Advanced Search Detection Fields – Vectra NDR (Formerly Detect for Network)

Text	Type
detection.assigned_date	date
detection.assigned_to	text
detection.campaign_summaries.duration	float
detection.campaign_summaries.id	long
detection.campaign_summaries.last_timestamp	date
detection.campaign_summaries.name	text
detection.campaign_summaries.num_detections	long
detection.campaign_summaries.num_hosts	long
detection.category	text
detection.certainty	long
detection.custom_detection	text
detection.description	text
detection.detection	text
detection.detection_category	text
detection.detection_type	text
detection.detection_url	text
detection.first_timestamp	date
detection.grouped_details.account_created_by	text
detection.grouped_details.account_uid	text
detection.grouped_details.account_uids	text
detection.grouped_details.accounts	text
detection.grouped_details.ad_category	text
detection.grouped_details.admin	text
detection.grouped_details.anomalous_profiles.account	text
detection.grouped_details.anomalous_profiles.count	long
detection.grouped_details.anomalous_profiles.first_timestamp	date
detection.grouped_details.anomalous_profiles.function_call	text
detection.grouped_details.anomalous_profiles.function_uuid	text
detection.grouped_details.anomalous_profiles.last_timestamp	date
detection.grouped_details.app_name	text
detection.grouped_details.app_protocol	text
detection.grouped_details.application	text
detection.grouped_details.artifact	text
detection.grouped_details.attacker_detail	text
detection.grouped_details.attempts	long
detection.grouped_details.authentication_method	text
detection.grouped_details.behavior	text
detection.grouped_details.browser	text
detection.grouped_details.bytes_received	long
detection.grouped_details.bytes_sent	long
detection.grouped_details.cdn_ips	text
detection.grouped_details.change	text
detection.grouped_details.city	text
detection.grouped_details.client	text
detection.grouped_details.client_application	text
detection.grouped_details.client_name	text
detection.grouped_details.client_token	text
detection.grouped_details.command	text
detection.grouped_details.command_arguments.data	text
detection.grouped_details.command_arguments.timestamp	date
detection.grouped_details.communication_type	text

detection.grouped_details.count	long
detection.grouped_details.country	text
detection.grouped_details.description	text
detection.grouped_details.destination_email	text
detection.grouped_details.detection_slug	text
detection.grouped_details.detection_source	text
detection.grouped_details.device_name	text
detection.grouped_details.dhcp_name	text
detection.grouped_details.directories.last_timestamp	date
detection.grouped_details.directories.object_count	long
detection.grouped_details.directories.relative_path	text
detection.grouped_details.directories.src_ip	text
detection.grouped_details.directories_table.last_timestamp	date
detection.grouped_details.directories_table.object_counts	long
detection.grouped_details.directories_table.relative_path	text
detection.grouped_details.directories_table.src_ips	text
detection.grouped_details.display_name	text
detection.grouped_details.distinct_traffic_ids	text
detection.grouped_details.dns_response	text
detection.grouped_details.domain_controllers.id	long
detection.grouped_details.domain_controllers.ip	text
detection.grouped_details.domain_controllers.name	text
detection.grouped_details.dos_type	text
detection.grouped_details.dst_account.id	long
detection.grouped_details.dst_account.uid	text
detection.grouped_details.dst_accounts.id	long
detection.grouped_details.dst_accounts.uid	text
detection.grouped_details.dst_cdn	text
detection.grouped_details.dst_geo	text
detection.grouped_details.dst_geo_lat	float
detection.grouped_details.dst_geo_lon	float
detection.grouped_details.dst_hosts.dst_host.id	long
detection.grouped_details.dst_hosts.dst_host.ip	text
detection.grouped_details.dst_hosts.dst_host.name	text
detection.grouped_details.dst_hosts.dst_ip	text
detection.grouped_details.dst_hosts.dst_port	long
detection.grouped_details.dst_hosts.id	long
detection.grouped_details.dst_hosts.ip	text
detection.grouped_details.dst_hosts.last_timestamp	date
detection.grouped_details.dst_hosts.name	text
detection.grouped_details.dst_ips	text
detection.grouped_details.dst_ports	long
detection.grouped_details.dst_profiles.count	long
detection.grouped_details.dst_profiles.function_call	text
detection.grouped_details.dst_profiles.function_uuid	text
detection.grouped_details.dst_protocol	text
detection.grouped_details.dst_subnets	text
detection.grouped_details.duration	long
detection.grouped_details.effective_session_interval_seconds	text
detection.grouped_details.email	text
detection.grouped_details.encrypted_extension	text
detection.grouped_details.encrypted_file_count	long
detection.grouped_details.encrypted_files	text
detection.grouped_details.encrypted_share	text
detection.grouped_details.event	text

detection.grouped_details.event_description	text
detection.grouped_details.events.accounts	text
detection.grouped_details.events.base_object	text
detection.grouped_details.events.bytes_received	long
detection.grouped_details.events.bytes_sent	long
detection.grouped_details.events.cadence	long
detection.grouped_details.events.couch_note_id	text
detection.grouped_details.events.count	long
detection.grouped_details.events.description	text
detection.grouped_details.events.dst_country	text
detection.grouped_details.events.dst_host.id	long
detection.grouped_details.events.dst_host.ip	text
detection.grouped_details.events.dst_host.name	text
detection.grouped_details.events.dst_hosts.id	long
detection.grouped_details.events.dst_hosts.name	text
detection.grouped_details.events.dst_ip	text
detection.grouped_details.events.dst_ips	text
detection.grouped_details.events.dst_ports	long
detection.grouped_details.events.duration	long
detection.grouped_details.events.error_code	text
detection.grouped_details.events.event_type	text
detection.grouped_details.events.first_timestamp	date
detection.grouped_details.events.grouping_field	text
detection.grouped_details.events.host	text
detection.grouped_details.events.http_method	text
detection.grouped_details.events.id	long
detection.grouped_details.events.is_normally_accessed_by_rdp	boolean
detection.grouped_details.events.last_seen	date
detection.grouped_details.events.last_timestamp	date
detection.grouped_details.events.multi_fields	text
detection.grouped_details.events.normal_bytes_sent	long
detection.grouped_details.events.num_attempts	long
detection.grouped_details.events.num_response_objects	long
detection.grouped_details.events.origin_ips	text
detection.grouped_details.events.phase1.port	long
detection.grouped_details.events.phase1.timestamp	date
detection.grouped_details.events.phase2.port	long
detection.grouped_details.events.phase2.timestamp	date
detection.grouped_details.events.protocol	text
detection.grouped_details.events.referrer	text
detection.grouped_details.events.reply_cache_control	text
detection.grouped_details.events.request	text
detection.grouped_details.events.response_code	text
detection.grouped_details.events.services	text
detection.grouped_details.events.sessions.app_protocol	text
detection.grouped_details.events.sessions.bytes_received	long
detection.grouped_details.events.sessions.dst_ip	text
detection.grouped_details.events.sessions.dst_port	long
detection.grouped_details.events.sessions.duration	long
detection.grouped_details.events.sessions.first_timestamp	date
detection.grouped_details.events.sessions.protocol	text
detection.grouped_details.events.sessions.target_host.id	long
detection.grouped_details.events.sessions.target_host.ip	text
detection.grouped_details.events.sessions.target_host.is_key_asset	boolean
detection.grouped_details.events.sessions.target_host.key_asset	boolean

detection.grouped_details.events.sessions.target_host.name	text
detection.grouped_details.events.subnet	text
detection.grouped_details.events.subtype	text
detection.grouped_details.events.target_domains	text
detection.grouped_details.events.target_summary.app_protocol	text
detection.grouped_details.events.target_summary.bytes_sent	long
detection.grouped_details.events.target_summary.dst_port	long
detection.grouped_details.events.target_summary.first_timestamp	date
detection.grouped_details.events.target_summary.last_timestamp	date
detection.grouped_details.events.target_summary.protocol	text
detection.grouped_details.events.total_bytes_rcvd	long
detection.grouped_details.events.total_bytes_sent	long
detection.grouped_details.events.url	text
detection.grouped_details.events.user_agent	text
detection.grouped_details.exchange_locations	text
detection.grouped_details.executed_functions	text
detection.grouped_details.extensions	text
detection.grouped_details.external_domain	text
detection.grouped_details.external_target.ip	text
detection.grouped_details.external_target.name	text
detection.grouped_details.file_extension	text
detection.grouped_details.file_name	text
detection.grouped_details.files	text
detection.grouped_details.files_downloaded	long
detection.grouped_details.files_shared	long
detection.grouped_details.files_table.extension	text
detection.grouped_details.files_table.name	text
detection.grouped_details.first_seen	date
detection.grouped_details.first_timestamp	date
detection.grouped_details.flow_connector_count	long
detection.grouped_details.flow_connectors	text
detection.grouped_details.forwarded_mailboxes	text
detection.grouped_details.full_path	text
detection.grouped_details.hashes_count	long
detection.grouped_details.high_mac_randomization	boolean
detection.grouped_details.host_detection	long
detection.grouped_details.host_id	long
detection.grouped_details.id	long
detection.grouped_details.indicators	text
detection.grouped_details.internal_host.id	long
detection.grouped_details.internal_host.ip	text
detection.grouped_details.internal_host.name	text
detection.grouped_details.internal_target.id	long
detection.grouped_details.internal_target.ip	text
detection.grouped_details.internal_target.name	text
detection.grouped_details.ip_login_attempts.first_timestamp	date
detection.grouped_details.ip_login_attempts.last_timestamp	date
detection.grouped_details.ip_login_attempts.num_attempts	long
detection.grouped_details.ip_login_attempts.src_ip	text
detection.grouped_details.ip_login_attempts.user_agent	text
detection.grouped_details.is_account_detail	boolean
detection.grouped_details.is_external	boolean
detection.grouped_details.is_host_detail	boolean
detection.grouped_details.ja3_hash	text
detection.grouped_details.ja3_hashes	text

detection.grouped_details.ja3s_hash	text
detection.grouped_details.ja3s_hashes	text
detection.grouped_details.keyboard_id	text
detection.grouped_details.keyboard_name	text
detection.grouped_details.last_seen	date
detection.grouped_details.last_timestamp	date
detection.grouped_details.mac_address	text
detection.grouped_details.mailboxes	text
detection.grouped_details.malware_file_count	long
detection.grouped_details.malware_files	text
detection.grouped_details.metadata.action	text
detection.grouped_details.metadata.answers	text
detection.grouped_details.metadata.attributes	text
detection.grouped_details.metadata.client	text
detection.grouped_details.metadata.cookie	text
detection.grouped_details.metadata.endpoint	text
detection.grouped_details.metadata.hassh	text
detection.grouped_details.metadata.hasshServer	text
detection.grouped_details.metadata.hostname	text
detection.grouped_details.metadata.issuer	text
detection.grouped_details.metadata.keyboard_layout	text
detection.grouped_details.metadata.mac	text
detection.grouped_details.metadata.name	text
detection.grouped_details.metadata.not_valid_after	date
detection.grouped_details.metadata.not_valid_before	date
detection.grouped_details.metadata.operation	text
detection.grouped_details.metadata.orig_h	text
detection.grouped_details.metadata.orig_ip_bytes	long
detection.grouped_details.metadata.orig_sluid	text
detection.grouped_details.metadata.path	text
detection.grouped_details.metadata.proto	text
detection.grouped_details.metadata.qtype_name	text
detection.grouped_details.metadata.query	text
detection.grouped_details.metadata.request_type	text
detection.grouped_details.metadata.resp_domain	text
detection.grouped_details.metadata.resp_h	text
detection.grouped_details.metadata.resp_hostname	text
detection.grouped_details.metadata.resp_ip_bytes	long
detection.grouped_details.metadata.resp_p	long
detection.grouped_details.metadata.resp_sluid	text
detection.grouped_details.metadata.result	text
detection.grouped_details.metadata.self_issued	boolean
detection.grouped_details.metadata.serial	text
detection.grouped_details.metadata.server	text
detection.grouped_details.metadata.server_name	text
detection.grouped_details.metadata.service	text
detection.grouped_details.metadata.subject	text
detection.grouped_details.metadata.uri	text
detection.grouped_details.metadata.username	text
detection.grouped_details.metadata.version	text
detection.grouped_details.mfa_status	text
detection.grouped_details.multi_fields	text
detection.grouped_details.named_pipe	text
detection.grouped_details.network_type	text
detection.grouped_details.normal_account_behavior.count	long

detection.grouped_details.normal_account_behavior.host_details.id	long
detection.grouped_details.normal_account_behavior.host_details.key_asset	boolean
detection.grouped_details.normal_account_behavior.host_details.name	text
detection.grouped_details.normal_account_behavior.host_luid	text
detection.grouped_details.normal_account_behavior.service_name	text
detection.grouped_details.normal_account_objects.id	long
detection.grouped_details.normal_account_objects.uid	text
detection.grouped_details.normal_accounts	text
detection.grouped_details.normal_admin_hosts.id	long
detection.grouped_details.normal_admin_hosts.ip	text
detection.grouped_details.normal_admin_hosts.name	text
detection.grouped_details.normal_bytes_received	float
detection.grouped_details.normal_bytes_sent	long
detection.grouped_details.normal_client_keyboards	text
detection.grouped_details.normal_domain_controllers.id	long
detection.grouped_details.normal_domain_controllers.ip	text
detection.grouped_details.normal_domain_controllers.name	text
detection.grouped_details.normal_dst_hosts.id	long
detection.grouped_details.normal_dst_hosts.ip	text
detection.grouped_details.normal_dst_hosts.name	text
detection.grouped_details.normal_host_behavior.account_details.id	long
detection.grouped_details.normal_host_behavior.account_details.uid	text
detection.grouped_details.normal_host_behavior.account_uid	text
detection.grouped_details.normal_host_behavior.count	long
detection.grouped_details.normal_host_behavior.service_name	text
detection.grouped_details.normal_keyboards	text
detection.grouped_details.normal_operations	text
detection.grouped_details.normal_product_ids	text
detection.grouped_details.normal_services	text
detection.grouped_details.normal_src_hosts.id	long
detection.grouped_details.normal_src_hosts.ip	text
detection.grouped_details.normal_src_hosts.name	text
detection.grouped_details.normal_users	text
detection.grouped_details.num_accounts	long
detection.grouped_details.num_ad_sessions	long
detection.grouped_details.num_attempts	long
detection.grouped_details.num_events	long
detection.grouped_details.num_files	long
detection.grouped_details.num_mailboxes_forwarded	long
detection.grouped_details.num_matches	long
detection.grouped_details.num_observations	long
detection.grouped_details.num_response_objects	long
detection.grouped_details.num_sessions	long
detection.grouped_details.num_successes	long
detection.grouped_details.operation	text
detection.grouped_details.operation_details.display_name	text
detection.grouped_details.operation_details.new_value	text
detection.grouped_details.operation_details.old_value	text
detection.grouped_details.operation_privilege.privilege	long
detection.grouped_details.operation_privilege.privilegeCategory	text
detection.grouped_details.operations	text
detection.grouped_details.operations_count	long
detection.grouped_details.origin_domain	text
detection.grouped_details.origin_geo	text
