

ILMO. SENHOR PREGOEIRO DO TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
ELETRÔNICO Nº 029/2021

RECORRENTE: TELETEX COMPUTADORES E SISTEMAS LTDA
RECORRIDA: ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA

CONTRARRAZÕES DE RECURSO PELA RECORRIDA

ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 09.571.988/0001-13, situada na SHIS QI 05 Bloco F Sala 206 - Centro Comercial Gilberto Salomão, Lago Sul, Brasília/ DF - CEP: 71615-560., vem à presença de Vossa Senhoria, apresentar tempestivamente suas contrarrazões ao recurso administrativo interposto, na forma a seguir exposta:

Trata-se de recurso interposto por TELETEX COMPUTADORES E SISTEMAS LTDA., pessoa jurídica de direito privado, inscrita no CNPJ sob nº. 79.345.583/0001-42, sediada na Rodovia BR 116, Linha Verde, nº. 12.500, Parolin, Curitiba, Estado do Paraná, em face da decisão da empresa ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA. ter sido declarada vencedora da licitação.

Seguem as contrarrazões de recurso contendo argumentação definitiva, com sólidos fundamentos para a manutenção da decisão do Ilmo. Sr. Pregoeiro.

Primeiro é importante indicar alguns equívocos contidos no recurso interposto pela licitante TELETEX COMPUTADORES E SISTEMAS LTDA. Na análise realizada, a licitante levou em consideração apenas o ponto a ponto e suas referências, quando este documento não é obrigatório segundo edital, e foi apresentado apenas para servir de roteiro e indicações para análise de todo conteúdo enviado. Para uma avaliação de dúvidas, o arcabouço completo de arquivos deveria ter sido analisado.

Abaixo seguem toda documentação enviada como arcabouço técnico de consulta, contemplando sete (7) pastas e duzentos e sessenta seis (266) arquivos, que foram divididos conforme estrutura de tópicos abaixo:

1. Getting Started (Pasta)
 - 1.1. Release Notes for ArcSight ESM 7.5
 - 1.2. ArcSight Platform 21.1 Release Notes
 - 1.3. Quick Start Guide to Reporting EPS Usage
 - 1.4. Technical Requirements for ESM 7.5
 - 1.5. Technical Requirements for ArcSight Platform 21.1
 - 1.6. ESM 101
 - 1.7. Release Notes for ArcSight ESM Threat Detector 2.10
2. Deployment and Configuration (Pasta)
 - 2.1. Administrator's Guide for ESM 7.5
 - 2.2. Administrator's Guide to ArcSight Platform 21.1

- 2.3. Installation Guide for ESM 7.5
- 2.4. Upgrade Guide for ESM 7.5
- 2.5. ArcSight Forwarding Connector Configuration Guide for ESM 7.5
- 2.6. Actor Model Import Connector for Microsoft Active Directory Configuration Guide for ESM 7.5
- 2.7. ESM Best Practices for ESM 7.5_Multitenancy and Managed Security Service Providers
- 2.8. Best Practices for ESM 7.5_Trends
- 2.9. ArcSight Administration and ArcSight System Standard Content Guide for ESM 7.5
- 2.10. Micro Focus Security ArcSight Logger

- 3. Interacting with ESM (Pasta)
 - 3.1. ArcSight Command Center User's Guide for ESM 7.5
 - 3.2. ArcSight Console User's Guide for ESM 7.5
 - 3.3. Active-Passive High Availability Module User's Guide for ESM 7.5
 - 3.4. Solutions Guide for ArcSight ESM Threat Detector 2.10

- 4. Development (Pasta)
 - 4.1. API Reference for ESM 7.5 Vol. 1: Core-Client Services
 - 4.2. API Reference for ESM 7.5 Vol. 2: Manager-Client Services (1.1)
 - 4.3. Asset Model Import FlexConnector Developer's Guide for ESM 7.5
 - 4.4. Service Layer (Web Services) Developer's Guide for ESM 7.5

- 5. Technical Notes (Pasta)
 - 5.1. Backup and Recovery Tech Note for Compact and Distributed Mode for ESM 7.5

