

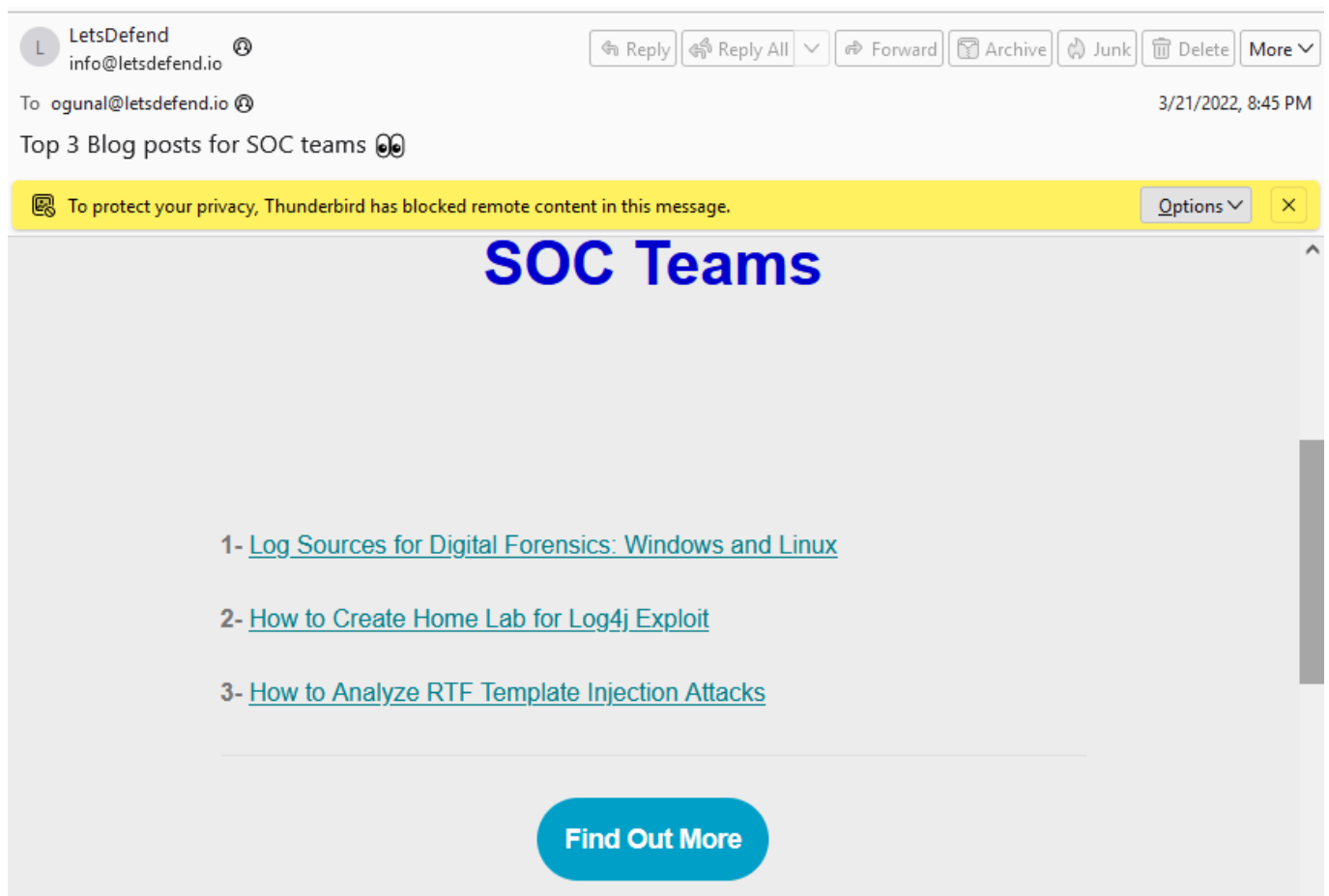
# **Phishing Email Analysis Report**

Cybersecurity Internship

Prepared by: Thumma Kiranmai

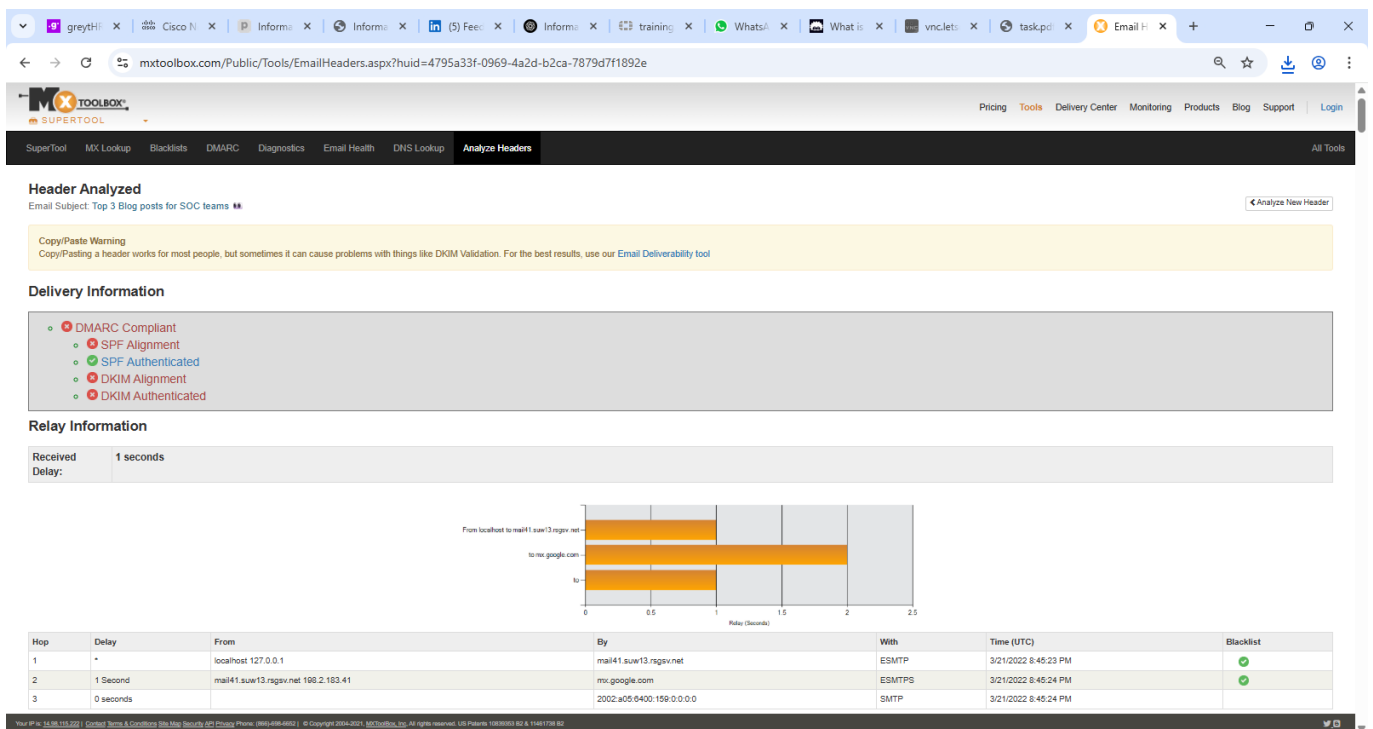
Date: May 27, 2025

## Received Email Analysis



This section displays an email designed to appear as a legitimate message from LetsDefend. The email offers cybersecurity blog content targeting SOC professionals. The sender address is shown as info@letsdefend.io. Despite appearing credible, the email client flags the message and blocks remote content to protect the user from potential trackers or embedded threats. The visual layout includes a call-to-action button and brief descriptions of blog topics. There's no visible malicious link, but a lack of personalization can be noted. The layout and format resemble promotional content. However, the legitimacy of such messages must be verified via backend metadata. The presence of tracking elements or third-party analytics scripts can't be ruled out. Overall, it appears to be a promotional email. This entry sets the context for technical analysis to follow. The visual format mimics typical newsletters used in targeted phishing.

# Email Header Analysis



This analysis focuses on the technical metadata of the email. It reveals that while SPF and DKIM passed authentication checks, both failed domain alignment. Consequently, DMARC evaluation failed. This misalignment often occurs when third-party services like Mailchimp send emails on behalf of an organization without full domain integration. The delivery path and DKIM signature point to mailchimpapp.net, not letsdefend.io. Email clients and servers use this information to assess trust. The fail result under DMARC suggests the message could be forged or misconfigured. This makes the message more likely to be flagged or rejected in enterprise filters. Email administrators must configure SPF and DKIM to align precisely. Domain alignment failures are a common vector for spoofing. The result indicates that even legitimate services can produce untrusted messages if setup is incorrect.

## SPF/DKIM Record Details

The screenshot displays the 'SPF and DKIM Information' section of the mxtoolbox.com website. It shows the following details:

- DMARC:** Letsdefend.io. The record is `v=DMARC1; p=none;`. A green status bar indicates it is passing.
- SPF:** Mail41.suw13.rsgsv.net:198.2.183.41. The record is `v=spf1 ip4:198.2.183.41 include:spf.mandrillapp.com -all`. A red status bar indicates it is failing.
- DKIM:** Mailchimpapp.net:k3. The record is `v=DKIM1; k=rsa; p=H1IB1jAN8qhk1Gw8BAQEFAAOQA8M1IBcgcAQZAsYqU5Sn7Fau5vF5X4BvR101RtBNLCY883H11ckx3DIE7257auw+qC3IARdF1L6CuLGNFxsG1gVr6png4ajc1e5QGr0eh8gxnDNbaASTX8FnfceF3U3oxLOF89EKgxn5SHCK; eKvB8PK3borKoZ9HtE1484f1qhcuXXIgtKtAuthHfUt2P888zh1X1gOe/w496ch7983c`. A red status bar indicates it is failing.

Below the records, a 'DKIM Signature Error' message states: 'There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info'. The 'Headers Found' section shows a table with one header: 'Delivered-To' with the value 'ogunal@letsdefend.io'.

This section isolates the authentication records within the header. It highlights SPF passing through permitted IPs but failing alignment due to the sender domain mismatch. DKIM was signed by mailchimpapp.net, indicating use of an external service. The key takeaway is that DKIM signatures must match the "From" domain to ensure trust. Failure to align SPF or DKIM leads to DMARC failure, weakening sender reputation. This configuration error is exploited in domain spoofing attacks. Even properly signed emails are untrusted if the domain isn't aligned. The key focus here is on DNS-level security protocols. Correct SPF, DKIM, and DMARC policies must align to pass all authentication layers. Organizations using third-party mailers must configure subdomains properly. This ensures alignment and prevents unintentional DMARC failures.

**Dkim Signature Error:**  
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info

### Headers Found

Header Name	Header Value
Delivered-To	oguna@letsdefend.io
X-Google-Smtp-Source	AldBPlZdsyR+DNC4kzH4sTVGRMTuZgqBPoT7WzDaZaQRebOMIABySvOstbkng1NaGo3C3CB
X-Received	by=2022.as5.1344.b0.033.7562.eofw with SMTP id 05-2002a2c1344000000b00537962e0fmr24595051yst.211.1047895524501. Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
ARC-Seal	i=; arsip-sha256:=1t647895524; cvnone; dggoogle.com; s=saro=20100816. b=DVPh/vjhuwCQ3K/tzcoNJR7m3hJZFsa90w/K/Fpmxakvo/V774YrHX4ke3.Jk0HT.Lt2ZjpWd4QZFGxglUwNB3ozhr808/qgQHCSHfDPQ44UvhvbnJSBCFBI9/SvpTrJkHf+hWuL/Gv4NDWNeISQhtShqUJ3BKnmDbUMnUs7Mw4OCBAZELJlVJXUmlG 5MlUg/WdUrkABGNZuzIoyouGCO2G3yGeGX4YrzEck/HuedCherFPqOmWkuJA3EI YRWdXanaYpLUdUwHvGFQbzQEZYXqFSMOuChCaadZdt7tonj7mdGsoayq3Xh PdyQ==
ARC-Message-Signature	i=; arsip-sha256:=related+relaxed; dggoogle.com; s=saro=20100816. hmime-version list-unsubscribe-post list-unsubscribe-list-id: feedback-id: message-id: date: reply-to: from: subject dkim-signature: bh=W7bT6TdXnhQCZuLwJv55a9q9zgiz2SnkJESQSVyhH0=: h=Fth+AvaAJAa=P831ze4hvYYLlDuBaF+Wnd3YLMXY 83UCOOXXmasRNvNi. tsgHevanNXjHPHyCoBqTaP68RaUenHW3jyMtbCxeKYzvP+Gsuew5ibovAMVR opv9/Dug4F8PtTvVmpgWPhpoc9evbuVP28ZWuWJK3k83veEDVluw/ZELHJeT /SC1QOdStNV1orfnu/QQh4Bsw4mwFAvQpaA8CbxWpoNEE3yroA2RqDKDfSm9Fc +HQBFQZJSR9TM8Bg2pThrtznZyElF RwaasA+ScTpJkkgajJA6ic2IKWlyOMV+ Zaoac==
ARC-Authentication-Results	i=1; mx.google.com; dkim-pass-header=in@mailchimpapp.net header=s+3; header=b:LDOOzGog; spfpass (google.com: domain of bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) smtp.mailfrom=bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net
Return-Path	<bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net>
Received-SPP	pass (google.com: dkim-pass-header=in@mailchimpapp.net header=s+3; header=b:LDOOzGog; spfpass (google.com: domain of bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) client-ip=198.2.183.41;
Authentication-Results	mx.google.com; dkim-pass-header=in@mailchimpapp.net header=s+3; header=b:LDOOzGog; spfpass (google.com: domain of bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) smtp.mailfrom=bounce-mc.us14_17121541.8906217-675c34a01@mail41.suw13.rgsrv.net
DKIM-Signature	v=1; arsip-sha256:=related+relaxed; d=machimpapp.net; s=h3; i=1647895523; v=1648197923; iinfo=3Detsdefend.io@mailchimpapp.net; h=From:Reply-To:Date:Subject:To:List-Unsubscribe:List-Unsubscribe-Post:Content-Type:MIME-Version; cc:Date:Subject:b=LDOOzGogUvnSSCE49TGX/NkUjsgr/XcZppzhFCTVMlw+F8WaknHAZTNob p/ydHtm7iod5MIeg4Rd3wvG8otJdcfclHEQDM+SYF3830vcGZRZoTTES19r IYXh482UrhfwUGPSNqhwUGrLuTwOdfg5wsud0aPaLXNkyPrOAwMcWew qSk8+SccJshuLdKduJDShqrFNua8j7HowdxZ+zzyQXIMBeUtaOsa4opSlUyWj VFZUU4w42EMikQuXuUGu39d5y9R2NRN2WZQDHxSLu/Ro21DpnDH8Xg c+hKuzZuyJw==
Subject	Top 3 Blog posts for SOC teams 📧
From	LetsDefend <info@letsdefend.io>
Reply-To	LetsDefend <info@letsdefend.io>
To	<oguna@letsdefend.io>
Date	Mon, 21 Mar 2022 20:45:17 +0000
Message-ID	<74bda5edf824cea3aad39e707mo list <74bda5edf824cea3aad39e707mo list @2022032104512.a02caoscf3.a268ce5a@mail41.suw13.rgsrv.net>
X-Mailer	Mailchimp Mailer - "CIDa02caoscf387534a01f"
X-Campaign	mailchimp74bda5edf824cea3aad39e707mo.a02caoscf3
X-campaignid	mailchimp74bda5edf824cea3aad39e707mo.a02caoscf3
X-Report-Abuse	Please report abuse for this campaign here:
X-MC-User	74bda5edf824cea3aad39e707mo
Feedback-ID	171215441-171215441.8906217.us14.mo
List-ID	74bda5edf824cea3aad39e707mo list <74bda5edf824cea3aad39e707mo list @2022032104512.a02caoscf3.a268ce5a@mail41.suw13.rgsrv.net>

# Received Field Chain

List-ID	74bdaedf6240ea0aad30e707mo list <74bdaedf6240ea0aad30e707.499857.list-id.moxv.net>
X-Accounttype	pd
List-Unsubscribe	<#>, <mailto:#>
List-Unsubscribe-Post	List-Unsubscribe=One-Click
Content-Type	multipart/alternative; boundary="-----=_MCPart_853182061"
MIME-Version	1.0

**Received Header**

```
Delivered-To: oguna1@letsdefend.io
Received: by 2002:a05:6400:159:0:0:0 with SMTP id hw25csp1949486ecb;
  Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
X-Google-Smtp-Source: ABdHP3zA6xyR4ONC14k2HsTVGWHtU2g8Poi7N2hdA2aQWbFOMJAAxy5Ort/bkg13a0t06KCB
X-Received: by 2002:a25:1344:0:b0:633:7592:9C8F with SMTP id 65-20020a25134400000000063375929C8F24595651ybt.211.1647895524591;
  Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647895524; cv=none;
  d=google.com; s=sarc-20160816;
  b=DVPYVh3jwOC3K1zcx0t3R7n3h32f466vKfPvnxKxV77v47Yk4k4ep13k8/ht
  1a223p0d4f2fXgyluAB0u8zrH08C0qC31frF09G44lehbx/838C761FV5vpt37n
  3k1f4w4wcl5G-vH0a2z50nF55J0N3080d0Pc7WkCwKCB0a2Z3jyWu3htg
  5MugNax3OKABON/zucyoy3jC80S23u6d4Yvz4EX/txedQerRfBqt0m8k1uA1E1
  YhIDKxwqP1K0uXrFFH062EZXVjWf55MDuHc6aAwZldTtn/onj7ncfcg0ay3Kx1
  P0yQ=
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=sarc-20160816;
  h=mime-version:list-unsubscribe-post:list-id
  :feedback-id:message-id:date:to:reply-to:from:subject:dkim-signature;
  bh=47/b1kdxhQy2u3v/05a99qt/028KCI5Q835V98;
  b=TFB4w/Pu41JaaP93t0G1b1/0aVYL0e8Hnd0VYKXV3kX0XyYmaz385u0d1
  sJghevaW1j3py3x0qTep98RbAfJcnk33jWlttBckevV2kVp+Igtuad5l0xvW4t
  opvK8lqf8PjTkvrtjngWfphcpc95b0uP28Z0dILKv3K830EDVfuVZELH4jT
  /5C1Q0d07N1ot+r5v/q2m8uwr4ndfAvqA15C0wpc/NEE3y0r42q0d0F5wzrc
  +1Q1Rf0G138P7H8gpp/0r1r1z1q1yF7h0abw-Sc0p3x0k3w3K4E1c2vWky0Wv+
  2a0a=
ARC-Authentication-Results: i=1; mx.google.com;
  dkimpass: header.i=@mailchimpapp.net header.s=sk3 header.b=LD0G2d0g;
  spfpass (google.com: domain of bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) smtp.mailfrom=bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net
Return-Path: (bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net)
Received: from mail141.suw13.rgsrv.net (mail141.suw13.rgsrv.net. [198.2.183.41])
  by mx.google.com with ESMTPS id 05-20020a0dc09000000002e30b050ca9516996580jwd.242.2022.03.21.13.45.23
  for <oguna1@letsdefend.io>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
  Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) client-ip=198.2.183.41;
Authentication-Results: mx.google.com;
  dkimpass: header.i=@mailchimpapp.net header.s=sk3 header.b=LD0G2d0g;
  spfpass (google.com: domain of bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net designates 198.2.183.41 as permitted sender) smtp.mailfrom=bounce-nc.us14_171215441.8996217-675c34a61f@mail141.suw13.rgsrv.net
DKIM-Signature: w=1; a=rsa-sha256; c=relaxed/relaxed; d=mailchimpapp.net;
```

