İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc333563892)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc333563893)

[ÖRNEK PARSING 4](#_Toc333563894)

[TEMEL PARSING YAPISI 5](#_Toc333563895)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
|  |  |  |  |
| 22.08.2012 | V1.0 | Ankara Ticaret Odası için geliştirilen IPS recorder için recorder geliştirme Formudur. | Hüseyin SEVİN |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | HP Tipping Point IPS |
| Versiyonu | V1400N |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | TippingPointIpsV1\_1400\_1SyslogRecorder |
| İstek yapan Adı Soyadı | Hüseyin SEVİN |
| Geliştirici Adı Soyadı | Onur SARIKAYA |
| İstek tarihi | 22.08.2012 |
| İstek yapılan kurum adı | ATO |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no | - |
| İlgili ham log yolu/dosya ismi | SyslogCatchAll\_ATO\_IPS |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | IPS cihazının ürettiği loğlar yeterli değil syslog’ a göre çok az sayıda log geliyor.  Tekrar bir güncelleme yapılabilir. |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 10.0.30.200:1130 : 31.error Aug 22 15:21:05 10.0.30.200 BLK v5 20120822T152105-0120 "IPS-ATO"/10.0.30.200 0 2 Block Major 00000002-0002-0002-0002-000000012109 "12109: HTTP: Multiple Vendor Hash Collision Denial of Service (ONLY enable when under DoS attack12109: HTTP: Multiple Vendor Hash Collision Denial of Service (ONLY enable when under DoS attackhttp" "12109: HTTP: Multiple Vendor Hash Collision Denial of Service (ONLY enable when under DoS attackhttp" http " " 31.44.205.11 32740 66.220.152.20 80 20120822T135541-0120 1 " " 0 ANY-ANY | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Aug 22 15:21:05 |
| SOURCENAME | 10.0.30.200 |
| EVENTCATEGORY | Block |
| EVENTTYPE | Error |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | IPS-ATO |
| CUSTOMSTR1 | Critical |
| CUSTOMSTR2 | 12109: HTTP: Multiple Vendor Hash Collision Denial of Service (ONLY enable when under DoS attackhttp |
| CUSTOMSTR3 | http |
| CUSTOMSTR4 | 31.44.205.11 |
| CUSTOMSTR5 | 66.220.152.20 |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| 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 |  |