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

| Text | Type |
|---|---|
| **host.active_traffic** | boolean |
| **host.assigned_date** | date |
| **host.assigned_to** | text |
| **host.assignment.assigned_by.id** | long |
| **host.assignment.assigned_by.username** | text |
| **host.assignment.assigned_to.id** | long |
| **host.assignment.assigned_to.username** | text |
| **host.assignment.date_assigned** | date |
| **host.assignment.events.actor** | long |
| **host.assignment.events.assignment_id** | long |
| **host.assignment.events.context.entity_c_score** | long |
| **host.assignment.events.context.entity_t_score** | long |
| **host.assignment.events.context.to** | long |
| **host.assignment.events.datetime** | date |
| **host.assignment.events.event_type** | text |
| **host.assignment.host_id** | long |
| **host.assignment.id** | long |
| **host.campaign_summaries.duration** | float |
| **host.campaign_summaries.id** | long |
| **host.campaign_summaries.last_timestamp** | date |
| **host.campaign_summaries.name** | text |
| **host.campaign_summaries.num_detections** | long |
| **host.campaign_summaries.num_hosts** | long |
| **host.certainty** | long |
| **host.detection_profile** | text |
| **host.detection_set** | text |
| **host.detection_summaries.assigned_date** | date |
| **host.detection_summaries.assigned_to** | text |
| **host.detection_summaries.certainty** | long |
| **host.detection_summaries.detection_category** | text |
| **host.detection_summaries.detection_id** | long |
| **host.detection_summaries.detection_type** | text |
| **host.detection_summaries.detection_url** | text |
| **host.detection_summaries.is_targeting_key_asset** | boolean |
| **host.detection_summaries.is_triaged** | boolean |
| **host.detection_summaries.state** | text |
| **host.detection_summaries.summary.abnormal_data_rate** | long |
| **host.detection_summaries.summary.accounts** | text |
| **host.detection_summaries.summary.active_time** | text |
| **host.detection_summaries.summary.app_protocols** | text |
| **host.detection_summaries.summary.artifact** | text |
| **host.detection_summaries.summary.authentication_attempts** | long |
| **host.detection_summaries.summary.bad_user_agent** | long |
| **host.detection_summaries.summary.beaconing** | long |

| | |
|---|---|
| **host.detection_summaries.summary.bytes_received** | long |
| **host.detection_summaries.summary.bytes_sent** | long |
| **host.detection_summaries.summary.cdn** | text |
| **host.detection_summaries.summary.client_names** | text |
| **host.detection_summaries.summary.client_tokens** | text |
| **host.detection_summaries.summary.common_shares** | text |
| **host.detection_summaries.summary.custom_model_query** | text |
| **host.detection_summaries.summary.dark_ips_contacted** | text |
| **host.detection_summaries.summary.description** | text |
| **host.detection_summaries.summary.distinct_traffic_ids** | long |
| **host.detection_summaries.summary.domain_controllers.id** | long |
| **host.detection_summaries.summary.domain_controllers.ip** | text |
| **host.detection_summaries.summary.domain_controllers.name** | text |
| **host.detection_summaries.summary.dos_types** | text |
| **host.detection_summaries.summary.dst_hosts.id** | long |
| **host.detection_summaries.summary.dst_hosts.ip** | text |
| **host.detection_summaries.summary.dst_hosts.name** | text |
| **host.detection_summaries.summary.dst_hosts.type** | text |
| **host.detection_summaries.summary.dst_ips** | text |
| **host.detection_summaries.summary.dst_ports** | long |
| **host.detection_summaries.summary.duration** | long |
| **host.detection_summaries.summary.executed_functions** | text |
| **host.detection_summaries.summary.files** | text |
| **host.detection_summaries.summary.first_matched** | date |
| **host.detection_summaries.summary.first_timestamp** | date |
| **host.detection_summaries.summary.function_uuids** | text |
| **host.detection_summaries.summary.ja3_hashes** | text |
| **host.detection_summaries.summary.last_matched** | date |
| **host.detection_summaries.summary.last_timestamp** | date |
| **host.detection_summaries.summary.mac_address** | text |
| **host.detection_summaries.summary.mac_randomization** | text |
| **host.detection_summaries.summary.matches** | long |
| **host.detection_summaries.summary.normal_bytes_received** | float |
| **host.detection_summaries.summary.num_accounts** | long |
| **host.detection_summaries.summary.num_attempts** | long |
| **host.detection_summaries.summary.num_dst_ips** | long |
| **host.detection_summaries.summary.num_events** | long |
| **host.detection_summaries.summary.num_failures** | long |
| **host.detection_summaries.summary.num_files** | long |
| **host.detection_summaries.summary.num_requests** | long |
| **host.detection_summaries.summary.num_response_objects** | long |
| **host.detection_summaries.summary.num_sessions** | long |
| **host.detection_summaries.summary.num_shares** | long |
| **host.detection_summaries.summary.num_successes** | long |
| **host.detection_summaries.summary.origin_ips** | text |
| **host.detection_summaries.summary.ports** | long |
| **host.detection_summaries.summary.probable_owner** | text |
| **host.detection_summaries.summary.protocol_ports** | text |

| | |
|---|---|
| **host.detection_summaries.summary.protocols** | text |
| **host.detection_summaries.summary.reason** | text |
| **host.detection_summaries.summary.roles** | text |
| host.detection_summaries.summary.services | text |
| **host.detection_summaries.summary.services_accessed.name** | text |
| **host.detection_summaries.summary.services_accessed.privilege_category** | text |
| **host.detection_summaries.summary.services_accessed.privilege_level** | long |
| **host.detection_summaries.summary.sessions_with_ad_activity** | long |
| **host.detection_summaries.summary.shares** | text |
| **host.detection_summaries.summary.src_accounts.id** | long |
| **host.detection_summaries.summary.src_accounts.name** | text |
| **host.detection_summaries.summary.src_accounts.privilege_category** | text |
| **host.detection_summaries.summary.src_accounts.privilege_level** | long |
| **host.detection_summaries.summary.src_hosts.id** | long |
| **host.detection_summaries.summary.src_hosts.name** | text |
| **host.detection_summaries.summary.src_hosts.privilege_category** | text |
| **host.detection_summaries.summary.src_hosts.privilege_level** | long |
| **host.detection_summaries.summary.subnet** | text |
| **host.detection_summaries.summary.suspicious_header_construction** | long |
| **host.detection_summaries.summary.target_domains** | text |
| **host.detection_summaries.summary.total_active_time** | text |
| **host.detection_summaries.summary.unusual_accounts** | text |
| **host.detection_summaries.summary.unusual_domain_controllers.id** | long |
| **host.detection_summaries.summary.unusual_domain_controllers.ip** | text |
| **host.detection_summaries.summary.unusual_domain_controllers.name** | text |
| **host.detection_summaries.summary.unusual_services** | text |
| **host.detection_summaries.summary.uuids** | text |
| **host.detection_summaries.summary.vendor** | text |
| **host.detection_summaries.tags** | text |
| **host.detection_summaries.threat** | long |
| **host.groups.description** | text |
| **host.groups.id** | long |
| **host.groups.last_modified** | date |
| **host.groups.last_modified_by** | text |
| **host.groups.name** | text |
| **host.groups.type** | text |
| **host.has_active_traffic** | boolean |
| **host.has_custom_model** | boolean |
| **host.has_shell_knocker_learnings** | boolean |
| **host.host_artifact_set.siem** | boolean |
| **host.host_artifact_set.source** | text |
| **host.host_artifact_set.type** | text |
| **host.host_artifact_set.value** | text |
| **host.host_artifact_set.vendor** | text |
| **host.host_url** | text |
| **host.id** | long |
| **host.ip** | text |
| **host.is_key_asset** | boolean |

| | |
|---|---|
| **host.is_targeting_key_asset** | boolean |
| **host.key_asset** | boolean |
| **host.last_detection_timestamp** | date |
| **host.last_modified** | date |
| **host.last_seen** | date |
| **host.last_source** | text |
| **host.ldap.account_disabled** | boolean |
| **host.ldap.account_lockedout** | boolean |
| **host.ldap.common_name** | text |
| **host.ldap.data_gathered_at** | text |
| **host.ldap.department** | text |
| **host.ldap.description** | text |
| **host.ldap.display_name** | text |
| **host.ldap.distinguished_name** | text |
| **host.ldap.dns_host_name** | text |
| **host.ldap.dns_hostname** | text |
| **host.ldap.email** | text |
| **host.ldap.employee_type** | text |
| **host.ldap.location** | text |
| **host.ldap.mac_address** | text |
| **host.ldap.machine_role** | text |
| **host.ldap.managed_by** | text |
| **host.ldap.manager** | text |
| **host.ldap.member_of** | text |
| **host.ldap.netbios_name** | text |
| **host.ldap.network_address** | text |
| **host.ldap.ntsecurity_descriptor** | text |
| **host.ldap.object_class** | text |
| **host.ldap.object_sid** | text |
| **host.ldap.operating_system** | text |
| **host.ldap.organization** | text |
| **host.ldap.password_expired** | boolean |
| **host.ldap.physical_location_object** | text |
| **host.ldap.pwd_last_set** | date |
| **host.ldap.sAMAccountName** | text |
| **host.ldap.service_principal_name** | text |
| **host.ldap.timestamp** | date |
| **host.ldap.title** | text |
| **host.ldap.user_principal_name** | text |
| **host.name** | text |
| **host.note** | text |
| **host.note_modified_by** | text |
| **host.note_modified_timestamp** | date |
| **host.previous_ips** | text |
| **host.privilege_category** | text |
| **host.privilege_level** | integer |
| **host.probable_owner** | text |
| **host.sensor** | text |

| | |
|---|---|
| **host.sensor_name** | text |
| **host.severity** | text |
| **host.shell_knocker.port** | long |
| **host.shell_knocker.protocol** | text |
| **host.state** | text |
| **host.suspicious_admin_learnings.host_manages.host_id** | long |
| **host.suspicious_admin_learnings.host_manages.host_key** | text |
| **host.suspicious_admin_learnings.host_manages.host_name** | text |
| **host.suspicious_admin_learnings.host_manages.ip** | text |
| **host.suspicious_admin_learnings.host_manages.protocols** | text |
| **host.suspicious_admin_learnings.managers_of_host.host_id** | long |
| **host.suspicious_admin_learnings.managers_of_host.host_key** | text |
| **host.suspicious_admin_learnings.managers_of_host.host_name** | text |
| **host.suspicious_admin_learnings.managers_of_host.ip** | text |
| **host.suspicious_admin_learnings.managers_of_host.protocols** | text |
| **host.tags** | text |
| **host.targets_key_asset** | boolean |
| **host.threat** | long |
| **host.url** | text |