VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Vectra metadata attributes and their descriptions

This document describes the important attributes in all the metadata streams supported by Vectra Recall™ and Vectra Stream™.

Common fields in all metadata streams (except DHCP)	
Field	**Description**
ts	Timestamp when the metadata record is generated. It is in date format (e.g. May 9, 2018, 10:09:25.366)
uid	Unique id of connection
id.ip_ver*	IP Version
id.orig_h	Originating endpoint IP address
id.orig_p	Originating endpoint TCP/UDP port
id.resp_h	Responding endpoint IP address
id.resp_p	Responding endpoint TCP/UDP port
orig_hostname*	Originating endpoint hostname
resp_hostname*	Responding endpoint hostname
local_orig	Boolean indicating if connection was locally originated
local_resp	Boolean indicating if connection was locally responded
orig_huid*	Unique identifier for the originating host if it is local
orig_sluid*	Unique identifier for the originating host session
resp_huid*	Unique identifier for the responding host if it is local
resp_sluid*	Unique identifier for the responding host session if it is local
sensor_uid	Unique identifier for Cognito sensor that observed the underlying traffic generating the metadata record
communityID	Identifier representing a given network flow with a hash of IP, port & protocol

Beacon** (metadata_beacon)	
Field	**Description**
beacon_type	The type of beacon. ‘single_resp_multiple_sessions’ type indicates a beacon to one destination comprising of multiple sessions
beacon_uid	The unique uid of the beacon
uid	The unique uid of the first connection for the reported beacon event
service	Service (e.g. “http” or “tls”)
proto	L4 protocol value. 6 is TCP, 17 is UDP
protoName	L4 protocol name (TCP or UDP)
orig_ip_bytes	Total bytes sent from originator to responder for this beacon_uid
resp_ip_bytes	Total bytes send from responder to originator for this beacon_uid
first_event_time	Timestamp of the first observed session for this beacon_uid
last_event_time	Timestamp of the last observed session for this beacon_uid
resp_domains	The responder domains in this event
ja3	Ja3 hash of client based on client SSL parameters
session_count	The number of sessions that comprise the beacon_uid

*Unique to Vectra, not in standard Bro output
**Beacon metadata is uniquely computed by Vectra platform, not in standard Bro output

DCE-RPC (metadata_dcerpc)	
Field	**Description**
rtt	Round trip time of request – response
endpoint	Endpoint name looked up from the uuid (e.g. IXnRemote, IWbemLoginClientID)
operation	Operation seen in the call (e.g. "RemoteCreateInstance")
username*	Username or account name that logged in. Names ending in '$' are machine names (not user account names)
hostname*	Hostname on which the user logged in
domain*	Domain of the host

DHCP (metadata_dhcp)	
Field	**Description**
ts	Timestamp when the metadata record is generated. It is in date format (e.g. May 9, 2018, 10:09:25.366)
uid	Unique id of connection
mac	MAC address in request
assigned_ip	Assigned IP in response
lease_time	DHCP lease time. DHCP Option 51
trans_id	Transaction id
dhcp_server_ip*	DHCP server IP address
orig_hostname*	Hostname from DHCP options. DHCP Option 12
dns_server_ips*	DNS server ips from DHCP options. DHCP Option 6
sensor_uid	Unique identifier for Cognito sensor that observed the underlying traffic generating the metadata record

DNS (metadata_dnsrecordinfo)	
Field	**Description**
proto	Protocol of DNS transaction—6 (for TCP) or 17 (for UDP)
trans_id	16-bit identifier assigned by DNS client
query	Domain name subject of the query
qclass / qclass_name	Value specifying the query class (e.g. 1 / Internet [IN])
qtype / qtype_name	query type value / descriptive name (e.g. A, AAAA, PTR, TXT)
rcode / rcode_name	Response code value in the DNS response (e.g. NXDOMAIN, NODATA)
AA	Authoritative answer. True if server is authoritative for the query
TC	Truncation flag. True if the message was truncated
RD	Recursion desired. True if recursive lookup of query requested
RA	Recursion available. True if server supports recursive queries
answers	List of answers to the query
TTLs	List of TTLs from the answers
auth	List of Authoritative responses for the query
total_answers	The total number of resource records in a reply message's answer section
total_replies	The total number of resource records in a reply message's answer, authority, and additional sections
rejected	The DNS query was rejected by the server
saw_query	Whether the full DNS query has been seen
saw_reply	Whether the full DNS reply has been seen

*Unique to Vectra, not in standard Bro output

HTTP (metadata_httpsessioninfo)	
Field	**Description**
method	HTTP Request Method
host	Value of the Host header
uri	URI used in the request
referrer	Value of the Referrer header
user_agent	Value of the User-Agent header
request_body_len	HTTP payload bytes in request
response_body_len	HTTP payload bytes in response
orig_mime_types	Content type header in originator request
resp_mime_types	Content type header in response
status_code	The status code in the HTTP response
status_msg	The status message corresponding to the status code
proxied	Value of x-forwarded-for header (e.g. X-FORWARDED-FOR -> 10.10.15.192)
cookie*	Cookie header
cookie_vars*	The variables in the cookie, without the values
request_cache_control*	Cache control header in the request, if present
response_cache_control*	Cache control header in the response, if present
response_expires*	Expires header in response, if present
request_header_count*	Count of headers in request
response_header_count*	Count of headers in response
orig_ip_bytes*	Bytes sent by originator to responder
resp_ip_bytes*	Bytes send by responder to originator
orig_pkts*	Number of packets sent from originator to responder
resp_pkts*	Number of packets sent from responder to originator
is_proxied*	Boolean value indicative of a proxied request
host_multihomed*	Boolean attribute that indicates whether the address in the host header is observed to be associated with one or multiple IPs

*Unique to Vectra, not in standard Bro output

ISession Connectivity (metadata_isession)		
Field	**Description**	
conn_state	Takes values: S0, S1, SF, REJ, S2, S3, RSTO, RSTR, RSTOS0, RSTRH, SH, SHR, or OTH	
	S0	Connection attempt seen, no reply.
	S1	Connection established, not terminated.
	SF	Normal establishment and termination. Note that this is the same symbol as for state S1. You can tell the two apart because for S1 there will not be any byte counts in the summary, while for SF there will be.
	REJ	Connection attempt rejected.
	S2	Connection established and close attempt by originator seen (but no reply from responder).
	S3	Connection established and close attempt by responder seen (but no reply from originator).
	RSTO	Connection established, originator aborted (sent a RST).
	RSTR	Responder sent a RST.
	RSTOS0	Originator sent a SYN followed by a RST, we never saw a SYN-ACK from the responder.
	RSTRH	Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.
	SH	Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder (hence the connection was “half” open).
	SHR	Responder sent a SYN ACK followed by a FIN, we never saw a SYN from the originator.
	OTH	No SYN seen, just midstream traffic (one example of this is a “partial connection” that was not later closed).
duration	Duration of connection in ms	
service	Service (e.g. “smb”)	
proto	L4 protocol value. 6 is TCP, 17 is UDP	
protoName	L4 protocol name (TCP, UDP or ICMP)	
orig_ip_bytes	Bytes sent from originator to responder	
resp_ip_bytes	Bytes send from responder to originator	

ISession Connectivity (metadata_isession)	
Field	**Description**
orig_pkts	Number of packets sent from originator to responder
resp_pkts	Number of packets sent from responder to originator
session_start_time	Timestamp when session started
resp_domain*	Domain of responder
orig_vlan_id*	VLAN_id of originator, if any
resp_vlan_id*	VLAN_id of responder, if any
first_orig_resp_data_pkt*	Base64 encoding of the first 16 bytes of the packet from originator to responder, represented as a string
first_resp_orig_data_pkt*	Base64 encoding of the first 16 bytes of the packet from responder to originator, represented as a string
first_orig_resp_data_pkt_time*	Timestamp of first data packet from originator to responder
first_resp_orig_data_pkt_time*	Timestamp of first data packet from responder to originator
first_orig_resp_pkt_time*	Timestamp of first packet from originator to responder
first_resp_orig_pkt_time*	Timestamp of first packet from responder to originator
resp_multihomed*	Boolean attribute that indicates whether the domain is observed to be associated with one or multiple IPs

Kerberos (metadata_kerberos_txn)	
Field	**Description**
client	Client name, including realm
service	Service being requested, including realm
success	Whether request was success or not
error_code	Error code if not a success
error_msg	Error message if not a success
request_type	Type of request. AS or TGT.
protocol*	L4 protocol. 6 (TCP) or 17 (UDP)
reply_timestamp*	Timestamp of reply
orig_host_observed_privilege*	The privilege represents the observed privilege based on the activity of an account seen to operate from the host. The scores can fall in three categories – Low (1, 2), Medium (3, 4, 5, 6, 7) and High (8, 9)
req_ciphers	The request ticket encryption type(s)
rep_cipher	The Response ticket encryption type

*Unique to Vectra, not in standard Bro output

LDAP* (metadata_ldap)	
Field	**Description**
message_id	Message id
baseObject	Base of the subtree in which the search is to be constrained
query_scope	The portion of the target subtree that should be considered (e.g. wholeSubtree)
query	Criteria to use to identify which entries within the scope should be returned
result	The result of the query in this request
matched_dn	The matched distinguished name
duration	Duration of the session
attributes	A set of attributes to request for inclusion in entries that match the search criteria and are returned
bind_error_count	If there are bind errors, count of the errors
encrypted_sasl_payload_count	If sasl encryption is used, the number of encrypted sasl payloads encountered
logon_failure_error_count	The count of logon errors
response_bytes	Number of bytes in the response
request_bytes	Number of bytes in the request
result_code	The result code (success or failure) in the response
result_count	The count of the entries in the result
ls_query	Boolean flag indicating whether the query was observed in the request
ls_close	Boolean flag indicating whether the close was observed

NTLM (metadata_ntlm)	
Field	**Description**
username	Username or account name that logged in
hostname	Hostname on which the user logged in
domain	Domain of the host
status	Status code in response
success	Whether the request was successful or not

RDP (metadata_rdp)	
Field	**Description**
cookie	Cookie value used by client machine (username)
keyboard_layout	Keyboard layout (language) of client machine (e.g. “US” “Encrypted Keyboard Layout”)
client_build	RDP client version used by client machine. Will be “unknown” if encrypted
client_dig_protocol_id	Product ID of client machine. Not populated if encrypted
desktop_width	Desktop width of client machine. 0 if encrypted
desktop_height	Desktop height of client machine. 0 if encrypted
result	If encrypted, result value is “encrypted” otherwise it will be empty

*Unique to Vectra, not in standard Bro output

Radius	
Field	**Description**
account_authentic	Identifies how the user was authenticated
account_delay_time	Identifies how long the sender has been trying to send the message for
account_input_gigawords	Identifies how many times the Acct-Input counter has rolled over for input
account_input_octets	How many bytes have been received
account_input_packets	How many packets the system has received
account_output_gigawords	Identifies how many times the Acct-Input counter has rolled over for output
account_output_octets	How many bytes have been set
account_output_packets	How many packets the system has sent
account_session_id	This is a unique ID that identifies the RADIUS Accounting Session which is sent in a separate packet.
account_session_time	Duration of service received by user
calling_station_id	This is the identifier of the calling station
connect_info	Identify the speed of the connection or other connection related information
delegated_ipv6_prefix	IPv6 Pool from which the IPv6 address was assigned
event_timestamp	Similar to ts but is the timestamp from the device, not from Vectra
filter_id	This identifies any ACL that is in use
framed_address	This field is available in the request that identifies the endpoint requesting authentication
framed_interface	Identifies the interface used when the user connects to the system
framed_ip_address	IP address of the endpoint device connecting to the system

Radius (con't)	
Field	**Description**
framed_ipv6_prefix	Indicates the framed IPv6 prefix for the user
framed_protocol	Identifies the Framed Protocol used when the user connects to the system
idle_timeout	Amount of time a session can be idle before it is disconnected
mac	MAC Address if observed as a field in the Radius message
nas_identifier	Identifies the role the authenticating client is requesting
nas_ip_address	This is an IP Address format, it can be the IP of the Device, the Endpoint, or Intermediate system, depending on implementation
nas_port	Physical Port Number of the Device Authenticating the User
nas_port_id	Text string identifying the port provided by the client
nas_port_type	This is the type of medium of the port (e.g. Ethernet, Wifi &c.)
reply_msg	Reply message from the server challenge. This is frequently shown to the user authenticating.
result	Success or Failed Authentication
service_type	Type of service the user has requested
session_timeout	This is the maximum session length
ttl	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.
tunnel_client	Address (IPv4, IPv6, or FQDN) of the initiator end of the tunnel, if present. This is collected from the Tunnel-Client-Endpoint attribute.
username	This is the username if observed in the Radius message
logged	The boolean attribute indicates if the request was previously logged

Radius (con't)	
Field	**Description**
password_seen	Boolean attribute indicating password was seen
radius_type	The value indicates if it is an access or accounting request
reply_timestamp	Timestamp when the reply message was received
dst_display_name	DNS Name of the Destination
dst_host_luid	This is the ID of the destination host with host ID
dst_luid	The LUID of the RADIUS Server
dst_luid_external	Value is True if the destination is external
src_display_name	DNS Name of the Source
src_host_luid	This is the ID of the Src with Host ID
src_luid	The LUID of the RADIUS Client
src_luid_external	Value is True if the source is external

SMB Files (metadata_smbfiles)	
Field	**Description**
action	Action taken on file
delete_on_close*	Flag indicating if the delete_on_close attribute is enabled. If enabled, a file close action may delete the file if it is the last close on the file
path	Path pulled from the tree this file was transferred to or from
name	Filename if one was seen
version	SMB version (SMBv1 or SMBv2)

