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 |
| 20.12.2012 | V1 | DSI kurumunda Websense ürünü üzerinde yer kalmadığı için log alma tipini Syslog olarakdeğiştirildi. | Şahan Savaşan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Websense |
| Versiyonu | V2 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | WSenseSyslogV\_1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Şahan SAVAŞAN |
| Geliştirici Adı Soyadı | Onur SARIKAYA |
| İstek tarihi | 21.01.2013 |
| İstek yapılan kurum adı | DSI |
| 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

|  |  |
| --- | --- |
| 01-16-2013 19:02:29 Local3.Debug 10.1.1.23  Jan 16 19:02:23 10.1.1.23 vendor=Websense product=Security product\_version=7.7.0 action=permitted severity=1 category=1904 user=LDAP://172.16.1.201 OU=19\_merkez,OU=bolge19,OU=\_bolgeler,DC=dsibim,DC=local/Güvenlik19 (OsmanÖzden) src\_host=10.119.5.7 src\_port=1575 dst\_host=www.youtube.com dst\_ip=173.194.35.142 dst\_port=80 bytes\_out=459 bytes\_in=85754 http\_response=200 http\_method=GET http\_content\_type=text/html;\_charset=utf-8 http\_user\_agent=Mozilla/5.0\_(Windows\_NT\_5.1)\_AppleWebKit/537.17\_(KHTML,\_like\_Gecko)\_Chrome/24.0.1312.52\_Safari/537.17 http\_proxy\_status\_code=200 reason=- disposition=1028 policy=role-8\*\*Default role=8 duration=13 url=http://www.youtube.com/ | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 01-16-2013 19:02:29 |
| SOURCENAME | OU=19\_merkez,OU=bolge19,OU=\_bolgeler,DC=dsibim |
| EVENTCATEGORY | 1904 |
| EVENTTYPE |  |
| RECORD\_NUMBER |  |
| USERSID | Güvenlik19 (OsmanÖzden) |
| LOGNAME |  |
| COMPUTERNAME | 172.16.1.201 |
| CUSTOMSTR1 | 10.1.1.23 |
| CUSTOMSTR2 | permitted |
| CUSTOMSTR3 | 10.119.5.7 |
| CUSTOMSTR4 | 173.194.35.142 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 | <http://www.youtube.com/> |
| CUSTOMSTR7 | Customstr6 alanına gelen string değeri 900 bytes üzerinde ise kalan kısım buaraya yazılacak. |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 1028 |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 200 |
| CUSTOMINT4 |  |
| CUSTOMINT5 | 1 |
| CUSTOMINT6 |  |
| CUSTOMINT7 | 459 |
| CUSTOMINT8 | 85754 |
| CUSTOMINT9 | 1575 |
| CUSTOMINT10 | 80 |
| DESCRIPTION | www.youtube.com |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | 01-16-2013 19:02:29 |
| SOURCENAME | OU=19\_merkez,OU=bolge19,OU=\_bolgeler,DC=dsibim |
| EVENTCATEGORY | category |
| EVENTTYPE |  |
| USERSID | DC=local/ |
| LOGNAME |  |
| COMPUTERNAME | user=LDAP:// |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | action |
| CUSTOMSTR3 | src\_host= |
| CUSTOMSTR4 | dst\_ip= |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 | url= |
| CUSTOMSTR7 | Customstr6 alanına gelen string değeri 900 bytes üzerinde ise kalan kısım buaraya yazılacak. |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | disposition= |
| CUSTOMINT2 |  |
| CUSTOMINT3 | http\_response= |
| CUSTOMINT4 |  |
| CUSTOMINT5 | severity |
| CUSTOMINT6 |  |
| CUSTOMINT7 | bytes\_out= |
| CUSTOMINT8 | bytes\_in= |
| CUSTOMINT9 | src\_port= |
| CUSTOMINT10 | dst\_port= |
| DESCRIPTION | dst\_host= |