

admin@avanandemo3.onmicrosoft.com

Permissions requested
Review for your organization

AVANAN Cloud Security Platform - Emails V2
avanan.com

This application is not published by Microsoft or your organization.

This app would like to:

Read and write user and shared mail

Send mail on behalf of others

Read and write user mailbox settings

Read and write all groups (preview)

Send mail as a user

Read and write user mail

Manage Exchange As Application

Read and write all user mailbox settings

Read and write contacts in all mailboxes

Read and write mail in all mailboxes

Send mail as any user

Use Exchange Web Services with full access to all mailboxes

Read and write directory data

Access directory as the signed in user

Read and write all groups

Read and write all directory RBAC settings

Read and write all users' full profiles

Read activity data for your organization

Read service health information for your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

Check Point Software Technologies Ltd. All rights reserved ©

Security Checkup - Threat Analysis Report

During the CheckUp

Objective: 15 minute call after week one of the health check to provide feedback on the initial observations and to cover any questions or concerns from the customer side.

Dependencies: None.

Deliverable: First report, cover any observations from the first week.

Conclusion of CheckUp

Objective: Provide final feedback on the findings after the health check, deactivation of the Harmony email and collaboration agent, and rollback of the customer environment to the initial state before the health check.

Dependencies: None.

Deliverable: Detailed discussion of the actual report generated for the customer and recommendations moving forward.

Outcome: Mutually agreed outcome of the health check offered and any agreed-on next steps.

HEC01

SECURITY CHECKUP

February 14, 2023 - March 16, 2023



SIX DEGREES CONSULTING

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
EMAIL PROTECTION OVERVIEW	4
EMAIL PROTECTION	7
MALWARE PROTECTION	8
SPAM PROTECTION	9
DATA LOSS PREVENTION	10
SHADOW IT	11
MICROSOFT TEAMS	12

This Security Checkup report provides a periodic overview of the threats detected in emails and other protected collaboration applications and how they were handled by the policy.



Phishing Emails
149



Spam Emails
26



Malware Emails
12

Events by Platform



Office 365 Mail
209



Gmail
13

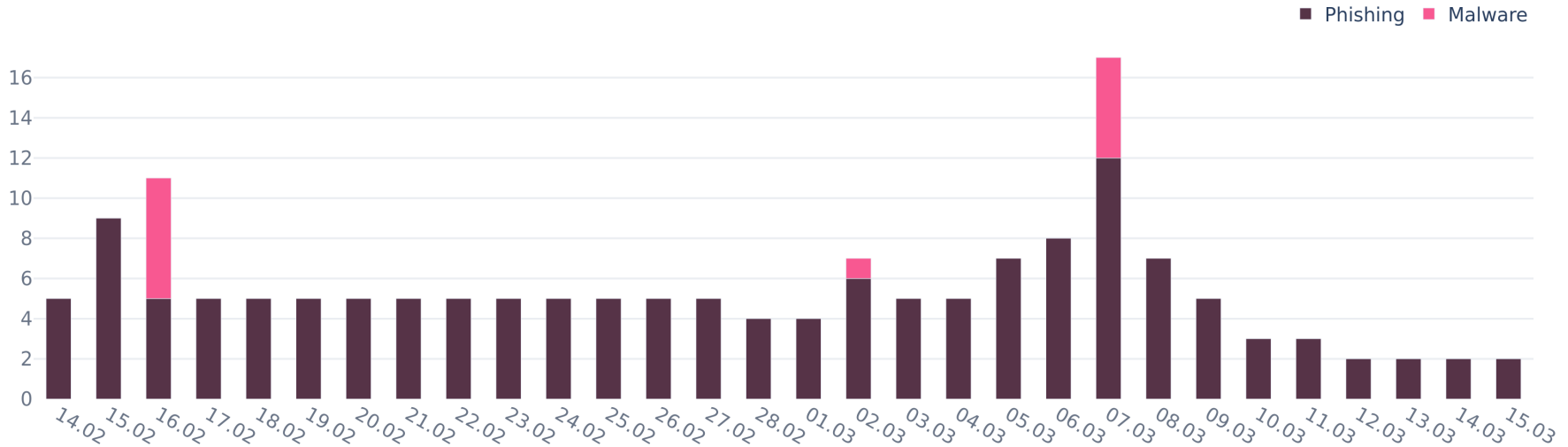


Microsoft Teams
6

Top Attacked Users

User Name	User Title	Department	
Tom Smith user1@hec01.onmicros..	Chief Executive Offi...	Executive	94
Maurice Moss maurice.moss@acmemx...	N/A	N/A	67
Mohammad Abulebda admin@hec01demo.com	N/A	N/A	11
Bob Smith user2@hec01.onmicros..	N/A	N/A	6
Jen Barber jen.barber@acmemx.co..	N/A	N/A	5

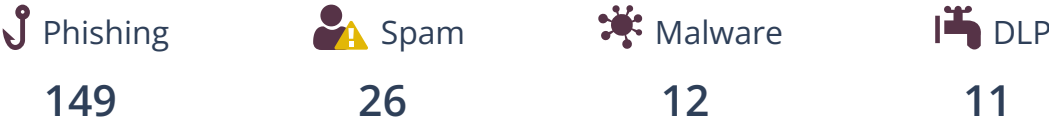
Events Trend



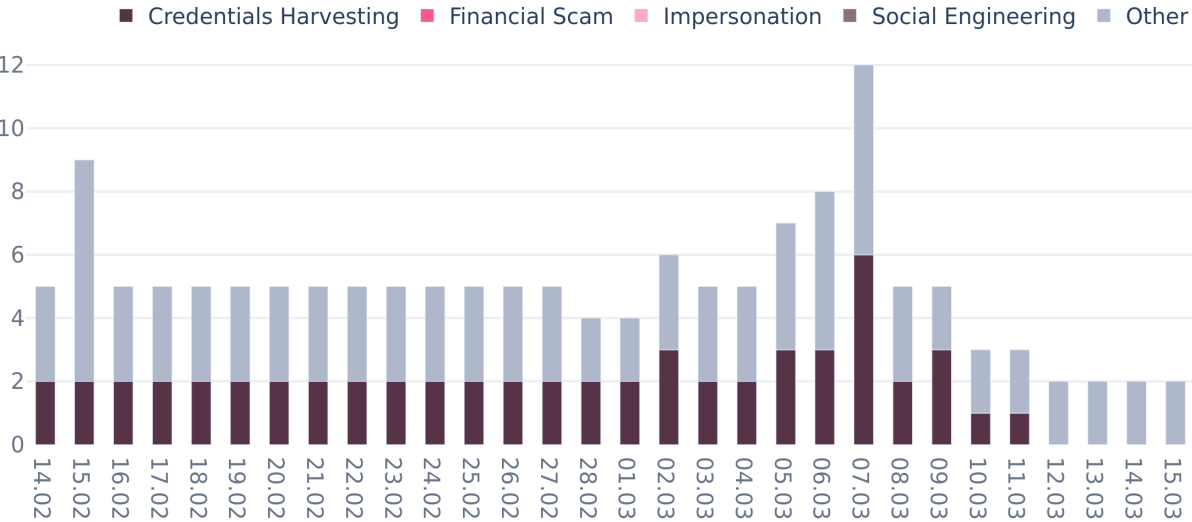
This page provides an overview of the detected email threats and how they were handled by the policy.

Total Security Events198

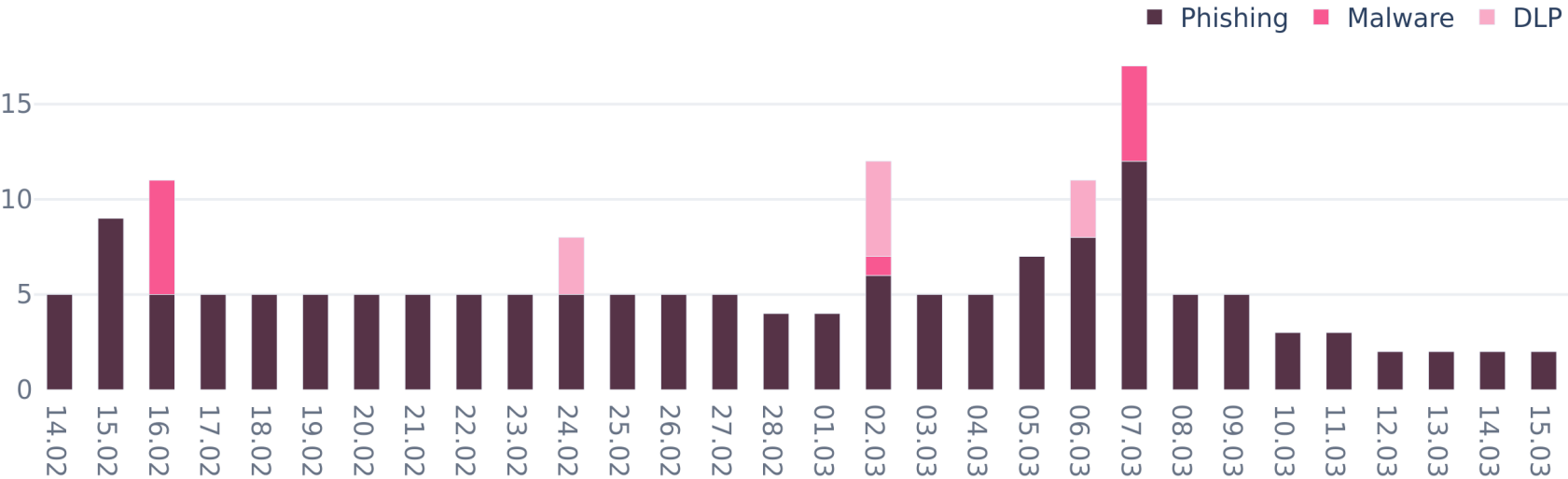
Out of which:



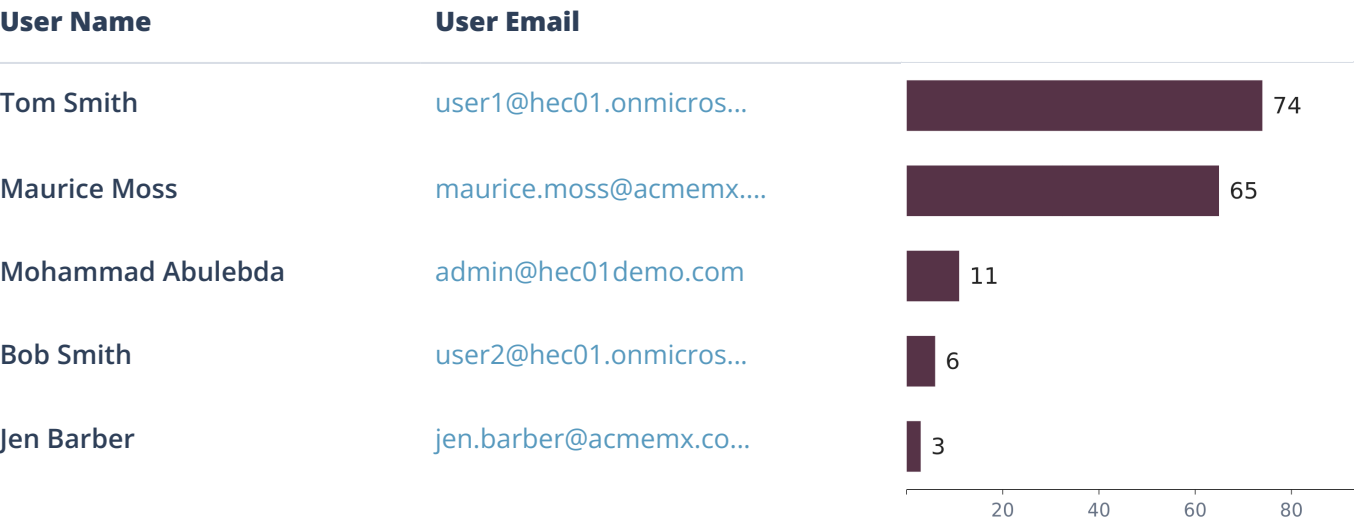
Top Phishing Detection Reasons



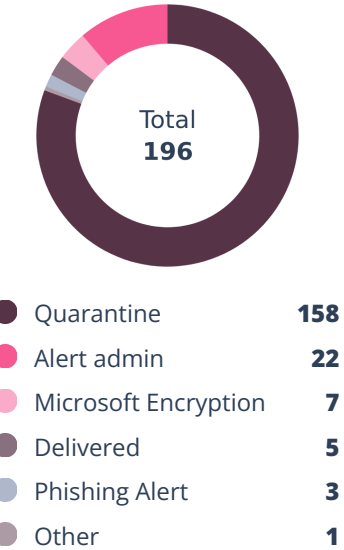
Events Trend



Top Attacked Users



Security Events by Enforcement

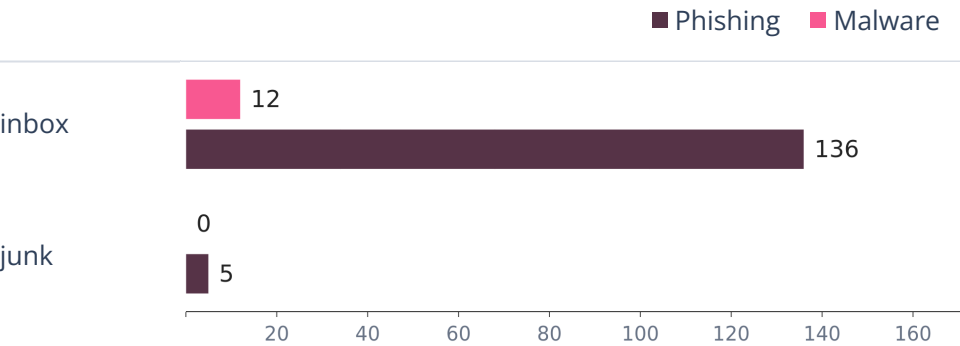


This page separates threats that Microsoft would deliver to the Inbox vs. Junk folder, if it wasn't for Check Point.

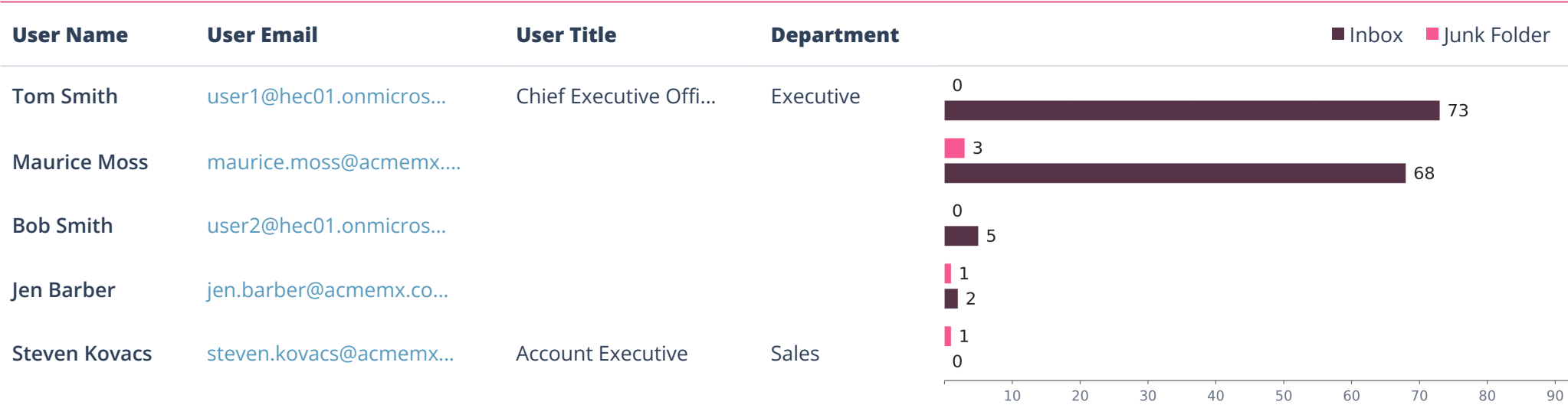
Threats Delivered by Microsoft to:



Threat Types in Inbox vs. Junk Folder



Top Attacked Users - Inbox vs. Junk Folder



This page is based on data from the last two weeks only (Mar 01, 2023 - Mar 16, 2023)

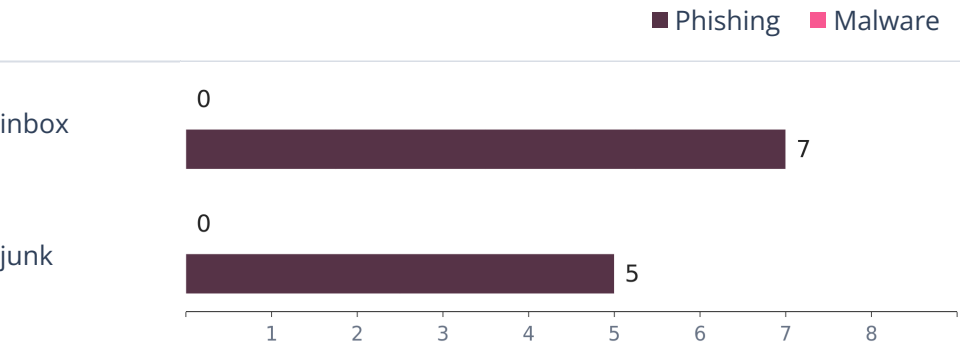
Some emails might have been quarantined by Microsoft, after being delivered to end users.

This page separates threats that Google would deliver to the Inbox vs. Junk folder, if it wasn't for Check Point.

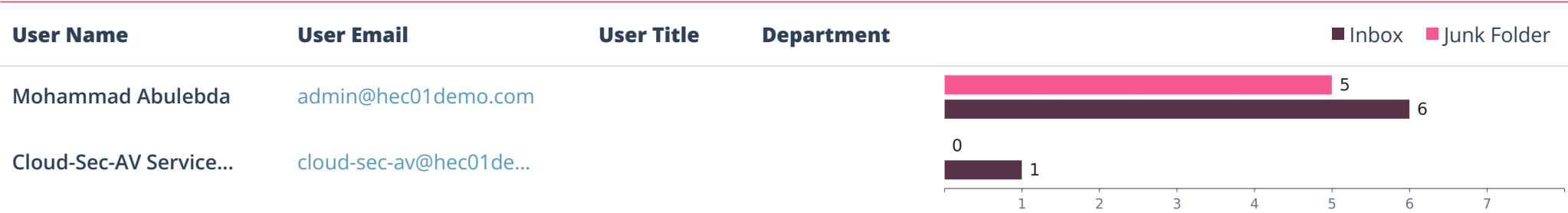
Threats Delivered by Google to:



Threat Types in Inbox vs. Junk Folder



Top Attacked Users - Inbox vs. Junk Folder



This page is based on data from the last two weeks only (Mar 01, 2023 - Mar 16, 2023)

Some emails might have been quarantined by Google, after being delivered to end users.

