



MINISTÉRIO DA CULTURA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA
COINT/CGINT/STII/GSE/GM/MinC
Site: - <http://www.cultura.gov.br>

APÊNDICE III

PROVA DE CONCEITO

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
ITEM 1	-
A solução deverá monitorar, no mínimo, os seguintes eventos do Microsoft Active Directory: Conta habilitada e desabilitada; Autenticação de conta (TGT); Renovação de acesso (TGS); Replicação de AD; Logon de conta no DC; Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS; Requisição de acesso NTLM; Alteração de senha de usuário; Conta de usuário bloqueada; Conta de usuário desbloqueada; Netlogon vulnerável; Criação, deleção e modificação de GPO; Tentativa de reset de senha; Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC; Alteração de política de kerberos;	
A solução deverá monitorar múltiplos domínios e servidores de arquivos Windows e NAS (Network Attached Storage) do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;	
Deverá ser possível definir os proprietários das pastas através da console;	
A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;	
A solução deverá exibir o repositório monitorado em formato hierárquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;	
A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);	
A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;	
A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e	

expressão regular;	
A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;	
A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;	
A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;	
Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada, caso ocorra ação que os envolva;	
Os alertas da solução deverão ser encaminhados via SMTP e SNMP;	
A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;	
A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalasções de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de descoberta de contas com NTLM e Kerberos; Ataques de força bruta;	
A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;	
A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;	
A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;	
A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;	
Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;	
No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas;	

Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;	
A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;	
A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;	
Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;	
A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente;	
A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;	
A solução deverá coletar no mínimo os seguintes eventos e metadados das ferramentas de borda:	
DNS: Client DNS query, Upstream DNS query, DNS Zone Transfer e DNS Client Update;	
Reputação da URL	
Tipo de conexão	
Tamanho do Upload;	
Login de VPN a partir de país listado em Blacklist;	
Login de VPN a partir de fonte suspeita;	
A solução deverá ter pesquisas pré-definidas de eventos do tipo:	
Requisições DNS feitas para sites malicioso;	
Maior download de sites de storage na semana;	
A solução deverá oferecer proteção e alerta para ataques do tipo:	
Tunelamento por DNS;	
Força bruta;	
A solução deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory, atendendo minimamente os seguintes critérios:	
Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada	

aplicação.	
Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.	
Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.	
Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.	
Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.	
Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.	
Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.	
Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.	
Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.	
Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.	
Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.	
Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.	
A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta.	
Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.	
Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.	
Possuir gráfico que represente os eventos de uma credencial específica em um	

intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.	
Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.	
Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.	
Ser capaz de processar eventos originados em IPv4 e IPv6.	
Possuir identificador único para todos os eventos processados pela solução.	
Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.	
Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida.	
O nível de dificuldade do desafio criptográfico deverá ser parametrizável.	