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 |
| 23.12.2012 | V2 | Eset Nod 32 V5 sürümü ile yenilenen DB registry yapısı için hazırlandı. | Şahan Savaşan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | EsetNod32 v5 |
| Versiyonu | V2 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | EsetNod32v5recorder |
| İstek yapan Adı Soyadı | Şahan SAVAŞAN |
| Geliştirici Adı Soyadı | Onur SARIKAYA |
| İstek tarihi | 23.12.2012 |
| İstek yapılan kurum adı | TPE |
| 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

Tip 1 EventLog tablosundan alınacak Veri için

|  |  |
| --- | --- |
| SELECT Client.PrimaryServer, Client.Name, Client.ComputerName, Client.MacAddress,  EventLog.DateReceived, EventLog.DateOccurred, EventLog.UserName, EventLog.FTPluginID,  FTPlugin.Txt, EventLog.LogLevel, EventLog.EventText, EventLog.ID  FROM Client INNER JOIN (EventLog INNER JOIN FTPlugin ON EventLog.FTPluginID = FTPlugin.ID) ON Client.ID = EventLog.ClientID; | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Log alımındaki date\_time bilgisi** |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| RECORD\_NUMBER |  |
| USERSID | Name |
| LOGNAME |  |
| COMPUTERNAME | ComputerName |
| CUSTOMSTR1 | PrimaryServer |
| CUSTOMSTR2 | MacAddress |
| CUSTOMSTR3 | DateReceived |
| CUSTOMSTR4 | DateOccurred |
| CUSTOMSTR5 | UserName |
| CUSTOMSTR6 | Txt |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | FTPluginID |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | ID |
| CUSTOMINT7 | EventText |
| CUSTOMINT8 | LogLevel |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

Tip 2 Firewall tablosu için

|  |  |
| --- | --- |
| SELECT Client.PrimaryServer, Client.Name, Client.ComputerName, Client.MacAddress,  FirewallLog.DateReceived, FirewallLog.DateOccurred, FirewallLog.UserName,  FirewallLog.LogLevel, FTHFwEvent.Txt, FirewallLog.Source, FirewallLog.Target,  FTHProtocol.Txt, FTHFwRuleName.Txt, FirewallLog.ID  FROM (((Client INNER JOIN FirewallLog ON Client.ID = FirewallLog.ClientID) INNER JOIN FTHFwEvent  ON FirewallLog.FTHFwEventHASH = FTHFwEvent.HASH) INNER JOIN FTHProtocol  ON FirewallLog.FTHProtocolHASH = FTHProtocol.HASH) INNER JOIN FTHFwRuleName  ON FirewallLog.FTHFwRuleNameHASH = FTHFwRuleName.HASH  ORDER BY FirewallLog.ID DESC; | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| RECORD\_NUMBER |  |
| USERSID | Name |
| LOGNAME |  |
| COMPUTERNAME | ComputerName |
| CUSTOMSTR1 | PrimaryServer |
| CUSTOMSTR2 | MacAddress |
| CUSTOMSTR3 | DateReceived |
| CUSTOMSTR4 | DateOccurred |
| CUSTOMSTR5 | UserName |
| CUSTOMSTR6 | FTHFwEvent.Txt |
| CUSTOMSTR7 | Source |
| CUSTOMSTR8 | Target |
| CUSTOMSTR9 | FTHProtocol.Txt |
| CUSTOMSTR10 | FTHFwRuleName.Txt |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | ID |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | LogLevel |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

Tip 3 ScanLog Tablosu için

|  |  |
| --- | --- |
| SELECT Client.PrimaryServer, Client.Name, Client.ComputerName, Client.MacAddress,  ScanLog.DateReceived, ScanLog.DateOccurred, ScanLog.UserName, ScanLog.FTScannerID,  FTScanner.Txt, ScanLog.TaskID, ScanLog.TaskType, ScanLog.Description, FTHScanStatus.Txt,  ScanLog.Scanned, ScanLog.Infected, ScanLog.Cleaned, ScanLog.Details, ScanLog.ID  FROM ((Client INNER JOIN ScanLog ON Client.ID = ScanLog.ClientID) INNER JOIN FTScanner  ON ScanLog.FTScannerID = FTScanner.ID) INNER JOIN FTHScanStatus  ON ScanLog.FTHScanStatusHASH = FTHScanStatus.HASH  ORDER BY ScanLog.ID DESC; | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Log alımındaki date\_time bilgisi** |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | FTScannerID |
| RECORD\_NUMBER |  |
| USERSID | Name |
| LOGNAME |  |
| COMPUTERNAME | ComputerName |
| CUSTOMSTR1 | PrimaryServer |
| CUSTOMSTR2 | MacAddress |
| CUSTOMSTR3 | DateReceived |
| CUSTOMSTR4 | DateOccurred |
| CUSTOMSTR5 | UserName |
| CUSTOMSTR6 | FTScanner.Txt |
| CUSTOMSTR7 | Description |
| CUSTOMSTR8 | FTHScanStatus.Txt |
| CUSTOMSTR9 | Details |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | TaskID |
| CUSTOMINT2 | TaskType |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | ID |
| CUSTOMINT7 |  |
| CUSTOMINT8 | Scanned |
| CUSTOMINT9 | Infected |
| CUSTOMINT10 | Cleaned |
| DESCRIPTION |  |

Tip 4 Threat Tablosu için ;

|  |  |
| --- | --- |
| SELECT Client.PrimaryServer, Client.Name, Client.ComputerName, Client.MacAddress,  ThreatLog.DateReceived, ThreatLog.DateOccurred, ThreatLog.UserName, ThreatLog.FTScannerID,  FTScanner.Txt, ThreatLog.LogLevel, FTHThreatObject.Txt, ThreatLog.Name, ThreatLog.Virus,  FTHActionTaken.Txt, ThreatLog.Info, ThreatLog.ID  FROM (((Client INNER JOIN ThreatLog ON Client.ID = ThreatLog.ClientID) INNER JOIN FTHActionTaken  ON ThreatLog.FTHActionTakenHASH = FTHActionTaken.HASH) INNER JOIN FTHThreatObject  ON ThreatLog.FTHThreatObjectHASH = FTHThreatObject.HASH) INNER JOIN FTScanner  ON ThreatLog.FTScannerID = FTScanner.ID  ORDER BY ThreatLog.ID DESC; | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Log alımındaki date\_time bilgisi** |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| RECORD\_NUMBER |  |
| USERSID | Client.Name |
| LOGNAME |  |
| COMPUTERNAME | ComputerName |
| CUSTOMSTR1 | Info |
| CUSTOMSTR2 | MacAddress |
| CUSTOMSTR3 | DateReceived |
| CUSTOMSTR4 | DateOccurred |
| CUSTOMSTR5 | UserName |
| CUSTOMSTR6 | FTScanner.Txt |
| CUSTOMSTR7 | FTHThreatObject.Txt |
| CUSTOMSTR8 | ThreatLog.Name |
| CUSTOMSTR9 | Virus |
| CUSTOMSTR10 | FTHActionTaken.Txt |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | ID |
| CUSTOMINT7 |  |
| CUSTOMINT8 | FTScannerID, |
| CUSTOMINT9 | LogLevel |
| CUSTOMINT10 |  |
| DESCRIPTION | PrimaryServer |