Phishing Email Analysis

Deep Investigation • IOC Analysis • Threat Detection

Prepared by: Sangram Rajput

Agenda

- Case Overview

- Header Analysis

- IP Investigation

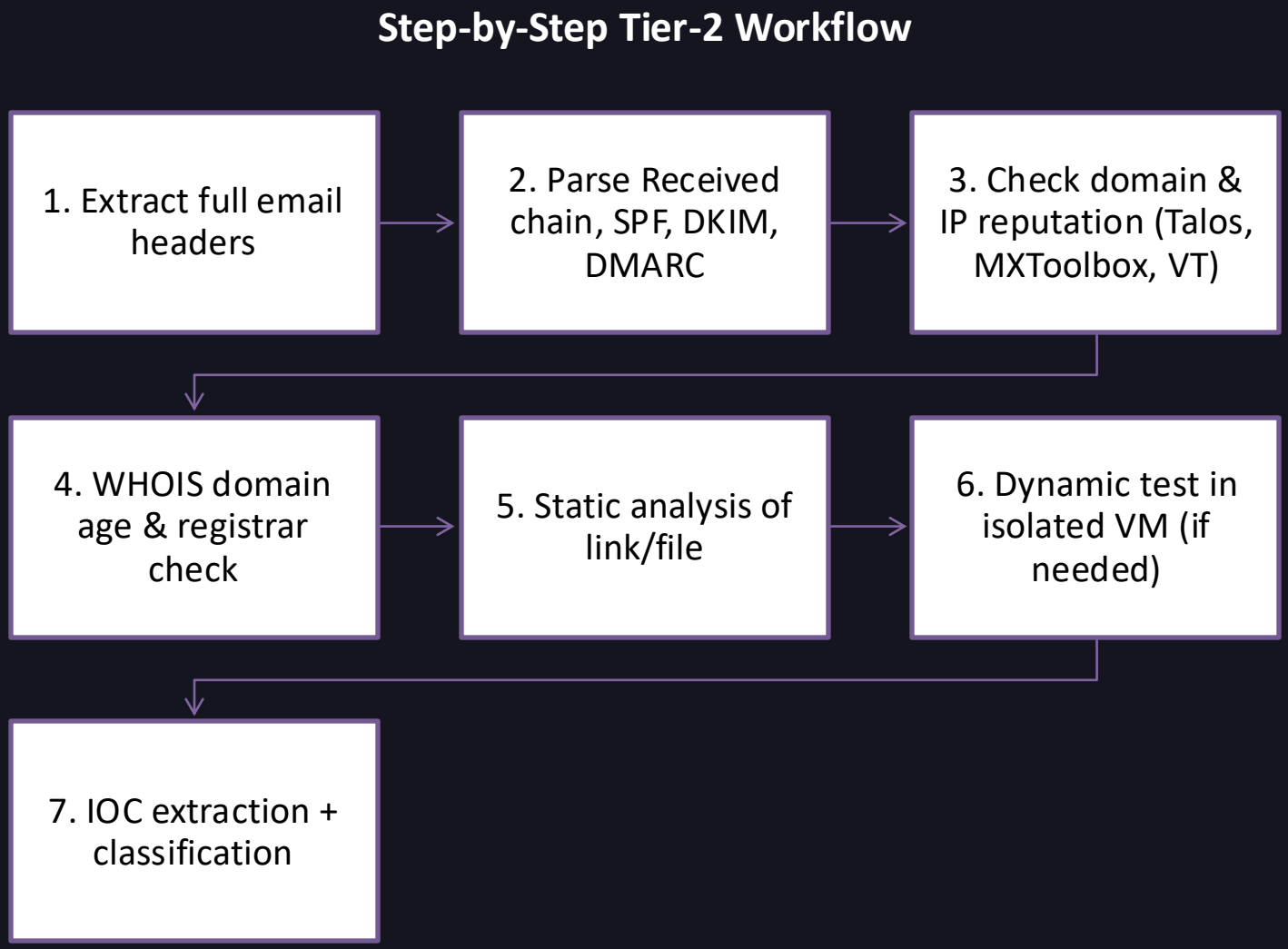
- Domain Investigation

- IOC Table

- MITRE ATT&CK Mapping

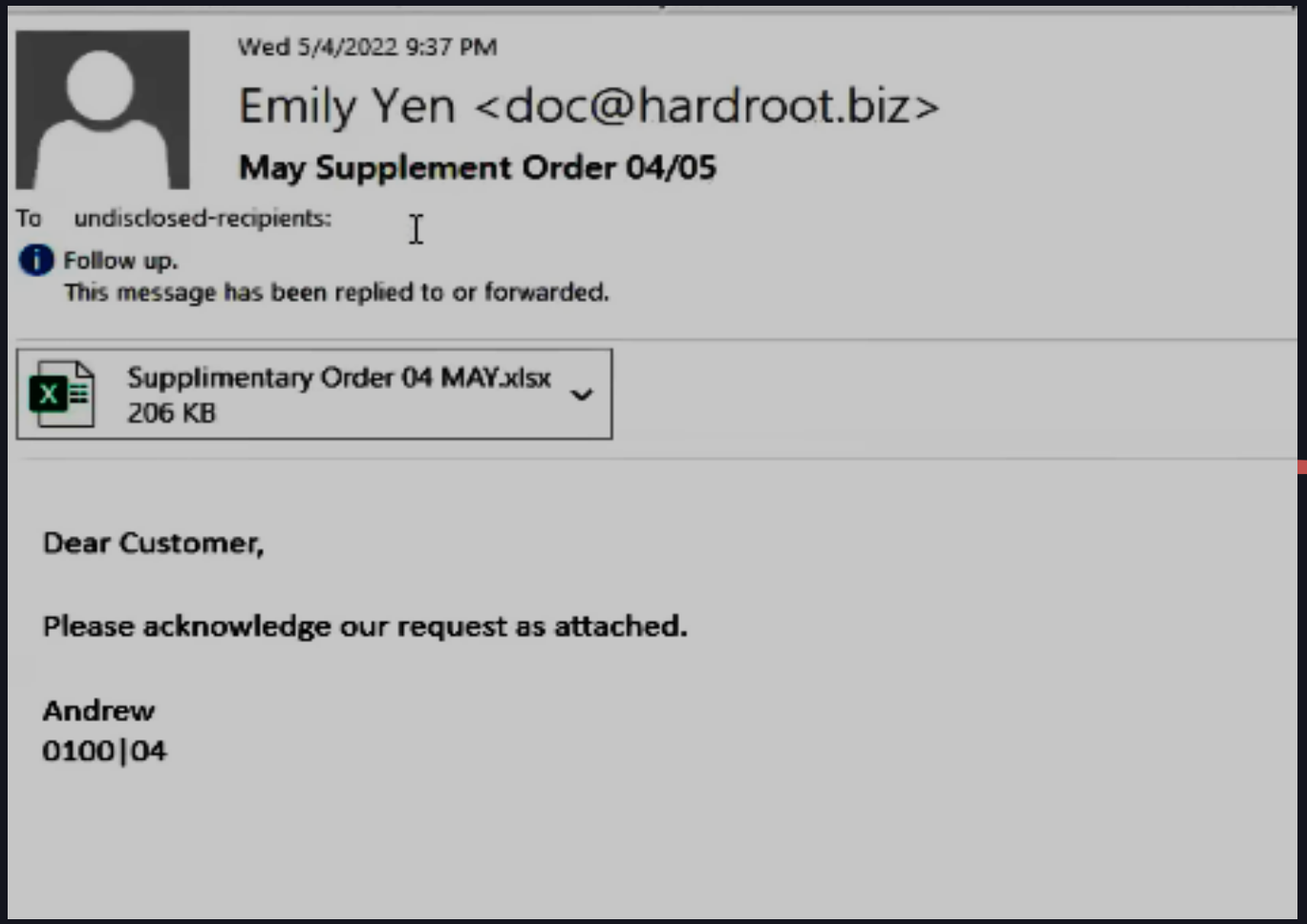
- Final Conclusion

Investigation Methodology



Full Email (User View)

- The attacker attempts social engineering by impersonating a security notification to lure the user into opening the attachment.

