İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING TİP 1 4](#_Toc330026388)

[TEMEL PARSING YAPISI TİP 1 5](#_Toc330026388)

[ÖRNEK PARSING TİP 2 6](#_Toc330026389)

[TEMEL PARSING YAPISI TİP 2 7](#_Toc330026388)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 03.01.2013 | V1 | Watchguard Firewall 5 Series | Kaan Emre KOŞAR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | Watchguard Firewall |
| Versiyonu | 5 Serisi |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi |  |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 03.01.2013 |
| İstek yapılan kurum adı | MİKES |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | \\Srv-print\c$\ProgramData\WatchGuard\logs\data\pg\_log\ (örnek dosya ismi: postgresql-2012-12-11\_000000.log) |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları | Log dosyaları, her gün gece paylaşılan klasöre, tarih atılarak kopyalanmaktadır. Ürün logları bir gün geriden takip edilecektir. Loglar içerisinde alınması gerekli olan 2 tip vardır ve buna göre parsing yapılmalıdır. Bu tipler haricindeki satırlar veritabanına alınmayacaktır. |

# TİP-1 ÖRNEK PARSING

|  |  |
| --- | --- |
| Örnek log:  2012-12-11 09:05:28 CONTEXT: COPY app\_requests\_20121211, line 1: "172.16.100.102#HYPERV-2#65.55.7.141#HTTP-proxy-USERS-00#SKATS3@mikes.com.tr#Web File Transfer#5#File..." | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2012-12-11 09:05:28 |
| SOURCENAME | HYPERV-2 |
| EVENTCATEGORY |  |
| EVENTTYPE | app |
| USERSID | SKATS3@mikes.com.tr |
| LOGNAME | “RecorderName” |
| COMPUTERNAME |  |
| CUSTOMSTR1 | 172.16.100.102 |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 65.55.7.141 |
| CUSTOMSTR4 | HTTP-proxy-USERS-00 |
| CUSTOMSTR5 | Web File Transfer |
| CUSTOMSTR6 | File... |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 5 |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |

# TİP-1 TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | date\_time |
| SOURCENAME | source\_domain |
| EVENTCATEGORY |  |
| EVENTTYPE | request\_type |
| USERSID | src\_user |
| LOGNAME | RecorderName |
| COMPUTERNAME |  |
| CUSTOMSTR1 | source\_ip |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | dest\_ip |
| CUSTOMSTR4 | policy |
| CUSTOMSTR5 | app\_name |
| CUSTOMSTR6 | cat\_name |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | app\_id |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |

# TİP-2 ÖRNEK PARSING

|  |  |
| --- | --- |
| Örnek log:  2012-12-11 00:05:57 CONTEXT: COPY by\_session\_requests\_20121210, line 1: "172.16.0.121#51605#23.21.167.232#80#tcp#4#2012-12-10 22:00:00#1#1#0" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2012-12-11 00:05:57 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | by\_session |
| USERSID |  |
| LOGNAME | “RecorderName” |
| COMPUTERNAME |  |
| CUSTOMSTR1 | 172.16.0.121 |
| CUSTOMSTR2 | 23.21.167.232 |
| CUSTOMSTR3 | 2012-12-10 22:00:00 |
| CUSTOMSTR4 | tcp |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 51605 |
| CUSTOMINT2 | 80 |
| CUSTOMINT3 | 4 |
| CUSTOMINT4 | 1 |
| CUSTOMINT5 | 1 |
| CUSTOMINT6 | 0 |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |

# TİP-1 TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | request\_type |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | src\_ip |
| CUSTOMSTR2 | dest\_ip |
| CUSTOMSTR3 | update\_time |
| CUSTOMSTR4 | protocol |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | src\_port |
| CUSTOMINT2 | dest\_port |
| CUSTOMINT3 | total\_count |
| CUSTOMINT4 | appliance\_id |
| CUSTOMINT5 | cluster |
| CUSTOMINT6 | direction |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |