İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | WatchGuardWebSyslog |
| Versiyonu | 11.7.3 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | WatchGuardWebV\_11\_7\_3\_0SyslogRecorder.dll |
| İstek yapan Adı Soyadı | Fatih Sakar |
| Geliştirici Adı Soyadı |  |
| İstek tarihi |  |
| İstek yapılan kurum adı | Mikes |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **172.16.0.1:45001 : local1.info Sep 3 10:01:46 MikesFireCluster http-proxy[1978]: Allow 1-MIKES-LOCAL 0-External tcp 172.16.0.34 95.0.178.58 50925 80 msg="HTTP Request" proxy\_act="Mikes-internet" op="GET" dstname="www.gold.com.tr" arg="/ImagesGld/banklogo/productDetail/cardbonus\_logo.jpg" sent\_bytes="1143" rcvd\_bytes="8337" elapsed\_time="0.187639 sec(s)" reputation="9" reason="262189" action="allow" (HTTP-proxy-USERS-00)** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY | **Allow** |
| EVENTTYPE | **GET (op)** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **HTTP Request (msg)** |
| CUSTOMSTR2 | **Mikes-internet (proxy\_act)** |
| CUSTOMSTR3 | **172.16.0.34 (src\_ip)** |
| CUSTOMSTR4 | **198.61.220.141 (dest\_ip)** |
| CUSTOMSTR5 | **http** |
| CUSTOMSTR6 | **www.gold.com.tr (dstname)** |
| CUSTOMSTR7 | **/ImagesGld/banklogo/productDetail/cardbonus\_logo.jpg (arg)** |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **50925** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 | **1143 (sent\_bytes)** |
| CUSTOMINT6 | **8337 (rcvd\_bytes)** |
| CUSTOMINT7 | **0.187639 (elapsed\_time)** |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| 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 |  |