# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı:4IPNET |
| Versiyonu: |
| Log Toplama Tipi: |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | Internal ID |
| CUSTOMSTR2 | Description |
| CUSTOMSTR3 | Source IP |
| CUSTOMSTR4 | Destination IP |
| CUSTOMSTR5 | X Source Port |
| CUSTOMSTR6 | X Destination Port |
| CUSTOMSTR7 | Direction |
| CUSTOMSTR8 | Duration |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | Source Port |
| CUSTOMINT3 |  |
| CUSTOMINT4 | X Source Port |
| CUSTOMINT5 | X Destination Port |
| CUSTOMINT6 | Destination Port |
| CUSTOMINT7 | byte |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 4IPNET SESSION LOGLARI.  **2/16/2011 10:39:06 Local7.Info 92.45.16.140 session:[New]test@local TCPMAC=00:19:d2:59:8b:99 SIP=192.168.100.81 SPort=61620 DIP=10.0.0.47DPort=8014** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2/16/2011 10:39:06** |
| SOURCENAME |  |
| EVENTCATEGORY | **session:** |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **92.45.16.140** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | **test@local** |
| CUSTOMSTR3 | **SIP=192.168.100.81** |
| CUSTOMSTR4 | **SPort=61620** |
| CUSTOMSTR5 | **DIP=10.0.0.47** |
| CUSTOMSTR6 | **DPort=8014** |
| CUSTOMSTR7 | **TCP** |
| CUSTOMSTR8 | **MAC=00:19:d2:59:8b:99** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

Ek Açıklamalar: