# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı: McAfeeIpsV7 |
| Versiyonu: |
| Log Toplama Tipi: Syslog |
| $IV\_ATTACK\_TIME$ | $IV\_ATTACK\_NAME$ | $IV\_ATTACK\_CONFIDENCE$ | $IV\_SOURCE\_IP$:$IV\_SOURCE\_PORT$ | $IV\_DESTINATION\_IP$:$IV\_DESTINATION\_PORT$ | $IV\_CATEGORY$ | $IV\_SUB\_CATEGORY$ | $IV\_DIRECTION$ | $IV\_RESULT\_STATUS$ | $IV\_APPLICATION\_PROTOCOL$ | $IV\_NETWORK\_PROTOCOL$ | $IV\_ATTACK\_COUNT$ |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY | $IV\_ATTACK\_NAME$ |
| EVENTTYPE | $IV\_ATTACK\_NAME$ ( : ile ayrılıyor içerisinde : sonrası Eventtype olarak geliyor.) |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | $IV\_ATTACK\_CONFIDENCE$ |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | $IV\_SOURCE\_IP |
| CUSTOMSTR4 | $IV\_DESTINATION\_IP$ |
| CUSTOMSTR5 | $IV\_CATEGORY$ |
| CUSTOMSTR6 | $IV\_SUB\_CATEGORY$ |
| CUSTOMSTR7 | $IV\_DIRECTION$ |
| CUSTOMSTR8 | $IV\_RESULT\_STATUS$ |
| CUSTOMSTR9 | $IV\_APPLICATION\_PROTOCOL$ |
| CUSTOMSTR10 | $IV\_NETWORK\_PROTOCOL$ |
| CUSTOMINT1 | $IV\_ATTACK\_COUNT$ |
| CUSTOMINT2 |  |
| CUSTOMINT3 | $:$IV\_SOURCE\_PORT$ |
| CUSTOMINT4 | $IV\_DESTINATION\_PORT$ |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Ham log basılacak |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| Örnek Log  172.16.1.12:54808 : security.error Jun 6 09:05:17 SyslogAlertForwarder: 2012-06-06 09:05:16 EEST | P2P: Groove Virtual Office Groove.Net Agent Detected | N/A | 10.1.1.12:N/A | 65.55.122.232:N/A | PolicyViolation | restricted-application | Outbound | Suspicious | http | N/A | 1 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY | P2P |
| EVENTTYPE | Groove Virtual Office Groove.Net Agent Detected |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | N/A (Buraya Null, Low, Medium veya high olarak geliyor.) |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.1.1.12 |
| CUSTOMSTR4 | 65.55.122.232 |
| CUSTOMSTR5 | PolicyViolation |
| CUSTOMSTR6 | restricted-application |
| CUSTOMSTR7 | Outbound |
| CUSTOMSTR8 | Suspicious |
| CUSTOMSTR9 | http |
| CUSTOMSTR10 | N/A (Null veya TCP VEYA UDP olarak geliyor.) |
| CUSTOMINT1 | 1 |
| CUSTOMINT2 |  |
| CUSTOMINT3 | N/A (Burada iki tip gelme ihtimali var Null veya Port no bunun için bir condition ihtiyacı olacak eğer null ise 0 olsun şeklinde) |
| CUSTOMINT4 | N/A (Burada iki tip gelme ihtimali var Null veya Port no bunun için bir condition ihtiyacı olacak eğer null ise 0 olsun şeklinde) |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Ham log basılacak |

Ek Açıklamalar: