DARKTRACE

Darktrace Advanced Search Field Descriptions

v4

Last Updated: December 6th 2019

Darktrace Advanced Search Field Descriptions

Version 4

Capture Loss

@type: capture_loss

Information on packets lost on the wire before reaching Darktrace.

Field	Optional	Description
epochdate	False	Timestamp for when the measurement occurred.
ts_delta	False	The time delay between this measurement and the last.
host	False	Darktrace's hostname label, e.g. dt-xxx-xx.
peer	False	Deep Packet Inspection's instance worker thread.
missed_acks	False	Number of missed ACKs from the previous measurement interval.
total_acks	False	Total number of ACKs seen in the previous measurement interval.
lag	True	Lag between the wall clock and packet timestamps.
pkts_recv	True	Number of packets received since the last stats interval.
pkts_dropped	True	Number of packets dropped since the last stats interval.
pkts_link	True	Number of packets seen on the link since the last stats interval.
megabytes_recv	True	Number of bytes received since the last stats interval.
pkts_percent_dropped	True	Percentage of dropped/link.
capture_percent_lost	False	Percentage of ACKs seen where the data being ACKed wasn't seen.

Conn and Conn Long

@type: conn and @type: conn_long

General information about connections.

Field	Optional	Description
epochdate	False	The time of the first packet.
uid	False	A unique identifier of the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
proto	False	The transport layer protocol of the connection.
service	True	Identification of application protocols being sent over the connection.
start_ts	False	The start of the connection - used for tracking of long connections.
oss_start_ts	True	The timestamp when packet was caught on network, if time is specified outside of Deep Packet Inspection (e.g. from ERSPAN).
duration	True	Length of the observed connection. For 3-way or 4-way connection tear-downs, this will not include the final ACK.
orig_bytes	True	The number of payload bytes sent by the originator. For TCP, as this is taken from sequence numbers, it may be inaccurate. (e.g. due to large connections).
resp_bytes	True	The number of payload bytes sent by the responder. Please see orig_bytes.
conn_state	True	Connection state at the end of the connection, see CONN::TCP CONN STATE.
conn_state_full	True	The human readable connection state, which varies for TCP and UDP connections, see CONN::TCP CONN STATE.
local_orig	True	If the connection originated locally, this value will be T. If it originated remotely, this value will be F.
local_resp	True	If the connection is responded to locally, this value will be T. If it was responded to remotely, this value will be F.
missed_bytes_orig	True	Indicates the number of bytes missed in content gaps on the originator's side, which is representative of packet loss. A value other than zero could in some cases cause protocol analysis to fail, but some analysis may have been completed prior to the packet loss or can recover after packet loss.
missed_bytes_resp	True	Indicates the number of bytes missed in content gaps on the responder's side, which is representative of packet loss. A value other than zero could in some cases cause protocol analysis to fail, but some analysis may have been completed prior to the packet loss or can recover after packet loss.

Field	Optional	Description
history	True	Records the state history of connections as a string of letters, taken from the following list: - s: a SYN without the ACK bit set - h: a SYN+ACK (“handshake”) - a: a pure ACK - d: a packet with payload (“data”) - f: a packet with FIN bit set - r: a packet with RST bit set - c: a packet with a bad checksum - t: a packet with retransmitted payload - i: an inconsistent packet (e.g. FIN+RST bits set) - q: a multi-flag packet (SYN+FIN or SYN+RST bits set) - ^: the connection’s direction was flipped by internal heuristic - g: an Antigena reset If the event comes from the originator, the letter is upper-case; if it comes from the responder, it is lower-case. Multiple packets of the same type will only be noted once (e.g. Only one “d” is recorded in each direction, regardless of how many data packets were seen.)
orig_pkts	True	Number of packets sent by the originator.
orig_ip_bytes	True	Number of IP level bytes sent by the originator (as seen on the wire, taken from the IP total_length header field).
resp_pkts	True	Number of packets sent by the responder.
resp_ip_bytes	True	Number of IP level bytes sent by the responder (as seen on the wire, taken from the IP total_length header field).
orig_ttl	True	The originator’s Time To Live (TTL) of the first seen packet for IPv4 traffic. For IPv6, “hop count”.
resp_ttl	True	The responder’s Time To Live (TTL) of the first seen packet for IPv4 traffic. For IPv6, “hop count”.
tunnel_parents	False	In the case of tunneled connections, indicates the connection *uid* values for any encapsulating parent connections used over the lifetime of this inner connection.
orig_percent_invalid_checksum	True	The percentage of packets with incorrect TCP checksum on the originator’s side of the connection. This field will be valid only for TCP traffic.
resp_percent_invalid_checksum	True	The percentage of packets with incorrect TCP checksum on the responder’s side of the connection. This field will be valid only for TCP traffic.

Field	Optional	Description
outer_vlan	True	The Outer VLAN for this connection, if applicable.
vlan	True	VLAN ID of the connection, if both VLANs are present, this one contains inner VLAN ID.
orig_cc	True	ISO 3166 Country code of the originator.
resp_cc	True	ISO 3166 Country code of the responder.
orig_asn	True	ASN string of originator. Shows which network provider an IP is from.
resp_asn	True	ASN string of responder. Shows which network provider an IP is from.
protosig	True	The protocol detected purely by signature matching.

CONN::TCP CONN STATE

Connection state for TCP connections.

Field	Value	Description
OTH	Midstream traffic	No SYN seen, just midstream traffic (a “partial connection” that was not later closed).
REJ	Rejected	Connection attempt rejected.
RST	RST	Only one side of the connection was inactive, and the other side sent RST.
RSTO	Originator aborted	Connection established, originator aborted (sent a RST).
RSTOS0	Originator SYN + RST	Originator sent a SYN followed by a RST. A SYN-ACK was not seen from the responder.
RSTR	Responder aborted	Responder sent a RST.
RSTRH	Responder SYN ACK + RST	Responder sent a SYN ACK followed by a RST. SYN from the (purported) originator was not seen.
S0	Attempt	Connection attempt seen, no reply.
S1	Established	Connection established, not terminated.
S2	Originator close only	Connection established and close attempt by originator seen, but no reply from responder.
S3	Responder close only	Connection established and close attempt by responder seen, but no reply from originator.
SF	SYN/FIN completion	Complete connection with normal establishment and termination.
SH	Originator SYN + FIN	Originator sent a SYN followed by a FIN. SYN ACK was not seen from the responder.
SHR	Responder SYN ACK + FIN	Responder sent a SYN ACK followed by a FIN. SYN from the originator was never seen.

CONN::UDP CONN STATE

Connection state for UDP connections.

Field	Value	Description
OTH	UDP connection	Other UDP traffic.
S0	UDP out	Connection has seen UDP outbound traffic only.
SF	UDP conversation	Connection has seen UDP traffic between originator and responder.
SHR	UDP in	Connection has seen UDP inbound traffic only.

DCE RPC

@type: dce_rpc

DCE RPC protocol information. Includes information about binding as well as operations.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
rtt	True	The round-trip time from the request to the response.
secondary_address	True	Secondary address - obtained from bind ACK packet. Represents a remote pipe name if contained within SMB or port if not.
endpoint_uuid	True	UUID corresponding to the DCE-RPC endpoint.
endpoint	True	Endpoint name found from the UUID given in the bind request.
opnum	True	Operation number seen in the request. Will be in hex.
operation	True	Operation seen in the request.
bind_result	True	Result of a bind operation.
operation_result	True	Result of a non-bind operation

DHCP

@type: dhcp

DHCP protocol information.

Field	Optional	Description
epochdate	False	The earliest time at which a DHCP message over the associated connection is observed.
uid	False	A unique identifier of the connection over which DHCP is occurring.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
mac	True	Client's hardware (MAC) address.
assigned_ip	True	Client's actual assigned IP address.
lease_time	True	IP address lease interval.
trans_id	False	A random number chosen by the client for this transaction.
subnet_mask	True	Subnet mask of the client, if present in packet (DHCP Option #1).
domain_name	True	The DNS domain name of the client, if present in packet (DHCP option #15).
dhcp_type	True	The DHCP type that generated this record.
host_name	True	Hostname if present (DHCP option 12).
released_ip	True	Client's released IP address.
requested_ip	True	Client's requested IP address.

DHCP DISCOVER

@type: dhcp_discover

The record type for periodically logging information about DHCP Discover requests. Information is gathered only when a Discover command is seen and so log_period can vary.

Field	Optional	Description
epochdate	False	The time at which the first Discover command in this log was seen.
uid	False	A unique identifier of the connection over which DHCP is occurring.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
num_dhcp_discover_requests	True	The number of discover requests made over this connection in the log period.
num_unique_requested_ips	True	The number of unique ip addresses (if any) requested over this connection in the log period.
log_period	True	The period over which the information presented has been collected.

DHCPv6

@type: dhcpv6

DHCPv6 protocol information.

Field	Optional	Description
epochdate	False	The earliest time at which a DHCP message over the associated connection is observed.
uid	False	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
cmd	False	DHCPv6 message types.
client_type	False	Client identifier type. See the table DHCPV6::UUID TYPES for more details.
client_id	False	Client's unique identifier of type - defined in client_type field.
server_type	True	Server's identifier type. See the table DHCPV6::UUID TYPES for more details.
server_id	True	Server's unique identifier of type, as defined in the server_type field.
iface_id	True	Information passed by the relay agent that identifies the interface on which the client message was received.
addr_type	True	IA Address type, as defined in DHCPV6::IA NA TYPES.
IPv6	True	IPv6 address from IA Address option.
addr_pref_time	True	The preferred lifetime for the IPv6 address in the option, in seconds.
addr_valid_time	True	The valid lifetime for the IPv6 address in the option, in seconds.
pfxIPv6	True	The prefix address.
pfx_pref_time	True	Preferred lifetime for the prefix in seconds.
pfx_valid_time	True	Preferred valid lifetime for the prefix in seconds.
resp_code	True	Response code in string format, for list of available codes, consult DHCPV6::DHCPV6 ERR CODE.
resp_msg	True	Reply message text.
opts	True	List of Option Request Options (OPTION_ORO).

DHCPV6::UUID TYPES

DHCP Unique Identifier (DUID) types.

Field	Description
DHCPV6::DUID_NONE	DUID missing.
DHCPV6::DUID_LLT	DUID Based on Link-layer Address Plus Time.
DHCPV6::DUID_EN	DUID Assigned by Vendor Based on Enterprise Number.
DHCPV6::DUID_LL	DUID Based on Link-layer Address.
DHCPV6::DUID_UUID	DUID Universally Unique Identifier.

DHCPV6::IA NA TYPES

IA Address option types.

Field	Description
DHCPV6::IA_NA	IA_NA Identity Association for Non-temporary Address Option.
DHCPV6::IA_PD	IA_PD Identity Association for Prefix Delegation.
DHCPV6::IA_TA	IA_TA Identity Association for Temporary Address Option.

DHCPV6::DHCPV6 ERR CODE

Error codes for DHCPv6 requests.

Field	Value
0	Success
1	UnspecFail
2	NoAddrsAvail
3	NoBinding
4	NotOnLink
5	UseMulticast

DHCPv6 Relay

@type: dhcpv6_relay

DHCPv6 RELAY_REPLY & RELAY_FORWARD protocol information.

Field	Optional	Description
epochdate	False	The earliest timestamp at which a DHCP message over the associated connection is observed.
uid	False	A unique identifier for the connection over which DHCPv6 is occurring.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
cmd	False	DHCPv6 message types assigned based on parser.
relay_cmd	False	Relay related message type. If available, should be the same as the field defined in cmd.
hops	False	Hop-count - number of hops over the relay agents.
link_addr	False	A global or site-local address that will be used by the server to identify the link on which the client is located.
peer_addr	False	The address of the client or relay agent from which the message to be relayed was received.
interface_id	False	Interface ID on which the client message was received by relay agent.
trans_id	False	Transaction ID of relay commands inside DHCPv6 packet.

DNS

@type: dns

DNS protocol information.

Field	Optional	Description
epochdate	False	The earliest time at which a DNS protocol message over the associated connection is observed.
oss_ts	True	The earliest Darktrace optional time at which a DNS protocol message over the associated connection is observed. This time is retrieved from directly from packet, either ERSPAN or IP optional timestamp.
uid	False	A unique identifier for the connection over which DNS messages are being transferred.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
proto	True	The transport layer protocol of the connection.
trans_id	True	A 16-bit identifier assigned by the program that generated the DNS query.
query	True	The domain name that is the subject of the DNS query.
query_class	True	The QCLASS value specifying the class of the query.
query_type	True	A QTYPE value specifying the type of query.
other_queries	True	Listing of additional DNS queries that came in same packet.
err_code	True	A descriptive name for the response code value.
answers	True	Recognized answers from the DNS server. This list only contains answers that are processed.
atypes	True	Types of answers. Listed in the same order as answers.
a_load	True	List of payloads related to answers given in the same order as answers.
TTLs	True	TTL of DNS packet.
unprocessed_atypes	True	List of answer types that DPI currently does not process.
unprocessed_payload_size	True	Payload lengths of answers that DPI currently does not process. Order given matches unprocessed_atypes.
unprocessed_TTLs	True	TTL of answers that DPI currently does not process. Order given matches unprocessed_atypes.
multicast_responder	True	If the connection has been identified as multicast, registers which IP represents the multicast responder.
details	True	Optional extra details related to this traffic.
rejected	True	Indicates the DNS query was rejected by the server. Detected from the response; if error code is set and there are no replies in the packet or if questions are missing.

Device Details

@type: device_details

Device details record.

Field	Optional	Description
epochdate	False	Earliest time at which the associated connection is observed.
ip	True	IP address that this event is related to. Can differ from connection source or destination.
mac	False	MAC address this event is related to. Please note this may not be the layer 2 Ethernet address of the packet, rather, an address extracted from the application protocol.
host	True	Hostname extracted from the event.
method	False	The source of device detail information, e.g. DHCP Request.
uid	True	Connection unique identifier.
src	True	Connection source IP address.
dst	True	Connection destination IP address.
src_p	True	Connection source port.
dst_p	True	Connection destination port.
subnet_mask	True	Subnet mask for the IP lease obtained via DHCP.
lease_time	True	IP lease time obtained via DHCP.
domain_name	True	DNS search domain provided via DHCP. Clients will suffix this domain when searching for hostnames that are not fully qualified.
released_ip	True	IP address that has been released from the associated mac address. For example, on DHCP Decline or Release packets.
outer_vlan	True	Outer VLAN tag of the connection.
vlan	True	VLAN tag of the connection.

FTP

@type: ftp

File Transfer Protocol information.

Field	Optional	Description
epochdate	False	Time when the FTP command was sent.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
user	True	User name for the current FTP session - default value is "".
command	True	The FTP command given by the client.
arg	True	Argument for the FTP command if given.
mime_type	True	The detected file type, if the command indicates a file transfer.
file_msg	True	The response message 'msg' containing file size, if the FTP command indicated a file transfer.
reply_code	True	Reply code from the server in response to the FTP command.
reply_msg	True	Reply message from the server in response to FTP the command.
data_channel (subtype)	True	The expected FTP data channel.
data_channel_passive	False	Whether PASV (passive) mode is toggled for the control channel.
data_channel_orig_h	False	The host that will be initiating the data connection.
data_channel_resp_h	False	The host that will be accepting the data connection.
data_channel_resp_p	False	The port at which the acceptor is listening for the data connection.
fuid	True	File's unique ID.

Files Identified

@type: files_identified

Metadata information on a given file.

Field	Optional	Description
epochdate	False	The time the file was first seen.
fuid	False	An identifier associated with a single file.
tx_hosts	True	If this file was transferred over a network connection this should show the host or hosts that the data sourced from.
rx_hosts	True	If the file was transferred over a network connection, this field should show the host or hosts that the data travelled to.
conn_uids	True	The connection unique identifier over which the file was transferred.
source	True	An identification of the source of the file data. For example, it may be a network protocol over which it was transferred, or a local file path which was read, or another input source.
mime_type	True	Probable mime type of the file found by direct assessment of bytes in the file instead of, for example, the content type header in the HTTP header.
filename	True	A filename for the file, if one is available from the source for the file.
seen_bytes	True	Number of bytes provided for analysis for the file.
total_bytes	True	Total number of bytes that are supposed to comprise the full file.
md5	True	An MD5 digest of the file contents.
sha1	True	A SHA1 digest of the file contents.
sha256	True	A SHA256 digest of the file contents.
uid	True	The first conn uid for a file transfer.
file_ident_descr	True	A protocol specific “description” for the file.
file_ident_ports	True	Ports used on the server side.

HTTP

@type: http

HTTP protocol information.

Field	Optional	Description
epochdate	False	Timestamp at which the request happened.
uid	False	A unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
trans_depth	False	Represents the pipelined depth into the connection of this request/response transaction.
method	True	Verb used in the HTTP request (GET, POST, HEAD, etc.).
host	True	Value of the HOST header.
uri	True	URI used in the request.
referrer	True	Value of the "referer" header. The variable itself is spelled correctly ("referrer"), but the description follows the conventional standard misspelling ("referer").
version	True	Value of the version portion of the request.
user_agent	True	Value of the User-Agent header from the client.
request_body_len	True	Actual uncompressed content size of the data transferred from the client.
response_body_len	True	Actual uncompressed content size of the data transferred from the server.
status_code	True	Status code returned by the server.
status_msg	True	Status message returned by the server.
info_code	True	Last seen 1xx informational reply code returned by the server.
info_msg	True	Last seen 1xx informational reply message returned by the server.
content_type	True	Content type of the file
tags	False	A set of indicators of various attributes, discovered and related to a particular request/response pair.
username	True	Username, if basic-auth is performed for the request.
proxied	True	All headers that may indicate if the request was proxied.
oss_ts	True	Timestamp when the request happened, received from outside of the Darktrace appliance. For example, from Erspan or an osSensor.
orig_fuids	True	An ordered vector of file unique IDs from the client.
orig_filenames	True	An ordered vector of filenames from the client.
orig_mime_types	True	An ordered vector of mime types from the client.
resp_fuids	True	An ordered vector of file unique IDs from the server.

Field	Optional	Description
resp_filenames	True	An ordered vector of filenames from the server.
resp_mime_types	True	An ordered vector of mime types from the server.
client_header_names	True	The vector of HTTP header names sent by the client. No header values are included here, just the header names.
server_header_names	True	The vector of HTTP header names sent by the server. No header values are included here, just the header names.
redirect_location	True	Redirect location given by the HTTP response.
flash_version	True	The unparsed Flash version from the HTTP header.

Hardware

@type: hardware

Information about hardware plugged into Microsoft Windows endpoint, only available for pre-Windows 7 endpoints via Dr. Watson.

Field	Optional	Description
epochdate	False	Timestamp at the time when the hardware was discovered.
uid	True	A connection unique identifier, if the hardware was discovered from a particular network connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
host	False	IP address of the host that the hardware was discovered on.
h_type	False	The type of hardware.
vendor	True	The product vendor name - looked up from the internal list of vendors.
device	True	The device name - looked up from the internal list of devices.

JAVA

@type: java

Java version information log.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
version	False	Java major-minor version number of the class file format being used.

JRMI

@type: jrmi

Java RMI log.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
version	False	Java RMI version number.
protocol	False	JRMI protocol
message	True	Message if available.

Kerberos

@type: kerberos

Kerberos protocol information.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	A unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
request_type	True	The request type. Permitted values: - "AS" : Authentication Service request. - "TGS" : Ticket Granting Service request. - "AP" : Application server access request. - "SAFE": Kerberos SAFE exchange request. - "PRIV": Kerberos PRIV request. - "CRED": Kerberos CRED request.
pa_data_auth	True	Pre-authentication part of the request.
pa_data_new	True	Pre-authentication part of the response.
client	True	Client's principal name, in the format: "cname@crealm [type of principal name]". Values for principal name type are listed in the table KRB::KRB NAME TYPE. If crealm is not specified, srealm or realm are used.
service	True	Server's principal name in format: "sname@srealm [type of principal name]". Values for principal name type are listed in KRB::KRB NAME TYPE.
hostaddrs	True	Host address if available.
krb_from	True	Requested start of ticket validity.
till	True	Requested end of ticket validity.
forwardable	True	Forwardable ticket requested.
renewable	True	Renewable ticket requested.
forwarded	True	Forwarded ticket flag included.
proxy	True	Proxy flag included.
success	True	Request result. Permitted values are True or False.
error_msg	True	Error message. For a full list of possible codes, please refer to the MIT Kerberos documentation.
auth_ticket (subtype)	True	Ticket seen in the request used for authentication.
auth_ticket_service	True	Service that the client is requesting a ticket for. The service principal name takes the format: "sname@srealm [type of principal name]". Values for principal name type are listed in the table KRB::KRB NAME TYPE.
auth_ticket_cipher	True	Ticket encryption type.
auth_ticket_ciphertext	True	Ticket's cipher text hash.

Field	Optional	Description
new_ticket (subtype)	True	Received ticket.
new_ticket_service	True	Service that the client is requesting a ticket for. The service principal name takes the format: “sname@srealm [type of principal name]”. Values for principal name type are listed in the table KRB::KRB NAME TYPE.
new_ticket_cipher	True	Ticket encryption type.
new_ticket_ciphertext	True	Ticket’s cipher text hash.
additional_tickets	True	Additional ticket from request, if available.
is_orig	True	Originator of message, used for _PRIV, _SAFE, _CRED messages.
issue	True	Additional information derived from parsing.
client_cert_subject	True	Subject of client certificate, if any.
client_cert_fuid	True	File unique ID of client certificate, if any.
server_cert_subject	True	Subject of server certificate, if any.
server_cert_fuid	True	File unique ID of server certificate, if any.

KRB::KRB NAME TYPE

Kerberos principal name types list as defined in IANA's document of Kerberos "Preauthentication and Type Data" registry.

Field	Value	Description
0	UNKNOWN_PRINCIPAL	Name type not known.
1	PRINCIPAL	Kerberos principal name, formed in this way: primary/instance@REALM. Where the primary is part of principal that can be either e.g. username or hostname, instance is optional string that qualifies the principal, e.g. fully qualified hostname. The realm is Kerberos realm.
2	SERVICE_INST	Service and other unique instance (krbtgt).
3	SERVICE_HSTN_INST	Service with host name as instance (telnet, rcommand).
4	SERVICE_XHST	Service with host as remaining components.
5	UID	Unique ID.
6	X500_PRINCIPAL	Encoded X.509 Distinguished name [RFC 2253].
7	SMTP_NAME	Name in form of SMTP email name.
10	ENTERPRISE_PRINCIPAL	Windows 2000 UPN, Enterprise name - may be mapped to principal name.
11	WELLKNOWN	Wellknown.

LDAP

@type: ldap

Information relating to LDAP connections.

Field	Optional	Description
epochdate	False	Timestamp when message was seen.
uid	False	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
operation	True	Type of LDAP operation.
services	True	A list of services triggered by LDAP bind.
version	True	Bind version.
authentication	True	Authentication type [Simple/SASL]. If the authentication type is SASL, the field is extended by mechanism in the form "SASL[]".
bind_name	True	If present, this field contains the name of the Directory Object that the client wishes to bind as.
password_seen	True	For bind requests, this field represents whether or not a plain text password was seen.
search_root	True	Base object relative to which the search will be performed.
search_scope	True	Scope of the Search operation. Options: "BaseObject", "SingleLevel", "WholeSubtree".
dereference_aliases	True	Policy for dereferencing aliases while searching. Options: "Never", "InSearching", "FindingBaseObj", "Always".
filter	True	Search filter.
attributes	True	Requested attributes.
entry	True	For Modify, Add, Del, and Compare requests - the name of the entry upon which to perform the operation.
comparison	True	For Compare requests - the attribute value assertion being tested.
response	True	Textual representation of message response.
issue	True	Contains more details if there was issue with packet processing.

Messages

@type: messages

Unusual or exceptional activity information.

Field	Optional	Description
epochdate	False	The timestamp when the message occurred.
uid	True	Unique identifier of the connection, if a connection is associated with this event.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
name	False	The identification name of the message that occurred.
addl	True	Additional information accompanying the message if any.
notice	True	If true, this message also fired a notice.
oss_ts	True	Timestamp when the message occurred, if it was intercepted outside of DPI's main interface.

Microsoft Watson Crash

@type: microsoftwatson_crash

Logs information whenever software crashes happen such as the application that crashed and why it crashed.

Field	Optional	Description
epochdate	False	Timestamp when the crash occurred.
uid	True	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
host	True	Host IP.
app (subtype)	False	Details of the application.
app_name	False	Name of the application.
app_version	False	Version of the application.
app_timestamp	False	Application timestamp.
arch	True	Indicates the architecture being used - either 32 or 64 bit.
mod_app (subtype)	False	The module that appears to be responsible for the crash.
mod_app_name	False	Name of the application.
mod_app_version	False	Version of the application.
mod_app_timestamp	False	Application timestamp.
exception_code	True	Exception code - for example stack overflow.
fault_offset	True	Dr Watson exception offset.

Microsoft Watson Platform

@type: microsoftwatson_platform

Logs information about platforms discovered from Dr Watson messages.

Field	Optional	Description
epochdate	False	Timestamp when the crash occurred.
uid	True	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
host	True	Host IP.
system_manufacturer	True	Name of the system manufacturer.
system_name	True	System name.

Mining

@type: mining

Cryptocurrency mining information seen over JSON-RPC protocol.

Field	Optional	Description
start_ts	False	Timestamp for when mining was first identified.
epochdate	False	Timestamp at which logging occurred.
uid	False	A unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
mining_protocol	False	The mining protocol detected, for example 'Stratum' or 'Minergate'.
login_credentials	True	Login credentials used for mining workers. Usually either a wallet ID or an email address, depending on the pool used.
orig_methods	True	JSON-RPC methods seen from the connection originator.
resp_methods	True	JSON-RPC methods seen from the responder.
orig_is_miner	False	Boolean flag that indicates if the miner is the originator of the connection.

MySQL

@type: mysql

MySQL protocol information.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
cmd	False	The SQL command that was issued.
arg	False	The argument issued to the command.
success	True	A boolean indicating if the command succeeded.
rows	True	The number of affected rows. If no rows are affected, this will not appear.
response	True	Server message, if present.

NTLM

@type: ntlm

Information on NTLM connections

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
username	True	Username given by the client.
hostname	True	Hostname given by the client.
domainname	True	Domain name given by the client.
authentication_success	True	True if the authentication was successful, false if unsuccessful, not present if response was not seen.
status	True	A string representation of the status code that was returned in response to the authentication attempt.

OS Version

@type: os_version

Operating system information.

Field	Optional	Description
epochdate	False	The timestamp of the first packet.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
uid	False	A unique identifier of the connection.
vlan	True	VLAN ID of the connection. If both VLANs are present, this contains the inner VLAN ID.
outer_vlan	True	The Outer VLAN for this connection, if applicable.
os_genre	True	Genre of operating system. For example, Linux, Windows, AIX...
os_version	True	Version of the operating system.
distance_ttl	True	How far away the host is from the sensor (TTL).
match_type	True	Quality of the match.
os_class	True	Operating system class.
http_name	True	Name of the HTTP client.
http_flavor	True	HTTP client flavor.
language	True	Detected language.
link_type	True	MTU-derived link type.
last_seen	True	Last time the host was seen in UNIX time. Zero is unseen.
bad_sw	True	Bad software. Indicates possible dishonest user-authentication or server.
last_nat	True	Last NAT detection time.
uptime	True	Last computed uptime. -1 is used for 'None'.
uptime_modulo_days	True	Uptime modulo in days.
src	True	IP address where the OS is being used.
reboot	True	Boolean to indicate if the known machine has rebooted flag.

PE

@type: pe

Information on Portable Executable files

Field	Optional	Description
epochdate	False	Current timestamp.
id	False	File identifier of this portable executable file.
machine	True	The target machine that the file was compiled for.
compile_ts	True	The time that the file was created.
os	True	The required operating system.
subsystem	True	The subsystem that is required to run this file.
is_exe	True	True, if the file is an executable. False, if just an object file.
is_64bit	True	True, if file is a 64-bit executable.
uses_aslr	True	True, if the file supports Address Space Layout Randomization.
uses_dep	True	True, if the file supports Data Execution Prevention.
uses_code_integrity	True	True, if the file enforces code integrity checks.
uses_seh	True	True, if the file uses structured exception handing.
has_import_table	True	True, if the file has an import table.
has_export_table	True	True, if the file has an export table.
has_cert_table	True	True, if the file has an attribute certificate table.
has_debug_data	True	True if the file has a debug table.
section_names	True	The names of the sections, in order.

POP3

@type: pop3

Post Office Protocol 3 information.

Field	Optional	Description
epochdate	False	Time when the protocol was first seen.
uid	False	Unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
messages_transferred	True	Number of message bodies transferred.
user	True	Value of the User Login from the client.
login_success	True	Result of login attempt.
commands_used	True	The pop3 commands issued by the client.
fuids	True	An ordered vector of file unique IDs seen attached to the message.

Packet Filter

@type: packet_filter

Information about applied packet filters.

Field	Optional	Description
epochdate	False	The time at which the packet filter installation attempt was made.
node	True	A string representation of the node that applied this packet filter. This is useful in the context of dynamically changing filters on DPI workers.
filter	False	The packet filter that is being set.
init	True	Indicates if this is the filter set during initialization.
success	True	Indicate if the filter was applied successfully.

RADIUS

@type: radius

Remote Authentication Dial-In User Service protocol information.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique identifier for the Radius connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
trans_id	False	RADIUS transaction ID.
username	True	The username, if present.
mac	True	The client's MAC address, if present.
framed_ip	True	The address given to the network access server, if present. This is only a hint from the RADIUS server and the network access server is not required to honor the address.
remote_ip	True	Remote IP address, if present. This is collected from the Tunnel-Client-Endpoint attribute.
remote_domain_name	True	Remote hostname, if present. This is collected from the Tunnel-Client-Endpoint attribute.
connect_info	True	The contents of the Connect-Info attribute, if present.
reply_msg	True	Reply message from the server challenge. This is frequently shown to the user authenticating.
result	True	Successful or failed authentication.
ttl	True	The duration between the first request and either the "Access-Accept" message or an error. If the field is empty, it means that either the request or response was not seen.

RDP

@type: rdp

Remote Desktop Protocol information.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
cookie	True	Cookie value used by the client machine. This will typically be a username.
result	True	Status result for the connection.
security_protocol	True	Security protocol chosen by the server.
keyboard_layout	True	Keyboard layout (language) of the client machine.
client_build	True	RDP client version used by the client machine.
client_name	True	Name of the client machine.
client_dig_product_id	True	Product ID of the client machine.
desktop_width	True	Desktop width of the client machine.
desktop_height	True	Desktop height of the client machine.
requested_color_depth	True	The color depth requested by the client.
cert_type	True	The type of encryption certificate used if the connection is encrypted with native RDP encryption.
cert_count	True	The number of certificates seen.
cert_permanent	True	Indicates if the provided certificate or certificate chain is permanent or temporary.
encryption_level	True	Encryption level of the connection.
encryption_method	True	Encryption method of the connection.

SIP

@type: sip

Session Initiation Protocol information.

Field	Optional	Description
epochdate	False	Timestamp when the request happened.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
trans_depth	False	Represents the pipelined depth into the connection of this request/response transaction.
method	True	Verb used in the SIP request (INVITE, REGISTER etc.).
uri	True	URI used in the request.
date	True	Contents of the Date: header from the client.
request_from	True	Contents of the request From: header.
request_to	True	Contents of the To: header.
response_from	True	Contents of the response From: header.
response_to	True	Contents of the response To: header.
reply_to	True	Contents of the Reply-To: header.
call_id	True	Contents of the Call-ID: header from the client.
seq	True	Contents of the CSeq: header from the client.
subject	True	Contents of the Subject: header from the client.
request_path	True	The client message transmission path, as extracted from the headers.
response_path	True	The server message transmission path, as extracted from the headers.
user_agent	True	Contents of the User-Agent: header from the client.
status_code	True	Status code returned by the server.
status_msg	True	Status message returned by the server.
warning	True	Contents of the Warning: header
sip_request_body_len	True	Contents of the Content-Length: header from the client
sip_response_body_len	True	Contents of the Content-Length: header from the server
content_type	True	Contents of the Content-Type: header from the server

SMB Access Failure

@type: smb_access_failure

SMB file access failure information.

Field	Optional	Description
epochdate	False	Timestamp when the log entry was created.
start_ts	True	Timestamp when batch logging started, only apparent for batch log entries (e.g. for failed creates for unknown files).
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
protocol_ver	False	SMB protocol version ("smb1" or "smb2").
sessionid	False	Session ID (SMB2) / User ID (SMB1).
filename	True	Name of file in transfer.
path	True	Path to the SMB share which the resource belongs to.
share_type	True	The type of SMB share.
error	True	Error type which caused the create (access-request) to be rejected/fail.
error_desc	True	Verbose description of error.
error_list	True	Lists all error codes seen and gives frequency counters for each. Used in batch logging.
details	True	Information about the log entry, e.g. corresponds to responses with unmatched requests and therefore no known filename.
total_errors	True	Total number of error responses seen. Used for batch logging of create failure responses for unknown files.

SMB Directory Query

@type: smb_dir_query

SMB directory query information.

Field	Optional	Description
epochdate	False	Timestamp when the directory query message was seen.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
protocol_ver	False	SMB protocol version ("smb1" or "smb2").
sessionid	False	Session ID.
result	True	Result of command (success, failure type, or unknown).
filename	True	The resource filename.
querypattern	False	Query string used/searched.
path	True	Path to the SMB share which the resource belongs to.
share_type	True	The type of SMB share.
details	True	Information regarding reasons for logging or issues in processing.

SMB ReadWrite

@type: smb_readwrite

SMB reading/writing data information.

Field	Optional	Description
epochdate	False	Timestamp when the read/write message was seen.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
protocol_ver	False	SMB protocol version ("smb1" or "smb2").
sessionid	False	Session ID (SMB2) / User ID (SMB1).
action	True	Action being performed. Either read, write, readwrite, move, delete or close. ReadWrite action suggests that there were both reads and writes commands seen int the last time period on this file.
result	True	Result of command. Either success, failure type, or unknown.
filename	True	Name of the file in transfer.
data_len	True	Total size of the resource in bytes on last handle creation. Only present if the handle creation was seen for this file.
mime	True	The MIME file type detected.
last_names	True	List of all previous filenames related to this file seen in this session.
attempted_rename	True	Attempted new name for file, only populated in the case of a MOVE action with a failure or unknown response.
read_status	True	Result of read request.
read_size	True	Total amount of data read in transfer in bytes.
read_start	True	Timestamp of the first read command seen for the resource.
read_packets	True	Number of packets seen for read command for the resource.
write_status	True	Result of write request.
write_size	True	Total amount of data written in transfer in bytes.
write_start	True	Timestamp of the first write command seen for the resource.
write_packets	True	Number of packets seen for write command for the resource.
delete_packets	True	Used in the case of unconfirmed delete requests/responses to unknown files. Gives the total number of delete packets seen for this log entry.
move_packets	True	Used in the case of unconfirmed move requests/responses to unknown files. Gives the total number of move packets seen for this log entry.
unknown_read_packets_list	True	Used in the case of unconfirmed readwrite requests to unknown files. Lists the number of read packets associated with each file.

Field	Optional	Description
unknown_write_packets_list	True	Used in the case of unconfirmed readwrite requests to unknown files. Lists the number of write packets associated with each file.
unknown_read_size_list	True	Used in the case of unconfirmed readwrite requests to unknown files. Lists the size of read data associated with each file.
unknown_write_size_list	True	Used in the case of unconfirmed readwrite requests to unknown files. Lists the size of write data associated with each file.
unknown_delete_packets_list	True	Used in the case of unconfirmed delete requests to unknown files. List the number of delete packets associated with each SMB share.
path	True	Path to the SMB share which the resource belongs to.
share_type	True	The type of SMB share.
details	True	Information regarding reasons for logging or issues in processing, e.g. log shows cumulative data transfer for this file, error access denied etc.

SMB Session

@type: smb_session

SMB session activity information.

Field	Optional	Description
epochdate	True	Timestamp when the SMB session was created.
uid	True	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
protocol_ver	False	SMB protocol version ("smb1" or "smb2").
sessionid	True	Session ID (SMB2) / User ID (SMB1).
mech_type	True	Mechanism type. Either Kerberos, NTLMSSP, or NTLM.
result	True	Authentication result. Either success, failure type, or unknown.
account	True	The username of the account.
client_hostname	True	Hostname the user logged in from.
domain	True	Desired primary authentication domain.
nativeOS	True	Native operating system of the CIFS client.
details	True	Information regarding reasons for logging or issues in processing (e.g. missing request).

SMB Transaction

@type: smb_transaction

SMB1 transaction information.

Field	Optional	Description
epochdate	True	Timestamp at the point of logging.
uid	True	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
sessionid	True	User ID (SMB1).
protocol_ver	False	SMB protocol version (will always be "smb1").
path	True	Path to the SMB share which the resource belongs to.
share_type	True	The type of SMB share.
transaction_name	True	The pathname of the mailslot/named pipe used.
statuses	True	List of status types and frequency seen in the interval.
start_ts	False	Timestamp of when the initial SMB transaction message was seen.

SMB::SHARETYPE

The type of share the resource exists under.

Field	Description
SMB::COMM	Serial communications device.
SMB::INVALID	Invalid or unknown share type.
SMB::MISSED	We did not see the relevant share connect to get the type.
SMB::PIPE	A named pipe share.
SMB::PRINT	A printer share.

SMTP

@type: smtp

SMTP protocol information.

Field	Optional	Description
epochdate	False	Time when the message was first seen.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
trans_depth	False	A count representing the depth of this message transaction in a single connection, where multiple messages were transferred.
helo	True	Contents of the Helo header.
mailfrom	True	Email addresses found in the From header.
rcptto	True	Email addresses found in the Rcpt header.
date	True	Contents of the Date header.
from	True	Contents of the From header.
to	True	Contents of the To header.
cc	True	Contents of the CC header.
reply_to	True	Contents of the ReplyTo header.
msg_id	True	Contents of the MsgID header.
in_reply_to	True	Contents of the In-Reply-To header.
subject	True	Contents of the Subject header.
x_originating_ip	True	Contents of the X-Originating-IP header.
first_received	True	Contents of the first Received header.
second_received	True	Contents of the second Received header.
last_reply	True	The last message the server sent to the client.
path	True	The message transmission path, as extracted from the headers.
user_agent	True	Value of the User-Agent header from the client.
tls	True	Indicates whether the connection has switched to using TLS.
fuids	True	An ordered vector of file unique IDs seen attached to the message.
decoded_subject	True	Decoded subject from SMTP SUBJECT header.

SNMP

@type: snmp

Information tracked per SNMP session.

Field	Optional	Description
epochdate	False	Timestamp of the first packet belonging to the SNMP session.
uid	False	The unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
duration	True	The amount of time between the first packet belonging to the SNMP session and the latest one seen.
version	False	The version of SNMP used.
community	True	The community string of the first SNMP packet associated with the session. This is used as part of SNMP's (v1 and v2c) administrative/security framework. See RFC 1157 or RFC 1901.
get_requests	True	The number of variable bindings in GetRequest/GetNextRequest PDUs seen for this session.
get_bulk_requests	True	The number of variable bindings in GetBulkRequest PDUs seen for this session.
get_responses	True	The number of variable bindings in GetResponse/Response PDUs seen for this session.
set_requests	True	The number of variable bindings in SetRequest PDUs seen for this session.
display_string	True	A system description of the SNMP responder endpoint.
up_since	True	The time at which the SNMP responder endpoint claims it has been up since.

SOCKS

@type: socks

Information on SOCKS events.

Field	Optional	Description
epochdate	False	Time when the proxy connection was first detected.
uid	False	Unique ID for the tunnel - may correspond to connection UID or be non-existent.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
version	False	Protocol version of SOCKS.
user	True	Username used to request a login to the proxy.
status	True	Server status for the attempt at using the proxy.
request (subtype)	True	Client requested SOCKS address. This could be an address, a name or both.
request_host	True	Host IP address.
request_name	True	Host name.
request_p	True	Client requested port.
bound (subtype)	True	Server bound address. This could be an address, a name or both.
bound_host	True	Host IP address.
bound_name	True	Host name.
bound_p	True	Server bound port.

SSDP

@type: ssdp

Simple Service Discovery Protocol information.

Field	Optional	Description
epochdate	False	Timestamp at which the last SSDP message that contributed to this log entry was seen.
start_ts	False	Timestamp at which the first SSDP message that contributed to this log entry was seen.
uid	False	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
method	False	The SSDP method (NOTIFY, M-SEARCH or (Search Response)).
total_messages	False	Total number of messages that contributed to this log entry.
ssdp_type	True	The SSDP type (ssdp:alive, ssdp:byebye, ssdp:update or "ssdp:discover").
usn	True	The Unique Service Name. Identifies a unique instance of a device or service for a NOTIFY message.
search_target	True	The search target of the M-SEARCH message.
version_info	True	String containing version information in the format: [Operating System Name/Version, UPnP Version, Product Name/Version] specified by the UPnP vendor.
location	True	URL to the UPnP description of the root device.
service_type	True	The Service/Notification Type, for NOTIFY messages only.
host	True	The domain name or IP address of the target device and port. Only included for unicast requests.
headers	True	List of all headers seen for this log entry.

SSH

@type: ssh

SSH protocol information.

Field	Optional	Description
epochdate	False	Time when the SSH connection began.
uid	False	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
version	False	SSH major version. Will either be one or two.
status_guess	True	Authentication status of SSH connection. SSH2 status, once the connection becomes encrypted, is determined by differences in packet sizes. This method is not possible in SSH1, so SSH1 status after encrypted traffic is seen will always be 'ssh1_unknown'.
auth_success	True	Authentication result: T=success, F=failure and unset=unknown.
auth_attempts	True	The number of authentication attempts observed. This is always at least one, as some servers may support no authentication at all. It's important to note that not all attempts correspond to failures, since some servers require two-factor auth (e.g. a password AND a pubkey).
direction	True	Direction of the connection. If the client was a local host logging into an external host, this would be OUTBOUND. INBOUND would be set for the opposite.
client	True	The client's version string.
server	True	The server's version string.
cipher_alg	True	The encryption algorithm in use.
mac_alg	True	The signing (MAC) algorithm in use.
compression_alg	True	The compression algorithm in use.
kex_alg	True	The key exchange algorithm in use.
host_key_alg	True	The server host key's algorithm.
host_key	True	The server's key fingerprint.

SSL

@type: ssl

SSL/TLS protocol information.

Field	Optional	Description
epochdate	False	Timestamp when the SSL connection was first detected.
uid	False	A unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
version	True	SSL/TLS version chosen by the server.
cipher	True	The SSL/TLS cipher suite chosen by the server.
client_ciphers	True	List of ciphers offered by client (only shown if a limited number are offered).
total_client_ciphers	True	Total number of ciphers offered by the client.
curve	True	The elliptic curve chosen by the server when using ECDH/ECDHE.
server_name	True	Value of the Server Name Indicator SSL/TLS extension - indicates the server name requested by the client.
resumed	True	A flag indicating if this SSL session was resumed reusing the key material exchanged in an earlier connection.
last_alert	True	Last alert seen during the connection.
next_protocol	True	Next application layer protocol, negotiated via TLS's Next Protocol Negotiation Extension.
established	True	A flag to indicate if this SSL session has been established successfully, or if it was aborted during the handshake.
client_hello_seen	True	Indicates the client hello was seen for this ssl connection.
cert_chain_fuids	True	An ordered vector of all certificate file unique IDs for certificates offered by the server.
client_cert_chain_fuids	True	An ordered vector of all certificate file unique IDs for the certificates offered by the client.
subject	True	Subject of the X.509 certificate offered by the server.
issuer	True	Subject of the signer of the X.509 certificate offered by the server.
client_subject	True	Subject of the X.509 certificate offered by the client.
client_issuer	True	Subject of the signer of the X.509 certificate offered by the client.
ocsp_status	True	Result of OCSP validation for this connection.
validation_status	True	Result of certificate validation for this connection.
ja3_client_fingerprint	True	JA3 SSL fingerprint.
ja3s_server_fingerprint	True	JA3S server SSL fingerprint.

Field	Optional	Description
application_guess	True	Description of the client application, if recognised.

STUN

@type: stun

Session Traversal Utilities for NAT protocol information.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
command	True	STUN Command.
result	False	Result of STUN command.
username	True	Username seen in list of optional attributes.
mapped_addr	True	Mapped-address or Xor-mapped-address. This indicates the reflexive transport address of the client. Xor-ed mapped-address is resolved.
mapped_port	True	Mapped-address or Xor-mapped-port - contains client's public port.
error_code	True	Error code returned in case of error response.
error_msg	True	Error message returned in case of error response.

SVCCTL

@type: svcctl

Service Control protocol information. Protocol is usually encapsulated within DCE-RPC.

Field	Optional	Description
epochdate	False	Timestamp for when the event happened.
uid	False	Unique ID for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.

Software

@type: software

Information used for representing and logging software, gathered from Windows CrpytoAPI HTTP requests.

Field	Optional	Description
epochdate	True	The time at which the software was detected.
uid	True	Unique identifier for the connection.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
host	False	The IP address detected running the software.
host_p	True	The port on which the software is running. Only valid for server software.
software_type	True	The type of software detected.
name	True	Name of the software (e.g. Apache).
version (subtype)	True	Version of the software.
version_major	True	Major version number.
version_minor	True	Minor version number.
version_minor2	True	Minor subversion number.
version_minor3	True	Minor updates number.
version_addl	True	Additional version string (e.g. "beta42").
unparsed_version	True	The full, unparsed version string.

Tunnel

@type: tunnel

Information relating to tunneled traffic (encapsulated connection).

Field	Optional	Description
epochdate	False	Time at which tunnel activity occurred.
uid	True	The unique identifier for the tunnel, which may correspond to a (Conn and Conn Long).uid field for non-IP-in-IP tunnels. This is optional, as there could be numerous connections for payload proxies such as SOCKS. These are treated as a single tunnel.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
tunnel_type	False	The type of tunneling protocol.
tunnel_action	False	The type of activity that occurred, refers to TUNNEL::ACTION)

TUNNEL::ACTION

Types of interesting activity that can occur within a tunnel.

Field	Description
Tunnel::CLOSE	A tunnel connection has closed.
Tunnel::DISCOVER	A new tunnel (encapsulating “connection”) has been detected.
Tunnel::EXPIRE	No new connections over a tunnel occurred in the given time interval.

X.509

@type: x509

Information on X.509 files.

Field	Optional	Description
epochdate	False	Current timestamp.
fid	False	File ID of this certificate.
certificate (subtype)	False	Basic information about the certificate. For individual items, look up certificate_* fields.
certificate_version	False	Version number.
certificate_serial	False	Serial number.
certificate_subject	False	The thing being secured by this certificate.
certificate_issuer	False	The issuer of this certificate.
certificate_not_valid_before	False	Timestamp before which certificate is not valid.
certificate_not_valid_after	False	Timestamp after which certificate is not valid.
certificate_key_alg	False	Name of the key algorithm.
certificate_sig_alg	False	Name of the signature algorithm.
certificate_key_type	True	Key type, if key parseable by openssl (either rsa, dsa or ec).
certificate_key_length	True	Key length in bits.
certificate_exponent	True	Exponent, if RSA-certificate.
certificate_curve	True	Curve, if EC-certificate.
san (subtype)	True	Subject alternative name extension of the certificate.
san_dns	True	List of DNS entries.
san_uri	True	List of URI entries.
san_email	True	List of email entries.
san_ip	True	List of IP entries.
basic_constraints (subtype)	True	Basic constraints extension of the certificate.
basic_constraints_ca	False	True if for a Certificate Authority i.e. an intermediate CA.
basic_constraints_path_len	True	Maximum path length.
uid	True	The first connection unique identifier for a file transfer.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.

Notice

@type: notice

Additional info on Deep Packet Inspection notices.

Field	Optional	Description
epochdate	True	An absolute time indicating when the notice occurred.
uid	True	A connection UID which uniquely identifies the endpoints concerned with the notice.
source_ip	False	The source's IP address.
source_port	False	The source's port number.
dest_ip	False	The destination's IP address.
dest_port	False	The destination's port number.
fuid	True	A file unique ID if this notice is related to a file.
file_mime_type	True	A mime type if the notice is related to a file.
file_desc	True	Additional info if the notice is related to a file.
proto	True	The transport protocol.
note	False	The notice type of the notice.
msg	True	The notice's message. Contents is dependent on the notice type of the notice.
details	True	The details of the notice. Contents is dependent on the notice type of the notice.
ics_info	True	ICS Specific additional information (in json format). Only present if analysis of ICS protocols is enabled.
sha1_file_hash	True	The sha1 hash of the file if this notice is related to a file and the hash is available.
md5_file_hash	True	The md5 hash of the file if this notice is related to a file and the hash is available.
sha256_file_hash	True	The sha256 of the file if this notice is related to a file and the hash is available. Note this is only added if sha256 file hashes are enabled.
src	True	The source's IP address.
dst	True	The destination's IP address.
p	True	The destination's port number.
n	True	Numeric size associated with notice. Meaning is dependent on the notice type of the notice.
oss_ts	True	An absolute time indicating when the notice occurred when using osSensors.
size	True	A numeric size associated with the notice.
clienthostname	True	Client hostname if available.
originated_from_source_ip	True	Indicates if the originator of the connection triggered the event.
outer_vlan	True	The Outer VLAN for this connection, if applicable.
vlan	True	The Inner VLAN for this connection, if applicable.

Field	Optional	Description
dpi_engine	True	The hostname of the DPI instance that raised this notice.

Notices

Deep Packet Inspection notice types. Each notice type has a corresponding metric from which models can be built.

Field	Description
CaptureLoss Packet Drops	Amount of packet drops on the host. Message contains the hostname that detected packet drops after filtering, with number of packets that were received and number of packets that were dropped. Description contains information about possible reason for packet drops.
Excessive Capture Loss	Notice is fired if the detected capture loss exceeds the percentage threshold. Message contains the hostname that detected capture loss and the estimated loss rate. Description contains information about possible reasons for drop rate.
Cryptocurrency Miner	Cryptocurrency miner found. Message contains the miner's IP and protocol in use. Description contains a list of the JSON-RPC methods seen during this connection. Once identified, this notice will fire periodically throughout the lifetime of the connection.
Cryptocurrency Mining Credential	Cryptocurrency mining credentials seen. Message contains the mining credential seen, usually either a wallet ID or email address, and the mining protocol detected.
Cryptocurrency Mining Pool Server	Cryptocurrency mining pool server found serving work to miners. Message contains the server's IP and protocol in use. Description contains a list of the JSON-RPC methods seen during this connection. Once identified, this notice will fire periodically throughout the lifetime of the connection.
Cryptocurrency Possible Mining	Potential cryptocurrency mining identified. Message contains the potential mining protocol in use. Description contains a list of the JSON-RPC methods seen during this connection. Once identified, this notice will fire periodically throughout the lifetime of the connection or until mining is confirmed.
DCERPC Bind	DCE RPC bind seen. Will contain both successful and unsuccessful bind attempts. As binding is also seen in alter_context requests, these can also cause these notices to fire. The message will always contains the service requested and file ID that correlate with the file ID of the associated SMB transfer. On a successful bind, the message will also contain the pipe name given by the bind acknowledgement. On a failed bind, the message will contain the associated error. If DCE RPC is not encapsulated within SMB, file ID will be blank. If the pipe name is not seen, as will be the case when using alter context to bind, the pipe name will be "UNKNOWN".

Field	Description
DCERPC Request	DCE RPC request. The message will contain the operation number and file ID correlating to the file ID of the associated SMB transfer. The message will also contain the name of the associated endpoint, if known. If DCE RPC is not encapsulated within SMB, file ID will be blank.
DynDNS DNS Request	A Dynamic DNS domain name was present in a DNS query Message contains “Found Dynamic DNS Hostname” along with the domain name matched against. Description contains the DNS query (which may be a subdomain of the matched address).
DynDNS HTTP Requests	A Dynamic DNS domain name was present in the host header of HTTP request. Message contains “Found Dynamic DNS Hostname” along with the domain name matched against. Description contains the HTTP host header value (which may be a subdomain of the matched address).
DynDNS SSL Requests	A Dynamic DNS domain name was present in the Server Name Indicator field of an SSL request. Message contains “Found Dynamic DNS Hostname” along with the domain name matched against. Description contains the SSL SNI field value (which may be a subdomain of the matched address).
FTP Bruteforce	Indication of FTP login bruteforcing. Message contains the host that is possibly being brute forced, the number of failed logins, the number of FTP servers involved and the duration over which the sample was taken.
FTP Data Expected	Indicates we are expecting to see an FTP data transfer. Message contains the port expected to be open for the transfer. Description contains the relevant FTP command and user who made the request.
FTP SITE EXEC	Successful “SITE EXEC” response was seen. Message contains the command and argument pair.
File Transfer (EXE)	End of an exe filetype transfer seen. Message contains the file’s mimetype, and the sha1 and md5 file hashes if available. Description contains the filename (if available), the file size seen in the transfer and the the transfer direction.
FileTransfer Exe Transfer Start	Beginning of an exe filetype transfer seen. Message contains the exe file’s detected mime type. Description contains the filename (if available), the reported size of the file in bytes and the transfer direction.

Field	Description
File Transfer (Octet Stream)	End of an octet-stream filetype transfer seen. Message contains the file's mimetype, and the sha1 and md5 file hashes if available. Description contains the filename (if available), the file size seen in the transfer and the the transfer direction.
File Transfer (RAR)	End of a rar filetype transfer seen. Message contains the file's mimetype, and the sha1 and md5 file hashes if available. Description contains the filename (if available), the file size seen in the transfer and the the transfer direction.
File Transfer (Unknown Binary)	End of an unknown binary filetype transfer seen. Message contains the file's mimetype, and the sha1 and md5 file hashes if available. Description contains the filename (if available), the file size seen in the transfer and the the transfer direction.
Incorrect File Type Found	Discovery of an incorrect file type. Message contains file name and file mime type. Details field contains file description.
KERBEROS App	Kerberos Application server request. Message is empty. Description contains sreaml, service, request ticket hash, request ticket cipher.
KERBEROS App Fail	Kerberos Application server access error. Message contains client's name, if available, in unencrypted form. Description might contain request type (please see Kerberos.request_type for list of types), error message, client's realm, service realm, service, ticket ciphertext, flags and start and end of validity for requested ticket.
Kerberos Login	Kerberos login (AS) request. Message contains client's name. Description may contain client's realm, server's realm, hostname if present, service's name, flags if available, ticket, ticket's cipher, and from and till timeouts if available.
Kerberos Login Failure	Kerberos login failed. Message contains client's name. Description may contain request type (please see Kerberos.request_type for list of types), error message, client's realm, service realm, service, ticket ciphertext, flags and start and end of validity of the requested ticket.

Field	Description
KERBEROS Ticket	Kerberos ticket (TGS) request. Message contains client's name. Description may contain client's realm, server's realm, service's name, ticket that was used to authenticate, ticket cipher used to authenticate, newly acquired ticket, newly acquired ticket's cipher, flags, and start and end time of ticket if available.
KERBEROS Ticket Fail	Kerberos ticket acquiring error. Message contains client's name. Description may contain request type (please see Kerberos.request_type for list of types), error message, client's realm, service realm, service, ticket ciphertext, flags and start and end of validity for requested ticket.
NTLM Login	Successful NTLM login. Message contains client's username. Description contains the client's domain, client's hostname, the result of the authentication and the login result.
NTLM Login Fail	Unsuccessful NTLM login. Message contains client's username. Description contains the client's domain, client's hostname, the result of the authentication and the login error result.
POP3 Login Success	Successful POP3 login. Message contains the user login from the client.
Server Serving Protocols on Non-Standard Port	Notice fires when a new server is detected on protocol/port combination. Message contains server's IP address, protocol of the connection over which server was discovered, port number on which server was accepting connection. Description contains protocol of the connection over which server was detected.
RADIUS Login	Radius Access Accept notice. Message contains username. Description contains hostname, MAC address, IP address and Connect-Info extension information.
RADIUS Login Fail	Radius Login Failure notice. Message contains username. Description contains hostname, MAC address, IP address and Connect-Info extension information.
RDP Client	Client connection result and data. Message can contain the client name, client build, color depth, and keyboard layout, when available. Description can contain the connection result, the client's Domain Information Groper product id, and screen size, when available.

Field	Description
RDP Cookie	Client connected with an RDP cookie. Message contains the RDP cookie. Description contains the result of the connection.
RDP Keyboard	Client connected with a specified keyboard layout. Message contains the requested keyboard layout type.
SMB Access Failure	SMB Access Failure Response(s). Message contains the relevant SMB share, filename, and the failure response type(s). Description contains the type of SMB share, indication of batch notice, and a verbose error description if non-batch.
SMB Delete Failure	SMB Unsuccessful Delete Action. Message contains the relevant SMB share, filename, and the SMB version. Description contains the delete failure reason, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the delete action.
SMB Delete Success	SMB Successful Delete Action. Message contains the relevant SMB share, filename, and the SMB version. Description contains verbose indication of success, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the delete action (success).
SMB Delete Unknown	SMB Delete Action with Unknown Result. Message contains the relevant SMB share, filename, and the SMB version. Description contains the reason for the notice, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the delete action (unknown).
SMB Directory Query Failure	SMB Directory Query Failure. Message contains the relevant SMB share, the directory path, the search query, and the SMB version. Description contains additional details, the SMB share type, and the result of the directory search.
SMB Directory Query Success	SMB Directory Query Success. Message contains the relevant SMB share, the directory path, the search query, and the SMB version. Description contains additional details, the SMB share type, and the result of the directory search (success).
SMB Directory Query Unknown	SMB Directory Query with Unknown Result. Message contains the relevant SMB share, the directory path, the search query, and the SMB version. Description contains additional details, the SMB share type, and the result of the directory search (unknown).

Field	Description
SMB Move Failure	SMB Unsuccessful Move Action. Message contains the relevant SMB share, the filename, the attempted rename, and the SMB version. Description contains the move failure reason, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the move action.
SMB Move Success	SMB Successful Move Action. Message contains the relevant SMB share, the original filename, new filename, and the SMB version. Description contains verbose indication of success, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the move action (success).
SMB Move Unknown	SMB Move Action with Unknown Result. Message contains the relevant SMB share, the original filename, the requested rename, and the SMB version. Description contains the reason for the notice, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the move action (unknown).
SMB Read Failure	SMB Unsuccessful Read Action(s). Message contains the relevant SMB share, filename, and the SMB version. Description contains the read failure reason, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the read action (failure).
SMB Read Success	SMB Successful Read Action(s). Message contains the relevant SMB share, filename, and the SMB version. Description contains verbose indication of success, the file's mime type, additional details, the SMB share type, the SMB version, the result of the read action (success), and the total number of bytes read.
SMB Read Unknown	SMB Read Action(s) with Unknown Result. Message contains the relevant SMB share, filename, and the SMB version. Description contains the reason for the notice, the file's mime type, additional details, the SMB share type, the SMB version, the result of the read action (unknown), and the total requested number of bytes to read.
SMB Session Failure	SMB Session Setup (login) Failure. Message contains the user who attempted to setup the SMB session. Description contains the client's hostname, the primary authentication domain, the authentication mechanism type, the SMB version, additional details, the anonymous login indication, and the reported OS version (SMB1 only).

Field	Description
SMB Session Success	SMB Session Setup (login) Success. Message contains the user who setup the SMB session. Description contains the client's hostname, the primary authentication domain, the authentication mechanism type, the SMB version, additional details, the anonymous login indication, and the reported OS version (SMB1 only).
SMB Sustained Mimetype Conversion	SMB Sustained Mime Type Conversion Detection. Message contains the total number of bytes read and written from files, and the most common mime type and list of mime types seen from read and write actions (in 30sec intervals). Score represents a balanced ratio of mimetypes that were read by the user versus mimetypes that were written by the user. The main assumption is that users read and write similar files in one session. This notice only appears if score is over or equal to 50%. Score is calculated only if data in transfer in the given period follows specific requirements.
SMB Write Failure	SMB Unsuccessful Write Action(s). Message contains the relevant SMB share, filename, and the SMB version. Description contains the write failure reason, the file's mime type, additional details, the SMB share type, the SMB version, and the result of the write action (failure).
SMB Write Success	SMB Successful Write Action(s). Message contains the relevant SMB share, filename, and the SMB version. Description contains verbose indication of success, the file's mime type, additional details, the SMB share type, the SMB version, the result of the write action (success), and the total number of bytes written.
SMB Write Unknown	SMB Write Action(s) with Unknown Result. Message contains the relevant SMB share, filename, and the SMB version. Description contains the reason for the notice, the file's mime type, additional details, the SMB share type, the SMB version, the result of the write action (unknown), and the total requested number of bytes to write.
SMTP Blocklist Blocked Host	The originator's address is seen in the block list error message. This is useful to detect local hosts sending SPAM with a high positive rate. Message contains the server hostname. Details field has the message from the reply.
SMTP Blocklist Error Message	An SMTP server sent a reply mentioning an SMTP block list. Message contains the server hostname. Details field has the message from the reply.
SSH Heuristic Login Failed	SSH Login Failure - determined heuristically. Can fire multiple times on the same connection representing multiple failed attempts Message contains details of the client and host.

Field	Description
SSH Heuristic Login Success	SSH Login Success - determined heuristically Message contains details of the client and host.
SSH Undetermined Encryption Step	Raised when an SSH2 connection has reached the encryption stage but analysis of encrypted packet sizes is unable to determine a successful or failed login. The message will contain a longer description of the type of notice. The details field will give the number of bytes delivered and not delivered in the connection.
SSL Invalid OCSP Response	SSL's OCSP response validation failed. Message contains OCSP reply message for failed validation. Description contains subject of the X.509 certificate offered by the server.
SSL Protocol Error	Indicates that the traffic has been detected as invalid SSL, either due to not being recognized by DPI or not being legitimate SSL traffic. Message informs that protocol violation was detected over SSL connection. Description contains reason for this message.
Outbound TOR	Notice fired when outbound use of TOR is detected on the network. Message contains information that TOR activity was detected. Description field displays SSL server that is being accessed and certificate issuer's CN.
Young SSL Certificate	Notice fires when a certificate younger than a system defined time interval is detected. Message contains age of certificate. Description contains, if present, server name that client is connecting to, Subject of certificate and start of validation of certificate.
Scan Address Scan	Address scans detect that a host appears to be scanning some number of destinations on a single port. This notice is generated when the number of unique hosts seen over the previous interval exceeds a certain threshold. Message contains suspected hostname, target hostname, number of unique ports scanned and duration of the scan. Details field contains either "local" or "remote".
Scan Port Scan	Port scans detect that an attacking host appears to be scanning a single victim host on several ports. This notice is generated when an attacking host attempts to connect to a threshold number of unique ports on a single host over the previous time interval. Message contains suspected hostname, target hostname, number of unique ports scanned and duration of the scan. Details field contains either "local" or "remote".

Field	Description
Scan Random Scan	Random scans detect that an attacking host appears to be scanning multiple victim hosts on several ports. This notice is generated when an attacking host attempts to connect to a threshold number of unique hosts and ports over the previous time interval. Message contains suspected hostname, target hostname, number of unique ports scanned and duration of the scan. Details field contains either “local” or “remote”.

US:+1 415 229 9100 UK:+44 (0) 1223 394 100 LATAM:+55 11 97242 2011 APAC:+65 6804 5010 info@darktrace.com darktrace.com