Top Attacked Users - All

User Name	User Email	User Title	Department	Phishing	Malware
Tom Smith	user1@hec01.onmicros...	Chief Executive Offi...	Executive	72	2
Maurice Moss	maurice.moss@acmemx....	N/A	N/A	60	5
Mohammad Abulebda	admin@hec01demo.com	N/A	N/A	11	0
Bob Smith	user2@hec01.onmicros...	N/A	N/A	1	5
Jen Barber	jen.barber@acmemx.co...	N/A	N/A	3	0
Cloud-Sec-AV Service...	cloud-sec-av@hec01de...	N/A	N/A	1	0
Steven Kovacs	steven.kovacs@acmemx...	Account Executive	Sales	1	0

Security Events by Department

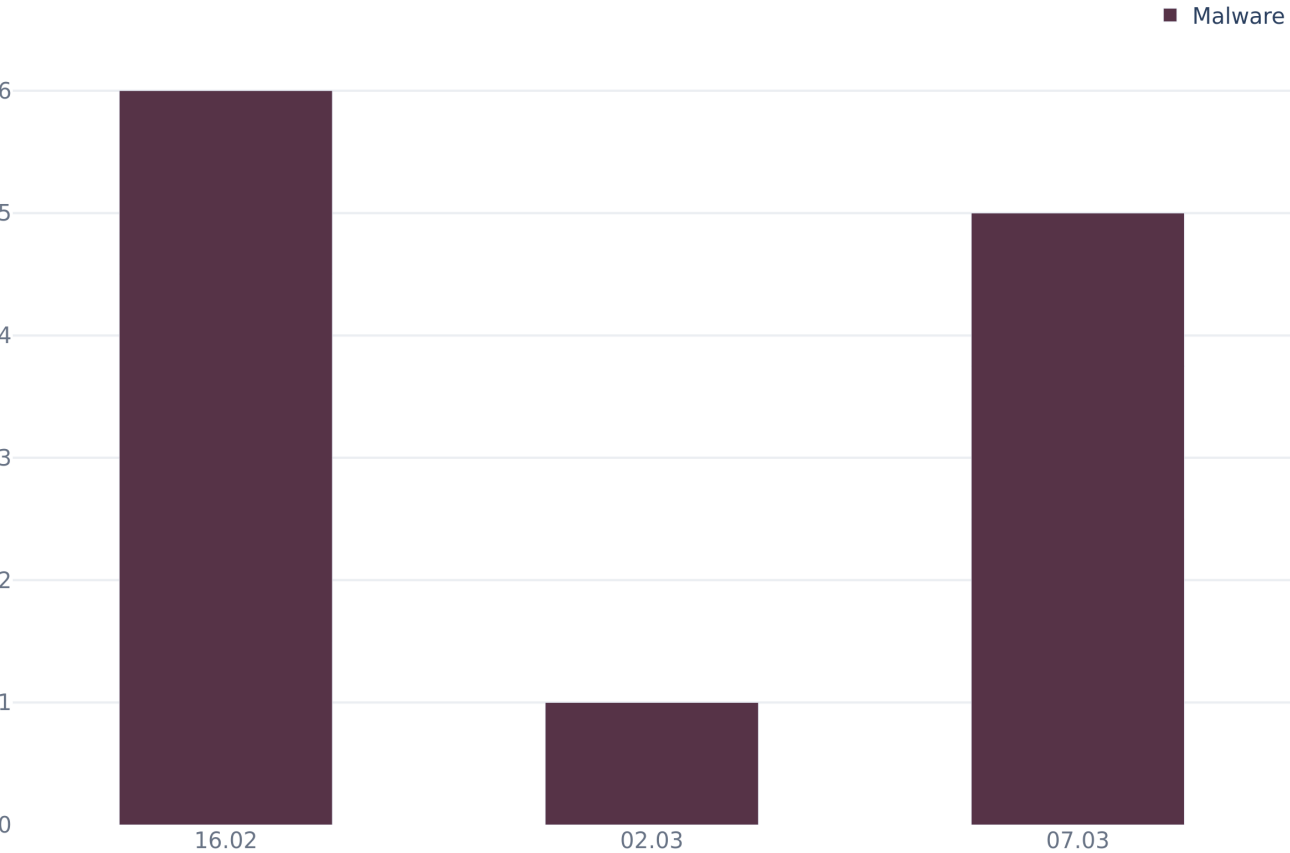


Clicks on Malicious Links



This page provides an overview of the malware detected files and how they were handled by the policy.

Malware Trend



Top Attacked Users

User Name	User Email	User Title	Department	Count
Bob Smith	user2@hec01.onmicros...	N/A	N/A	5
Maurice Moss	maurice.moss@acmemx....	N/A	N/A	5
Tom Smith	user1@hec01.onmicros...	Chief Executive Offi...	Executive	2

Malware Events by Enforcement



This page provides an overview of the detected Spam emails and how they were handled by the policy.

