# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı: MSFirewall\_2008 |
| Versiyonu: 1.0 |
| Log Toplama Tipi: Dosya |

# TEMEL PARSING YAPISI

date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpsyn tcpwin icmptype icmpcode info path

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | date time |
| SOURCENAME | path |
| EVENTCATEGORY | Action |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME | MSFirewall\_2008 |
| COMPUTERNAME | <makine-adı> / Remote Recorder Bağlantı Değerinden alınacak. |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | src-ip |
| CUSTOMSTR4 | dst-ip |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | protocol |
| CUSTOMSTR8 | tcpflags |
| CUSTOMSTR9 | Tcpsyn + icmptype |
| CUSTOMSTR10 | Tcpwin + icmpcode |
| CUSTOMINT1 | src-port |
| CUSTOMINT2 | dst-port |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 | size |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | info |

Genel Yapı: Ayraç olarak boşluk kullanılıyor. Her zaman iki dosya var. Dolunca dosyanın adını old yapıp kaydırıyor. Diğerini de sıfırlıyor. Dosya dolduğunda boyutu sıfırlanıp baştan başlıyor. Log kaybetmemek için eğer eşleme olmazsa .old dosyasına bakmak sonuna kadar gidip orijinal dosyaya geçmek yeterli. Her ikisinde de eşleme olmazsa pfirewall.log dosyasından başlanacak.