Here we see the complete relay path - the chain of servers the message passed through. It's listed in reverse chronological order. The last server listed is the original sender. The topmost entry shows the final mail server delivering to the inbox. This section proves the message originated from an unexpected domain, not LetsDefend. Relay hops through domains like mailchimpapp.net raise red flags. This field is critical for tracing spoofed or forged emails. It allows analysts to map the true origin of the email. Received chains should always include expected servers. If unknown mail relays appear, the message may have been hijacked or relayed via spoofing. Security systems use these headers to build trust scores. Unexpected IPs reduce message trust and increase the chance of being marked as spam or phishing.

## MX Server Details

The screenshot shows the MXToolbox SuperTool interface. The domain 'letsdefend.io' is entered in the search bar. The results show several MX records pointing to Google's mail infrastructure (aspmx.l.google.com). A table below the records shows the DMARC status: 'DMARC Policy Not Enabled' and 'DMARC Quarantine/Reject policy not enabled'.

Pref	Hostname	IP Address	TTL	Blacklist Check	SMTP Test
1	aspmx.l.google.com	142.250.31.26 Google LLC (AS15169)	5 min	Blacklist Check	SMTP Test
1	aspmx.l.google.com	2607:fb0:4004:c19::1b	5 min	Blacklist Check	
5	alt1.aspmx.l.google.com	172.253.116.27 Google LLC (AS15169)	5 min	Blacklist Check	SMTP Test
5	alt1.aspmx.l.google.com	2a00:1450:400b:c02::1b	5 min	Blacklist Check	
5	alt2.aspmx.l.google.com	173.194.76.27 Google LLC (AS15169)	5 min	Blacklist Check	SMTP Test
5	alt2.aspmx.l.google.com	2a00:1450:400c:c00::1a	5 min	Blacklist Check	
10	alt3.aspmx.l.google.com	142.250.102.26 Google LLC (AS15169)	5 min	Blacklist Check	SMTP Test
10	alt3.aspmx.l.google.com	2a00:1450:4025:402::1b	5 min	Blacklist Check	
10	alt4.aspmx.l.google.com	192.178.156.27 Google LLC (AS15169)	5 min	Blacklist Check	SMTP Test
10	alt4.aspmx.l.google.com	2a00:1450:4013:c1c::1b	5 min	Blacklist Check	
15	64th4rasg2q3fe4gfh3snylozsdqwhfdeivz63fesb3j63i35cq.mx-verification.google.com	(No A Record)	5 min	Blacklist Check	SMTP Test

Test	Result
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled

This section reveals the mail exchange (MX) configuration of the letsdefend.io domain. The domain uses Google's mail infrastructure (aspmx.l.google.com) to send and receive legitimate messages. If a message claims to be from letsdefend.io but comes from any other server (e.g., emkei.cz or an unknown IP like 101.99.94.116), it is clearly forged. This comparison allows analysts to confirm whether an email was truly sent by the organization it claims to represent. If there's no match between the originating IP and the official MX record, spoofing is likely. MX verification is a vital part of email threat hunting. Organizations should regularly monitor and secure their MX settings. Third-party spoofing attempts often bypass DMARC by using unregistered servers. Validating against MX records is a fast way to detect these cases.

## Remediation Recommendations

- Enforce strict DMARC policies ('reject' or 'quarantine') for all corporate domains.
- Regularly audit and align SPF and DKIM records with all approved mail services.
- Avoid using third-party mailing tools unless properly authenticated and authorized.
- Implement security awareness training to help users spot spoofed or suspicious emails.
- Utilize secure email gateways to pre-filter suspicious emails using AI and signature-based detection.
- Enable logging and analysis of mail headers in SOC workflows for regular anomaly checks.
- Monitor domain DNS settings via tools like MXToolbox and update them when needed.