フィールドの抽出

フィールド抽出の概要

このアプリケーションは、フィールドの抽出に大きく依存します。ほとんどのレポートが要約データから生成されるので、正常かつ正確なレポートを作成するには、フィールドの正しい抽出を確保することが重要です。

アクセス ログ

ヒント

- 必ずタイムスタンプが正しく索引されるようにします。
- 「*」を検索し、アプリケーション固有のフィールドが必ず指定フィールドに入力されるようにします。次の項目には、取得したフィールドのより詳細なチェックが含まれます。
- 下の検索をコピー アンド ペーストします。結果は表示されず、ほとんど取得されません。1000 の結果が返される場合 – transforms.conf は、索引された固有のログ形式に応じて調整する必要があります。

```
sourcetype=wsa_accesslogs | head 1000 | fillnull value="!!!!!"
x_webcat_code_abbr x_wbrs_score x_webroot_scanverdict
x_webroot_threat_name x_webroot_trr x_webroot_spyid
x_webroot_trace_id x_mcaffe_scanverdict x_mcafee_filename
x_mcafee_scan_error x_mcafee_detecttype x_mcafee_av_virustype
x_mcafee_virus_name x_sophos_scanverdict x x_sophos_filename
x_sophos_virus_name x_ids_verdict x_icap_verdict
x_webcat_req_code_abbr x_webcat_resp_code_abbr
x_resp_dvs_threat_name x_wbrs_threat_type x_avc_app x_avc_type
x_avc_behavior x_request_rewrite x_avg_bw x_bw_throttled
x_user_type
x_resp_dvs_verdictnamex_req_dvs_threat_namex_suspect_user_agent
x_wbrs_threat_reason dvc_time duration dvc_ip result http_status
bytes_in http_method dest_url user_id_dom hierarchy hierarchy_domain
mime_type acl_tag user_id user_domain dest_domain | stats count by
```

```
x_webcat_code_abbr x_wbrs_score x_webroot_scanverdict
x_webroot_threat_name x_webroot_trr x_webroot_spyid
x_webroot_trace_id x_mcaffe_scanverdict x_mcafee_filename
x_mcafee_scan_error x_mcafee_detecttype x_mcafee_av_virustype
x_mcafee_virus_name x_sophos_scanverdict x x_sophos_filename
x_sophos_virus_name x_ids_verdict x_icap_verdict
x_webcat_req_code_abbr x_webcat_resp_code_abbr
x_resp_dvs_threat_name x_wbrs_threat_type x_avc_app x_avc_type
x_avc_behavior x_request_rewrite x_avg_bw x_bw_throttled
x_user_type
x_resp_dvs_verdictnamex_req_dvs_threat_namex_suspect_user_agent
x_wbrs_threat_reason dvc_time duration dvc_ip result http_status
bytes_in http_method dest_url user_id_dom hierarchy hierarchy_domain
mime_type acl_tag user_id user_domain dest_domain | convert
ctime(dvc_time) | search user_id="!!!!" AND host="!!!!" AND
src_ip="!!!!" AND cause="!!!!" AND action="!!!!" AND
dest_domain="!!!!"
```

- ホストの抽出が正しいことを確認します。これは、インストール ガイドにおける入力ストラテジーの一部です。ホスト抽出が適切に行われるようにするため、フォルダ構造を適切に確立しておく必要があります。
- 当マニュアルの「ホスト ルックアップ ファイル」セクションで説明した通り、ホストは名前変更される場合があります。

トラフィック監視ログ

L4TM レポートは、L4TM データ（サマリーデータではない）から生成されます。レポート機能を保つためには、フィールド抽出を実行できるようにしておく必要があります。形式はアクセスログほど多目的ではありませんが、同様の手法で確認することができます。

ヒント 結果が少ない、または結果がないことを確認するには、この Search を使用します。

```
sourcetype=wsa_trafmonlogs | head 1000 | fillnull value="!!!!"
dvc_time log_level action proto src_ip src_port dest_ip dest_host
dest_port | stats count by dvc_time log_level action proto src_ip
src_port dest_ip dest_host dest_port | search src_ip="!!!!"
```