# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı: PALO ALTO – traffic log |
| Versiyonu: |
| Log Toplama Tipi: Windows Paylaşımından okunacak \*.csv dosyası |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | Generate Time |
| SOURCENAME | - |
| EVENTCATEGORY | Category |
| EVENTTYPE | Action |
| USERSID | Source User |
| LOGNAME | <> |
| COMPUTERNAME | - |
| CUSTOMSTR1 | Inbound interface |
| CUSTOMSTR2 | Outbound interface |
| CUSTOMSTR3 | Source IP |
| CUSTOMSTR4 | Destination IP |
| CUSTOMSTR5 | NAT Source IP |
| CUSTOMSTR6 | NAT Destination IP |
| CUSTOMSTR7 | IP Protocol |
| CUSTOMSTR8 | - |
| CUSTOMSTR9 | Rule |
| CUSTOMSTR10 | Aplication |
| CUSTOMINT1 | Domain |
| CUSTOMINT2 | Repeat Count |
| CUSTOMINT3 | Source Port |
| CUSTOMINT4 | Destination Port |
| CUSTOMINT5 | NAT Source Port |
| CUSTOMINT6 | NAT Destination Port |
| CUSTOMINT7 | Session ID |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| Örnek Log | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

Ek Açıklamalar: