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 | Cyberoam |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | CyberoamSyslogV\_1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Emir AY |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 19.12.2012 |
| İstek yapılan kurum adı | Galatasaray Üniversitesi |
| 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

|  |  |
| --- | --- |
| date=2012-11-29 time=12:29:57 timezone="EET" device\_name="CR1000i" device\_id=C010001334-8KGA74 log\_id=050901616001 log\_type="Content Filtering" log\_component="HTTP" log\_subtype="Allowed" status="" priority=Information fw\_rule\_id=0 user\_name="12503202@ogr.gsu.edu.tr" user\_gp="UG\_Ogrenci" iap=12 category="SearchEngines" category\_type="Neutral" url="sp.ask.com/toolbar/config/partner/vanilla/default\_1.12wid/ie/PopupWidgetGamesFF.xml" contenttype="text/xml" httpresponsecode="" src\_ip=10.1.3.46 dst\_ip=195.175.70.24 protocol="TCP" src\_port=2611 dst\_port=80 sent\_bytes=0 recv\_bytes=6925 domain=sp.ask.com | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | date=2012-11-29 time=12:29:57 |
| SOURCENAME | device\_name="CR1000i" |
| EVENTCATEGORY | log\_component="HTTP" |
| EVENTTYPE | log\_type="Content Filtering" |
| USERSID | device\_id=C010001334-8KGA74 |
| LOGNAME |
| COMPUTERNAME | user\_name="12503202@ogr.gsu.edu.tr" |
| CUSTOMSTR1 | protocol="TCP" |
| CUSTOMSTR2 | user\_gp="UG\_Ogrenci" |
| CUSTOMSTR3 | src\_ip=10.1.3.46 |
| CUSTOMSTR4 | dst\_ip=195.175.70.24 |
| CUSTOMSTR5 | category="SearchEngines" |
| CUSTOMSTR6 | contenttype="text/xml" |
| CUSTOMSTR7 | domain=sp.ask.com |
| CUSTOMSTR8 | status="" |
| CUSTOMSTR9 | url="sp.ask.com/toolbar/config/partner/vanilla/default\_1.12wid/ie/PopupWidgetGamesFF.xml" |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | fw\_rule\_id=0 |
| CUSTOMINT2 | iap=12 |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 | src\_port=2611 |
| CUSTOMINT6 | dst\_port=80 |
| CUSTOMINT7 | httpresponsecode="" |
| CUSTOMINT8 | sent\_bytes=0 |
| CUSTOMINT9 | recv\_bytes=6925 |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| date=2012-11-29 time=12:27:48 timezone="EET" device\_name="CR1000i" device\_id=C010001334-8KGA74 log\_id=010101600001 log\_type="Firewall" log\_component="Firewall Rule" log\_subtype="Allowed" status="Allow" priority=Information duration=129 fw\_rule\_id=88 user\_name="okunal@gsu2.edu" user\_gp="UG\_Akademik\_Personel" iap=22 ips\_policy\_id=0 appfilter\_policy\_id=14 application="" in\_interface="PortA" out\_interface="PortC" src\_mac=00: 0:00: 0:00: 0 src\_ip=172.19.245.118 src\_country\_code= dst\_ip=83.175.184.26 dst\_country\_code=POL protocol="TCP" src\_port=50102 dst\_port=22105 sent\_pkts=3 recv\_pkts=0 sent\_bytes=152 recv\_bytes=0 tran\_src\_ip=194.27.192.252 tran\_src\_port=0 tran\_dst\_ip= tran\_dst\_port=0 srczonetype="" dstzonetype="" dir\_disp="" connevent="Stop" connid="4085766180" vconnid="" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | date=2012-11-29 time=12:27:48 |
| SOURCENAME | device\_name="CR1000i" |
| EVENTCATEGORY | status="Allow" |
| EVENTTYPE | log\_type="Firewall" |
| USERSID | device\_id=C010001334-8KGA74 |
| LOGNAME |  |
| COMPUTERNAME | user\_name="okunal@gsu2.edu" |
| CUSTOMSTR1 | protocol="TCP" |
| CUSTOMSTR2 | " user\_gp="UG\_Akademik\_Personel" |
| CUSTOMSTR3 | src\_ip=172.19.245.118 |
| CUSTOMSTR4 | dst\_ip=83.175.184.26 |
| CUSTOMSTR5 | src\_mac=00: 0:00: 0:00: 0 |
| CUSTOMSTR6 | in\_interface="PortA" |
| CUSTOMSTR7 | out\_interface="PortC" |
| CUSTOMSTR8 | tran\_src\_ip=194.27.192.252 |
| CUSTOMSTR9 | tran\_dst\_ip= |
| CUSTOMSTR10 | connevent="Stop" |
| CUSTOMINT1 |  |
| CUSTOMINT2 | fw\_rule\_id=88 |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 | src\_port=50102 |
| CUSTOMINT6 | dst\_port=22105 |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | ips\_policy\_id=0 |
| CUSTOMINT10 | appfilter\_policy\_id=14 |
| 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 |  |