INFRA S.A.

ANEXO XIII

Brasília, 17 de dezembro de 2024.

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Tabela 1. *Lista de componentes da solução.*

Grupo	Item	CATMAT/CATSER (Aproximado)	Descrição	Unidade	Forma de Aquisição	Forma de Pagamento
1	1	27502(CATMAT)	Serviços de Simulação de Violação e Ataques Cibernéticos	Unidade	Produto	Única

GRUPO 01

1. SUBSCRIÇÃO DE SOLUÇÃO PARA VALIDAÇÃO DE SEGURANÇA CONTÍNUA

1.1. ***Requerimentos Gerais***

1.1.1. A solução deve proporcionar simulação, avaliação e gestão estendida da postura de segurança da organização, permitindo medir a efetividade através de testes e avaliações do nível de proteção do perímetro e de ambientes internos para que haja uma compreensão completa quanto a efetividade dos controles de segurança.

1.1.2. A solução deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.

1.1.3. A plataforma deve fornecer minimamente um caminho para validação de brechas e simulações de ataques (BAS)

1.1.4. A solução deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.

1.1.5. A solução deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:

1.1.6. Reconhecimento – Validação de domínios e subdomínios a fim de identificar fraquezas e vulnerabilidades expostas na internet referente a organização. Nesta fase, a solução deverá utilizar de fontes de inteligência aberta (OSINT) para descoberta de credencias e outras informações as quais possam beneficiar um atacante.

1.1.7. Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalação de privilégio.

1.1.8. Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

1.1.9. Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais .

1.1.10. Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

1.1.11. A solução deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

1.1.12. A solução deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

1.1.13. A solução deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

1.1.14. As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

1.1.15. A solução deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

1.1.16. A solução deve possuir suporte e licenciamento realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

1.1.17. A solução deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

2. REQUERIMENTOS FUNCIONAIS E ARQUITETURA

2.1. A solução deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD, OKTA, JumpCloud entre outros.

2.2. A solução deve permitir a integração com diferentes plataformas de segurança via API.

2.3. Todos os componentes da solução devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

2.4. Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

2.5. A solução deve suportar a comunicação dos componentes instalados por meio de um proxy web.

2.6. O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

2.7. A solução deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

2.8. A solução deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

2.9. Todos os produtos de segurança que não possuírem integração direta, devem poder ser integrados por meio soluções de correlacionamento de eventos (SIEM), permitindo a integração com produtos não homologados.

2.10. A solução deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.

2.11. A solução deve permitir avaliar as capacidades de defesa da organização contra táticas,

técnicas e procedimentos utilizados por grupos criminosos conhecidos.

2.12. A solução deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.

2.13. O portfólio de ataques da solução deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS, Microsoft DRAPE e NIST.

2.14. As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.

2.15. A solução deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:

2.16. Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:

2.16.1. Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.

2.16.2. Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo estes realizar a descoberta de hosts vulneráveis e simular a ploriferação para eles através de técnicas utilizando protocolos tais como SMB.

2.16.3. Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.

2.16.4. Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.

2.16.5. MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

2.17. Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

2.17.1. Phishing: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção de ataques de phishing, acessando IPs e URLs reais associados a ataques de phishing identificados recentemente.

2.17.2. Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.

2.17.3. C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.

2.17.4. Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.

2.17.5. Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.

2.17.6. Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares que simulam o comportamento de worms, trojans e ransomware.

2.18. Para validação do vetor de email gateway a plataforma deve oferecer simulações de ataque

para:

2.18.1. Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.18.2. Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.18.3. Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente

2.18.4. Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.18.5. Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.18.6. Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.18.7. True File Type Detection: Validação da efetividade dos recursos de proteção de e-mail através do envio de arquivos com diferentes extensões não pertencentes ao seu formato de arquivo original, este teste deve apoiar na identificação de possíveis brechas que podem ser utilizadas para comprometer o ambiente através da falsificação de formatos originais de arquivos.

2.19. Para validação do vetor de web application firewall (WAF) a plataforma deve oferecer simulações de ataque para minimamente:

2.19.1. SQL injection;

2.19.2. Cross-site scripting (XSS);

2.19.3. File inclusion for remote code execution;

2.19.4. Command injection.

2.20. Para validação de vazamento de dados (DLP) a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

2.20.1. HTTP & HTTPS: Exfiltração de dados por HTTP/S, injetando dados confidenciais em cabeçalhos de solicitação HTTP/S enviados para um servidor remoto.

2.20.2. Browser HTTP & HTTPS: Exfiltração de dados através de navegadores como IE, Edge e/ou Chrome.

2.20.3. DNS: Exfiltração de dados pela porta 53.

2.20.4. Tunelamento DNS: Exfiltração de dados sobre o protocolo DNS (túnel através de servidores DNS públicos). Injetando dados confidenciais em uma solicitação de DNS enviada a servidores DNS públicos.

