ADVENT OF CYBER 2022 EMAIL ANALYSIS

What To Analyze?

✓	From	Sender address
✓	To	Receiver address including CC BCC
✓	Date	Time when email was sent
✓	Subject	Subject of email
✓	Return path	Reply to, the return path where reply will be sent
✓	Domain key DKIM Signatures	Signatures provided by email services for authenticity
✓	SPF	Server that sent the mail
✓	Message ID	Unique ID of mail
✓	MIME Version	Used MIME Version
✓	X-Header	The receivers mail provider add this field
✓	X-Received	Mail server that email went through
✓	X-Spam Status	Spam score of the mail
✓	X-Mailer	Email client name

Checklist	Evaluation
Valid address in “From”,”To” and “CC” ?	If invalid? RED FLAG
Is “From” & “To” Same?	If yes then, RED FLAG
Is From and Return Path Same?	If not same, RED FLAG
Was the email sent from valid server	If no, RED FLAG
Does message ID Field Exist?	Empty and malformed are RED FLAGS
Do the hyperlinks redirect to suspicious links	If yes, RED FLAG
Do attachment contain malware? Or Suspicious FIle	If Yes? RED FLAG

VIRUSTOTAL INQUEST ipinfo.io TALOS

urlscan.io
A sandbox for the web

browserling Simple Email Reputation