- 6. Datasheets (Pasta)
 - 6.1. Security ArcSight Compliance Insight Package for IT Governance
 - 6.2. ArcSight Enterprise Security Manager datasheet
 - 6.3. ArcSight Connector Supported Products
 - 6.4. ArcSight Connectors
 - 6.5. ArcSight Data Platform

- 7. ArcSight SmartConnectors 8.2.0 (Pasta)
 - 7.1. A-Z-Config-Guides (subpasta)
 - 7.2. Overview of SmartConnectors

Ao ignorar todos os documentos, e utilizar individualmente o ponto a ponto e sua referência, a licitante recorrente tenta induzir o Contratante ao erro, ao ignorar material técnico produzido pelo fabricante e fornecido pela licitante ATA COMERCIO E SERVIÇOS DE INFORMÁTICA.

Importante ressaltar que todos os documentos, manuais e arquivos do fabricante Microfocus visam ensinar os usuários e administradores a instalar, configurar, administrar, e utilizarem a plataforma ArcSight, e não são criados ou possuem uma construção hierárquica com a função comprobatória de um "Termo de Referência", e por isso, em alguns momentos faz-se necessário a comprovação por vários documentos diferentes e interpretação dos mesmos.

Quanto aos conectores, o MicroFocus ArcSight contempla uma vasta gama de coleta através de conectores chamados “Smart Connectors” – conectores criados pelo time da MicroFocus – e “FlexConnectors” que é um “Smart Connector” aberto (com um SDK) para próprio desenvolvimento de coletas que ainda não são contempladas por “Smart Connectors”, sejam de produtos de mercado ainda não criados pelo time da MicroFocus como para aplicações in-house do cliente.

Documentação de FlexConnector:

1. User Guide for Quick Flex Parser Tool 1.1
(<https://community.microfocus.com/cyberres/productdocs/w/connector-documentation/39014/user-guide-for-quick-flex-parser-tool-1-1>):
 - 1.1. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/SmartConnector_5F00_QuickFlex_5F00_1.0.pdf
 - 1.2. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/User-Guide-for-Quick-Flex-Parser-Tool-1.1.pdf
 - 1.3. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/SmartConnector_5F00_QuickFlex_5F00_1_2D00_1.pdf
2. Release Notes for Quick Flex Parser Tool 1.1
(<https://community.microfocus.com/cyberres/productdocs/w/connector-documentation/38973/release-notes-for-quick-flex-parser-tool-1-1>):
 - 2.1. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/QuickFlex_5F00_RelNotes_5F00_1.0.1.pdf
 - 2.2. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/QuickFlex_5F00_RelNotes_5F00_1.1.pdf
 - 2.3. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/7206.QuickFlex_5F00_RelNotes_5F00_1.1.pdf
 - 2.4. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/QuickFlex_5F00_RelNotes.pdf
 - 2.5. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/4064.QuickFlex_5F00_RelNotes.pdf
3. ArcSight FlexConnector Developer's Guide
(<https://community.microfocus.com/cyberres/productdocs/w/connector-documentation/38943/arc-sight-flexconnector-developer-s-guide>):

- 3.1. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/FlexConn_5F00_DevGuideConfig.pdf
- 3.2. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/4846.FlexConn_5F00_DevGuideConfig.pdf
- 3.3. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/8561.FlexConn_5F00_DevGuideConfig.pdf
- 3.4. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/FlexConn_5F00_DevGuide.pdf
- 3.5. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/4834.FlexConn_5F00_DevGuide.pdf
- 3.6. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/6746.FlexConn_5F00_DevGuide.pdf
- 3.7. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/5635.FlexConn_5F00_DevGuide.pdf
- 3.8. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/4278.FlexConn_5F00_DevGuide.pdf
- 3.9. https://community.microfocus.com/cfs-file/_key/communityserver-wikis-components-files/00-00-00-00-23/4745.FlexConn_5F00_DevGuide.pdf
4. ArcSight SmartConnectors 8.2.0 Documentation
<https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/#gsc.tab=0>

Após esclarecimento inicial quanto ao material de comprovação enviado e tecnologia de conectores do ArcSight, nos resta, esclarecer as dúvidas levantadas para três (3) subitens dentre os cento e trinta e dois (132) itens exigidos no termo de referência (12.1, 12.3. e 12.8).

12. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listados abaixo:

12.1. Firewalls: VMWare NSX

Abaixo estamos apresentando o código do Smart Connectors existente para coleta de VMWare, que se encontra disponível na comunidade do ArcSight um Flex Connector para coleta de eventos do VMWare NSX, e transcrito abaixo:

FlexAgent Regex Configuration File

do.unparsed.events=true

regex=[^bhcorp]*(\\w+)\\.bhcorp\\.ad (dfwpklogs) [^INET]*(INET|INET6) (\\S+) (.*)

token.count=5

token[0].name=hostname

token[0].type=String

token[1].name=custString1

token[1].type=String

token[2].name=custom2

token[2].type=String

token[3].name=Message

token[3].type=String

token[4].name=message

token[4].type=String

submessage.messageid.token=Message

submessage.token=message

event.name=Message

event.deviceHostName=hostname

event.deviceCustomString1=custString1

event.message=message

event.deviceCustomString2=custom2

event.deviceVendor=__stringConstant(VMWare)

event.deviceProduct=__stringConstant(NSX)

#l10n.filename.prefix=

submessage.count=2

submessage[0].messageid=match

submessage[0].pattern.count=3

submessage[0].pattern[0].regex=(\\w+) (domain\\-\\S+) (\\w+) (\\d+) (\\w+)

(\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+)\\->(\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+)

submessage[0].pattern[0].fields=event.deviceAction,event.deviceCustomString4,event.deviceOutboundInterface,event.bytesIn,event.transportProtocol,event.sourceAddress,event.sourcePort,event.destinationAddress,event.destinationPort

submessage[0].pattern[1].regex=(\\w+) (domain\\-\\S+) (\\w+) (\\d+) (\\w+)

(\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+)\\->(\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+) (\\S+)

```
submessage[0].pattern[1].fields=event.deviceAction,event.deviceCustomString3,event.deviceOutboundInterface,event.bytesIn,event.transportProtocol,event.sourceAddress,event.sourcePort,event.destinationAddress,event.destinationPort,event.deviceCustomString4
```

```
submessage[0].pattern[2].regex=(\\w+) (domain\\-\\S+) (\\w+) (\\d+) PROTO (\\d+) (\\d+\\.\\d+\\.\\d+\\.\\d+)\\->(\\d+\\.\\d+\\.\\d+\\.\\d+)
submessage[0].pattern[2].fields=event.deviceAction,event.deviceCustomString4,event.deviceOutboundInterface,event.bytesIn,event.transportProtocol,event.sourceAddress,event.destinationAddress
```

```
submessage[1].messageid=TERM
submessage[1].pattern.count=2
submessage[1].pattern[0].regex=(domain\\-\\S+) (\\w+) (\\w+) (\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+)\\->(\\d+\\.\\d+\\.\\d+\\.\\d+|[^/]*)\\V(\\d+) (\\d+\\V\\d+ \\d+\\V\\d+)
submessage[1].pattern[0].fields=event.deviceCustomString3,event.deviceOutboundInterface,event.transportProtocol,event.sourceAddress,event.sourcePort,event.destinationAddress,event.destinationPort,event.deviceCustomString4
```

```
submessage[1].pattern[1].regex=(domain\\-\\S+) (\\w+) PROTO (\\d+) (\\d+\\.\\d+\\.\\d+\\.\\d+)\\->(\\d+\\.\\d+\\.\\d+\\.\\d+) (\\d+\\V\\d+) (\\d+\\V\\d+)
submessage[1].pattern[1].fields=event.deviceCustomString4,event.deviceOutboundInterface,event.transportProtocol,event.sourceAddress,event.destinationAddress,event.deviceCustomString5,event.deviceCustomString6
```

12.1. Firewalls: PfSense

O pfSense é um firewall open source, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e/ou roteador de redes. O nome deriva do fato que o software utiliza a tecnologia packet-filtering. Como uma variação do Linux FreeBSD, o PfSense não é citado na lista de connectors, pois utiliza mesmo padrão de log do FreeBSD, e a interpretação desses logs para o armazenamento, policiais e Correlacionamento utiliza o flexconnector do Linux.

Como é uma adaptação do sistema operacional FreeBSD, o conector do sistema operacional sobrepõe o do pfSense.

12.3. Plataformas de Virtualização: Acropolis/KVM

Conforme documentação do fabricante Nutanix sobre a solução Acropolis para hiperconvergência a forma de envio de logs para um sistema remoto (syslog) e/ou um SIEM é através da configuração de rsyslog via CLI (link de referência: <https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2>)

Na base de conhecimento não é citado nenhum tipo específico de SIEM ou solução de syslog para recebimento, assim, apenas um syslog e rsyslog, sendo assim, inferindo que qualquer sistema que coleta eventos via syslog é capaz de interpretar suas mensagens.

O documento também informa que diversos módulos podem ser configurados para envio via syslogs entre eles o módulo ACROPOLIS.

5. Choose a module to forward log information from and specify the level of information to collect.

```
<ncli> rsyslog-config add-module server-name=<remote_server_name> module-name=<module_name> level=<log_level>
```

Replace <module_name> with one of the following:

- ACROPOLIS - The acropolis services are responsible for task scheduling, execution, stat collection, publishing, etc. For more information, see [Acropolis Services in the Nutanix Bible](#).

Por se tratar de mensagens usando o padrão genérico utiliza os níveis padrão de um Syslog: INFO, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING e NOTICE. Também é disponibilizado um exemplo de mensagem que pode ser coletada:

For example, if you set level to INFO, it also covers the levels above it (i.e. EMERGENCY, ALERT, CRITICAL, ERROR, WARNING and NOTICE). If you select INFO for a module, you do not have to select any of the levels above it for the same module.

Note: CVMs send system audit logs to the syslog server by default even when no modules are configured for the server. Below is an example of these audit logs:

```
2021-09-09T08:56:01.353708-05:00 ntnx-xxx-cvm audispd[5307]: node=ntnx-xxx-cvm type=PROCTITLE msg=audit (1631195761.351:193118) :
proctitle=2F7573722F62696E2F707974686F6E322E37002D42002F686F6D652F6E7574616E69782F736572766963656162696C6974792F62696E2F7573696E672D67666C616773002F6
E7574616E69782F736572766963656162696C6974792F62696E2F63726F6E5F736572766963656162696C6974792E7079
```

Sendo assim, por se tratar de um Syslog padrão o Microfocus ArcSight pode utilizar o Smart Connector for Syslog padrão para a coleta de mensagens:

<https://www.microfocus.com/documentation/arc-sight/arc-sight-smartconnectors/pdfdoc/arc-sight-cef-syslog/arc-sight-cef-syslog.pdf>

No documento abaixo são informados os tipos de Syslogs e suas coletas:

https://www.microfocus.com/documentation/arc-sight/arc-sight-smartconnectors/AS_SmartConn_getstart_HTML/#GettingStarted/smartconn_type_syslog.htm%3FTocPath%3DTypes%2520of%2520SmartConnectors%7C_10

Desta forma, o ponto questionado pela empresa TELETEX como não atendido, na verdade fica demonstrado que sim, é atendido através da coleta padrão do ArcSight através de um SmartConnector para Syslog.

12.3. Plataformas de Virtualização: Oracle VM

Segundo informações do fabricante Oracle os arquivos de logs do Oracle VM são gerados em arquivos de texto (https://docs.oracle.com/cd/E50245_01/E50251/html/vmadm-tshoot-server-logs.html) conforme portal do fabricante Oracle e figura abaixo:

https://docs.oracle.com/cd/E50245_01/E50251/html/vmadm-tshoot-server-logs.html

Oracle® VM
Administrator's Guide for Release 3.3

6.2.1.2 Oracle VM Server Log Files

The Oracle VM Server log files you should check when troubleshooting problems with Oracle VM Server are listed in [Table 6.2 "Oracle VM Server log files"](#).

