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

Text	Type
account.account_type	text
account.certainty	long
account.detection_set	text
account.detection_summaries.certainty	long
account.detection_summaries.detection_category	text
account.detection_summaries.detection_id	long
account.detection_summaries.detection_type	text
account.detection_summaries.is_targeting_key_asset	boolean
account.detection_summaries.is_triaged	boolean
account.detection_summaries.state	text
account.detection_summaries.summary.account_uids	text
account.detection_summaries.summary.app_name	text
account.detection_summaries.summary.app_names	text
account.detection_summaries.summary.client_applications	text
account.detection_summaries.summary.commands	text
account.detection_summaries.summary.countries	text
account.detection_summaries.summary.description	text
account.detection_summaries.summary.destination_emails	text
account.detection_summaries.summary.display_names	text
account.detection_summaries.summary.emails	text
account.detection_summaries.summary.encrypted_extensions	text
account.detection_summaries.summary.encrypted_file_count	long
account.detection_summaries.summary.files_downloaded	long
account.detection_summaries.summary.login_attempts	long
account.detection_summaries.summary.malware_files	long
account.detection_summaries.summary.mfa_status	text
account.detection_summaries.summary.num_attempts	long
account.detection_summaries.summary.num_mailboxes_forwarded	long
account.detection_summaries.summary.operations	text
account.detection_summaries.summary.oss	text
account.detection_summaries.summary.reasons	text
account.detection_summaries.summary.recipients	text
account.detection_summaries.summary.recipients_count	long
account.detection_summaries.summary.services_accessed.name	text
account.detection_summaries.summary.services_accessed.privilege_category	text
account.detection_summaries.summary.services_accessed.privilege_level	long
account.detection_summaries.summary.shares	text
account.detection_summaries.summary.src_accounts.id	long
account.detection_summaries.summary.src_accounts.name	text
account.detection_summaries.summary.src_accounts.privilege_category	text
account.detection_summaries.summary.src_accounts.privilege_level	long
account.detection_summaries.summary.src_hosts.id	long
account.detection_summaries.summary.src_hosts.name	text
account.detection_summaries.summary.src_hosts.privilege_category	text

account.detection_summaries.summary.src_hosts.privilege_level	long
account.detection_summaries.summary.src_ips	text
account.detection_summaries.summary.subject	text
account.detection_summaries.summary.target_list	text
account.detection_summaries.summary.team_names	text
account.detection_summaries.summary.user_agents	text
account.detection_summaries.summary.workloads	text
account.detection_summaries.tags	text
account.detection_summaries.threat	long
account.id	long
account.last_detection_timestamp	date
account.ldap.account_disabled	boolean
account.ldap.account_lockedout	boolean
account.ldap.common_name	text
account.ldap.data_gathered_at	text
account.ldap.department	text
account.ldap.description	text
account.ldap.display_name	text
account.ldap.distinguished_name	text
account.ldap.email	text
account.ldap.employee_type	text
account.ldap.location	text
account.ldap.managed_by	text
account.ldap.manager	text
account.ldap.member_of	text
account.ldap.netbios_name	text
account.ldap.ntsecurity_descriptor	text
account.ldap.object_class	text
account.ldap.object_sid	text
account.ldap.organization	text
account.ldap.password_expired	boolean
account.ldap.pwd_last_set	date
account.ldap.sAMAccountName	text
account.ldap.telephone_number	text
account.ldap.timestamp	date
account.ldap.title	text
account.ldap.user_principal_name	text
account.name	text
account.note	text
account.note_modified_by	text
account.note_modified_timestamp	date
account.privilege_category	text
account.privilege_level	long
account.probable_home_host	text
account.severity	text
account.state	text
account.tags	text
account.threat	long