Readme - Detailed

Cisco Secure Email consists of two groups of attributes: **Basic attributes** and **Event attributes**. Below examples explain how these fields can be used in queries with ‘OR’ and ‘AND’ operators.

	Field Group	**STIX fields**
1	**Basic attributes**	
	• ‘LIKE’ operator supported for string type fields. • ‘AND’ and ‘OR’ operators supported between basic fields.	email-addr:value email-message:from_ref email-message:sender_ref email-message:to_refs email-message:subject email-message:x_message_id_header email-message:x_cisco_mid email-message:x_sender_ip_ref file:name file:hashes.'SHA-256' ipv4-addr:value ipv6-addr:value domain-name:value x-oca-host:hostname

	Query Example: (Operators between basic attributes)
	
	`[email-addr:value = 'test@xyz.com'] START t'2023-09-14T16:43:00.000Z' STOP t'2023-09-30T16:43:00.000Z'`
	
	`[email-addr:value = 'test@xyz.com' AND email-message:subject LIKE 'warnings'] START t'2023-09-14T16:43:00.000Z' STOP t'2023-09-30T16:43:00.000Z'"`
	
	`[file:name LIKE 'Microsoft' AND file:hashes.'SHA-256' = '271c0119ac4455fc8db4ef4a8caf8e2bfcfb8bbd3b8c894e117a9ae9f7111111'] START t'2023-07-19T01:56:00.000Z' STOP t'2023-09-01T01:57:00.003Z'"`	

	[email-addr:value = 'test@xyz.com' OR email-message:subject LIKE 'warnings'] START t'2023-09-14T16:43:00.000Z' STOP t'2023-09-30T16:43:00.000Z'" **Expected result:** STIX objects will be returned if data found in data source.	
2	**Message Event Attributes – (Grouped in x-cisco-email-msgevent)**	
	• ‘OR’ operator is supported between message event fields. • ‘AND’ operator is not supported between message event fields.	x-cisco-email-msgevent:advanced_malware_protection_mailflow_direction x-cisco-email-msgevent:advanced_malware_protection x-cisco-email-msgevent:app_forwarding x-cisco-email-msgevent:content_filters_name x-cisco-email-msgevent:content_filters_direction x-cisco-email-msgevent:content_filters_action x-cisco-email-msgevent:dane_failure x-cisco-email-msgevent:message_status x-cisco-email-msgevent:message_delivered x-cisco-email-msgevent:dlp_violations_names x-cisco-email-msgevent:dlpViolationsSeverities x-cisco-email-msgevent:dlp_action x-cisco-email-msgevent:dmarc_from x-cisco-email-msgevent:dmarc_action x-cisco-email-msgevent:etf_sources x-cisco-email-msgevent:etf_iocs x-cisco-email-msgevent:forged_email_detection x-cisco-email-msgevent:geo_location x-cisco-email-msgevent:graymail x-cisco-email-msgevent:hard_bounced x-cisco-email-msgevent:ip_reputation x-cisco-email-msgevent:macro_mailflow_direction x-cisco-email-msgevent:macro_file_types_detected x-cisco-email-msgevent:message_filters x-cisco-email-msgevent:message_direction

		x-cisco-email-msgevent:contained_malicious_urls x-cisco-email-msgevent:contained_neutral_urls x-cisco-email-msgevent:outbreak_filters_url_rewritten_byof x-cisco-email-msgevent:outbreak_filtersVofThreatCategory x-cisco-email-msgevent:in_outbreak_quarantine x-cisco-email-msgevent:quarantined_to x-cisco-email-msgevent:reply_to x-cisco-email-msgevent:s_mime x-cisco-email-msgevent:domain_categories x-cisco-email-msgevent:sdr_categories x-cisco-email-msgevent:sdr_threat_levels x-cisco-email-msgevent:soft_bounced x-cisco-email-msgevent:spam_positive x-cisco-email-msgevent:quarantined_as_spam x-cisco-email-msgevent:quarantine_status x-cisco-email-msgevent:threat_name x-cisco-email-msgevent:suspect_spam x-cisco-email-msgevent:url_categories x-cisco-email-msgevent:url_reputation x-cisco-email-msgevent:safeprint_ext x-cisco-email-msgevent:virus_positive x-cisco-email-msgevent:web_interaction_tracking_urls x-cisco-email-msgevent:web_interaction_tracking_mailflow_direction x-cisco-email-msgevent:mail_policy x-cisco-email-msgevent:mail_policy_direction

	Query Example:
	`[x-cisco-email-msgevent:spam_positive = 'true' OR x-cisco-email-msgevent:direction = 'incoming'] START t'2023-07-19T01:56:00.000Z' STOP t'2023-09-01T01:57:00.003Z'`
	
	Expected Result: STIX object matching any of these fields are returned if data found in data source.
	
	Query Example:
	`[x-cisco-email-msgevent:virus_positive = 'true' AND x-cisco-email-msgevent:spam_positive = 'true'] START t'2023-07-19T01:56:00.000Z' STOP t'2023-09-01T01:57:00.003Z'`
	
	Expected Result: Returns error as AND isn't supported between message attributes.	

3	**Basic and Event Attribute:**	
	• 'AND' operator is supported between basic and event fields. • 'OR' operator is supported between basic and event fields	

	Query Example:
	`[email-message:from_ref = 'user1@xyz.com' AND x-cisco-email-msgevent:spam_positive = 'true'] START t'2023-07-19T01:56:00.000Z' STOP t'2023-09-01T01:57:00.003Z'"`
	
	Expected Result: STIX objects satisfying both the condition are returned if data found in data source.
	
	Query Example:
	`[ipv4-addr:value = '1.1.1.1' OR x-cisco-email-msgevent:message_status = 'DELIVERED']START t'2023-07-19T01:56:00.000Z' STOP t'2023-09-01T01:57:00.003Z'`
	
	Expected Result: STIX object satisfying any of the above condition is returned if data found in data source.	

4	**Event Attributes - Dependent Fields:**	
	These event fields will work only when given in combination.	[content_filters_name, content_filters_direction, content_filters_action] [advanced_malware_protection_mailflow_direction, advanced_malware_protection]

		[macro_mailflow_directiony, macro_file_types_detected] [web_interaction_tracking_urls, web_interaction_tracking_mailflow_direction] [mail_policy, mail_policy_direction]

	Query Example:
	`[x-cisco-email-msgevent:content_filters_name = 'test' AND x-cisco-email-msgevent:content_filters_direction = 'inbound' AND x-cisco-email-msgevent:content_filters_action = 'stopped'] START t'2023-08-01T16:43:26.000Z' STOP t'2023-08-30T16:43:26.003Z'`
	Expected Result: STIX objects returned if data found in data source.
	Query Example:
	`[x-cisco-email-msgevent:content_filters_name = 'test' AND x-cisco-email-msgevent:content_filters_direction = 'inbound'] START t'2023-08-01T16:43:26.000Z' STOP t'2023-08-30T16:43:26.003Z'`
	Expected Result: Returns Error as all the required combination fields aren't given.	

5	**Event Attributes - Enum Supported:**	
	• 'IN' operator is supported for the fields which can have more than one value.	message_status: [DELIVERED, DROPPED, ABORTED, BOUNCED] app_forwarding: [app_success, app_failed] dlpViolationsSeverities: [critical, high, medium, low] x-oca-host:hostname: [All_Hosts] dlp_action: [delivered, encrypted, dropped] dmarc_action: [none, quarantine, reject, passed, failed]

		etf_iocs: [file_hash, url, domain] s_mime: [smime_successful, smime_failed] quarantine_status: [POLICY, AMP, AV, UNCLASSIFIED, DLP, OUTBREAK] content_filters_direction: [inbound, outbound] content_filters_action: [stopped] advanced_malware_protection_ailflow_direction: [incoming, outgoing] advanced_malware_protection: [amp_clean, amp_malicious, amp_unknown, amp_unscannable, amp_lowrisk] macro_mailflow_direction: [inbound, outbound] web_interaction_tracking_mailflow_direction: [inbound, outbound] mail_policy_direction: [inbound, outbound]

	Query Example:
	`[x-cisco-email-msgevent:message_status = 'DELIVERED' ] START t'2023-08-01T16:43:26.000Z' STOP t'2023-08-30T16:43:26.003Z'`
	Expected Result: STIX objects returned if data found in data source.
	Query Example:
	`[x-cisco-email-msgevent:content_filters_direction IN ('inbound', 'outbound') START t'2023-05-19T01:56:00.000Z' STOP t'2023-10-01T01:57:00.003Z'"`
	Expected Result: STIX objects returned if data found in data source.	