Table 6.2 Oracle VM Server log files

Log File	Purpose
xend.log	Contains a log of all the actions of the Oracle VM Server daemon. Actions are normal or error conditions. This log contains the same information as output using the xm log command. This file is located in the <code>/var/log/xen</code> directory.
xend-debug.log	Contains more detailed logs of the actions of the Oracle VM Server daemon. This file is located in the <code>/var/log/xen</code> directory.
xen-hotplug.log	Contains a log of hotplug events. Hotplug events are logged if a device or network script does not start up or become available. This file is located in the <code>/var/log/xen</code> directory.
qemu-dm_pid.log	Contains a log for each hardware virtualized guest. This log is created by the <code>quemu-dm</code> process. Use the <code>ps</code> command to find the <code>pid</code> (process identifier) and replace this in the file name. This file is located in the <code>/var/log/xen</code> directory.
ova-agent.log	Contains a log for Oracle VM Agent. This file is located in the <code>/var/log/</code> directory.
osac.log	Contains a log for Oracle VM Storage Connect plug-ins. This file is located in the <code>/var/log/</code> directory.
ovm-console.log	Contains a log for the Oracle VM virtual machine console. This file is located in the <code>/var/log/</code> directory.
ovmwatch.log	Contains a log for the Oracle VM watch daemon. This file is located in the <code>/var/log/</code> directory.

Copyright © 2014, 2017 Oracle and/or its affiliates. All rights reserved. [Legal Notices](#)

Assim para isso a MicroFocus disponibiliza conectores do tipo Flex Connector file reader ou folder reader que consistem em ler os arquivos e extrair as informações contida neles.

Conforme descrito em documento oficial do fabricante no link abaixo:

https://www.microfocus.com/documentation/arcSight/arcSight-smartconnectors/AS_SmartConn_getstart_HTML/#GettingStarted/smartconn_type_file.htm%3FTocPath%3DTypes%2520of%2520SmartConnectors%7C_3

12.8. VPN: OpenVPN

Abaixo estamos apresentando o código do Smart Connectors existente para coleta de OpenVPN, que se encontra disponível na comunidade do ArcSight um Flex Connector para coleta de eventos do OpenVPN, e transcrito abaixo:

```
-----
arcsight flexconnector openvpn
regex=(openvpn)\\[.*\\]:\\s(.*)

token.count=2
token[0].name=type
token[0].type=String
token[1].name=body
token[1].type=String

event.deviceVendor=__stringConstant("openvpn")
event.deviceProduct=__stringConstant("openvpn")
event.sourceUserPrivileges=__stringConstant("openvpn")
event.deviceProcessName=__stringConstant("openvpn")

event.flexString2=body
event.name=type
event.message=body
```

```
submessage.messageid.token=type  
submessage.token=body  
submessage.count=1
```

```
submessage[0].messageid=openvpn  
submessage[0].pattern.count=3
```

```
submessage[0].pattern[0].regex=(^[^V]+)\V(\d+.\d+.\d+.\d+:(\d+)\s+.*  
submessage[0].pattern[0].mappings=$1|$2|$3|$4  
submessage[0].pattern[0].fields=event.targetUserName,event.attackerAddress,event.attackerPort,event.message
```

```
submessage[0].pattern[1].regex=(\d+.\d+.\d+.\d+:(\d+)\s+.*  
submessage[0].pattern[1].mappings=$1|$2|$3  
submessage[0].pattern[1].fields=event.attackerAddress,event.attackerPort,event.message
```

```
submessage[1].pattern.count=1  
submessage[1].pattern[0].regex=(.*)  
submessage[1].pattern[0].fields=event.message  
submessage[1].pattern[0].extramappings=event.reason=__stringConstant("unparsed")
```

Por todo o exposto, pugna a recorrente, respeitosamente, pelo total provimento das razões apresentadas, e requer seja confirmada a decisão de declarar a empresa ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA. vencedora da licitação, nos termos da fundamentação.

Nestes termos, pede deferimento.

Brasília/DF, 02 de dezembro de 2021.

ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA
Frederico Almeida de Mendonça Küsel
Representante