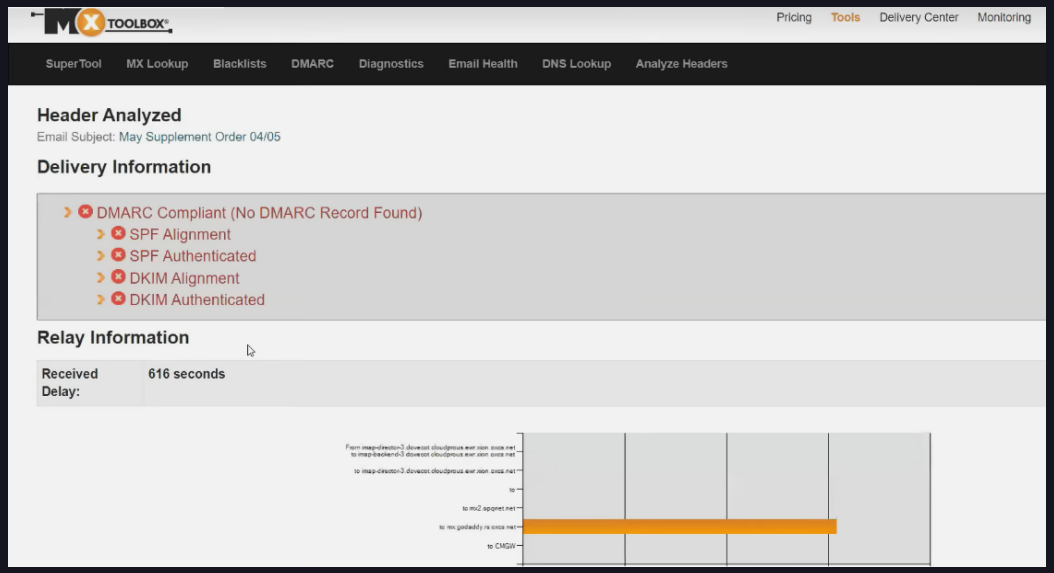


Header Analysis

SPF failed, DKIM/DMARC missing, and non-Microsoft sending servers confirm spoofing

Headers Found

Header Name	Header Value
From	"Emily Yen" <doc@hardroot.biz>
To	<undisclosed-recipients:>
Subject	May Supplement Order 04/05
Date	Wed, 4 May 2022 21:37:09 +0530
Message-ID	<3b09905aaa0c1813e5725c294f5dc5a8@lawaholdings.co.bw>
MIME-Version	1.0
Content-Type	multipart/mixed; boundary="----=_NextPart_000_0010_01D8C3AE.70560100"
X-Mailer	Microsoft Outlook 16.0
X-CMAE-Analysis	v=2.4 cv=YvvK+6UX c=1 sm=1 tr=0 ts=6272a731 cx=a_idp_d a=Dj3c+FHrcchNxiG6n/fo3A==:117 a=Dj3c+FHrcchNxiG6n/fo3A==:17 a=oZkiemNP1mAA:10 a=Q02_sXRfmUInSk7_BrYA:9 a=CjuIK1q_8ugA:10 a=NkTa0eAkhXMAxvwh2FwA:9 a=fMZ_E1ClfQA:10 a=IC_P5zELcC8A:10 a=k92MKxcbr7QA:10 a=gKT_8TCvE1r4shHETz0G:22 a=Z5ABNNGmrOfJ6cZ5bIyy:22 a=QOGEsqRv6VhmHaoFNykA:22
X-CMAE-Envelope	MS4xfNsETP1QpJUApYqq1fbCwciMi0c75kKj6ViC9rVb1q0d+BfZPvzqonyyjozSZDrvP2wt2u1TUQV/2hBJTYjoRVy9dh9FpAHCVgEOmdTzeZeYb8qYs+VL/ kbfWHvilzSqPm+DRdFOaTpoT+4DRKohDGoyTyaH4TMtC+hPSQ7I8Q23XHuJKlaA8aWqfPS9pm0eJgg==
Thread-Index	AQKzUibJnXF8xTSqwnuzicahp+uesQ==
X-Sender	doc@hardroot.biz
X-OlkEid	00000000D6AB40BA601F9742A4C86F3FC35C047D0700178FD8DA7507254D88C87DBF448EE1D2000000000221000178FD8DA7507254D88C87DBF448EE1D2000000001C00000081A0C022449BF34D8F38B80C89009984



MX TOOLBOX

Pricing Tools Delivery Center Monitoring

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers

Header Analyzed

Email Subject: May Supplement Order 04/05

Delivery Information

- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	616 seconds

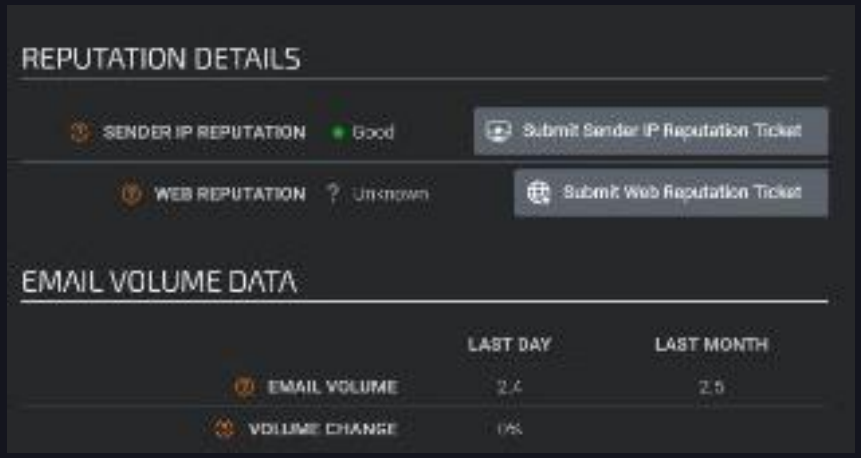
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	imap-director-3.dovecot.cloudprous.ewr.xion.oxcs.net 10.105.5.3	imap-backend-3.dovecot.cloudprous.ewr.xion.oxcs.net	LMTP	5/4/2022 4:17:53 PM	✓
2	0 seconds	mx.godaddy.rs.oxcs.net 10.105.2.1	imap-director-3.dovecot.cloudprous.ewr.xion.oxcs.net	LMTP	5/4/2022 4:17:53 PM	✓
3	*	network			5/4/2022 4:07:37 PM	
4	0 seconds	mail.opqnet.net 198.45.164.22	mx2.opqnet.net	SMTP	5/4/2022 4:07:37 PM	✗
5	10 minutes	p3plibsmtp02-14.prod.phx3.secureserver.net 68.178.213.14	mx.godaddy.rs.oxcs.net	cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits) (No client certificate requested)	5/4/2022 4:17:53 PM	✓
6	0 seconds	mx2.opqnet.net 198.45.164.20	CMGW	cipher ECDHE-RSA-AES256-GCM-SHA384 256/256 bits) (Client did not present a certificate)	5/4/2022 4:17:53 PM	✓

Header Findings

- From: “Emily Yen” doc@hardroot.biz
- Return-Path mismatch: suspicious
- Originating IP: 196.45.164.22 (flagged)
- SPF: Fail
- DKIM: None
- DMARC: None
- Received chain shows non-Microsoft server → spoofing

IP reputation Analysis

- *The IP has generally good reputation but being blacklisted by two vendors increases the suspicion.*



IP Address Information

Analysis Date	2025-11-26 09:47:05
Elapsed Time	1 seconds
Detections Count	1/100
IP Address	**196.45.164.22** Find Sites | IP Whois
Reverse DNS	mail.opqnet.net
ASN	AS33781
ISP	OPQ Net
Continent	Africa
Country Code	(BW) Botswana
Latitude / Longitude	Google Map
City	Gaborone
Region	South East

LISTED	Anonmails DNSBL	196.45.164.22 was listed Detail	1800	489	Ignore
LISTED	BARRACUDA	196.45.164.22 was listed Detail	900	91	Ignore
OK	0SPAM			87	
OK	0SPAM RBL			91	
OK	Abusix Mail Intelligence Blacklist			3	
OK	Abusix Mail Intelligence Domain Blacklist			2	
OK	Abusix Mail Intelligence Exploit list			3	
OK	BACKSCATTERER			3	
OK	BLOCKLIST.DE			3	
OK	CALIVENT			145	

Domain reputation & Whois Analysis

- Domain is old, its reputation shows neutral but it is blacklisted by one vendor.

Seclookup	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean

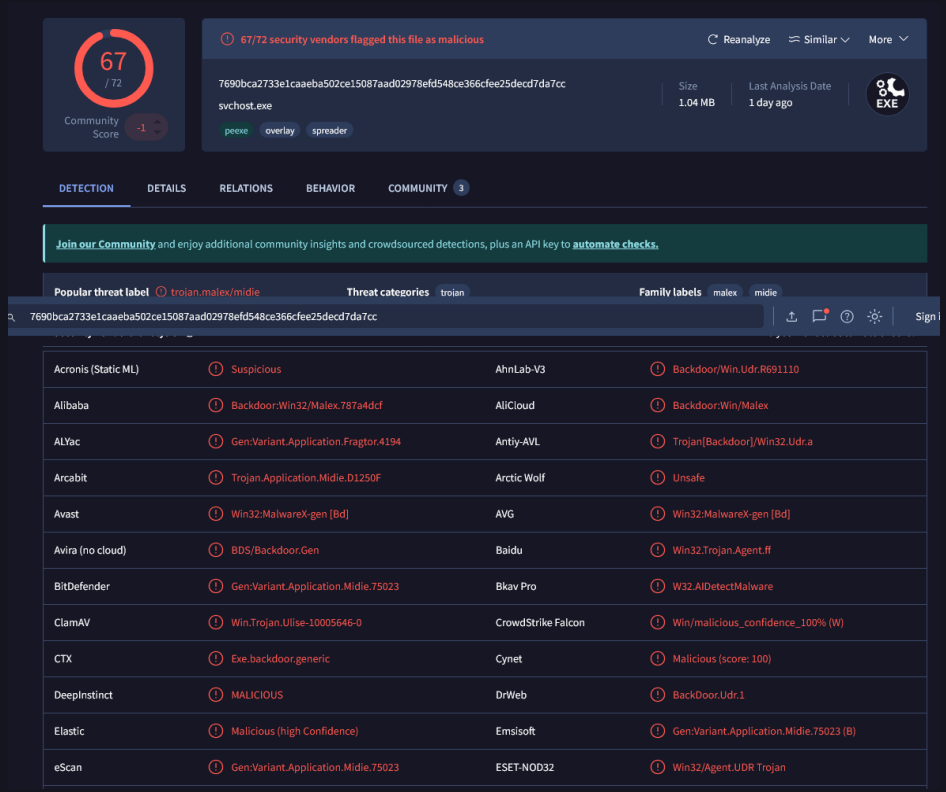
REPUTATION DETAILS

WEB REPUTATION — Neutral

Registrar	Cosmotown, Inc. IANA ID: 1509 URL: www.ccdomain.co.kr Whois Server: whois.ccdomain.co.kr abuse@cosmotown.com
Registrar Status	autoRenewPeriod, ok
Dates	3,299 days old Created on 2016-11-14 Expires on 2025-11-13 Updated on 2025-10-23
Name Servers	NS3.AMINZTECH.COM (has 198 domains) NS4.AMINZTECH.COM (has 198 domains)
Domain Status	Registered And No Website
IP History	12 changes on 12 unique IP addresses over 9 years
Hosting History	10 changes on 5 unique name servers over 9 years

File Analysis

- Macro-enabled XLSX file flagged by 60+ vendors as malicious.



DETECTION ALIASES

Backdoor/Win.Udr.R691110
detected
Win32:MalwareX-gen [Bd]
Gen:Variant.Application.Midie.75023
backdoor
Win.Trojan.Ulise-10005646-0
win/malicious_confidence_100
BackDoor.Udr.1
Generic.mg.8dda406bd55e7948
W32/Udr.AT!tr
Trojan.Win32.Malex
Trojan (005690671)
BackDoor-DSA (trojan)
Trojan:Win32/Malex.AMX!MTB
Dialer.CKP (dialer)
Trojan.Malex.AA11
Backdoor.Udr!1.65B3
DFI - Malicious PE
Troj/Malex-AI
Trojan.Win32.VSX.PE04C9v
W32/Udr.A.gen!Eldorado
OScope.Backdoor.Udr
Gen:Variant.Application.Fragtor.4194
malicious_detection_score_-1.0
malicious (high confidence)
Detected
Generic.Malware.Gen.DDS
BehavesLike.Win32.Backdoor.tc
SMG.Heur!gen

⚠ Malicious File Analysis (Supplementary Order 04 MAY.xlsx)

- File Type: XLSX with embedded macro
- Behavior: Attempts to connect to external IP
- The attached file was identified as `win.trojan.vilse.`
- a backdoor capable of remote access, persistence, and data exfiltration.
- 60/72 security vendors flagged this file as malicious
- Screenshot Placeholder: VirusTotal / Talos

Indicator of Compromise (IOC) Table

IOC Type	Value	Source	Notes
Sender Email	doc@hardroot.biz	Headers	Emily Yen
Malicious Domain	Hardroot.biz	WHOIS / Talos	Registered 2016-11-16 Blacklisted by one vendor
IP	196.45.164.22	Talos / VirusTotal/ IPVoid	Reputation - good Blacklisted by two vendors Country - Botswana
Attachment Hash (SHA256)	<7690bca2733e1caaeba502ce15087aad02978efd548ce366cfee25decd7da7cc>	VirusTotal / Talos	Marked malicious by 67 engines

MITRE ATT&CK Mapping

- T1566 — Phishing
- T1598 — Spearphishing Link
- T1059 — Execution (if script executed)
- T1204 — User Execution

The attacker’s behavior aligns with multiple ATT&CK techniques including phishing delivery (T1566), malicious link/attachment usage (T1598, T1204), and possible script execution (T1059).

Incident Summary

- Phishing email impersonating security notification
- Malicious file attached
- SPF/DKIM authentication failed — sender spoofing
- IOC analysis confirms high-confidence phishing attempt
- File analysis says that it's a backdoor (win.trojan.vilse)

This was a high-confidence phishing attack involving sender spoofing, malicious attachment analysis, and multiple matched IOCs. The backdoor indicates intent for long-term compromise.

Conclusion & Recommendations

- Ask all users who received same mail to delete that email
- If any user has opened the file, isolate that machine from the network.
- Block malicious domain and IP immediately
- Implement DMARC with reject policy
- Conduct user phishing-awareness training

Immediate containment, user awareness, and email authentication hardening (SPF, DKIM, DMARC) are crucial to prevent recurrence.

Skills Demonstrated

🛠️ Technical Analysis Skills

- Email Header Analysis
- SPF/DKIM/DMARC Authentication Checks
- Domain & IP Reputation Investigation
- Static & Dynamic File Analysis (Malware/VT)

🧩 Threat Intelligence & Mapping

- IOC Extraction & Documentation
- MITRE ATT&CK Technique Mapping

📄 SOC Operational Skills

- Tier-2 Incident Investigation
- Professional Report Writing

Thank You !

For queries or walk-through, feel free to ask.

Prepared by: Sangram Rajput