Contratante: TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL - TRE / MS

Processo Administrativo n.º **0007345-36.2020.6.12.8000**

Pregão Eletrônico n.º **29/2021**

DECLARAÇÃO DE ATENDIMENTO

A Ata Comércio e Serviços de Informática, inscrita no CNPJ 09.571.988/0001-13, declara que através das Soluções ArcSight do fabricante Microfocus, que atende a todos os itens exigidos no Termo de Referência. Os documentos comprobatórios se encontram anexo nos documentos de habilitação e também no site do fabricante com endereço de hyperlink.

DOCUMENTAÇÃO TÉCNICA - REFERÊNCIA

Documentação técnica está contida em **7 pastas**, todos os arquivos são no formato "**pdf**", mas podem ser **acessados também em "HTML"** através de link informado. Os arquivos estão divididos nas pastas conforme estrutura de topicos 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.pdf

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.pdf
6.2 - ArcSight Enterprise Security Manager datasheet.pdf
6.3 - ArcSight Connector Supported Products.pdf
6.4 - ArcSight Connectors.pdf
6.5 - ArcSight Data Platform.pdf

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

https://www.microfocus.com/documentation/arcsight/arcsight-esm-7.5/#gsc.tab=0	Além do arquivo compactado (.zip) contendo os documentos off-line nas 5 pastas conforme supracitado, neste link todos estão disponíveis pelo Fabricante Microfocus.
https://community.microfocus.com/cyberres/productdocs/w/logger/38737/logger-documentation-list	
https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/#gsc.tab=0	

ITEM DO TERMO DE REFERÊNCIA	Atendimento	Documento, ou hyperlink	Página
DO OBJETO			
1. O presente Termo de Referência tem por objeto determinar as condições que disciplinarão a contratação de uma solução de software para gerenciamento de eventos e logs de segurança da informação (SIEM - Security Information and Event Management) com suporte e atualização.	Sim	6.2 - ArcSight Enterprise Security Manager datasheet.pdf	1 a 4
2. Aplicam-se à prestação dos serviços a serem contratados as condições indicadas neste Termo de Referência e na Minuta do Contrato, sendo estas complementadas, de forma subsidiária, pelas demais normas aplicadas ao objeto da contratação.	Sim	Serviço técnico da BlackBull Network, que irá respeitas exigências do TR.	
3. A contratação dos serviços objeto deste Termo de Referência será realizada mediante licitação, na modalidade de Pregão, em sua forma eletrônica, do tipo menor preço.	Sim	Comprovação não se aplica.	
ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO OFERTADA			
1. Todos os componentes da solução devem permitir sua instalação em ambiente virtual, servidores físicos de propósito genérico ou em *appliance* virtual especializado.	Sim	1.4 - Technical Requirements for ESM 7.5.pdf	6 e 7
		1.5 - Technical Requirements for ArcSight Platform 21.1.pdf	1 a 9
2. Deverá permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft *Active Directory* ou LDAP.	Sim	2.1 - Administrator's Guide for ESM 7.5.pdf	146
3. A solução deverá estar licenciada de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos atinja rajadas de três vezes o volume licenciado nas horas de pico.	Sim	7.2 Overview of SmartConnectors.pdf	14
4. A comunicação entre os componentes da solução deve ser feita através de criptografia, garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP.	Sim	2.1 - Administrator's Guide for ESM 7.5.pdf	95 a 99
5. Juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, a contratada deverá prover acesso a biblioteca de casos de uso do fabricante, que contenha conteúdo para download que inclua pacotes especializados de *dashboards* e coletores desenvolvidos pelo fabricante.	Sim	https://www.microfocus.com/en-us/support/ArcSight%20Enterprise%20Security%20Manager%20(ESM)	Base de informação e comunidades do fabricante.
6. A solução deverá implementar compressão dos eventos em cada fase do ciclo de vida do evento: transmissão, armazenamento online e *offline* dos eventos.	Sim	1.6 - ESM 101.pdf	25 28 e 29 30 a 32
7. O coletor da solução deverá ser capaz de coletar, aplicar *parsing* , normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real (*near-real-time*).	Sim	1.6 - ESM 101.pdf	17 e 18 28 e 29
8. Rotular eventos por zonas diferentes mesmo que estejam em redes com mesma faixa endereçamento IP.	Sim	1.6 - ESM 101.pdf	132 a 134
9. Será considerada nesse Edital a seguinte definição para conector: software desenvolvido e suportado pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações detalhadas de configurações de cada ativo suportado.	Sim	7.4 Overview of SmartConnectors.pdf	1 a 31
		7.1 A-Z-Config-Guides (pasta)	PDF por parsing de Fabricante.
		6.3 - ArcSight Connector Supported Products.pdf	1 a 8
10. Ajustar o horário dos eventos, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de sincronização de NTP (*Network Time Protocol*) com os servidores locais.	Sim	2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	639
11. Ofuscar os campos sensíveis dos eventos (como senhas, identidade funcional, números de cartões de crédito e outros similares).	Sim	2.1 - Administrator's Guide for ESM 7.5.pdf	22 e 23
		2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	619
		2.9 - ArcSight Administration and ArcSight System Standard Content Guide for ESM 7.5.pdf	11 e 12
12. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:	Sim	Comprovação apresentada nos subitens.	
1. Firewalls: Checkpoint R80.x, VMWare NSX, PfSense;	Sim	7.1 A-Z-Config-Guides / checkpoint-syslog-config.pdf	12 a 76
	Sim	6.3 - ArcSight Connector Supported Products.pdf	2, 4, e 6
2. Switches: HPE e Aruba;	Sim	6.3 - ArcSight Connector Supported Products.pdf	3 e 5

2. Switches: HPE e Aruba;	Sim	7.1 A-Z-Config-Guides / HPEArubaSyslogConfig.pdf	1 a 12
3. Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM;	Sim	6.3 - ArcSight Connector Supported Products.pdf	2 a 5
4. Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOs, Oracle Linux), Windows Server (2008, 2012, 2016) e FreeBSD; 5. Antivirus: TrendMicro, Clamav;	Sim	6.3 - ArcSight Connector Supported Products.pdf	1 a 8
6. Servidores de E-mail: Zimbra e Microsoft Exchange;	Sim	6.3 - ArcSight Connector Supported Products.pdf	3 e 5
7. Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e MicroSoft IIS 7 (ou superior);	Sim	7.1 A-Z-Config-Guides / Microsoft-IISSyslog.pdf	1 a 20
	Sim	6.3 - ArcSight Connector Supported Products.pdf	2, 4, 6
8. VPN: OpenVPN;	Sim	6.3 - ArcSight Connector Supported Products.pdf	4
13. Para coleta de logs deve suportar, no mínimo, os seguintes métodos:	Sim	Comprovação apresentada nos subitens.	
1. Syslog (UDP, TCP e TLS);	Sim	7.2 Overview of SmartConnectors.pdf	18
		1.6 - ESM 101.pdf	20, 25, 30
2. CIFS;	Sim	3.1 - ArcSight Command Center User's Guide for ESM 7.5.pdf	161, 178, e 179
3. FTP;	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	27., 353, 354 e 362
4. MySQL;	Sim	7.2 Overview of SmartConnectors.pdf	13
5. MS SQL;	Sim	7.2 Overview of SmartConnectors.pdf	13
6. Oracle;	Sim	7.2 Overview of SmartConnectors.pdf	13
7. API;	Sim	7.2 Overview of SmartConnectors.pdf	14
8. JSON;	Sim	6.2 - ArcSight Enterprise Security Manager datasheet.pdf	1
		2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	434 a 439
9. CEF;	Sim	7.2 Overview of SmartConnectors.pdf	25 e 26
14. Suportar a coleta de dados de no mínimo 250 (duzentos e cinquenta) tipo de ativos geradores de eventos distintos, com documentação completa individual por tecnologia.	Sim	6.4 - ArcSight Connectors.pdf	1 e 2
15. A solução deve permitir coletar dados de *feeds* externos.	Sim	6.3 - ArcSight Connector Supported Products.pdf	1
		2.10 - Micro Focus Security ArcSight Logger.pdf	25 e 680
16. Suportar o modo de criptografia em todos os conectores.	Sim	2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	662 a 664
		7.2 Overview of SmartConnectors.pdf	8 e 9
17. Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional.	Sim	2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	477
		7.2 Overview of SmartConnectors.pdf	7
18. A solução deve ser capaz de marcar (através de *tag*, *label* ou similar) os eventos com base em unidade organizacional: departamento, setor, secretaria ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento.	Sim	1.6 - ESM 101.pdf	33 e 34 114 a 118 156
19. A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único.	Sim	1.6 - ESM 101.pdf	31 a 35 75 e 76
20. O coletor da solução deverá ser capaz de armazenar os dados localmente (*cache*) em caso de indisponibilidade da comunicação com os destinos dos eventos.	Sim	1.6 - ESM 101.pdf	38
		2.9 - ArcSight Administration and ArcSight System Standard Content Guide for ESM 7.5.pdf	33 e 34
1. O envio dos dados em cache deve ocorrer imediatamente após a disponibilização do destino do evento.	Sim	1.6 - ESM 101.pdf	38
		2.9 - ArcSight Administration and ArcSight System Standard Content Guide for ESM 7.5.pdf	33 e 34

22. Deverá ter a capacidade de guardar eventos normalizados/tratados e brutos em forma comprimida.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	25
		2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	432 e 433
		2.1 - Administrator's Guide for ESM 7.5.pdf	42
23. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	242 a 245
		2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	531 a 536
		1.6 - ESM 101.pdf	81 87 a 90 145 E 149
24. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução.	Sim	1.6 - ESM 101.pdf	31 32 74 a 77
		2.10 - Micro Focus Security ArcSight Logger.pdf	25 e 26
25. A solução deve permitir múltiplos perfis de configuração.	Sim	1.6 - ESM 101.pdf	48
26. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.	Sim	1.6 - ESM 101.pdf	77 a 80
		2.1 - Administrator's Guide for ESM 7.5.pdf	59 e 61
27. Deverá implementar a coleta, processamento e correlação de informações de fluxo de rede Netflow v9/ SFlow.	Sim	7.2 Overview of SmartConnectors.pdf	16
		6.2 - ArcSight Enterprise Security Manager datasheet.pdf	1
		6.3 - ArcSight Connector Supported Products.pdf	3
28. A solução deverá realizar no conector a agregação de eventos semelhantes que ocorram dentro de um limite de tempo e quantidade de eventos específicos, devendo permitir agregar os eventos cuja única diferença seja o horário de ocorrência.	Sim	1.6 - ESM 101.pdf	36 e 37
		7.2 Overview of SmartConnectors.pdf	10
29. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução.	Sim	1.6 - ESM 101.pdf	18 a 20
30. Permitir a categorização manual de eventos (já normalizados) que não se encaixem em nenhuma categoria existente, cuja nova categoria poderá ser aplicada nos eventos futuros de mesma característica.	Sim	1.6 - ESM 101.pdf	34 a 36
31. No caso de a solução ofertada utilizar arquitetura distribuída, de forma a evitar a perda de eventos por sobrecarga ou indisponibilidade de correlacionadores, deverá fornecer função, interna ou externa, de balanceamento de cargas de serviço:	Sim	Comprovação apresentada nos subitens.	
1. O balanceamento de carga deverá implementar os métodos *Weighted Round Robin* ou *Round Robin*;	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	506 e 507
2. Prover um IP virtual ou definir nos agentes todos os servidores que fazem função de correlacionador como destino das fontes geradoras de eventos.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	505 e 506
3. Ao receber um evento, a solução deverá buscar um conector com capacidade de processamento disponível, de forma a garantir que não haverá perda de eventos por sobrecarga de conectores.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	505 a 507
32. Deverá armazenar no mínimo os seguintes dados: eventos, alertas, e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.	Sim	1.6 - ESM 101.pdf	76 e 77
33. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão.	Sim	1.6 - ESM 101.pdf	111 e 112
		2.10 - Micro Focus Security ArcSight Logger.pdf	92 a 94
34. Ter a capacidade de definir políticas diferentes de retenção dos dados on-line por tecnologia, conectores, dispositivos e *compliance*, ou seja, poderão ser definidos tempos de retenção diferentes para cada tipo de dados mantidos no banco de dados da solução, disponíveis para consulta imediata.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	26
35. De forma a permitir seu uso em auditorias e processos forenses, não deverá ser possível, sob nenhuma hipótese, a seleção, alteração e exclusão de eventos individuais.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	524 e 525
		1.6 - ESM 101.pdf	17 e 18 76 e 77
1. Deve ser possível apenas o expurgo de eventos conforme a política de retenção, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros.	Sim	1.6 - ESM 101.pdf	111 a 113
36. Permitir o expurgo dos dados de forma automática de acordo com a personalização do prazo de retenção que precede o expurgo.	Sim	1.6 - ESM 101.pdf	111 a 113

37. Deverá permitir a utilização de volumes de armazenamento locais e externos. Deverá permitir a segregação de tipos de eventos diferentes em grupos lógicos de armazenamento diferentes, com políticas de retenção diferentes, de forma a permitir a otimização de performance.	Sim	1.6 - ESM 101.pdf	77 a 80
38. Deverá permitir exportar eventos para formato pdf e csv.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	29
		2.10 - Micro Focus Security ArcSight Logger.pdf	213 e 214
		1.6 - ESM 101.pdf	93
1. Deverá permitir que o usuário defina quais campos do evento serão exportados.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	29 a 31
39. Deverá implementar funcionalidade de ajuda (helper) para facilitar a criação de queries.	Sim	1.6 - ESM 101.pdf	103 a 105
40. Deverá implementar assistente gráfico para criação de queries.	Sim	1.6 - ESM 101.pdf	103 a 105
41. Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas.	Sim	1.6 - ESM 101.pdf	93 e 94
42. Deverá implementar alertas por syslog, SNMP e e-mail.	Sim	1.6 - ESM 101.pdf	49
		2.10 - Micro Focus Security ArcSight Logger.pdf	394 e 395
		2.10 - Micro Focus Security ArcSight Logger.pdf	403 a 405
43. Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	165 e 169
44. Possuir relatórios pré-configurados (templates) separados em categorias.	Sim	1.6 - ESM 101.pdf	103 a 109
45. Deverá suportar pelo menos 03 dos seguintes formatos de relatórios: html, pdf, csv, doc, xls, xml e zip.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	213 e 214
46. Permitir o agendamento de geração de relatórios e o envio dos mesmos por e-mail.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	217 e 218
47. Possuir ferramenta ou interface gráfica para desenho de modelos de relatórios ou *dashboards* personalizados.	Sim	1.6 - ESM 101.pdf	85 a 92
48. Apresentar painéis de controles gráficos (*dashboards*) que mostrem o status do ambiente, dos logs de eventos, além de apresentar resultados de consultas tempestivas, quando se fizerem necessárias.	Sim	1.6 - ESM 101.pdf	86 a 92
49. Deverá implementar tecnologia de pesquisa distribuída nos múltiplos elementos (componentes) da solução.	Sim	1.6 - ESM 101.pdf	93
50. Apresentar relatórios de eventos, alertas e incidentes em nível técnico (analítico, *drill down*) e gerencial (sintético / *dashboards*).	Sim	1.6 - ESM 101.pdf	22 e 23
51. Permitir pesquisa nos eventos, e a partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e permitir o *drill-down* (detalhamento) até o nível dos dados brutos (*raw*), para efetiva investigação de incidentes, identificação de causa raiz e análise forense.	Sim	1.6 - ESM 101.pdf	22 e 23
52. Possuir conformidade com as normas ISO 27001 e LGPD.	Sim	6.1 -Security ArcSight Compliance Insight Package for IT Governance.pdf	1 e 2
53. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria devidamente reconhecidos como seguros.	Sim	1.6 - ESM 101.pdf	112
54. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.	Sim	1.6 - ESM 101.pdf	75 e 77
55. Deverá permitir que os campos de logs de dispositivos diferentes estejam presentes no mesmo resultado, bem como deverá ser possível a seleção dos campos que estarão presentes no resultado.	Sim	1.6 - ESM 101.pdf	98 a 109
56. Deverá permitir acrescentar campos de uma fonte em outra fonte.	Sim	1.6 - ESM 101.pdf	99 a 109
57. Deverá ser fornecido com solução de gerenciamento central com as seguintes características mínimas:	Sim	Comprovação apresentada nos subitens.	
1. Deverá implementar, de forma centralizada, a configuração de políticas e a monitoração de todos os conectores e da solução de centralização de eventos;	Sim	1.6 - ESM 101.pdf	15 a 27
2. Deverá permitir a implementação de atualização e distribuição de novas políticas de segurança pelos elementos/componentes gerenciados;	Sim	1.6 - ESM 101.pdf	15 a 27
3. Deverá possuir regras de monitoração pré-configuradas, as quais podem ser editadas ou apagadas;	Sim	1.6 - ESM 101.pdf	15 a 27
4. Deverá interagir diretamente com a biblioteca de casos de uso do fabricante da solução para download e atualizações de conteúdo;	Sim	1.6 - ESM 101.pdf	15 a 27
5. Deverá possuir interface WEB acessível por HTTPS e CLI por SSH, com suporte ao padrão UTF-8;	Sim	1.6 - ESM 101.pdf	15 a 27
6. Deverá possuir tela de monitoração com as seguintes características:	Sim	1.6 - ESM 101.pdf	15 a 27
1. Tabela com percentuais e gráfico de pizza do status dos elementos/componentes monitorados agregados por tipo, mostrando o número de elementos em cada estado, bem como o número total de nós;	Sim	1.6 - ESM 101.pdf	15 a 27 85

2. Listagem de todos os elementos/componentes que estão reportando problemas;	Sim	1.6 - ESM 101.pdf	15 a 27
3. Permitir a visualização do sumário de monitoração por tipo de produto;	Sim	1.6 - ESM 101.pdf	15 a 27
58. Deverá possuir tela de gerenciamento de configuração para gerenciar e criar configurações, sincronizar a configuração entre componentes/elementos e automatizar a configuração inicial dos mesmos.	Sim	1.6 - ESM 101.pdf	23 a 27
59. Deverá permitir o *backup e* a restauração da configuração da solução de gerenciamento, assim como a configuração de usuários e grupo de usuários.	Sim	5.1 - Backup and Recovery Tech Note for Compact and Distributed Mode for ESM 7.5.pdf	1 a 16
60. Deverá ser possível visualizar o consumo de licenças da solução.	Sim	1.3 - Quick Start Guide to Reporting EPS Usage.pdf	5 e 6
61. Deverá permitir a visualização das taxas em eventos por segundo (EPS), *flows* por minuto (FPM) ou volume de dados diário (conforme a métrica adotada pela solução) de entrada e de saída de cada conector.	Sim	1.3 - Quick Start Guide to Reporting EPS Usage.pdf	1 a 11
62. Deverá permitir a visualização dos dispositivos gerenciados por localização, host e tipo.	Sim	1.6 - ESM 101.pdf	85 a 92
63. Permitir adição, visualização, edição e exclusão da localização de dispositivos.	Sim	1.6 - ESM 101.pdf	85 a 92
64. Permitir a adição de atributos de um dispositivo, a importação de dispositivos a partir de um arquivo CSV, visualização e remoção de dispositivos, visualização de todos os dispositivos de uma localidade e varredura (*scan*) de dispositivos para detecção de novos conectores.	Sim	1.6 - ESM 101.pdf	22 a 27
65. Deverá permitir a apresentação de árvore hierárquica de dispositivos.	Sim	1.6 - ESM 101.pdf	85 a 92
66. Deverá apresentar para cada dispositivo: nome ou endereço IP, versão do agente (se aplicável), status de problemas encontrados no dispositivo, modelo, tipo e versão.	Sim	1.6 - ESM 101.pdf	114 a 125
67. Deverá implementar as seguintes ações nos elementos/componentes de centralização de logs: *reboot* , *shutdown* , *upgrade* remoto, editar ou remover a configuração, configurar um ou múltiplos elementos/componentes.	Sim	2.10 - Micro Focus Security ArcSight Logger.pdf	46 a 73
68. Deverá implementar o gerenciamento de conectores: adição, edição de conectores, atualização de parâmetros, gerenciar os destinos e *failover* de logs de múltiplos conectores, gerenciamento de configurações em lote, envio de comandos, visualização interativa de diagnóstico, edição de conectores customizados, compartilhamento de conectores, download e upload de conectores.	Sim	1.6 - ESM 101.pdf	15 a 27
		3.1 - ArcSight Command Center User's Guide for ESM 7.5.pdf	149 a 195
69. Deverá ser fornecido com os seguintes modelos para o desenvolvimento de conectores customizados: arquivo, banco de dados por ID, múltiplos bancos de dados, expressão regular para arquivo, expressão regular para pasta de arquivos, SNMP, banco de dados por tempo e arquivo xml.	Sim	2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	600 a 604
70. Deverá permitir o gerenciamento dos eventos arquivados.	Sim	2.2 - Administrator's Guide to ArcSight Platform 21.1.pdf	450 a 461
71. Deverá permitir o gerenciamento de *peers* de centralizadores de logs.	Sim	1.6 - ESM 101.pdf	21, 93, 164, 165 e 166
72. Deverá permitir que a configuração dos elementos/componentes seja criada diretamente na solução de gerenciamento, importada de um elemento ativo e enviada a múltiplos elementos gerenciados.	Sim	1.6 - ESM 101.pdf	15 a 27
73. Deverá permitir a comparação de duas configurações e a checagem de configurações ativas com a configuração definida como base para aquele elemento/componente.	Sim	1.6 - ESM 101.pdf	15 a 27
74. Deverá possuir o conceito de subscrição de configurações, em que elementos subscritos recebem em conjunto as configurações atualizadas ou novas diretamente da solução de gerenciamento.	Sim	2.1 - Administrator's Guide for ESM 7.5.pdf	205 a 208
75. Deverá permitir a configuração de usuários e grupos de usuários, seus dispositivos associados e os respectivos privilégios (administrador, relatórios, pesquisas, operação, gerenciamento).	Sim	1.6 - ESM 101.pdf	10 e 14
76. Deverá implementar *dashboards* com funcionalidade de *drill down* para visualização do status dos dispositivos monitorados, incluindo informações de uso de CPU, fluxo de eventos, e estatísticas de utilização de disco, consumo do licenciamento.	Sim	1.6 - ESM 101.pdf	85 a 97
77. Deverá implementar visão de topologia que apresente graficamente, a relação entre os dispositivos de origem dos eventos, os conectores e os destinos, com a visualização do status, tipo de dispositivo, número de dispositivos de cada tipo, dispositivos ativos e inativos, tráfego em EPS/volume de dados.	Sim	1.3 - Quick Start Guide to Reporting EPS Usage.pdf	5 a 7
		2.1 - Administrator's Guide for ESM 7.5.pdf	49, 52, e 231
		2.9 - ArcSight Administration and ArcSight System Standard Content Guide for ESM 7.5.pdf	29 73 a 74
78. O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores.	Sim	1.6 - ESM 101.pdf	77 a 80
79. O correlacionador deve efetuar a análise dos eventos em near real-time (tempo próximo ao real).	Sim	1.6 - ESM 101.pdf	77 a 80 90 a 93
80. Deve permitir ao administrador a criação de novas regras e a edição das existentes.	Sim	1.6 - ESM 101.pdf	23 a 27 67 e 70
81. O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido.	Sim	1.6 - ESM 101.pdf	23 a 27 67 e 70
82. O correlacionador deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e que não foram previstos ou observados anteriormente.	Sim	1.6 - ESM 101.pdf	24 a 27 67 e 70
83. O correlacionador deve permitir a correlação de eventos e alertas com dados existentes em listas (*watchlist*). Deve permitir também a criação de novas listas e a personalização das existentes.	Sim	1.6 - ESM 101.pdf	77 a 93
84. O correlacionador deve permitir a execução das regras agendadas contra eventos passados para análise histórica de atividades suspeitas, que executam em frequência e horário específico.	Sim	1.6 - ESM 101.pdf	78 a 93
85. O correlacionador deve ter a capacidade de fazer a correlação entre eventos oriundos de:	Sim	Comprovação apresentada nos subitens.	

1. Agentes (ou solução similar) ou coletores de outros correlacionadores;	Sim	1.6 - ESM 101.pdf	19 34 a 37 59 69 e 70
		- ArcSight Connector Supported Products.pdf	1 a 8
2. Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);	Sim	1.6 - ESM 101.pdf	19 34 a 37 59
		- ArcSight Connector Supported Products.pdf	1 a 8
3. Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);	Sim	1.6 - ESM 101.pdf	19 34 a 37 59
		- ArcSight Connector Supported Products.pdf	1 a 8
4. Ativos e Banco de Dados (por exemplo, catraca e consultas (queries) a banco de dados);	Sim	1.6 - ESM 101.pdf	19 34 a 37 59
		- ArcSight Connector Supported Products.pdf	1 a 8
86. O correlacionador deve ser capaz de inserir os alertas gerados no próprio fluxo de correlação ou no fluxo de eventos. Deve permitir a correlação de tais alertas/eventos, derivados de alertas, com novos eventos e/ou regras, no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade.	Sim	1.6 - ESM 101.pdf	78 a 93
87. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:	Sim	Comprovação apresentada nos subitens.	
1. Severidade do evento;	Sim	1.6 - ESM 101.pdf	32
2. Criticidade do ativo;	Sim	1.6 - ESM 101.pdf	40, 41, e 84
3. Existência de vulnerabilidade no ativo;	Sim	1.6 - ESM 101.pdf	84, 148
88. Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno.	Sim	1.6 - ESM 101.pdf	98 a 108
89. Possuir a funcionalidade de definição de prioridade para os eventos, alertas e incidentes.	Sim	1.6 - ESM 101.pdf	148 a 152
90. Como resultado da aplicação de regras, o correlacionador deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comandos e abrir caso na ferramenta de incidentes interna.	Sim	1.6 - ESM 101.pdf	23 a 26 107 a 109
91. O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução.	Sim	1.6 - ESM 101.pdf	112 e 113
92. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede.	Sim	1.6 - ESM 101.pdf	98 a 108
93. A solução deve incluir regras pré-programadas (out-of-the-box) tanto para normalização de logs quanto para correlação de eventos, bem como permitir que se escrevam / definam regras próprias / personalizadas.	Sim	1.6 - ESM 101.pdf	15
94. Fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados na correlação de eventos.	Sim	1.6 - ESM 101.pdf	15 e 16 49 a 51
95. A solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo.	Sim	3.2 - ArcSight Console User's Guide for ESM 7.5.pdf	59
		1.6 - ESM 101.pdf	53 a 80
96. A correlação de eventos deve possuir uma linha de base (*baseline*) comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal.	Sim	1.6 - ESM 101.pdf	90 a 93
97. A solução deve possuir a capacidade de prover contextualização de dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em um único console, otimizando com isso a capacidade e prazos de análise no processo de resposta a incidentes de segurança.	Sim	1.6 - ESM 101.pdf	49 a 52 98 a 108
98. A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo definidos pela contratada.	Sim	1.6 - ESM 101.pdf	40, 41, e 84
99. Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis.	Sim	2.1 - Administrator's Guide for ESM 7.5.pdf	95 a 99
100. Manter seu próprio log de auditoria.	Sim	1.6 - ESM 101.pdf	76 e 77
101. Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;	Sim	7.2 Overview of SmartConnectors.pdf	14
102. Permitir testar as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução, sem afetar a execução das regras em produção.	Sim	1.6 - ESM 101.pdf	15 e 16 49 a 51
103. Permitir a inserção manual de anotações em alertas.	Sim	1.6 - ESM 101.pdf	44 a 46
104. A solução deve ser capaz de notificar os administradores, ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.	Sim	1.6 - ESM 101.pdf	49 a 51 53 a 80
105. Deve permitir a visualização de eventos e alertas de segurança em tempo próximo ao real, sem necessidade de refazer consultas no banco de dados e/ou *storage* para atualização das visualizações (atualização da visualização de eventos e alertas de segurança em contexto de memória).	Sim	1.6 - ESM 101.pdf	76 e 77
		3.1 - ArcSight Command Center User's Guide for ESM 7.5.pdf	17 a 30

106. Deverá se integrar com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente. Deve permitir o registro de ações tomadas e planejadas.	Sim	3.1 - ArcSight Command Center User's Guide for ESM 7.5.pdf	35 e 36
		https://community.microfocus.com/cyberres/b/sws-22/posts/arcsight-esm-participates-in-mitre-engenuity-att-ck-evaluations	
DA INSTALAÇÃO DA SOLUÇÃO			
1. A solução, deverá ser instalada no prédio-sede do TRE/MS, sito na Rua Desembargador Leão Neto do Carmo, n.º 23, Parque dos Poderes, Campo Grande-MS, das 12:00h às 18h.	Sim	Serviço técnico da BlackBull Network, que irá respeitas exigências do TR.	
1. A empresa deverá agendar previamente o dia, horário e local para a instalação da solução que, no primeiro momento se tratará dos subitens 1.1, 1.3 e 1.5, no horário das 12:00h às 18:00h, de segunda à sexta-feira, através do telefone (67) 2107- 7123 (Ulysses Almeida Neto ou Gustavo Pinho).	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
2. O treinamento previsto no subitem 1.6 também deverá ser agendado previamente, após a instalação dos subitens 1.1, 1.3 e 1.5.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
3. Os subitens 1.2 e 1.4 serão exeutados sob demanda, ou seja, apenas se verificado a insuficiência dos demais itens da solução.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
2. Nos termos do inciso III, art. 3º do Decreto nº 7.174/2010, para os produtos importados será exigido, no momento da entrega, a comprovação de origem dos mesmos e a quitação dos tributos de importação a eles referentes, sob pena de rescisão contratual e multa.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
3. O PRAZO MÁXIMO DA INSTALAÇÃO E TREINAMENTO DA SOLUÇÃO (SUBITENS 1.1, 1.3, 1.5 e 1.6) será de, no máximo, 15 (quinze) dias, contados do dia útil subsequente à mensagem eletrônica responsável pelo encaminhamento da nota de empenho e/ou da Requisição de fornecimento.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
1. Caso a Nota de Empenho e/ou Requisição de fornecimento seja encaminhado através de serviço postal, fax ou outro meio disponível, a contagem do prazo se dará através da comprovação do efetivo recebimento do instrumento por parte do licitante.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
2. Fica a licitante vencedora obrigada a enviar aviso de recebimento das mensagens eletrônicas que lhes são enviadas. Caso não o faça, considerar-se-á ciente do seu conteúdo, no 1º dia útil seguinte ao seu envio.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
4. Caso a empresa verifique a impossibilidade de cumprir com o prazo de entrega estabelecido, deverá encaminhar ao TRE/MS solicitação de prorrogação de prazo de entrega, da qual deverão constar: motivo do não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
1. A comprovação de que trata esta cláusula deverá ser promovida não apenas pela alegação da empresa contratada, mas por meio de documento que relate e justifique a ocorrência que ensejará o descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
5. A solicitação de prorrogação de prazo será analisada pelo TRE/MS na forma da lei e de acordo com os princípios de razoabilidade e proporcionalidade, informando-se à empresa da decisão proferida.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
6. Em caso de denegação da prorrogação do prazo de entrega, e caso não cumpra o prazo inicial, o fornecedor ficará sujeito às penalidades previstas para atraso na entrega.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
7. O recebimento provisório e definitivo dos materiais será de responsabilidade da Equipe de Apoio à contratação, designada nos estudos preliminares desta contratação, conforme descrito a seguir:	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
1. apresentação do documento fiscal, com identificação do fornecedor e do comprador (TRE/MS), descrição do equipamento entregue, quantidade, preços unitário e total; e	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
2. compatibilidade do equipamento entregue com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
8. Atendidas as condições indicadas na cláusula 7 acima, será registrado o recebimento provisório mediante atestado no verso da Nota Fiscal, ou, em termo próprio.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
1. O atestado de recebimento registrado em canhoto de nota fiscal, ou documento similar, não configura o recebimento definitivo do material.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	
9. O recebimento definitivo deverá ser efetuado em até 10 (dez) dias úteis, contados da data do recebimento provisório, satisfeitas as condições abaixo:	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.	

1. correspondência de nome da solução com os indicados na nota de empenho ou proposta da fornecedora;	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.
2. compatibilidade dos subitens com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.
3. realização de testes, quando previstos no Termo de Referência ou caso a unidade recebedora entenda necessário;	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.
4. conformidade do documento fiscal quanto à identificação do comprador (TRE/MS), descrição da solução, quantidade, preços unitário e total.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.
10. Verificada alguma falha no fornecimento, será feito o registro formal e informado à empresa fornecedora, para que proceda à sua correção no prazo de até 5 (cinco) dias úteis.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.
1. Ao prazo previsto neste item, aplica-se o disposto nos itens 4 a 6 deste Capítulo.	Sim	Serviço técnico da licitante BlackBull Network, comprovando através de Atestados técnicos.