detection.grouped_details.origin_geo_lat	float

detection.grouped_details.origin_geo_lon	float
detection.grouped_details.origin_ip	text
detection.grouped_details.origin_port	long
detection.grouped_details.origin_protocol	text
detection.grouped_details.original_extension	text
detection.grouped_details.original_extensions	text
detection.grouped_details.os	text
detection.grouped_details.other_matches.key	text
detection.grouped_details.other_matches.value	text
detection.grouped_details.period_identified	text
detection.grouped_details.ports	long
detection.grouped_details.previous_countries	text
detection.grouped_details.previous_device_names	text
detection.grouped_details.previous_os_browsers.browser	text
detection.grouped_details.previous_os_browsers.os	text
detection.grouped_details.primary_match	text
detection.grouped_details.product_id	text
detection.grouped_details.protocol	text
detection.grouped_details.protocol_port	text
detection.grouped_details.proxy_ip	text
detection.grouped_details.query	text
detection.grouped_details.realm	text
detection.grouped_details.reason	text
detection.grouped_details.reasons	text
detection.grouped_details.received_normal_pattern	text
detection.grouped_details.received_pattern	text
detection.grouped_details.recipients	text
detection.grouped_details.recipients_count	long
detection.grouped_details.request_type	text
detection.grouped_details.resource	text
detection.grouped_details.resp_domain	text
detection.grouped_details.response_code	text
detection.grouped_details.result	text
detection.grouped_details.results	text
detection.grouped_details.role	text
detection.grouped_details.scope	text
detection.grouped_details.sent_normal_pattern	text
detection.grouped_details.sent_pattern	text
detection.grouped_details.service_accessed.name	text
detection.grouped_details.service_accessed.privilege_category	text
detection.grouped_details.service_accessed.privilege_level	long
detection.grouped_details.service_accesses.first_seen	date
detection.grouped_details.service_accesses.last_seen	date
detection.grouped_details.service_accesses.name	text
detection.grouped_details.service_accesses.normal_service_behavior.account_details.id	long
detection.grouped_details.service_accesses.normal_service_behavior.account_details.uid	text
detection.grouped_details.service_accesses.normal_service_behavior.account_uid	text
detection.grouped_details.service_accesses.normal_service_behavior.count	long
detection.grouped_details.service_accesses.normal_service_behavior.host_details.id	long
detection.grouped_details.service_accesses.normal_service_behavior.host_details.key_asset	boolean
detection.grouped_details.service_accesses.normal_service_behavior.host_details.name	text
detection.grouped_details.service_accesses.normal_service_behavior.host_luid	text
detection.grouped_details.service_accesses.privilege_category	text
detection.grouped_details.service_accesses.privilege_level	long
detection.grouped_details.services	text

detection.grouped_details.sessions.app_protocol	text
detection.grouped_details.sessions.bytes_received	long
detection.grouped_details.sessions.bytes_sent	long
detection.grouped_details.sessions.dst_ip	text
detection.grouped_details.sessions.dst_port	long
detection.grouped_details.sessions.first_timestamp	date
detection.grouped_details.sessions.last_timestamp	date
detection.grouped_details.sessions.protocol	text
detection.grouped_details.sessions.tunnel_type	text
detection.grouped_details.share	text
detection.grouped_details.shares	text
detection.grouped_details.sql_fragment	text
detection.grouped_details.src_account.id	long
detection.grouped_details.src_account.name	text
detection.grouped_details.src_account.privilege_category	text
detection.grouped_details.src_account.privilege_level	long
detection.grouped_details.src_host.id	long
detection.grouped_details.src_host.ip	text
detection.grouped_details.src_host.is_key_asset	boolean
detection.grouped_details.src_host.key_asset	boolean
detection.grouped_details.src_host.name	text
detection.grouped_details.src_host.privilege_category	text
