ESTADO DO RIO GRANDE DO SUL
POLÍCIA CIVIL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL
DIVISÃO DE ASSESSORAMENTO ESPECIAL

ANEXO C - SISTEMA DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA (SIEM)

1. DA DEFINIÇÃO

1.1. O SIEM é uma solução que ajuda as organizações a detectar, analisar e responder a ameaças de segurança antes que elas prejudiquem as operações da organização.

1.2. A tecnologia SIEM coleta dados de log de eventos de várias fontes, identifica atividades que se desviam da norma com análise em tempo real e toma as medidas apropriadas.

1.3. Em suma, o SIEM oferece as organizações visibilidade das atividades nas redes delas para que elas possam responder rapidamente a possíveis ataques cibernéticos e atender aos requisitos de conformidade.

2. DOS REQUISITOS

2.1. O sistema deve possuir arquitetura para alta disponibilidade e escalabilidade, suportando a implementação com múltiplos servidores/instâncias em operação simultânea, com redundância dos dados coletados e indexados.

2.2. A solução deve possibilitar a atualização, de modo a refletir a ocorrência de novas políticas de alarme, atualizações de padrões de logs de tecnologias ou escopo monitorado.

2.3. A solução deve armazenar os logs por 3 meses no modo online e 9 meses no modo off-line.

2.4. A solução oferecida deverá obrigatoriamente fazer parte do Quadrante Mágico do Gartner mais atual.

2.5. Detectar anomalias de comportamento com base em alterações em uma linha de base e estatísticas.

Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS
CEP: 90040-001 - Fone: 51 3288-2116
E-mail: dtip-dae@pc.rs.gov.br

ESTADO DO RIO GRANDE DO SUL
POLÍCIA CIVIL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL
DIVISÃO DE ASSESSORAMENTO ESPECIAL

2.6. Deve rastrear e identificar ameaças através de inteligência artificial ou aprendizado de máquina.

2.7. Possibilitar a integração para abertura de chamados automaticamente a partir do evento.

2.8. Possibilitar a integração com outras plataformas de segurança através de API.

2.9. Deve permitir a criação de políticas para gestão do espaço consumido em disco, com definições de prioridades de performance e longevidade do armazenamento.

2.10. Indexar todos os dados assim que são recebidos, organizados em índices ou estrutura similar.

2.11. Deve disponibilizar mecanismo de busca de dados armazenados, seja com busca textual ou com linguagem específica.

2.12. Possibilitar notificações e alarmes parametrizados pelos administradores.

2.13. Permitir comunicação criptografada com clientes e sistemas integrados.

2.14. Deve permitir a criação de Dashboards com visualizações/gráficos de grafos, pizza, linha, área e barra. Tais visualizações devem ser atualizadas **próximo ao tempo real**, assim que o sistema indexa novos dados.

2.15. Permitir integração para autenticação com Active Directory (AD) e/ou LDAP.

2.16. Permitir a segregação de funções para gestão da solução.

2.17. Possuir relatórios pré-prontos com indicadores.

2.18. Possibilitar a produção de relatórios personalizados.

2.19. Possuir relatórios de conformidade (LGPD, GDPR).

2.20. Suportar o modo de criptografia em todos os conectores com 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.

Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS
CEP: 90040-001 - Fone: 51 3288-2116
E-mail: dtip-dae@pc.rs.gov.br

2.21. A coleta de eventos de dispositivos (ativos geradores de eventos) não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como CSV, arquivo texto, JSON, XML, SYSLOG, ODBC, JDBC, SNMP TRAP v1, v2c e v3, entre outros.

2.22. Garantir a integridade e inviolabilidade dos eventos coletados.

2.23. Em caso de solução on-premises, poderá ser um servidor físico ou virtual, desde que atenda aos requisitos deste TR.

2.24. Cabe a CONTRATANTE o fornecimento das máquinas virtuais para instalação do sistema, de acordo com requisitos do fabricante.

2.25. A instalação deve ser feita no ambiente da CONTRATANTE pela CONTRATADA dos módulos necessários para que a solução atenda aos requisitos deste TR.

2.26. Deve coletar os logs da respectiva infraestrutura, não limitando-se às quantidades informadas:

2.26.1. 6 (seis) Hypervisor VMware ESXi.

2.26.2. 120 (cento e vinte) Linux Servers.

2.26.3. 15 (quinze) Windows Servers.

2.26.4. 8000 (oito mil) Workstations.

2.26.5. 1 (um) Storage scale-out NAS.

2.26.6. 1 (um) Appliance Backup/Data Protection.

2.26.7. 1500 (mil e quinhentos) Network Switches.

2.26.8. 10 (dez) Network Wireless LAN.

2.26.9. 2 (dois) Network Firewalls.

2.26.10. 2 (dois) Network IPS/IDS.

2.26.11. 4 (quatro) Network Web Proxy.

2.26.12. 4 (quatro) Network VPN.

2.26.13. 2 (dois) Web Application Firewalls.

2.26.14. 4 (quatro) Network Load Balancers.

2.26.15. 60 (sessenta) WebServers.

2.26.16. 15 (quinze) Database.

2.26.17. 2 (dois) Antivirus, DLP, EDR, etc.

2.26.18. 4 (quatro) Servidores DHCP.

2.26.19. 1 (uma) Solução de MFA.

2.26.20. 6 (seis) Soluções de DNS.

2.26.21. 1 (uma) Solução LDAP.

2.26.22. 1 (uma) Solução de Inventário.

2.26.23. 1 (uma) Solução de distribuição de patches.

2.26.24. 1 (uma) Solução de Honeypot.

2.26.25. 1 (uma) Solução de Server Host Intrusion Detection/Prevention (HIPS) Solutions.

2.26.26. 10000 (dez mil) Users.

3. CARACTERÍSTICAS GERAIS

3.1. A solução de segurança proposta deverá ter sido desenvolvida por um único fabricante de modo que tanto o suporte da solução, quanto as funcionalidades sejam integradas e 100% compatíveis.

3.2. O licenciamento da solução SIEM deverá ser em nome da CONTRATANTE e não deverá ter limitador de consumo ou o formato de licenciamento deverá ser por volume de pico de 7.000 Eventos por segundo e considerar no contrato o crescimento anual de 10% deste volume de eventos.

3.3. Todo o gerenciamento dos componentes e funções administrativas devem ser feitas através de uma única interface web, acessível por navegador, sem a necessidade de instalação de aplicação adicionais.

3.4. A solução de SIEM precisa ter na console o módulo de fluxos de redes (NDR) disponível de forma nativa, possibilitando no futuro a ativação como modulo adicional na mesma console.

3.5. A solução deverá ser fornecida para instalação e uso no idioma Português Brasil (pt_br) e Inglês.

3.6. As soluções que processam flows da mesma forma que processam logs, devem considerar que para cada conexão IP os geradores de flows como: NetFlow, IPFix e AWS VPC Flow, geram duas mensagens de flows (inbound+outbound), e, em uma console única.

3.7. Deve-se considerar que ao longo do tempo um mesmo flow de rede (NetFlow, sFlow, jFlow e IPFIX) poderá ser atualizado pelo gerador de flows.

3.8. A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real.

3.9. Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução.

3.10. Deve permitir a definição de metadados customizados/personalizados, para extrair dados existentes na linha de log (raw), usando recursos como expressões regulares ou algum recurso gráfico para essa extração.

3.11. Propriedades customizadas devem poder ser usadas em regras de correlação online e em regras de correlação histórica.

3.12. Permitir a agregação de eventos semelhantes.

3.13. Gerar alertas/incidentes com base nas regras definidas previamente.

3.14. Deverá ser fornecido com módulo integrado para o gerenciamento dos incidentes identificados pela solução.

3.15. Deve permitir armazenar os eventos, inclusive os normalizados, de forma compactada.

3.16. Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema.

3.17. Os painéis gráficos (dashboards) devem ser customizáveis, por usuário.

3.18. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento.

3.19. Permitir a visualização, na interface web, dos eventos relacionados a um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução.

3.20. Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog.

3.21. Ter a capacidade de reenviar os logs e flows, em formato nativo, para outros sistemas em tempo real.

3.22. Ter a capacidade de reenviar eventos já normalizados para outros sistemas de correlacionamento em tempo real.

3.23. Deve permitir filtrar e selecionar os eventos que serão inseridos na solução.

3.24. Normalizar e categorizar os eventos em um padrão único que será usado pela solução.

3.25. Possuir suporte nativo, suportado pelo fabricante, para coleta, reconhecimento e normalização de pelo menos, 350 tipos de fontes de dados logs.

3.26. Deve possuir no mínimo 450 regras de correlação online, especializadas na detecção de incidentes de segurança, produzidas, suportadas e atualizadas pelo fabricante da solução.

3.27. Tratar eventos em formato “comprimido” (zip, gz, tar.gz), sem a necessidade da descompressão manual.

3.28. Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado.

3.29. Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento.

3.30. Um único componente da solução deve ser capaz de coletar, processar e normalizar tanto os eventos de segurança e eventos de negócio (não relacionados à segurança).

3.31. Tanto os eventos de segurança quanto os de negócios devem ser normalizados para um único padrão de eventos.

3.32. A solução deve permitir a integração de dispositivos ou logs não suportados nativamente.

3.33. A integração de logs ou dispositivos deve ser realizada na interface web, com o uso de expressões regulares, JSON, XML, Chave/valor e recurso similar, sem exigir o uso de linguagens de programação ou scripts.

3.34. Deve permitir a criação automática de data sources pela detecção do tipo de fonte do log, dentre as nativamente suportadas, enviados via Syslog.

3.35. Deve permitir a criação automática de data sources pela detecção do tipo de fonte do log, dentre os tipos de logs customizados na solução, quando enviados via Syslog.

4. RELATÓRIOS

4.1. A solução deve apresentar, no mínimo as seguintes características relacionadas a geração de relatórios:

4.1.1. Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede.

4.1.2. Deve possuir relatórios de conformidade com normas reguladoras do mercado, no mínimo: SOX, PCI 2.0 e ISO-27001.

4.1.3. Deve permitir a criação de relatórios relacionados a: incidentes, logs, flows de rede, vulnerabilidades.

4.1.4. Deve possuir relatórios classificados em grupos temáticos, permitindo a criação novos agrupamentos de relatórios pelo usuário.

4.1.5. Deve permitir a customização de novos relatórios baseados em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes.

4.1.6. Deve gerar relatórios de eventos, alertas/incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF, HTML, XLS, CSV e XML.

4.1.7. Permitir o agendamento de relatórios de forma periódica e notificar/enviar automaticamente por e-mail os relatórios gerados para os destinatários dos mesmos.

4.1.8. Os usuários devem poder visualizar apenas os seus próprios relatórios ou relatórios disponibilizados por outros usuários, os administradores devem poder visualizar todos os relatórios.

4.1.9. Deve ser possível definir perfis de usuários com permissão/restrição de edição dos modelos de relatórios.

4.1.10. Deve ser possível realizar relatórios baseados em dados com IPv6.

4.1.11. A funcionalidade de cópia de segurança deve preservar os dados de relatórios.

4.1.12. Os relatórios nativos da solução devem poder ser editados e duplicados para novos relatórios.

4.1.13. Deve permitir a geração de relatórios que contenham os eventos associados a um incidente detectado por regras de correlação.

5. MÓDULO DE USER BEHAVIOR ANALYTICS (UBA)

5.1. Componente ou módulo especializado na monitoração de desvios de comportamento dos usuários e o risco envolvido.

5.2. O módulo de User Behavior Analytics (UBA) deve ser licenciado para processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM.

5.3. Deve integrar nativamente com a solução de SIEM e ser capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco.

5.4. Deve ser capaz de importar dados de usuário em bases LDAP, CSV e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail e cargo.

5.5. Deve permitir a definição de atributos customizados na importação do usuário via LDAP.

5.6. O modelo de análise de comportamento do usuário usando modelos de Machine Learning, deve abranger a análise/retenção dos dados no mínimo por 30 dias, permitindo uma análise abrangente do usuário.

5.7. Deve permitir a criação de modelos customizados de machine learning para a identificação de desvios de comportamento do usuário.

5.8. Deve permitir selecionar usuários que não devem fazer parte da análise com modelos de Machine Learning.

5.9. Permitir a criação de listas de observação com os principais usuários sob monitoração.

5.10. Deve possibilitar a inclusão de usuários nas listas de observações selecionando aqueles já existentes na solução de UBA que combinem com uma expressão regular ou similar.

5.11. Deve permitir a isenção de determinadas identidades do processo de score de risco.

5.12. Essas identidades não teriam riscos computados relacionados as suas atividades.

5.13. Deve permitir a inclusão de anotações dentro da monitoração de cada identidade com o objetivo de melhor gerenciamento de risco e do histórico e ações tomadas.

ESTADO DO RIO GRANDE DO SUL
POLÍCIA CIVIL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL
DIVISÃO DE ASSESSORAMENTO ESPECIAL

5.14. Deve possuir dashboards dos usuários com maior pontuação de risco e realizar um drill down para entender quais as categorias de risco e as ações que contribuíram para o score atual.

