devoteam

“People-First”

Um novo paradigma na ciber-resiliência

com a Alert Readiness Framework

Creative tech for Better Change

Sobre a Devoteam

A Devoteam é uma empresa de consultoria tecnológica especializada em cloud, cibersegurança, data e sustentabilidade.

Tech Native há mais de 25 anos, a Devoteam orienta empresas através da transformação digital sustentável para desbloquear todo o seu potencial.

Com mais de 10.000 colaboradores em mais de 25 países na Europa, Médio Oriente e África, a Devoteam está empenhada em colocar a tecnologia ao serviço das pessoas.

Para concretizar esta visão, associamo-nos às principais Plataformas Cloud mais importantes do mundo, Microsoft Azure, Google Cloud e AWS.

Creative tech for Better Change

People-First

Índice

Resumo executivo

O panorama atual da cibersegurança é marcado por um conjunto cada vez mais complexo de ameaças, exigindo mais do que apenas defesas tecnológicas. Um fator crucial, mas frequentemente ignorado neste domínio, é o elemento humano, uma vez que mais de 80% das violações de cibersegurança acontecem devido a erro humano. Esta estatística realça uma vulnerabilidade significativa - a falha na sensibilização e no comportamento humano em cibersegurança.

Para fazer face a este desafio, a tradicional concentração em soluções centradas na tecnologia e em programas periódicos de sensibilização está a revelar-se insuficiente. O que é necessário agora é uma mudança fundamental na abordagem - **avançar para uma estratégia "People-First"**. Esta estratégia realça o papel do comportamento humano e da tomada de decisões como sendo fundamentais para reforçar as defesas de cibersegurança. Trata-se de uma mudança de mera consciência da cibersegurança para a tornar uma parte intrínseca da cultura organizacional e das operações diárias.

A Alert Readiness Framework (ARF) é fundamental para facilitar esta mudança. Apresenta uma abordagem estruturada que integra a metodologia "People-First" no núcleo das práticas de cibersegurança. Esta framework não se limita a responder às ameaças de forma reativa, mas envolve proativamente todos os indivíduos da organização no processo contínuo de criação de ciber-resiliência.

Este resumo executivo descreve a necessidade de adotar uma abordagem que coloque as pessoas em primeiro lugar no âmbito da ARF para combater eficazmente as ameaças à cibersegurança. Sublinha a transição dos métodos tradicionais para uma estratégia holística que coloca as pessoas na vanguarda da cibersegurança. Nas secções que se seguem, aprofundamos os pormenores da ARF, ilustrando a forma como incorpora esta mudança de paradigma e o impacto transformador que pode ter na ciber-resiliência organizacional.

Introdução

À medida que navegamos na era digital, o rosto da cibersegurança está a evoluir continuamente, moldado tanto pelas tecnologias emergentes como pela natureza em constante mudança das ameaças. No entanto, no meio desta paisagem complexa, há um elemento que permanece consistentemente no centro dos desafios da cibersegurança: **o fator humano**. Apesar dos avanços nas tecnologias de segurança, o erro humano continua a ser uma das principais causas das violações de cibersegurança, sublinhando uma vulnerabilidade crítica na nossa abordagem à proteção dos ativos digitais.

A sabedoria convencional em cibersegurança há muito que está ancorada a **soluções centradas na tecnologia** e a medidas reativas. Embora estes componentes sejam, sem dúvida, essenciais, muitas vezes ofuscam a importância da dimensão humana. Reconhecer e abordar o fator humano não é apenas divulgar informações; trata-se de promover uma cultura em que a cibersegurança é compreendida, valorizada e praticada por todos numa organização.

Este documento apresenta a **Alert Readiness Framework (ARF)** como uma ferramenta para as organizações que procuram adotar uma abordagem mais holística à cibersegurança. A ARF distingue-se pela sua capacidade de integrar medidas técnicas com uma atenção especial ao elemento humano, alinhando as práticas de cibersegurança com os comportamentos e ações dos indivíduos. Ao defender uma abordagem que coloca as pessoas em primeiro lugar, a ARF visa transformar a cultura organizacional, tornando a cibersegurança uma responsabilidade partilhada e uma parte da vida quotidiana.

Nas secções seguintes, exploraremos os componentes da ARF, a forma como aborda o elemento humano na cibersegurança e os passos que as organizações podem dar para implementar eficazmente esta framework. O objetivo é fornecer informações sobre a criação de um ambiente cibernético mais resiliente, em que a tecnologia e os fatores humanos trabalhem em conjunto para combater o espectro em evolução das ciberameaças.

Compreender o desafio humano na cibersegurança

No domínio da cibersegurança, o envolvimento eficaz dos utilizadores apresenta desafios multifacetados que ultrapassam as limitações dos programas de sensibilização tradicionais. Estes desafios radicam não só na complexidade técnica da cibersegurança, mas também nos aspetos comportamentais e psicológicos do envolvimento dos utilizadores.

- **A barreira da mentalidade duradoura:** Um dos desafios mais significativos é a mentalidade duradoura dos utilizadores que, após formações regulares, voltam frequentemente aos seus comportamentos originais. O impacto transitório das sessões de formação não consegue incutir uma consciencialização a longo prazo, levando a um lapso na vigilância e a um regresso a práticas menos seguras.
- **O desafio da extensão:** Outro obstáculo é a integração dos utilizadores como extensões ativas da equipa de cibersegurança. Embora os utilizadores sejam cruciais na identificação e comunicação de potenciais ameaças, manter este nível de envolvimento de forma consistente é um desafio. Existe uma falha entre a sensibilização esporádica e a participação ativa e contínua nos esforços de cibersegurança.
- **A segurança como uma reflexão tardia:** Frequentemente, a cibersegurança é vista como uma reflexão tardia e não como um aspeto integrante das operações diárias. Os utilizadores podem dar prioridade à conveniência ou à eficiência em detrimento dos protocolos de segurança, aumentando inadvertidamente a vulnerabilidade às ciberameaças.

- **Ultrapassar a condescendência:** A condescendência em cibersegurança representa um risco substancial. Os utilizadores, uma vez familiarizados com determinados procedimentos ou protocolos, podem tornar-se menos vigilantes, subestimando a natureza evolutiva das ciberameaças.
- **Criar uma cultura de segurança sustentada:** O desafio final reside na transformação da cultura organizacional para dar prioridade à cibersegurança de forma consistente. Trata-se de criar um ambiente em que a cibersegurança não seja apenas uma responsabilidade do departamento de TI, mas um aspeto fundamental no papel de cada colaborador.

À medida que os ciberataques se tornam cada vez mais sofisticados e organizados, torna-se imperativo que as organizações reforcem a sua própria organização e vigilância. Neste complexo puzzle da cibersegurança, o fator humano surge como um interveniente crucial e essencial para reforçar as defesas contra estas ameaças complexas e em evolução.

Apresentação da Alert Readiness Framework (ARF)

Numa era marcada pelos rápidos avanços tecnológicos e pela escalada das ciberameaças, a Alert Readiness Framework (ARF) surge como uma ferramenta vital para melhorar a ciber-resiliência das organizações. Com uma abordagem exclusivamente centrada nas organizações, a ARF não é apenas uma solução de cibersegurança; é uma estratégia abrangente que se alinha estreitamente com a dinâmica operacional e a missão principal de uma organização.

Como funciona a ARF: Uma visão geral simplificada

A eficácia da ARF reside no seu mecanismo operacional simples, mas robusto que pode ser resumido em algumas etapas fundamentais:

Definir âmbitos contextuais: Cada organização da ARF está dividida em âmbitos contextuais. Estes âmbitos são áreas ou departamentos específicos dentro da organização, cada um com o seu perfil de risco e necessidades de cibersegurança únicos. Ao definir estes âmbitos, a ARF garante que a resposta às ciberameaças é adaptada e eficaz, abordando as vulnerabilidades específicas de cada área.

Organizar as fontes relevantes: Esta etapa envolve a recolha e organização de fontes de dados relevantes. Estas fontes englobam uma série de informações, incluindo indicadores técnicos, business intelligence e fatores humanos, que contribuem para uma compreensão abrangente da postura de cibersegurança da organização.

Calcular o nível de alerta atual: Utilizando os dados recolhidos, a ARF calcula o nível de alerta atual da organização. Este nível representa o estado atual do risco de cibersegurança, determinado pela análise de vários fatores, como informações sobre ameaças, avaliações de vulnerabilidades e relatórios de incidentes recentes.

Identificar e/ou Definir e Implementar Controlos (RTP e RTI): Com base nos níveis de alerta definidos e nos âmbitos contextuais, a ARF identifica e/ou orienta a implementação de dois tipos de controlos principais: Reduzir a Probabilidade (RTP) e Reduzir o Impacto (RTI). Os controlos RTP são medidas proativas destinadas a reduzir a probabilidade de incidentes de cibersegurança, enquanto os controlos RTI focam-se na minimização do impacto, caso ocorra um incidente.

Definir planos de resposta contextual: Uma das principais etapas da ARF é a preparação e implementação de Planos de Resposta Contextuais (CRPs). Estes planos detalham as ações específicas a tomar quando o nível de alerta muda, quer seja para cima ou para baixo.

Uma estrutura para a cibersegurança proativa

A metodologia da ARF é revolucionária na medida em que faz com que as organizações passem de uma postura reativa de cibersegurança para uma postura proativa. Para tal, monitoriza continuamente o panorama cibernético, ajusta os níveis de alerta conforme necessário e garante a adoção de medidas adequadas e específicas para diferentes cenários. Esta abordagem dinâmica permite que as organizações se mantenham à frente de potenciais ameaças num estado de preparação adequado e respondam eficazmente aos desafios cibernéticos em evolução.

Integração da cibersegurança na estratégia empresarial

Um aspeto crítico da ARF é o seu foco na integração da cibersegurança na estratégia empresarial global. Ao alinhar as práticas de cibersegurança com os objetivos empresariais, a ARF assegura que a proteção dos ativos e das infra-estruturas de informação está em sintonia com os objetivos mais amplos da organização, melhorando assim a resiliência empresarial global.

Em resumo, a Alert Readiness Framework é uma solução estratégica e centrada no negócio que simplifica e melhora a abordagem de uma organização à cibersegurança. O seu processo metódico de definição de âmbitos contextuais, organização de dados, avaliação de níveis de risco e identificação/implementação de controlos direcionados estabelece a ARF como uma ferramenta essencial para as organizações modernas que navegam no complexo panorama cibernético.

Abordagem “People-First” na ARF

A implementação da Alert Readiness Framework (ARF), centrada no elemento humano, significa uma mudança das estratégias convencionais de cibersegurança para um modelo mais holístico e centrado nos comportamentos. Esta abordagem focada nas pessoas é fundamental para reforçar os aspetos RTP (Reduzir a Probabilidade) e RTI (Reduzir o Impacto) da ARF, garantindo um sistema de ciberdefesa abrangente e resiliente.

Integração do elemento humano na ARF

- **Foco comportamental na avaliação de riscos:** No âmbito da estratégia RTP, uma componente significativa da avaliação de riscos na ARF envolve a análise das vulnerabilidades do comportamento humano. Isto inclui a identificação de erros comuns, suscetibilidade à engenharia social e potenciais ameaças internas, adaptando depois a estrutura para mitigar estes riscos.
- **Níveis de alerta personalizados com controlos geridos pelo ser humano:** Os níveis de alerta da ARF são concebidos exclusivamente para incluir controlos e orientações centrados no ser humano. Cada nível não só indica a gravidade da ameaça cibernética, como também define expectativas e ações comportamentais específicas para os colaboradores, garantindo que a sua resposta está alinhada com o nível atual de ameaça.
- **Formação comportamental integrada no sistema de alerta:** Uma caraterística fundamental da ARF é a integração da formação comportamental no seu sistema de alerta. Para cada nível de alerta, são ativados módulos de formação específicos, centrados nos comportamentos e competências relevantes necessários para responder e gerir eficazmente as ameaças a esse nível. Isto assegura que todos os colaboradores têm os conhecimentos e as competências necessários para agir adequadamente em diferentes condições de ameaça.

- **Programas contínuos de consciencialização e envolvimento:** Para além das tradicionais sessões de formação anuais, a ARF defende a existência de programas de sensibilização e envolvimento contínuos. Estes programas são desenvolvidos para manter a cibersegurança na mente dos colaboradores, assegurando que as práticas seguras se tornam habituais e enraizadas na cultura organizacional
- **Feedback em tempo real e aprendizagem adaptativa:** A ARF dá destaque a um ambiente de aprendizagem dinâmico em que o feedback em tempo real dos colaboradores é utilizado para adaptar e melhorar continuamente a framework. Esta abordagem permite a rápida integração das lições aprendidas com incidentes reais ou exercícios de formação na estrutura, melhorando as estratégias de RTP e RTI.

Aplicação prática na estrutura da ARF

- **Aprendizagem baseada em cenários e simulações:** A ARF utiliza aprendizagem baseada em cenários e simulações que refletem as ciberameaças da vida real, ajudando os colaboradores a compreender o seu papel na prevenção e mitigação destas ameaças. Este método é crucial para traduzir o conhecimento teórico em competências práticas e acionáveis.
- **Formação específica por função e responsabilidades:** Reconhecendo que diferentes funções dentro de uma organização têm diferentes níveis de exposição a riscos cibernéticos, a ARF oferece formação específica para cada função. Isto garante que cada colaborador compreende as suas responsabilidades e ações específicas em diferentes níveis de alerta, contribuindo eficazmente para a ciber-resiliência global da organização.
- **Incentivar uma cultura de segurança proativa:** O objetivo final da abordagem "People-First" da ARF é cultivar uma cultura de segurança proativa. Isto implica a criação de um ambiente em que todos os colaboradores estão conscientes do seu papel na cibersegurança, participam ativamente na salvaguarda dos ativos digitais da organização e têm poderes para tomar iniciativas nas atividades de ciberdefesa.

Desafios e considerações

À medida que as organizações integram a Alert Readiness Framework (ARF), enfrentam desafios únicos que decorrem da sua natureza centrada nas empresas e da necessidade de quebrar os comportamentos tradicionais nas abordagens de cibersegurança.

Alinhar a cibersegurança com os objetivos comerciais

Um dos principais desafios é garantir que as iniciativas de cibersegurança estejam alinhadas com os objetivos comerciais mais amplos. A ARF aborda esta questão integrando a cibersegurança em todos os processos empresariais, mas a transição para este modelo integrado exige uma mudança significativa de mentalidade e de práticas em toda a organização.

Ultrapassar as mentalidades tradicionais

Outro desafio significativo consiste em ultrapassar a visão tradicional da cibersegurança como um domínio exclusivo das TI. A ARF defende um quadro que seja compreensível e acionável a todos os níveis da organização, o que exige uma mudança na cultura e na estratégia organizacionais.

Adaptação à evolução tecnológica

As organizações também precisam de se adaptar ao panorama tecnológico em rápida evolução. A ARF incentiva a adoção de abordagens inovadoras de cibersegurança em resposta à expansão da superfície de ameaça provocada pelas novas tecnologias.

Adesão dos dirigentes

É fundamental garantir o empenhamento dos executivos ao mais alto nível. O seu apoio é fundamental para impulsionar mudanças nas políticas e promover uma cultura em que a cibersegurança seja uma prioridade.

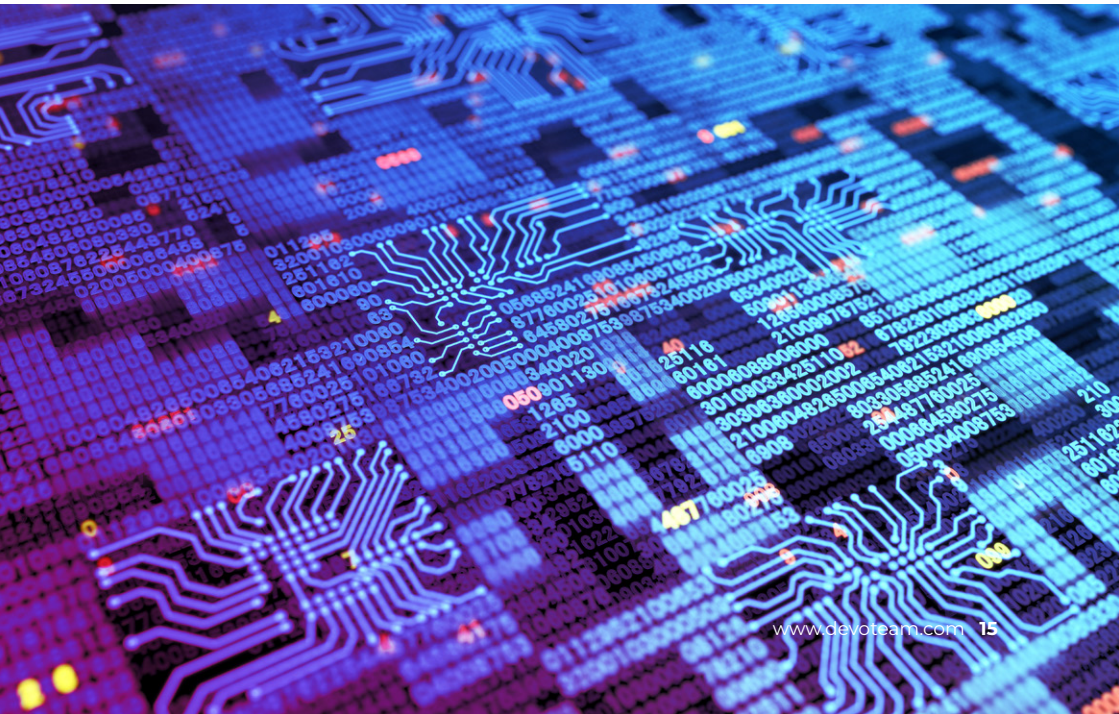
Colaboração entre departamentos

A implementação da ARF exige a colaboração entre vários departamentos. Esta abordagem holística é essencial para desenvolver uma estratégia abrangente de cibersegurança.

Participação dos colaboradores

Os colaboradores desempenham um papel vital no sucesso da ARF. O envolvimento regular através de formação, simulações e processos de feedback é crucial para reforçar uma cultura consciente da segurança.

Em conclusão, estes desafios realçam a necessidade de uma abordagem unificada da cibersegurança, salientando a importância da adaptação a novos paradigmas e da promoção da colaboração a todos os níveis organizacionais.



Vantagens para os primeiros utilizadores

A adoção antecipada da ARF oferece às organizações a oportunidade de liderar a inovação em cibersegurança, trazendo inúmeras vantagens estratégicas.

- **Definição de normas do setor:** Os primeiros a adotar a ARF podem influenciar as normas e as melhores práticas do setor da cibersegurança, posicionando-se como líderes e estabelecendo novos padrões de referência neste domínio.
- **Ganhar vantagem competitiva:** A implementação da ARF proporciona uma vantagem competitiva, melhorando a reputação de uma organização e criando confiança nos clientes, demonstrando um compromisso com uma segurança abrangente que valoriza os fatores humanos.
- **Criar resiliência e confiança:** Melhorar proativamente a postura de cibersegurança através da ARF reforça a resiliência organizacional, criando confiança entre os clientes e as partes interessadas, crucial numa era em que as ciberameaças podem afetar significativamente a reputação das organizações.
- **Melhorando os processos internos e o envolvimento dos colaboradores:** Os primeiros utilizadores podem aproveitar a ARF para melhorar os processos internos e o envolvimento dos colaboradores. O foco na aprendizagem e adaptação contínuas promove um ambiente de trabalho dinâmico, impulsionando a inovação e a satisfação.
- **Orientar a evolução do setor:** As organizações que adotam a ARF podem orientar outras na indústria, potencialmente promovendo novas colaborações e parcerias, e liderando o caminho para práticas inovadoras de cibersegurança.

Em resumo, a adoção precoce da ARF não só melhora a postura de cibersegurança, como também posiciona as organizações para a liderança da indústria, a diferenciação competitiva e relações mais fortes com as partes interessadas. Este investimento estratégico alinha os esforços de cibersegurança com os objetivos organizacionais mais amplos, marcando um passo em frente significativo na resiliência e inovação organizacionais.

Conclusão:

Pioneirismo num futuro centrado nas pessoas com a Alert Readiness Framework

À medida que concluímos a nossa exploração da Alert Readiness Framework (ARF), torna-se evidente que a adoção da ARF significa uma mudança crítica para uma abordagem mais resiliente e focada nas pessoas em cibersegurança. Esta framework inovadora não só aborda os desafios no panorama da cibersegurança, como também anuncia uma nova era em que as estratégias centradas no ser humano estão na vanguarda da proteção dos ativos digitais.

Destacar o elemento humano na cibersegurança

No centro da ARF está o destaque do elemento humano, um aspeto crucial que tem sido muitas vezes ofuscado nas estratégias tradicionais de cibersegurança. Ao colocar as pessoas em primeiro lugar, a ARF transforma cada membro da organização num participante ativo na ciberdefesa, promovendo uma cultura em que a cibersegurança é uma responsabilidade coletiva, profundamente enraizada no ethos organizacional.

Postura abrangente de cibersegurança

A adoção da ARF conduz a uma postura abrangente de cibersegurança que se integra perfeitamente e apoia os principais processos empresariais da organização. Este alinhamento garante que a cibersegurança não é um esforço autónomo, mas uma componente essencial da estratégia empresarial global, aumentando a resiliência organizacional contra as ciberameaças em evolução.

Melhorar a continuidade da atividade e eliminar comportamentos tradicionais

A ARF desempenha um papel fundamental no reforço da continuidade das atividades, preparando as organizações para enfrentarem proativamente as potenciais perturbações causadas pelas ciberameaças. Além disso, quebra os comportamentos tradicionais entre a cibersegurança e outras funções empresariais, defendendo uma abordagem unificada que eleva a cibersegurança a uma questão de interesse empresarial abrangente.

Linguagem unificadora em toda a organização

A ARF estabelece uma linguagem comum para a cibersegurança, tornando-a facilmente compreensível e acionável para todos, desde os executivos aos colaboradores da linha da frente. Esta linguagem comum desmistifica a cibersegurança, tornando-a parte integrante das operações diárias e dos processos de tomada de decisão.

Olhando para o futuro: Um projeto para a ciber-resiliência

Ao adotarem a ARF, as organizações não estão apenas a adotar um novo enquadramento; estão a defender uma mudança de paradigma para um modelo de cibersegurança que coloca as pessoas em primeiro lugar. Esta mudança é crucial numa era em que o fator humano desempenha um papel significativo nas violações da cibersegurança. A ARF oferece um modelo para a construção de um ambiente de cibersegurança resiliente, ágil e com visão de futuro, bem equipado para enfrentar os desafios atuais e futuros.

Ao olharmos para o futuro, a ARF é um farol para as organizações que se esforçam por navegar nas complexidades da era digital de forma segura e eficaz. A sua abordagem, que coloca as pessoas em primeiro lugar, combinada com estratégias avançadas de gestão do risco, posiciona-a como uma ferramenta essencial para as organizações empenhadas em serem pioneiras num mundo digital seguro, resiliente e centrado no ser humano.

O papel da Devoteam Cyber Trust na implementação da ARF

A Devoteam Cyber Trust, uma empresa de consultoria de excelência com presença em 18 países da EMEA, está excecionalmente posicionada para facilitar a implementação da Alert Readiness Framework (ARF). A nossa abordagem, baseada numa extensa base de conhecimento em estruturas de segurança e privacidade, é **adaptada para fornecer serviços de cibersegurança de alta qualidade**.

Os nossos pontos fortes e únicos

- **Vasta rede de especialistas**: Com mais de 850 consultores de cibersegurança na EMEA e 98% dos nossos colaboradores certificados na área, a nossa profundidade de conhecimentos é inigualável.
- **Serviços de consultoria de ponta a ponta**: Oferecemos uma gestão abrangente do programa e conhecimento da estrutura, garantindo que todos os aspetos da implementação da ARF sejam meticulosamente planeados e executados.
- **Estratégias de implementação personalizadas**: A nossa capacidade de colocar as questões corretas, documentar processos e apresentar cenários baseados na experiência de implementação permite-nos oferecer soluções personalizadas que se alinham com os requisitos únicos de cada organização.
- **Apoio operacional**: Estendemos o nosso apoio para além da implementação e da operação contínua, assegurando que a ARF não é apenas implementada, mas também efetivamente integrada no tecido organizacional.
- **Integração GRC**: A nossa experiência no apoio à implementação ou personalização da Governação, Gestão de Riscos e Conformidade (GRC) é crucial para alinhar a ARF com os processos empresariais existentes e os requisitos regulamentares.

Com a Devoteam Cyber Trust, as organizações podem navegar com confiança nas complexidades da implementação da ARF, aproveitando os nossos vastos recursos, a nossa experiência e abordagem personalizada para melhorar a sua postura de segurança cibernética e resiliência de negócios.

Referências / Notas Finais

- “Alert Readiness Framework First Edition.” Devoteam. https://www.devoteam.com/alert-readiness-framework/
- International Data Corporation (IDC) reports and publications. [General reference].
- ISO/IEC 27001 Information Security Management standards. [General reference].
- PCI Security Standards Council. “PCI DSS Quick Reference Guide.” [General reference].


Creative tech for Better Change