Mandiant

DTM MONITOR & RESEARCH TOOLS FIELDS

When creating Monitors in Digital Threat Monitoring (DTM), the Topics you select for your Monitor Conditions are actually search groups. These search groups match your values against a set of related entity types making it easier to build effective Monitors.

For example, using the `Network Information` topic with a `must contain` Operator and a value of `acme.com` would match if `acme.com` was found in a domain name, URL, or Typosquatted domain. This is because the `Network Information` topic searches across all of those entity types.

For more information about creating Monitors using the DTM API, see **Digital Threat Monitoring API (https://docs.mandiant.com/home/digital-threat-monitoring-api)**.

The following table includes the available fields in the monitors and the type of data you should enter.

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
Bank Identification Number	group_bin	bin	Complete Bank Identification Number
		bin_foreign	Foreign (non-US) Bank Identification number
		bin_partial	Partial Bank Identification number
Brand	group_brand	identity_name	A name of a person, place, company, or thing
		name	A name of a person, place, company, or thing
		organization	The name of an organization
		product	The name of a product
		brand	Brand name or trademark
		product_batch_name	A batch number for a product
Crypto	group_crypto	atom_address	Wallet address for the Cosmos (ATOM) cryptocurrency
		bch_address	Wallet address for the Bitcoin Cash (BCH) cryptocurrency
		btc_address	Wallet address for the Bitcoin (BTC) cryptocurrency
		dash_address	Wallet address for the Dash cryptocurrency
		doge_address	Wallet address for the Doge cryptocurrency
		ltc_address	Wallet address for the Litecoin cryptocurrency
		xlm_address	Wallet address for the Stellar (XLM) cryptocurrency

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
		xmr_address	Wallet address for the Monero (XMR) cryptocurrency
		zec_address	Wallet address for the Zcash (ZEC) cryptocurrency
Filenames & Paths	group_paths	filename	A name or identifier for a file
		path	A location of a file or folder on a filesystem
		registry_key	A path in the Windows registry
Free Text Search	keyword		Will text search all fields of the document for the given keyword(s)
Hash	group_hash	md5_hash	A MD5 cryptographic hash
		sha1_hash	A SHA1 cryptographic hash
		sha256_hash	A SHA256 cryptographic hash

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
Industry	label_industry	label_industry	Industry code of the affected industries of the original document `{ 'ind.aeromil': 'Aerospace and Defense', 'ind.agri': 'Agriculture', 'ind.auto': 'Automotive', 'ind.chemmat': 'Chemicals & Materials', 'ind.civil': 'Civil Society & Non-Profits', 'ind.constructeng': 'Construction & Engineering', 'ind.edu': 'Education', 'ind.energyutils': 'Energy & Utilities', 'ind.fin': 'Financial Services', 'ind.gov': 'Governments', 'ind.health': 'Healthcare', 'ind.hosp': 'Hospitality', 'ind.legalprofserv': 'Legal & Professional Services' , 'ind.manuf': 'Manufacturing', 'ind.mediaentertain': 'Media & Entertainment', 'ind.oilgas': 'Oil & Gas', 'ind.pharma': 'Pharmaceuticals', 'ind.retail': 'Retail', 'ind.tech': 'Technology', 'ind.telecom': 'Telecommunications', 'ind.transport': 'Transportation' }`
Language	label_language	label_language	Two-character **ISO 639-1 (https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes)** language code specifying the detected language type
		city	A city or locality name
		country	A country or nationality name