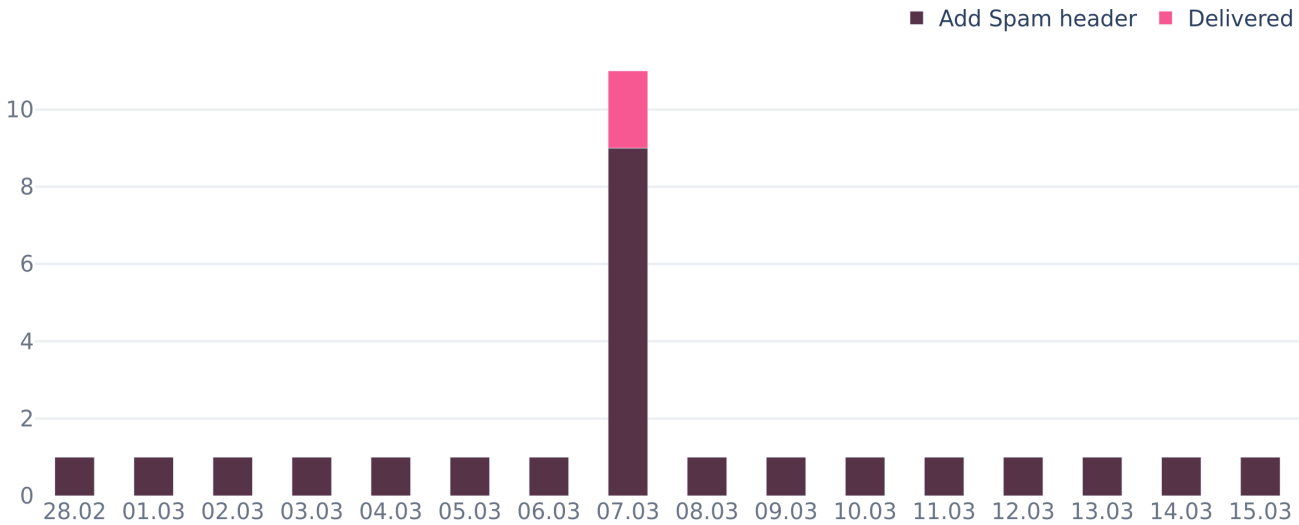
 Spam Emails

26

Spam Events by Enforcement



Events Trend



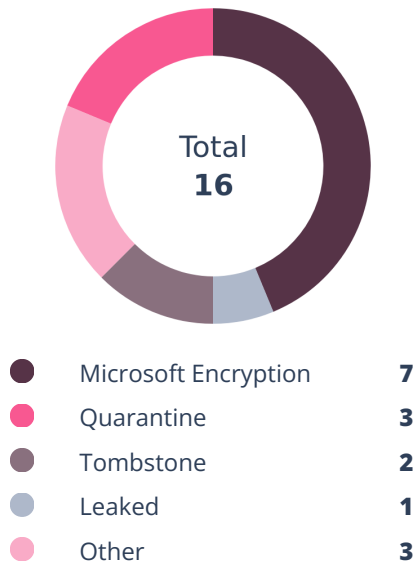
Top Attacked Users

User Name	User Title	Department	Count
Tom Smith user1@hec01.onmicros..	Chief Executive Offi...	Executive	18
Jen Barber jen.barber@acmemx.co..	N/A	N/A	2
Maurice Moss maurice.moss@acmemx...	N/A	N/A	2
Steven Kovacs steven.kovacs@acmemx..	Account Executive	Sales	2
Douglas Reynholm douglas.reynholm@acm..	President & Son of F...	Boss	1

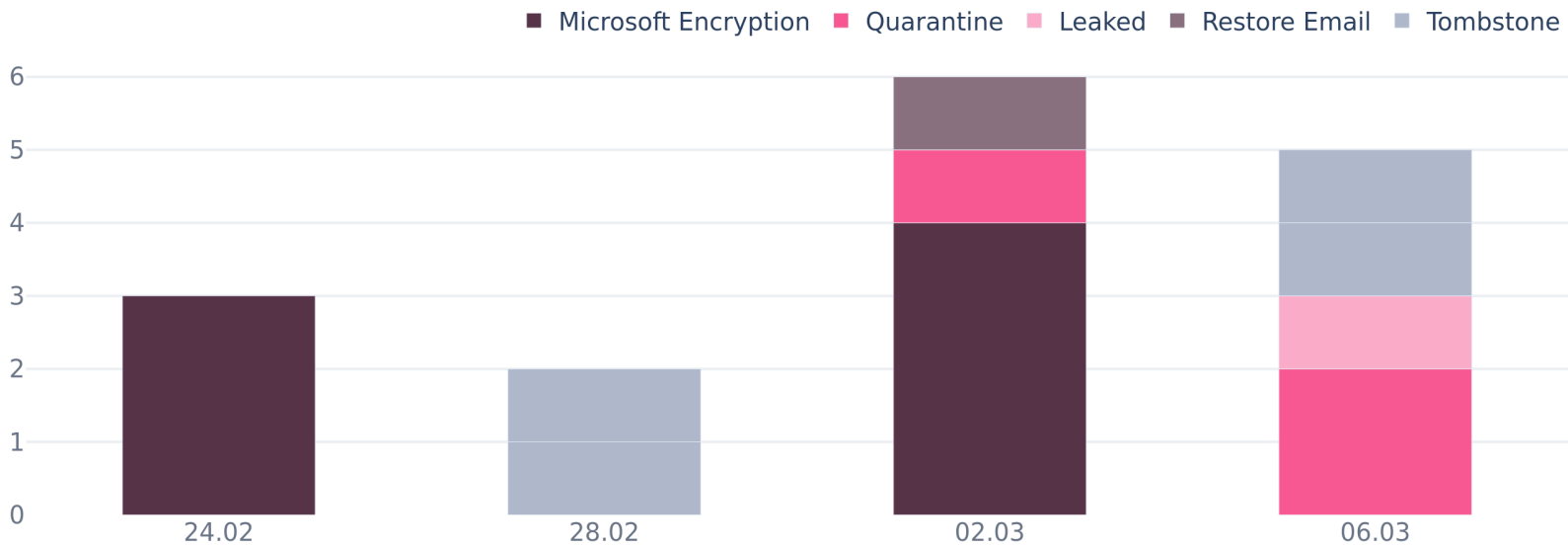
Top Senders

vincent.vega@wallace.angrybomb.com	16
wayne.campbell@hec01demo.com	9
sloane.peterson@cronocorp.com	1

DLP Events by Action



DLP Events Trend



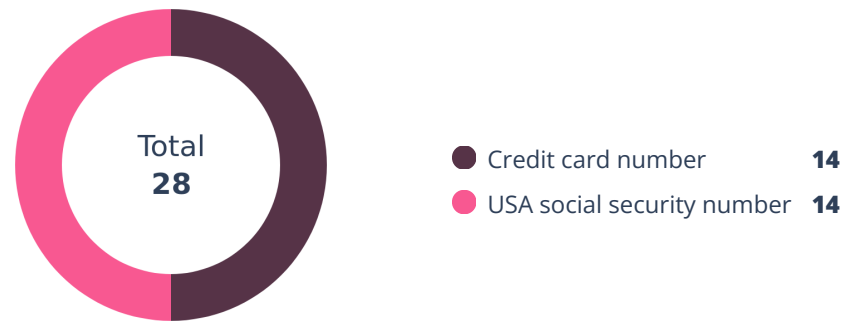
DLP Events by Platform



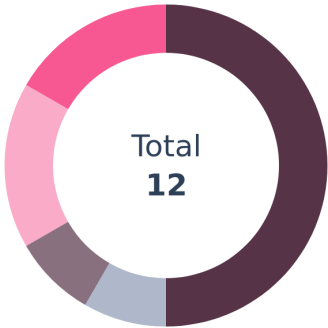
Top Violating Users

User Name	User Email	User Title	Department	Count
Tom Smith	user1@hec01.onmicros...	Chief Executive Offi...	Executive	15

Top Data Types Leaked

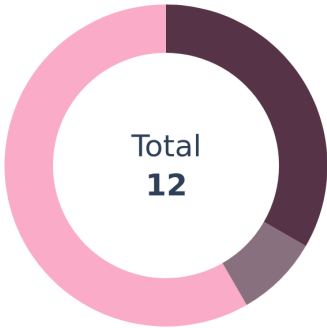


Newly Detected Platforms



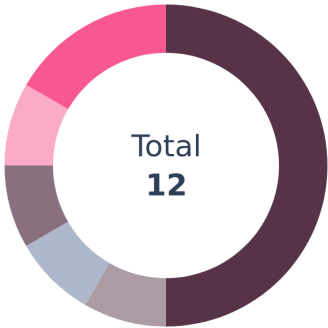
- Social Network 6
- Online Data Storage 2
- Collaboration 1
- Online Marketing 1
- Other 2

Detected Apps by Risk



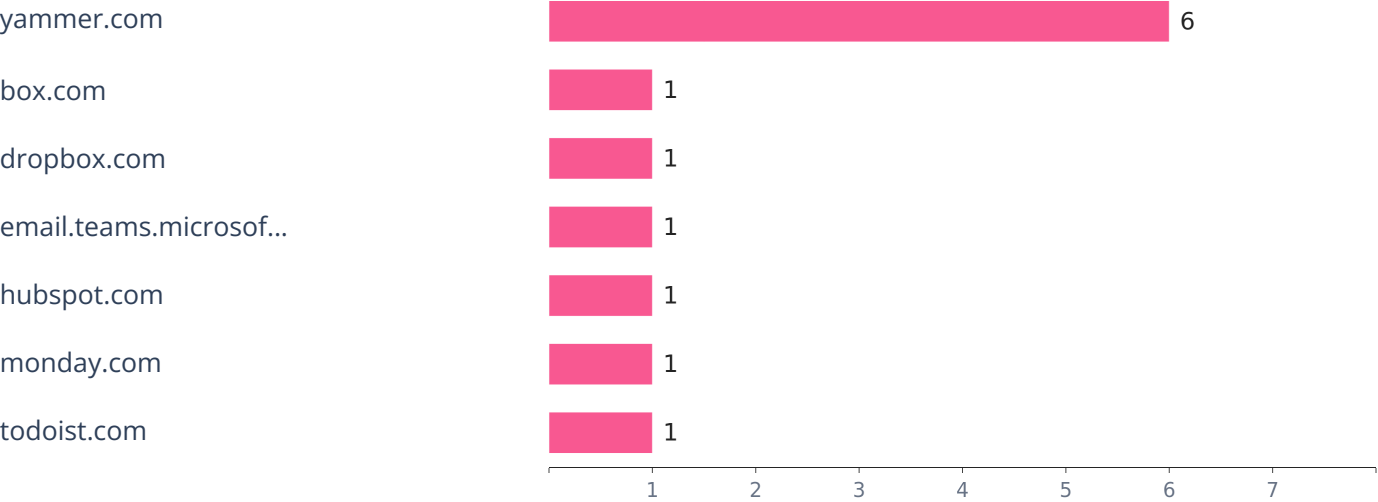
- Critical 4
- Medium 7
- Low 1

Detected Apps by Category



- Social Network 6
- Online Data Storage 2
- Collaboration 1
- Online Marketing 1
- Project Management 1
- Task Management 1

