# RECORDER GELİŞTİRME İSTEK FORMU

|  |
| --- |
| Ürün Adı: PALO ALTO – threat 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 | Threat/Content Name |
| 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  1,2011/01/25 06:00:17,0004C100832,THREAT,vulnerability,2,2011/01/25 06:00:12,193.189.142.31,88.202.62.1,192.168.0.10,88.202.62.1,Dis\_Web\_Server\_erisim,,,web-browsing,vsys1,DMZ,Internet,ethernet1/1,ethernet1/4,,2011/01/25 06:00:17,99208,1,80,61633,80,61633,0x40,tcp,alert,,HTTP Non RFC-Compliant Response Found(32880),any,informational,server-to-client | |
| **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:

Loglar da KeyWords mevcut. Loglar virgül ile ayrılmış durumda.

Domain,Receive Time,Serial #,Type,Threat/Content Type,Config Version,Generate Time,Source address,Destination address,NAT Source IP,NAT Destination IP,Rule,Source User,Destination User,Application,Virtual System,Source Zone,Destination Zone,Inbound Interface,Outbound Interface,Log Action,Time Logged,Session ID,Repeat Count,Source Port,Destination Port,NAT Source Port,NAT Destination Port,Flags,IP Protocol,Action,URL,Threat/Content Name,Category,Severity,Direction