SMB Mapping (metadata_smbmapping)	
Field	**Description**
path	Name of the tree path
service	Type of re-originator of the tree
version	SMB version (SMBv1 or SMBv2)
username*	Username or account name that logged in. Names ending in '$' are machine names (not user account names)
hostname*	Hostname on which the user logged in
domain*	Domain of the host

*Unique to Vectra, not in standard Bro output

SMTP (metadata_smtp) - Available in Vectra Stream Only	
Field	**Description**
helo	Contents of the Helo header
mail_from	Email addresses found in the From header
rcpt_to	Email addresses found in the Rcpt header, formatted as a comma separated list
date	Contents of the Date header
from	Contents of the From header
to	Contents of the To header, formatted as a comma separated list
cc	Contents of the CC header, formatted as a comma separated list
reply_to	Contents of the ReplyTo header
msgid	Contents of the MsgID header
in_reply_to	Contents of the In-Reply-To header
Subject	Contents of the Subject header
x_originating_ip	Contents of the X-Originating-IP header
first_received	Contents of the first Received header, which signifies the first SMTP server to receive this message, (i.e. sending server)
second_received	Contents of the second Received header, which signifies the second SMTP server to receive this message
user_agent	Value of the User-Agent header from the client
tls	Indicates that the connection has switched to using TLS
spf_helo_status	Based on the 'Received-SPF' header in smtp. This header specifies the SPF status (Sender Policy Framework) One of pass/fail/neutral/softfail/none/temperror/permerror See: https://tools.ietf.org/html/rfc7208#section-9.1
spf_mailfrom_status	One of pass/fail/neutral/softfail/none/temperror/permerror
dkim_status	pass/fail/none. Based on the 'Authentication-results' header
dmarc_status	pass/fail/none. Based on the 'Authentication-results' header

SSH (metadata_ssh)	
Field	**Description**
version	SSH major version (1 or 2)
client	The client's version string
server	The server's version string
cipher_alg	The encryption algorithm in use
mac_alg	The signing (MAC) algorithm in use
compression_alg	The compression algorithm in use
kex_alg	The key exchange algorithm in use
host_key_alg	The server host key's algorithm
host_key	The server's key fingerprint
hassh	hassh hash of client based on client SSH parameters
hasshServer	haashServer hash of server based on client SSH parameters

SSL (metadata_ssl)	
Field	**Description**
server_name	SNI value
next_protocol	Next protocol the server chose using the application layer next protocol extension, if present
cipher	SSL/TLS cipher suite chosen from server
version/version_num	SSL version number
curve	Elliptical curve number for ECDHE
issuer	Server cert issuer
subject	Server cert subject
client_issuer	Client cert issuer
client_subject	Client cert subject
client_version_num*	SSL version number sent by the client
client_version*	SSL version string sent by the client
client_extension*	Client extensions
client_curve_num*	Elliptical curve number sent by the client
client_ec_point_format*	Elliptical curve point format offered by the client
ja3	Ja3 hash of client based on client SSL parameters
ja3s	Ja3s hash of server based on server SSL parameters
server_extensions	Server extensions

X509 (metadata_x509)	
Field	**Description**
certificate.version	Version of the server certificate (SSI V3, TLS V1, TLS V2, etc.)
certificate.serial	Unique serial number given by certificate authority or certificate signed authority. Usually 40 hexadecimal characters
certificate.subject	Owner of the certificate (distinguished name)
certificate.issuer	Combination of country, organizations, common name, issuer, URI
certificate.key_alg	Name of the public key algorithm that is used in data transmission, e.g. RSA encryption
certificate.key_length	Number of bits used in the encryption, e.g. 2,048-bit encryption
certificate.key_type	Three key types, depending upon the key algorithm
certificate.not_valid_after	Time after the certificate is invalid
certificate.not_valid_before	Time before the certificate is invalid
certificate.exponent	Key exponent
certificate.sig_alg	Name of the signature algorithm
certificate.self_issued	Boolean flag indicating whether the certificate is self-issued or backed by a CA
certificate.curve	Curve, if EC-certificate
certificate.cn	Common name that identifies the host name of the certificate
san.dns	Specifying a list of additional host names for a single certificate along with DNS names that are associated with SAN (Subject Alternative Name)
san.email	Email address associated with the SAN
san.ip	IP address of the SAN in the digital certificate
san.other_fields	Other fields in the SAN
san.uri	URL name associated with SAN
basic_constraints.ca	Flag indicating whether the subject of the certificate is a CA
basic_constraints.path_len	Maximum depth of valid certification paths that include this certificate

For more information about Vectra metadata attributes, please contact a service representative or email us at info@vectra.ai.

Email info@vectra.ai vectra.ai

Version: **041522**