detection.grouped_details.src_host.privilege_level	long
detection.grouped_details.src_ip	text
detection.grouped_details.src_ips	text
detection.grouped_details.src_port	long
detection.grouped_details.src_profiles.count	long
detection.grouped_details.src_profiles.function_call	text
detection.grouped_details.src_profiles.function_uuid	text
detection.grouped_details.state	text
detection.grouped_details.subject	text
detection.grouped_details.subnet	text
detection.grouped_details.target	text
detection.grouped_details.target_accounts.id	long
detection.grouped_details.target_accounts.uid	text
detection.grouped_details.target_domains	text
detection.grouped_details.target_entity	text
detection.grouped_details.target_host.dst_dns	text
detection.grouped_details.target_host.id	long
detection.grouped_details.target_host.ip	text
detection.grouped_details.target_host.name	text
detection.grouped_details.target_objects.target	text
detection.grouped_details.target_table.target	text
detection.grouped_details.targets.dst_hosts.id	long
detection.grouped_details.targets.dst_hosts.ip	text
detection.grouped_details.targets.dst_hosts.name	text
detection.grouped_details.targets.events.bytes_received	long
detection.grouped_details.targets.events.http_segment	text
detection.grouped_details.targets.events.last_seen	date
detection.grouped_details.targets.events.response_code	text
detection.grouped_details.targets.events.sql_fragment	text
detection.grouped_details.targets.events.user_agent	text
detection.grouped_details.team_name	text
detection.grouped_details.threat_feeds	text
detection.grouped_details.total_bytes_rcvd	long

detection.grouped_details.total_bytes_sent	long
detection.grouped_details.unusual_accounts	text
detection.grouped_details.unusual_clients	text
detection.grouped_details.unusual_domain_controllers.id	long
detection.grouped_details.unusual_domain_controllers.ip	text
detection.grouped_details.unusual_domain_controllers.name	text
detection.grouped_details.unusual_instances	long
detection.grouped_details.unusual_services	text
detection.grouped_details.uri	text
detection.grouped_details.url	text
detection.grouped_details.user_agent	text
detection.grouped_details.user_personal_sharepoint	text
detection.grouped_details.user_type	text
detection.grouped_details.uuid	text
detection.grouped_details.vendor	text
detection.grouped_details.via	text
detection.grouped_details.workload	text
detection.grouped_details.x_forwarded_for	text
detection.groups.description	text
detection.groups.id	long
detection.groups.last_modified	date
detection.groups.last_modified_by	text
detection.groups.name	text
detection.groups.type	text
detection.id	long
detection.is_custom_model	boolean
detection.is_marked_custom	boolean
detection.is_targeting_key_asset	boolean
detection.is_triaged	boolean
detection.last_timestamp	date
detection.normal_domains	text
detection.note	text
detection.note_modified_by	text
detection.note_modified_timestamp	date
detection.sensor	text
detection.sensor_name	text
detection.src_account.certainty	long
detection.src_account.id	long
detection.src_account.name	text
detection.src_account.privilege_category	text
detection.src_account.privilege_level	long
detection.src_account.threat	long
detection.src_account.url	text
detection.src_host.certainty	long
detection.src_host.groups.description	text
detection.src_host.groups.id	long
detection.src_host.groups.last_modified	date
detection.src_host.groups.last_modified_by	text
detection.src_host.groups.name	text
detection.src_host.groups.type	text
detection.src_host.id	long
detection.src_host.ip	text
detection.src_host.is_key_asset	boolean
detection.src_host.name	text
detection.src_host.threat	long

detection.src_host.url	text
detection.src_ip	text
detection.src_linked_account.certainty	long
detection.src_linked_account.id	long
detection.src_linked_account.name	text
detection.src_linked_account.privilege_category	text
detection.src_linked_account.privilege_level	long
detection.src_linked_account.threat	long
detection.src_linked_account.url	text
detection.state	boolean