Locations **Monitor Topic**	group_locatio n **Monitor API Topic**	**Monitor Matches on Topics & Research Tools Entities**	**Description**
		location_name	The name of a physical place or location
Lucene Text Query (Advanced)	lucene		Searches all text fields of documents based on the **Lucene query syntax** **(https://www.elastic.co/guide/en/elasticsearch/reference/7.15/query-dsl-query-string-query.html#query-string-syntax)** For more information about using Lucene in DTM, see **Lucene Queries in DTM** **(https://docs.mandiant.com/home/dtm-lucene-queries)**
Mime-Type	label_type	label_type	Detected MIME type of the originating document. Valid types include: application/font-sfnt, application/javascript, application/json, application/octet-stream, application/pdf, application/pgp-keys, application/postscript, application/vmd.ms-opentype, application/appleworks3, application/dosexec, application/x-empty, application/x-sqlite3, application/x-tar, application/x-wine-extension-ini, application/x-xar, image/gif, image/svg, image/xvg+xml, image/x-portable-greymap, message/news, message/rfc822, text/html, text/plain, text/troff, text/x-asm, text/x-awk, text/x-c, text/x-c++, text/x-diff, text/x-fortran, text/x-java, text/x-lisp, text/x-m4, text/x-makefile, text/x-ms-regedit, text/x-mdos-batch, text/x-objective-c, text/x-pascal, text/x-perl, text/x-php, text/x-po, text/x-python, text/x-ruby, text/x-shellscript, text/x-tex, text/xml, text/x-sgi-movie
Network Information	group_network	domain	An **RFC1035** **(https://datatracker.ietf.org/doc/html/rfc1035)** domain name
		ipv4_address	An IPv4 Address
		ipv6_address	An IPv6 Address
		typosquatted_domain	Accepts a plain fully qualified domain name (not URL's) and will attempt to detect and alert when similar domains are registered
		url	An **RFC1738** **(https://www.ietf.org/rfc/rfc1738.txt)** uniform resource locator (URL)
		client_identifier	An OpenID client identifier

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
Person or Identity	group_identity	email_address	An **RFC5322 (https://datatracker.ietf.org/doc/html/rfc5322)** e-mail address
		identity_name	A name of a person, place, company, or thing
		name	A name of a person, place, company, or thing
		phone_number	A partial or complete phone number
		telegram_user_name	A username for the Telegram messaging platform
		twitter_handle	A user name for the Twitter platform
Search Collection Type	doc_type	doc_type	The specific document type to match, valid types include: • Compromised Credentials • Document Analysis (supported in API only) • Domain Discovery • Email (supported in API only) • Forum Posts • Messages • Pastes • Shop Listings • Web Content
Social Media	group_social	twitter_handle	X (formerly Twitter) handle
		telegram_user_name	Telegram username
		hashtag	Hashtag value
		name	Social media username
		icq_uin	ICQ User ID Number
		jid	Cisco Jabber user ID

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
Threat Type	label_threat	Pre-defined list	Threat specifier of the original document. Valid types include: • `information-security/anonymization` : Anonymization • `information-security/apt` : Advanced Persistent Threat • `information-security/botnet` : Botnet • `information-security/compromised` : Compromised Infrastructure • `information-security/doxing` : Personal Information Disclosure • `information-security/exploit` : Exploit • `information-security/health-risk` : Health Risk • `information-security/information-leak` : Information Leak • `information-security/information-leak/confidential` : Confidential Document Leak • `information-security/information-leak/credentials` : Credential Leak • `information-security/information-leak/payment-cards` : Credit Cards • `information-security/malicious-activity` : Malicious Activity • `information-security/malicious-infrastructure` : Malicious Infrastructure • `information-security/malware` -> Malware • `information-security/malware/ransomware` : Ransomware • `information-security/malware/ransomware-victim-listing` : Ransomware Victim Listing • `information-security/phishing` : Phishing • `information-security/security-research` : Security Research • `information-security/spam` : Spam
Threat Intel	group_threats	cve	A **Common Vulnerabilities and Exposures (CVE) (https://www.cve.org/)** Identifier
		threat_group_name	The name of a threat group
		threat_name	The name of a particular type of threat
		service_name	The name of a service

Monitor Topic	Monitor API Topic	Monitor Matches on Topics & Research Tools Entities	Description
		cwe	A **Common Weakness Enumeration (CWE) (https://cwe.mitre.org/)** Identifier
Tokens & Key	group_keys	access_token	Access token used by applications to authenticate against protected resources
		crypto_key_private	Asymmetric cryptography private key
		crypto_key_public	Asymmetric cryptograph public key
		password_plaintext	A detected plaintext password
		predict_password_plaintext	A detected plaintext password (lower confidence)