2.20.5. Tunelamento ICMP: Exfiltração de dados sobre cabeçalhos ICMP. Injetando dados confidenciais em um pacote de eco (ECHO) enviado para um servidor remoto.

2.20.6. Telnet: Exfiltração de dados pela porta de rede Telnet 23.

2.20.7. Exfiltração de dados sobre o protocolo SFTP.

2.20.8. Outras Portas: Exfiltração através do upload de dados confidenciais para servidores de hospedagem de arquivos externos por meio de portas de rede abertas.

2.20.9. Email: Usando email corporativo no Outlook para transmitir dados confidenciais.

2.20.10. Serviços de nuvem: Exfiltração de dados confidenciais para ou por meio de serviços e aplicativos em nuvem.

2.20.11. Dispositivos Removíveis: Exfiltração de dados confidenciais através da cópia para dispositivos de mídia removíveis, como USB.

2.21. Para validação de movimentação lateral a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

2.21.1. Pass-the-Password;

2.21.2. Pass-the-Ticket;

2.21.3. Pass-the-Hash;

2.21.4. Brute Force;

2.21.5. LLMNR/NBT-NS Poisoning and Relay;

2.21.6. Kerberoast;

2.21.7. Password Spraying;

2.21.8. Steal LAPS passwords.

2.22. A solução deve fornecer a possibilidade de criar modelos customizados nos vetores de ataque sem causar impactos ao ambiente.

2.23. Para o cenário de movimentação lateral, o agente da solução deve poder atuar exatamente como um atacante no ambiente, não devendo este depender da implementação de outros agentes para validação dos diferentes métodos. A plataforma deve possuir capacidade de realizar um “pivoting” na rede e fornecer um mapa de toda trilha percorrida e alvos alcançados, podendo os alvos serem considerados ou não joias da coroa (Crown Jewels).

2.24. A solução deve fornecer um caminho para validação completa da cadeia de ataque (Full Kill-chain), permitindo assim que seja avaliadas fases tais como pré-exploração, exploração e pós-exploração.

2.25. A solução deve permitir a criação de campanhas de phishing customizadas para avaliação da conscientização dos colaboradores em cenários reais, as campanhas devem minimamente permitir que sejam criados conteúdos através da plataforma em português.

2.26. Cada um dos testes ou ações hospedadas na base de conhecimento da solução, deve ter uma descrição e o código da técnica ou das táticas de acordo com a nomenclatura do MITRE.

2.27. A solução deve ter a capacidade de repetir periodicamente os testes que o usuário deseja e comparar os resultados de cada execução com um resultado esperado, permitindo definir se o ataque foi detectado, bloqueado e que tipo de registro foi detectado no SIEM ou nas tecnologias de segurança testadas.

2.28. Os componentes de ataque devem poder ser instalados, minimamente, nos seguintes ambientes:

2.28.1. Windows 11 build 22000+, 10 build 1067, 8.1, 7 SP1;

2.28.2. Server 2012 ou superior;

2.28.3. Linux Alpine 3.12, Ubuntu 16.04, Debian 10, CentOS 7, RHEL 7, Fedora 33, openSUSE 15 e SUSE Enterprise 12 SP2 ou versões superiores;

2.28.4. MacOS 10.15x ou superior.

2.29. A solução deve realizar as simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

3. REQUERIMENTOS DE GESTÃO E RELATÓRIO

3.1. A solução deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

3.2. A console deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

3.3. A console deve fornecer uma visão global dos itens que foram identificados.

3.4. A solução deve possuir uma interface amigável em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

3.5. Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

3.6. A solução deve permitir a geração de relatórios técnicos ou gerenciais aos quais devem conter minimamente:

3.6.1. Informações sobre o score de risco atual;

3.6.2. Descrição e recomendação para correção dos problemas encontrados;

3.6.3. Técnicas e táticas utilizadas;

3.6.4. Frameworks adotados para gerar o score;

3.6.5. Parecer técnico.

3.7. A solução deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

3.8. A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

3.9. A solução deve fornecer um caminho simples para minimamente:

3.9.1. Gerenciar usuários da plataforma;

3.9.2. Gerenciar logs e atividades em execução.

3.9.3. A console deve fornecer uma guia para download e gestão dos agentes implementados.

Documento assinado eletronicamente por **MARCO ANTONIO GOÉS DE OLIVEIRA**, **Integrante Técnico**, em 17/12/2024, às 15:46, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Saboia**, **Integrante Requisitante**, em 17/12/2024, às 15:49, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Renato Ricardo Alves**, **Superintendente de Tecnologia da Informação**, em 17/12/2024, às 16:02, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5. Bairro Asa Sul, - Bairro Asa Sul
Brasília/DF, CEP 70.070-010
Telefone: