EMAIL TAGS

The EMAIL Console offers multiple layers of depth for any audience; executives can access clear, visualized stats about email activity and EMAIL intervention, security professionals can monitor trend alerts and oversee organizational email hygiene, and cybersecurity analysts can leverage the depth of Information available to perform complex investigations of any potential malicious activity detected.

Tags are utilized by EMAIL to summarize model alerts and email or message features into brief, recognizable categories for quick investigation. Tags are not limited to indicating malicious factors; Type tags give important contextual Information which includes both positive, negative and neutral factors. Models can be instructed to add tags as an action. Any email tagged with a critical tag will be surfaced in the main Dashboard for visibility.

- Critical tags indicate that EMAIL has identified highly concerning features within the mail or message which may indicate a malicious intent.
- Warning tags suggest that the email has features which deviate from the 'pattern of life' for the organization and the sender/recipient.
- Type / Info tags provide contextual Information about an email or message including detected features, and existing communication history to better inform an investigation.

The following tags have been broken up by general purpose and type of activity detected.

Intent Tags

The following tags attempt to generalize categorize malicious intent present in the email, according to Darktrace／EMAIL's analysis.

Tag	Category	Description	Emails	Messages
Extortion	Critical	Extortion aims to create a sense of panic in the recipient by presenting them with a threatening, often customized message which includes a demand for payment, often in the form of cryptocurrency.	True	False
Solicitation	Critical	The goal of solicitation is to convince a recipient to open a line of communication with the sender which could lead ultimately to the transfer of payments or a backdoor to compromise of the network. Such emails often contain minimal traceable content such as links or attachments.	True	False
Spam	Critical	Spam represents a lazy attempt to engage the recipient in commercial transactions which are at best unwanted and at worst fraudulent. Such emails are typically distributed in bulk to maximise the chance of recipient engagement.	True	False

Attack Methods and Targeted Approaches

In addition to intent tags, the following critical tags attempt to categorize the specific attack method or end goal of the malicious actor more precisely.

Tag	Category	Description	Emails	Messages
Cloud Platform Abuse	Critical	Someone appears to be abusing a legitimate cloud platform to share files or other unwanted material with the recipient.	True	False
Credential Harvesting	Critical	There is evidence that a link within this email is intended to take the recipient to a fake login page which will request a corporate password. Some element of social engineering is typically present to draw the recipient' attention to the link.	True	False
Document Anomalies	Critical	There is something irregular about the context of the document attached to this email. Documents containing sensitive information have the potential to be used exploitatively - for example, using trust with the recipient to induce a fraudulent payment or further sharing of information.	True	False
Email Account Takeover	Critical	The system believes this is a malicious email which has originated from a legitimate corporate mailbox. This suggests someone has taken over the mailbox and may be using it to deceive internal users.	True	False
Malware or Ransomware	Critical	A file attached to this email has properties consistent with a novel malware or ransomware threat which may infect the recipient' device when opened.	True	False
Multistage Payload	Critical	The system believes this malicious email is encouraging the recipient to follow a series of steps before delivering a payload or attempting to harvest sensitive information. Attacks are often structured this way in an attempt to evade detection.	True	False
Payment Scare	Critical	The email appears to be warning the recipient about a fake payment issue in order to solicit further engagement.	True	False
Phishing Attachment	Critical	This email contains an attachment which the system considers to be highly unexpected in the context of previous sender and recipient activity. The attachment may be a precursor to further malicious activity - for example, by convincing the recipient to follow harmful instructions or engage in communications via another channel.	True	False
Phishing Link	Critical	The email contains a link which the system considers to be highly unexpected in the context of previous sender and recipient activity. The linked webpage may be a precursor to further malicious activity - for example, by convincing the recipient to follow harmful instructions or engage in communications via another channel.	True	False

Tag	Category	Description	Emails	Messages
Compromise Indicators	Warning	The internal account involved in this transaction is exhibiting behaviour consistent with a compromised account, such as logging in from an unusual location or sending files to many new addresses.	True	True
Suspicious Attachment	Warning	This email contains an attachment with some suspicious properties. The system will action this attachment as a precaution.	True	True
Suspicious Link	Warning	This email contains a link with some suspicious properties. The system will action this link as a precaution.	True	True

User, Service and Brand Impersonation

The following critical and warning tags identify attempts to pretend that the sender is a legitimate correspondent or internal service. These tags have replaced the general spoofing tag.

Tag	Category	Description	Emails	Messages
Brand Impersonation	Critical	The email appears to be impersonating a well-known brand.	True	False
Fake Account Alert	Critical	The email appears to be an alert about one of the recipient's accounts but was not sent by a legitimate system. This is a common social engineering tactic which can trick the recipient into sharing their password or downloading malware onto their device.	True	False
Forged Address	Critical	Analysis of the email' source and the sender's neglect of validation suggests the address may be forged for malicious purposes.	True	False
Internal IT Impersonation	Critical	The email appears to be impersonating an internal notification system. This is a common social engineering tactic which can trick the recipient into sharing their password or downloading malware onto their device.	True	False
Lookalike Domain	Critical	The sender domain is very similar to a known contact domain but is not established within the environment. It may have been registered for the purpose of deceiving internal users.	True	False
User Impersonation	Critical	The display name of this email is very similar to an internal user but was sent from an email address not normally used by the person.	True	False
VIP Impersonation	Critical	The display name of this email is very similar to a high-profile internal user but was sent from an email address not normally used by the person. The system autonomously determines the high-profile users within the organization. These can be viewed and curated on the VIPs list.	True	False

Tag	Category	Description	Emails	Messages
Spoofing Indicators	Warning	Elements of these emails contain some weak indicators which are suggestive of spoofing attempts where an attacker may be masquerading as a known contact or commonly used service.	True	False

Potential Data Loss

The following tags are linked to unusual outbound user activity that may be indicative of accidental or deliberate data loss.

Tag	Category	Description	Emails	Messages
Data Loss	Warning	This email appears to contain content that is not normally sent outside the organization. This may indicate accidental disclosure or deliberate exfiltration of sensitive data.	True	True
Misdirected Email	Warning	This email may have been sent to the wrong person.	True	False
New Correspondent File Transfer	Warning	An attachment is being sent to an external recipient which is new to the environment and whose domain is rare or freemail.	True	True
New Sensitive File Transfer	Warning	An internal user is sending out a file with a sensitivity label which appears unexpected based on their previous email activity.	True	False
Personal Account File Transfer	Warning	An internal user appears to be sending an attachment to their own personal account.	True	False
Response to Solicitation	Warning	This outbound email is a response to an earlier inbound email which had some suspicious properties.	True	False

Non-Productive Communications

The following tags attempt to identify unsolicited and unproductive communications.

Tag	Category	Description	Emails	Messages
Cold Call	Warning	Someone at an external organization is trying to start a conversation with a user who has not had any communication with that organization previously. This is likely an opening attempt to sell a product or service.	True	False
Graymail	Warning	A benign email which has no productive value for the organization. This includes newsletters, announcements, and advertisements for products and services.	True	False
Non-Productive	Warning	The email has no productive value for the organization. This encompasses phishing, spam and	True	False

Tag	Category	Description	Emails	Messages
Mail		graymail.		
Unknown Bulk Mailer	Warning	A commercial email intended for a wide audience. Like Graymail, this encompasses newsletters, announcements, and advertisements for products and services. In addition, the system can find no evidence of association between internal users and the sending organization. The system will apply a junk action to this email.	True	False

Unusual or New Correspondent

The following tags identify a new correspondent or unusual, inconsistent behavior from an existing correspondent.

Tag	Category	Description	Emails	Messages
First Time Contact	Warning	This is the first time the internal and external addresses involved in this transaction have had any interaction.	True	False
Inconsistent Content	Warning	The content of the email, body, links or attachments show some level of deviation from the normal pattern life pattern of the sender.	True	False
Low Mailing History	Warning	The external address in this transaction has a low history of sending into the organization	True	False
No Association	Warning	Little or no evidence exists that there is any relationship of trust between the external sender and the internal organization.	True	True
Out of Character	Warning	Out of Character emails involve a user exhibiting a significant deviation from their usual behavior. This may indicate that their account has been compromised and is being used to abuse trust with the recipient, getting them to accept a file or click on a link.	True	False
Singular Relationship	Warning	There is a direct relationship between the sender and recipient which is not shared by other internal addresses	True	True
Unknown Correspondent	Warning	The external address involved in this transaction belongs to a human user who has received no recent emails from internal users.	True	False
Unknown Intent	Warning	The sender is using methods to hide the content of their email, such as via an encryption service. The system was able to determine the email was suspicious by analysis of previous sender and recipient activity.	True	False
New Conversation	Type	This conversation was only recently created.	False	True
New Correspondent	Type	The external address involved in this transaction belongs to a human user who has a	True	True

Tag	Category	Description	Emails	Messages
		low mailing history but some domain association. The address is new but potentially expected.		

Established Correspondence

The following tags identify a correspondent or domain with a consistent, active or established history of communication.

Tag	Category	Description	Emails	Messages
Active Conversation	Type	An email which is part of an active communication between the organization and an external address. Communication must be recent and bidirectional.	True	False
Consistent Content	Type	The content of the email is in keeping with the previous patterns of communication from this source	True	False
Established Conversation	Type	This conversation has been ongoing for at least several days.	False	True
Established Correspondent	Type	The external address involved in this transaction has had significant two-way correspondence with internal users previously.	True	True
Established Domain Relationship	Type	The external domain involved in this transaction has had significant two-way correspondence with internal users previously.	True	False
High Mailing History	Type	The external address in this transaction has an established history of sending into the organization	True	False
Known Correspondent	Type	The external address involved in this transaction belongs to a human user who has been contacted by internal users previously.	True	True
Known Domain Relationship	Type	The external domain involved in this transaction has been contacted by internal users previously.	True	False
Moderate Mailing History	Type	The external address in this transaction has a moderate history of sending into the organization	True	False

Context

The following tags are used to identify contextual factors such as the message or recipient type.

Context (Shared)

Tag	Category	Description	Valid for Emails	Valid for Messages
Wide Distribution	Warning	Typifies an automated or bulk mailer which is sent to a wide number of individuals in the organization	True	True
Automated Report	Type	An email which is produced via an automated system which is typically periodic in nature and for some internal operational purpose	True	True
Narrow Distribution	Type	Typifies an automated or bulk mailer which is sent to a small number of individuals in the organization	True	True
VIP	Type	An internal user involved in this thread is on the VIP list.	True	True

Context (Emails)

Tag	Category	Description	Valid for Emails	Valid for Messages
Personal Address	Warning	A likely personal address of an internal individual	True	False
Validation Issues	Warning	The sender has not provided a valid mechanism for confirming the header-From address as authentic. Not enough emails have been sent to determine if the origin is normal for the sender.	True	False
Account Confirmation	Type	The recipient is being requested to access or confirm an external web account	True	False
Automatic Response	Type	An email that has been automatically produced as a result of a received email. This may be the result of Out of Office responders or other forms of automatically generated responses.	True	False
Calendar	Type	Calendar invites or other scheduling exchanges	True	False
Freemail	Type	An email from an email domain likely to be a free self sign-up service	True	False
Mailer	Type	This email was sent by an automated system and uses some industry-standard practices for legitimate automated mail distribution.	True	False
Notification	Type	An email whose purpose is directed towards the recipient, rather than a general audience, and was sent from an automated system.	True	False
Undeliverable	Type	Undeliverable mail reports and email bounces	True	False

Context (Messages)

Tag	Category	Description	Emails	Messages
Detailed Message	Warning	This message contains a significant amount of formatting beyond what is typical for usage on the platform.	False	True
Long Message	Warning	This message contains a large amount of text beyond what is typical for most usage on the platform.	False	True
Channel	Type	This conversation is classified as a Channel within Teams.	False	True
Chat	Type	This conversation is classified as a Chat within Teams.	False	True
External Creator	Type	The first message seen in this conversation was sent by an external address.	False	True
First Message	Type	This is the first message seen in this conversation.	False	True
Internal Creator	Type	The first message seen in this conversation was sent by an internal address.	False	True
Meeting	Type	This conversation has been created for a meeting.	False	True
Message from Creator	Type	This message is from the address that sent the first message seen in this conversation.	False	True
Multi Organization	Type	There is more than one external domain in this conversation.	False	True
Primarily External	Type	The participants in this conversation are mostly external.	False	True
Primarily Internal	Type	The participants in this conversation are mostly internal.	False	True
Recent Call	Type	There was recently a call between the participants in this conversation.	False	True
Recently Added Correspondent	Type	The external address sending or receiving this message was only recently added to the conversation.	False	True
Recently Added Internal User	Type	The internal address sending or receiving this message was only recently added to the conversation.	False	True
Short Message	Type	This message contains a small amount of text consistent with most usage on the platform.	False	True