5.15. Deve permitir ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou precisam ser monitoradas.

5.16. A monitoração de desvios de comportamento de usuário deve detectar no mínimo:

5.16.1. Tentativa de acesso a contas suspensas e desabilitadas.

5.16.2. Usuário vítima de phishing.

5.16.3. Acesso negado repetido.

5.16.4. Usuário acessando a VPN a partir de uma localidade atípica.

5.16.5. Usuário acessando a VPN a partir de horários atípicos.

5.16.6. Conta utilizada numa quantidade atípica de atividades.

5.16.7. Acesso a máquinas Linux e Windows com contas de serviço.

5.16.8. Primeiro uso de um recurso importante por um usuário.

5.16.9. Acesso a endereços considerados suspeitos por bases de Threat feed/IP Reputation.

5.16.10. Detecção de comandos em blacklist por um usuário.

5.16.11. Conta de usuário criada e deletada rapidamente.

5.16.12. Detecção de ataque de negação de serviço pela deleção de contas.

5.16.13. Conta anômala criada a partir de uma nova localização.

5.16.14. Conta anômala em Cloud, criada a partir de uma nova localização.

5.16.15. Detecção de comportamento de Ransomware.

5.16.16. Múltiplos bloqueios em upload de arquivos, seguido de um upload com sucesso.

5.17. Compliance para General Data Protection Regulation (GDPR) ou Lei Geral de Proteção a Dados (LGPD).

5.18. Deve ser capaz de aprender de forma supervisionada ou não supervisionada os comportamentos dos usuários.

5.19. Deve permitir o uso LDAP/AD para definição de grupos de usuários que deverão ser analisados como "Peer Groups" por algoritmos de machine learning.

6. DA COMPROVAÇÃO DE REQUISITOS E TESTE DE CONFORMIDADE

6.1. A licitante no momento da apresentação da proposta deverá enviar documentação garantindo a comprovação detalhada da aderência do sistema ofertado aos requisitos técnicos do edital.

6.2. O licitante classificado em primeiro lugar será convocado para realizar Teste de Conformidade do sistema ofertado, para avaliação técnica de compatibilidade com o solicitado no Termo de Referência, conforme os prazos abaixo:

6.2.1. Prazo para iniciar o Teste de Conformidade e apresentar a pertinente documentação técnica: no máximo **2 (dois) dias úteis**, a contar da suspensão da sessão pública do certame.

6.2.2. Prazo para concluir o Teste de Conformidade: no **máximo 5 (cinco) dias úteis**, a contar do início do teste.

6.3. O Teste de Conformidade servirá para resguardar a segurança da futura contratação e para indicar preliminarmente que o sistema tem condições básicas para atendimento aos requisitos técnicos.

6.4. A condução do Teste de Conformidade se dará conforme descrito no subitem 6.8 deste anexo.

6.5. O sistema a ser utilizado no Teste de Conformidade não poderá ser diferente do apresentado na proposta de preço**.**

6.6. A fim de garantir que a(s) ferramenta(s) ofertadas tenha condições de suportar plenamente os processos modelados pela CONTRATANTE, o sistema deverá comprovar todas as funcionalidades e especificações descritas neste Anexo do Termo de Referência.

ESTADO DO RIO GRANDE DO SUL
POLÍCIA CIVIL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL
DIVISÃO DE ASSESSORAMENTO ESPECIAL

6.7. Caso o Teste de Conformidade da autora da melhor proposta seja reprovado, a proposta será recusada e será convocada a autora da segunda melhor proposta para realizar o teste, e assim sucessivamente.

6.8. Roteiro do Teste de Conformidade.

6.8.1. O licitante classificado em primeiro lugar será convocado a realizar Teste de Conformidade do sistema de gerenciamento de chamados ofertado, para avaliação técnica de compatibilidade com o Termo de Referência, observadas as condições abaixo**:**

6.8.1.1. Disposições gerais:

6.8.1.1.1. A CONTRATANTE designará uma comissão técnica que acompanhará o licitante em todas as etapas do teste.

6.8.1.1.2. O licitante deverá prover o ambiente de hardware, software e demais recursos necessários à realização do teste, em quantidade e especificação suficientes para a execução de todos os passos.

6.8.1.1.3. O Roteiro de teste deverá ser proposto pela licitante e deverá comprovar todas as especificações técnicas constantes no Termo de Referência.

6.8.1.1.4. Poderá ser solicitada, durante a execução do Roteiro Proposto, a demonstração de qualquer funcionalidade listada nas especificações técnicas constantes no Termo de Referência.

6.8.1.2. Locais, horários e prazos:

6.8.1.2.1. O teste será realizado, em sessão aberta, nas dependências da CONTRATANTE de maneira presencial.

6.8.1.2.2. O licitante terá um prazo de até **2 (dois) dias úteis** após o encerramento da fase de lances para iniciar o Teste de Conformidade, sob pena de recusa de sua proposta pelo não cumprimento do prazo.

6.8.1.2.3. Após o início do teste, o licitante terá um prazo de até **5 (cinco) dias úteis** para concluí-lo, sob pena de recusa de sua proposta pelo não cumprimento do prazo.

Nome do documento: ANEXO_C_Sistema_de_Gerenciamento_de_Eventos_e_Informacoes_de_Seguranca_Rev7_Final.docx

Documento assinado por	Órgão/Grupo/Matrícula	Data
HENRIQUE SMIDT SEEWALD	PC / 400705 / 322135002	25/03/2024 15:53:19