IDE_013/2023 - Informativo de Declaração de Exclusividade 16/03/2023

Solicitamos às empresas nacionais fabricantes dos produtos ou similares abaixo citados que se manifestem, com a devida comprovação e nos termos de nossa Norma de Emissão de Declaração de Exclusividade, em até **05 dias úteis após a divulgação deste informe (até 18h do dia 13/03)**. Decorrido este prazo e não havendo manifestações em contrário, será expedida a respectiva declaração.

EMPRESA: AWARE CONSULTORIA

PRODUTOS / SERVIÇOS

Metodologia AWARE de Inteligência, Prontidão Cibernética e Proteção de Dados
Abordagem de Defesa Ativa constituída por conjunto de processos, tecnologias e operadores, integrados a rede internacional de parceiros do campo da Inteligência, com a capacidade de ultrapassar o perímetro corporativo da organização-cliente, de forma não-intrusiva, extrínseca e imparcial, oferecendo varreduras, diagnósticos e perícias que alcançam ameaças, vulnerabilidades e desconformidades, inclusive em terceiras partes, cadeias produtivas e camadas da Internet inacessíveis às soluções de segurança cibernética internas da organização.
Viabiliza a fusão, sob medida e não-rotineira, seguindo toda a legislação vigente e sob critérios rígidos de sigilo e proteção de dados, de capacidades de vanguarda em contrainteligência, alertas e detecção de ameaças cibernéticas. Implementa sistema produtivo local, integrando profissionais de análise e curadoria com experiência de campo e especializados nas disciplinas pertinentes e na operação dos componentes intangíveis e insumos nacionais e internacionais, para o desenvolvimento e entrega de investigações, diagnósticos e remediações cibernéticas baseados em conhecimento de inteligência sob medida aos seus Clientes.
Oferece elevado grau de abrangência, profundidade e precisão, para monitoramento de todas as camadas da Internet (Aberta, Deep e Dark Web) e do mundo cibernético, e detecção de incidentes em IT, OT e IoT, viabilizando a segurança preventiva para a implementação de projetos de Indústria 4.0, Conformidade LGPD, Cidades Inteligentes, Bancos de Dados, Serviços Online, Internet das Coisas, dentre outros.
Compreende os seguintes serviços, que podem ser prestados de forma urgente, eventual, periódica ou continua, incluindo ou não alertas temporizados 24hx7dx365d:
1) Serviço de Proteção Contra Riscos Digitais – AWARE PROTEÇÃO
Conjunto de serviços prestados com escaneamento ativo e proprietário de 4,3 Bilhões de dispositivos endereçáveis em IPV4 em cada um de 24 horas (frequência), com alcance que ultrapassa a camada superficial de metadados e chega ao nível de Conteúdo em cada IP exposto, com monitoramento não-intrusivo (nenhuma instalação de hardware ou software ou acesso lógico solicitado ao Cliente), em modo 24hx7dx365d, com modelo metodológico e operacional padronizado, integrado e sincronizado, e curadoria por inteligência aumentada (artificial + humana) analisando e deparando incidentes positivos reais (true positive"), contextualizados e investigados, viabilizando alertas preventivos e tempestivos de vulnerabilidades ou ameaças de incidentes, com gradação por severidade, e sambem diagnósticos situacionais, laudos, pareceres técnicos, relatórios de inteligência acionável, aderente à legislação de privacidade e proteção de dados, inclusive sob a perspectiva de Conformidade e Governança LGPD (Lei Geral de Proteção de Dados Pessoais), com os seguintes módulos aplicáveis sob medida para cada Cliente:
a) Prevenção Contra a Violação de Dados
Módulo de serviço de Monitoramento de documentos e bases de dados inseguras e publicamente acessíveis que possam conter conjuntos de dados sensíveis pertencentes ao Clienteou terceiras partes relacionadas ou não, responsáveis por vazamentos de dados do Cliente. Capaz de vasculhar em modo Ativo e no nível de Conteúdo dos serviços de armazenamento de arquivos, aplicações em Nuvem (Cloud) e bases de dados abertas, com frequência de 24 horas, contemplando:
- Escaneamento de portas livremente acessíveis em todos os endereços IPV4 para detectar dispositivos conectados de armazenamento inseguros que contenham documentos sensíveis pertinentes ao Cliente, inclusive examinando sistemas vulneráveis de propriedade de funcionários e terceiras partes (fornecedores, parceiros ou clientes de clientes) envolvidos na troca de informações sensíveis do Cliente;
- Escaneamento de conteúdos expostos em plataformas de compartilhamento e colaboração online, serviços de armazenagem em Nuvem (Cloud) líderes de mercado, plataformas de compartilhamento de códigos, ferramentas de compartilhamento de arquivos e soluções de gestão de projetos em modelo de Software como Serviços (SaaS);
- Algoritmos de aprendizagem de máquina com mais de 8 anos de dados proprietários e exclusivos para aprimoramento de padrões e precisão, continuamente aperfeiçoados pelo escaneamento e processamento de mais de 4 bilhões de pontos de dados coletados diariamente;
- Cobertura, no mínimo, das seguintes fontes: SMB, FTP(S), GCS, AWS S3, MySQL, Azure Storage, ElasticSearch e MongoDB.
- Escopo mínimo de Varredura: File Servers and NAS, Network Virtual Drives, Web Services, Unprotected Databases, Cloud Storage Services, Cloud Drive Services, Code-sharing Platforms, File-sharing Platforms e Project Management Tools.
- Padrão de desempenho: capacidade de detecção de 800.000 documentos expostos por minuto com depuração de 0,01% falso positivo.
b) Descoberta e Vigilância de Ativos
Módulo de serviço de Prevenção de ataques nocivos pela detecção de vulnerabilidades e proteção de máquinas, dispositivos e serviços Web, incluindo ativos estabelecidos fora do campo de visibilidade normal da equipe de TI do Cliente, ou seja, "Ativos Shadow", contemplando:
- Detecção Ativa de infraestruturas vulneráveis de TI (tecnologia da informação / IT), TO (tecnologias operacionais / OT) e IdC (Internet das Coisas / IoT) que possam ser explorados como parte de ataques cibernéticos de grande complexidade. Os riscos incluem pegadas malignas ("footprinting"), penetração em infraestruturas, roubo de dados e ataques "ransomware" (sequestros com cobrança por resgate).
- Cobertura, no mínimo, das seguintes fontes: RDP, TeamViewer, Modbus, Fox, Bacnet, Dicom, Telnet e Docker.
- Escopo mínimo de Varredura: File Servers & File Transfers, Remote Desktop Services, Industrial Systems, Smart Building Tecnology, Unprotected Databases, Internet of Things, DevOps Tools e Authentication Services.
- Padrão de Desempenho: foco em CVE > 7 (MITRE Std) e com depuração de 0,01% falso positivo.
c) Proteção de Domínio
Módulo de serviço de proteção contra ameaças de falsificação de nomes de domínios e riscos de utilização não-autorizada de recursos de TI ("Shadow IT") por meio de detecção de domínios fraudulentos ou com erros de URL (nomes incorretos, "Typosquatting").
- Patrulha contra ameaças dormentes e identificação de configurações não-autorizadas de nomes de domínios e servidores de mensagens (MX) em tempo real por meio de monitoramento contínuo de buscas anônimas de DNS.
- Combinação única de requisições ativas e passivas de DNS vigilantes para a detecção de tentativas de falsificação, desvio, phishing ou estacionamento de domínios (parking).
- Capacidade de monitorar, de um ponto de vista de DNS passivo, inversões, trocas ou repartições de domínios, assim como falsificação ("spoofing") de subdomínios.
- Cobertura, no mínimo, das seguintes fontes: Feeds DNS passivos, Zone files e Certificate transparency logs.
- Escopo mínimo de Varredura: Domain Name Servers.
- Padrão de Desempenho: capacidade para 200.000 alertas/mês por domínio monitorado (incluindo todos os subdomínios) e com depuração de 0,01% falso positivo.
d) Salvaguarda de Contas e Credenciais
Módulo de serviço de proteção contra comprometimento de credenciais corporativas (endereços de email, nomes de login, senhas, etc), sejam estas vazadas, violadas ou simplesmente expostas, contemplando, no mínimo, as seguintes fontes: "paste sites", bancos de dados abertos, fóruns Deep e Dark Web, gangues de sequestro ("Ransomware") e diálogos de Hackers.
- Capacidade de alerta sobre a exposição de credenciais na Internet antes que estas sejam comprometidas por agentes malignos, mediante escaneamento de credenciais hospedadas em bases de dados em Nuvem (Cloud) ou em dispositivos de armazenagem inseguros e conectados.
- Capacidade de alerta preventivo para eliminar a credencial exposta antes que um eventual ataque efetivamente ocorra.
- Escopo mínimo de Varredura: Leak-sharing Platforms, Unprotected Databases, Paste Sites, Multiple Criminal Forums, Carding Markets e Global Marketplaces.
- Padrão de Desempenho: Base de dados com mais de 10 bilhões de credenciais expostas (login & senha), capacidade de detecção mínima de 335.000 postagens na Deep e Dark Web por dia e de 3000 novas bases de dados expostas escaneadas por dia.
e) Monitoramento Deep e Dark Web
Módulo de serviço de Monitoramento contemplando varredura ativa de centenas de fontes específicas na Deep e Dark Web, incluindo fóruns Tor, aplicativos de mensagem, e mercados Hackers, de forma a identificar e indexar eventuais dados roubados, investigando e alertando nossos Clientes.
- Tipos de incidentes cobertos neste serviço incluem: exploração de vulnerabilidades, ataques a computadores, esquemas de fraude, e riscos de "targeting" a VIPs. Cobertura, no mínimo, das seguintes fontes: TOR, I2P, IRC, WhatsApp, Discord e Telegram.
- Escopo mínimo de Varredura: Specialized Groups on Community Platforms; Haking, Security and Technology Blogs and Forums; Multiple Criminal Forums, Carding Markets, Global Marketplaces; Paste Sites; Instant Messaging Applications; e Chat Applications.
- Padrão de Desempenho: capacidade de detecção mínima mensal de 10 Milhões de postagens na Deep e Dark Web, em um mínimo de 600.000 discussões monitoradas (incluindo grupos de discussão privados), e 125.000 threads monitoradas por mês e com depuração de 0,01% falso positivo.
f) Perícia Cibernética (Cyber Due Diligence)
Módulo de serviço de Perícia, com coleta ativa e passiva, investigação, análise e emissão de Laudo de Riscos Digitais e Exposição Cibernética realizado em terceira parte relacionada ao Cliente diretamente.
- Abordagem efetivamente imparcial e isenta, com os seguintes princípios: extrínseca (fora do perímetro desta organização-alvo); e não-intrusiva (dispensando qualquer instalação de software ou hardware, ou abertura de acesso lógico às premissas da organização-alvo).
- Camadas de Diagnóstico: 7 camadas: (a) bases de dados desprotegidas em bancos de dados abertos; (b) domínio sensível em aplicações em Nuvem (Cloud); (c) documentos expostos em dispositivos de armazenamento conectados; (d) atividades maliciosas na Deep e Dark Web; (e) credenciais expostas na Internet; (f) desvios de URLs e domínios ("typosquatting"); e (g) ativos vulneráveis pertencentes à superfície de ataque da organização-alvo.
- Escopo mínimo de Varredura: (a) Dispositivos baseados em IP, hospedando compartilhamento de arquivos, bancos de dados, armazenamento em Nuvem (Cloud), computadores de trabalho remoto e serviços de autenticação; (b) Fóruns na Deep e Dark Web, mercados de violação de cartões ("Carding") e diálogos de Hackers criminosos; (c) Aplicativos de mensagens instantâneas; (d) Paste sites; (e) Repositórios de códigos baseados em Nuvem (Cloud), bem como plataformas colaborativas.
- Capacidades mínimas disponíveis para investigações especiais ou específicas, envolvendo verificação de vulnerabilidade ou exposição: (a) Protocolos de Internet das Coisas – IdC/IoT (Indústria 4.0, SCADA, automação de Cadeia Produtiva, etc.); (b) Protocolos de equipamentos médicos (DICOM e outros); (c) Protocolos de Edifícios Inteligentes (ar-condicionado inteligente, elevadores inteligentes, etc); e (d) Diagnóstico suplementar a processos de Auditoria e Governança no âmbito da LGPD (Lei Geral de Proteção de Dados).
2) Serviço de Avaliação Global de Riscos Cibernéticos – AWARE CHECK-UP
Conjunto de serviços expressos (tempo de resposta ao Cliente de até 24 horas), não-intrusivos (nenhuma instalação de hardware ou software ou acesso lógico solicitado ao Cliente), em modo eventual, periódico ou contínuo (24hx7dx365d), que identifica desconformidades e também riscos de ataques ransomware, decorrentes de análise de varredura passiva de Inteligência que agrega mais de 400 fontes OSINT a Datalake próprio de registros, com modelo metodológico e operacional padronizado, integrado e sincronizado, e curadoria por inteligência aumentada (artificial + humana), viabilizando visão gerencial específica ou multidimensional integrada dos riscos (tecnológicos + financeiro + regulatório), com gradação de apontamentos por severidade, e também diagnósticos situacionais, laudos, pareceres técnicos, relatórios de inteligência acionável, aderente à legislação de privacidade e proteção de dados, inclusive sob a perspectiva de Conformidade e Governança LGPD (Lei Geral de Proteção de Dados Pessoais), com os seguintes módulos aplicáveis sob medida para cada Cliente:
a) Aferição Do Grau de Risco Cibernético
Módulo de serviço expresso – até 24 horas – que emite laudo de avaliação de grau de risco cibernético, com agregação de vulnerabilidades classificadas por grupos (Salvaguardas, Privacidade, Resiliência e Reputação) em até 20 categorias de risco. Oferece ao Cliente visualização amigável e acessível ao público não-técnico, com quantificação de risco representada em padrão de cores tipo "semáforo" e avaliação de severidade com ponderação por escala "A a F".
- Aderência mínima aos seguintes Modelos de Pontuação/Avaliação: Common Vulnerability Scoring System (CVSS), MITRE Cyber Threat Susceptibility Assessment (CTSA), Open FAIR, Common Weakness Risk Analysis Framework (CWRAF), Common Weakness Scoring System (CWSS).
- Base de dados própria mínima: mais de 400 milhões de Domain Names e 4 bilhões de Subdomínios, 4 bilhões de Service Fingerprints, 10 bilhões de certificados SSL, 1 bilhão de DNS e Whois, 100 bilhões de páginas Web e mais de 34 milhões de Empresas, obtidas de fontes OSINT como internet-wide scanners, hacker forums e deep / dark web, disponíveis para averiguação instantânea.
- Padrão de Desempenho: escaneamento não-intrusivo passivo coletando vulnerabilidades em um mínimo de 400 fontes OSINT em ciclo menor que 24 horas sem nenhum contato lógico direto com o Cliente.
b) Apontamento de Vulnerabilidades e Riscos Cibernéticos
Módulo de serviço expresso – até 24 horas – que emite laudo com apontamentos detalhados de vulnerabilidades identificadas para o Cliente. Os apontamentos são classificados por grupos (Salvaguardas, Privacidade, Resiliência e Reputação) em até 20 categorias de risco. Oferece ao Cliente visualização amigável e acessível ao público não-técnico, com lista detalhada de vulnerabilidades classificadas por grau de severidade.
- Aderência mínima aos seguintes Modelos de Pontuação/Avaliação: Common Vulnerability Scoring System (CVSS), MITRE Cyber Threat Susceptibility Assessment (CTSA), Common Weakness Risk Analysis Framework (CWRAF), Common Weakness Scoring System (CWSS).
- Base de dados própria mínima: mais de 400 milhões de Domain Names e 4 bilhões de Subdomínios, 4 bilhões de Service Fingerprints, 10 bilhões de certificados SSL, 1 bilhão de DNS e Whois, 100 bilhões de páginas Web e mais de 34 milhões de Empresas, obtidas de fontes OSINT como internet-wide scanners, hacker forums e deep / dark web, disponíveis para averiguação instantânea.
- Padrão de Desempenho: escaneamento não-intrusivo passivo coletando vulnerabilidades em um mínimo de 400 fontes OSINT em ciclo menor que 24 horas sem nenhum contato lógico direto com o Cliente.
c) Avaliação e Aferição do Grau de Conformidade Cibernética
Módulo de serviço expresso – até 24 horas – que emite laudo de avaliação de grau de conformidade do Cliente face a leis, padrões e melhores práticas globais de cibersegurança, correlacionando evidências coletadas online que podem ser complementadas com questionário em modelo Shared Assessment preenchido pelo Cliente. Oferece ao Cliente visualização amigável e acessível também ao público não-técnico, mapeando analiticamente os resultados de forma ponderada percentualmente, conforme cada padrão de conformidade.
- Cobertura mínima dos seguintes Padrões e Legislações: LGPD/GDPR, NIST 800-53, ISO27001, CIS, PCI-DSS, COBIT e HIPAA.
3) Serviço de Cultura Cibernética
Serviço voltado ao provimento de ações de sensibilização, educação, treinamento, capacitação e ensaios operacionais para uso e aproveitamento dos resultados dos serviços de Inteligência, Prontidão Cibernética e Proteção de Dados, de acordo com Metodologia AWARE.