Top Popular Services



Top Active Users

User Name	User Title	Department	Count
Maurice Moss maurice.moss@acmemx.com	N/A	N/A	6
Jen Barber jen.barber@acmemx.com	N/A	N/A	2
Douglas Reynholm douglas.reynholm@acmemx.c..	President & Son of Founde...	Boss	1
Robin Harris robin.harris@acmemx.com	Event Marketing Manager	Marketing	1
Steven Kovacs steven.kovacs@acmemx.com	Account Executive	Sales	1

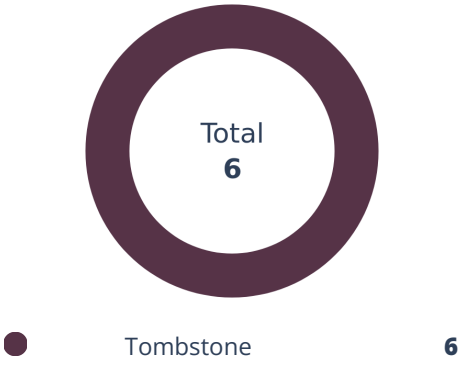
Total Security Events6

Out of which:

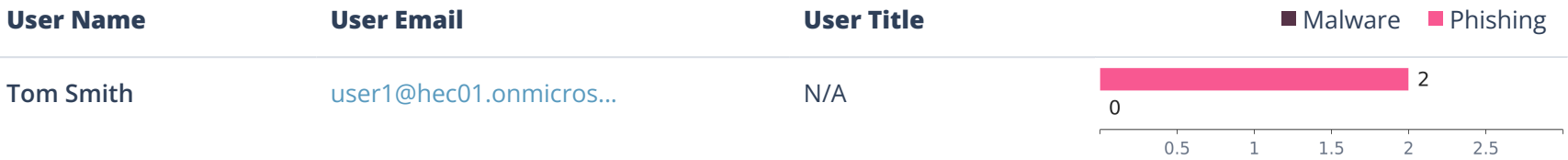
DLP4

Phishing2

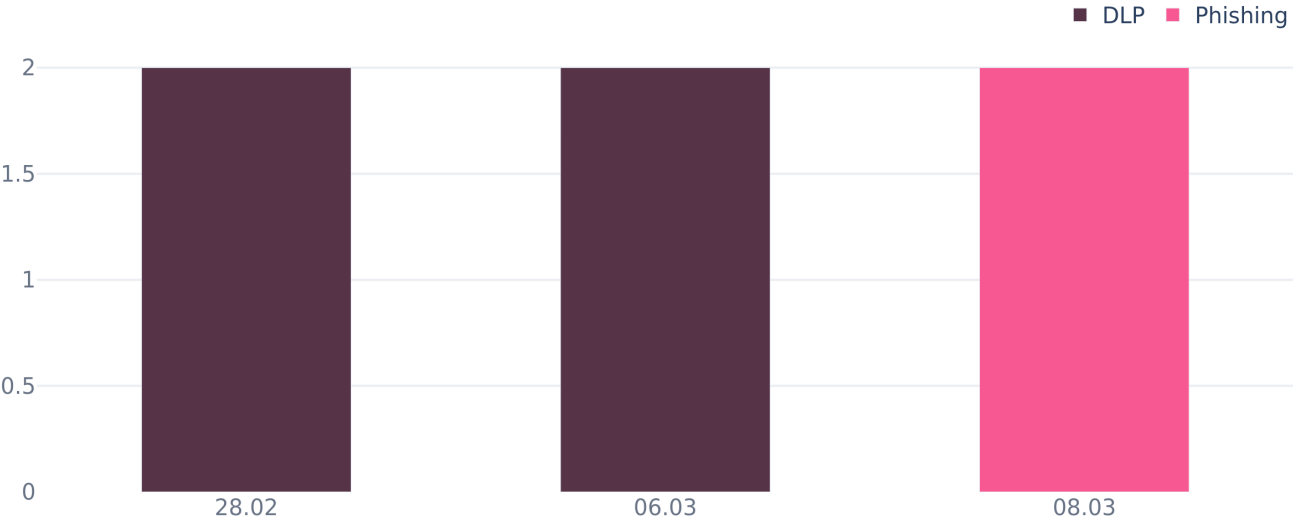
Enforcement Actions



Top Users Sending Malicious Messages



Security Events Over Time



Top Users Leaking Sensitive Data

