BEYONDSOFT®
beyond your expectations

Obtenha a estrutura para

Fortaleçer o seu Centro de Operações de Segurança.

Índice

Cibersegurança – O Cenário Atual

Identificar e compreender as ameaças à segurança cibernética.

Pré-requisitos para a implementação de operações de segurança robustas

Cinco benefícios de um centro de operações de segurança

Estrutura de um Centro de Operações de Segurança eficaz

Próxima etapa

Cibersegurança

A Paisagem Contemporânea

Organizações de diversas dimensões operam em escala global há décadas para se resguardarem contra ameaças no ciberespaço. Existe um investimento contínuo e significativo na melhoria e na ampliação de soluções de segurança, tanto por meio de pesquisa e desenvolvimento interno, quanto através de parcerias, colaborações e terceirização.

Este white paper visa oferecer uma compreensão abrangente das diversas ameaças à segurança cibernética que prevalecem no cenário digital, além de delinear o roteiro que pode ser seguido para se proteger contra elas.

Identificar e compreender as ameaças à segurança cibernética.

Os primeiros passos para abordar qualquer ameaça consistem em identificá-la, categorizá-la e compreendê-la. As ameaças cibernéticas atuais podem ser classificadas em cinco categorias distintas:

- Phishing
- Ataques de ransomware.
- Violação de dados pessoais ou sigilosos
- Ataques de força bruta
- Ataques a plataformas de nuvem

A segurança cibernética, ou segurança de TI (tecnologia da informação), refere-se à proteção de sistemas e redes digitais contra ataques de agentes maliciosos.

As consequências desses ataques podem incluir o roubo de dados, danos a hardware ou software, interrupções nos negócios, paralisações completas das operações ou até mesmo prejuízos à reputação da sua empresa. Grandes organizações com ativos físicos e digitais distribuídos por diversas regiões são mais suscetíveis a esses ataques. Sempre que uma nova ameaça emerge, as organizações frequentemente reagem adotando ferramentas e softwares de segurança adicionais. Embora essa abordagem pareça lógica e aborde a ameaça imediata, ela acarreta o risco inerente de problemas relacionados à governança, manutenção e recursos humanos necessários para garantir sua operação a longo prazo.

Os recentes desenvolvimentos no panorama geopolítico e as alterações nas exigências resultantes da cultura de trabalho híbrido introduziram um elemento adicional de incerteza a um contexto já complexo. A seguir, alguns dos principais fatores que contribuirão para a continuidade e a expansão dos ataques cibernéticos ao longo do tempo:

- Crise Econômica
- Aumento de Comprometimentos de E-mails Corporativos
- Guerra de Informação Impulsionada por IA
- Instabilidade Geopolítica
- Surgimento de Tecnologias Disruptivas
- Segurança na Nuvem

Pré-requisitos para a constituição

Operações de Segurança Robustas

Antes de decidir criar, adquirir, expandir o seu conjunto de talentos ou trazer um parceiro para auxiliar nas operações de segurança, aqui estão alguns pré-requisitos que poderá considerar:

1. Desenvolva uma compreensão abrangente da superfície de ataque global da sua organização.

Um dos pilares mais significativos da postura de segurança cibernética de qualquer organização é a compreensão da extensão da superfície de ataque. Isso é fundamental do ponto de vista do planeamento. Sem um conhecimento abrangente da superfície de ataque da sua organização, qualquer planeamento operacional para proteger os ativos será infrutífero. Frequentemente, esses dispositivos são instalados e armazenados em locais acessíveis a um grande número de utilizadores.

- Quantos dispositivos estão expostos ao perímetro?
- Quantas estações de trabalho estão a executar sistemas operacionais desatualizados?
- Quantos servidores estão alojados no local?

Essas questões evidenciam a relevância da gestão de ativos na postura de segurança global de uma organização. Ao elaborar um inventário abrangente dos ativos presentes no ambiente, a sua organização pode adquirir uma compreensão mais clara da superfície de ataque geral e, simultaneamente, identificar quais ativos estão vulneráveis ao perímetro.
A sua avaliação permitirá que a sua organização priorize e refine com precisão o programa de operações de segurança, desenvolvendo um programa mais robusto de deteção de vulnerabilidades e gestão de posturas de segurança. Além de criar um inventário de ativos, a implementação do monitoramento de endpoints em todo o ambiente auxiliará a sua organização na revisão de portas públicas, desativação de portas desnecessárias e restrição de destinos de portas. Este tipo de monitoramento é crucial para proporcionar visibilidade das ações realizadas por potenciais agentes de ameaça. Embora outros tipos de fontes de log possam complementar essa visibilidade, não podem substituí-la.

2. Monitore fontes críticas de registos para ameaças à segurança

Reconhecemos igualmente que a ausência de visibilidade possibilita que ameaças à segurança permaneçam indetectadas, o que pode resultar em danos significativos à reputação de uma organização. O monitoramento de logs, por exemplo, é de extrema importância para a identificação de ameaças substanciais. Isso abrange logs provenientes de diversas fontes, como firewalls, soluções de Detecção e Resposta de Endpoints (EDR), sistemas de Gerenciamento de Identidade e Acesso (IAM), sistemas de Detecção de Intrusão (IDS)/Detecção e Resposta de Rede (NDR) e serviços em nuvem utilizados em ambientes corporativos.

3. Implemente a Autenticação Multifator (MFA).

Ao exigir múltiplas formas de autenticação, torna-se significativamente mais difícil para indivíduos não autorizados obterem acesso a sistemas e dados sensíveis dentro de uma rede ou sistema. Recomendamos que a sua organização avalie a configuração geral de MFA em relação a diversos tipos de ameaças. Essas contramedidas incluem a limitação da taxa de solicitações de autenticação, a adição de uma etapa após o prompt de autenticação e o treinamento em conscientização de segurança para o utilizador final.

4. Incutir uma Cultura e Estratégia de Segurança Zero-Trust

À medida que a sua organização adota diversos serviços baseados em nuvem para gerir as necessidades de carga de trabalho da sua equipa e lhes concede acesso a um ambiente remoto ou híbrido, estabelecer uma cultura Zero-Trust e estratégias de segurança robustas são decisões cruciais para a sua empresa. O Zero-Trust concentrar-se-á no utilizador, não no perímetro, e limitará todo o acesso, a menos que possa ser verificado.

Existem várias abordagens para implementar estratégias de Confiança Zero, incluindo a adoção de autenticação multifator e outras ferramentas de gestão de identidade. A implementação de uma estratégia de Confiança Zero, juntamente com soluções pertinentes, diminuirá o risco de compromissos de contas e proporcionará uma segurança adicional às organizações.

5. Compreenda o Modelo de Responsabilidade Compartilhada e Elimine Erros de Configuração

É fundamental reconhecer onde se encerram as responsabilidades de segurança de um prestador de serviços de nuvem e onde se iniciam as responsabilidades da sua organização.

Isso é também denominado modelo de responsabilidade partilhada. Neste modelo, o fornecedor de nuvem é responsável pela segurança da nuvem, enquanto você é responsável pela segurança no interior da nuvem.

As especificações desta responsabilidade podem variar consoante o modelo de serviço de nuvem adotado pela sua organização, como IaaS, PaaS ou SaaS.

Sem um domínio sólido desses conceitos, a configuração da segurança na nuvem pode tornar-se complexa e confusa, resultando em configurações inadequadas ou na ausência de segurança apropriada. É essencial que você compreenda para onde os dados estão a ser transferidos na nuvem e estabeleça protocolos e criptografias seguras a serem implementadas uma vez na nuvem. Esses protocolos devem incluir o conhecimento e as restrições sobre quem pode aceder aos dados e aplicações no ambiente de nuvem.

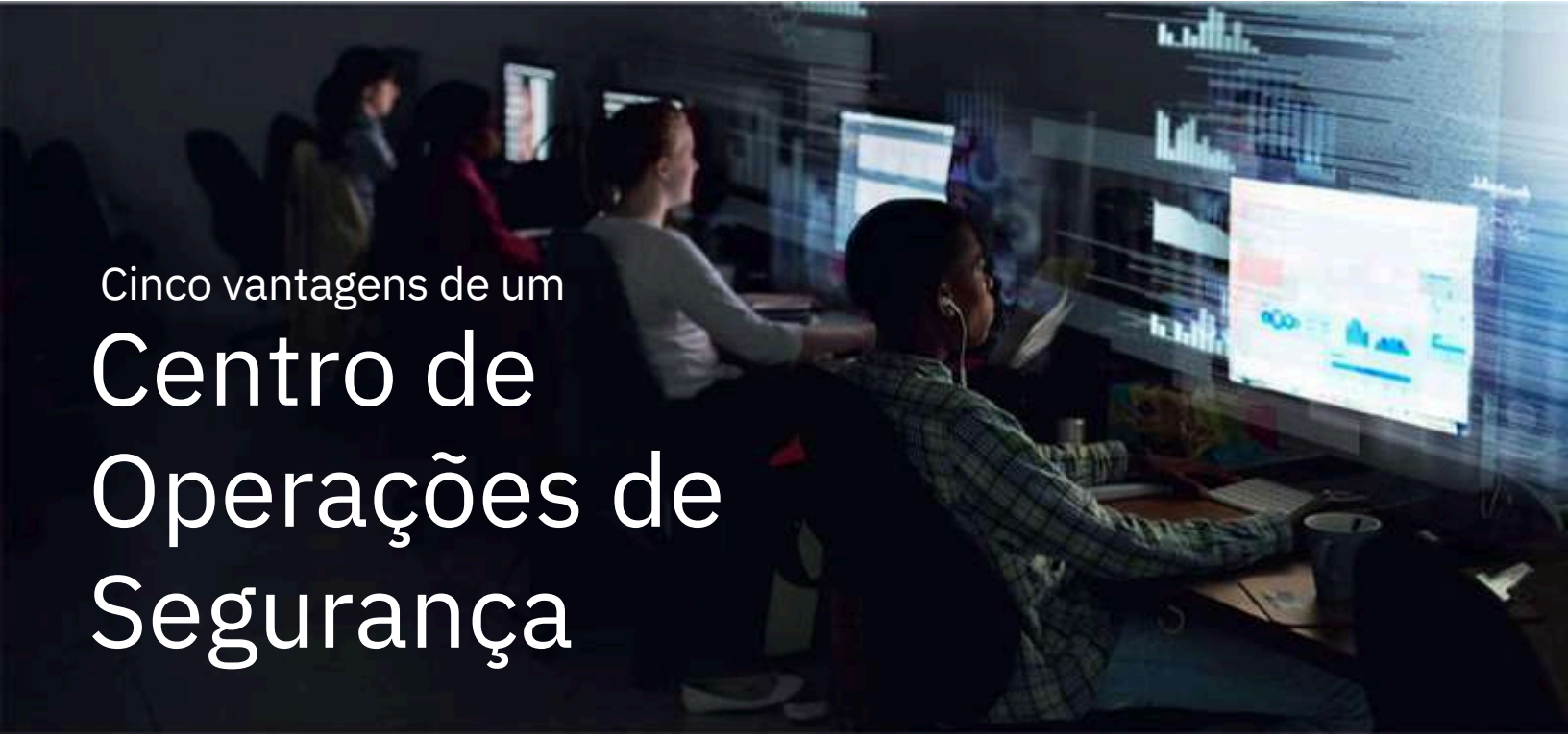
6. Implementar um programa abrangente de sensibilização sobre segurança/cultura orientada para a segurança cibernética.

Ao implementar um programa abrangente de sensibilização sobre segurança, os utilizadores podem compreender como se tornam alvos e como podem atuar como uma linha de defesa fundamental contra agentes de ameaças e tentativas de violação. Um programa sólido inclui formação regular sobre tendências e temas atuais — como gestão de senhas, hábitos de navegação, táticas de engenharia social e como reportar e responder a atividades suspeitas.

Dada a crescente frequência e complexidade dos ataques cibernéticos, a questão já não é se um ataque ocorrerá, mas sim quando. A implementação de um Centro de Operações de Segurança (SOC) é fundamental para abordar a questão do "quando" do ataque cibernético e reforçar a resiliência da sua organização face a ameaças cibernéticas, minimizando o impacto em caso de comprometimento.

A Beyondsoft desempenha um papel fundamental na ajuda à criação de operações de segurança robustas e proativas, que fortalecem a sua postura de segurança cibernética e a protegem de forma eficaz contra ameaças em constante evolução.

MengKhong Tong, Presidente e Director de Operações
Equipe NABG na Beyondsoft



Cinco vantagens de um

Centro de Operações de Segurança

- Caça ativa de ameaças
- Aprimoramento na deteção de incidentes e no tempo de resposta
- Economia de custos.
- Maior visibilidade em segurança e gestão centralizada de incidentes.
- Auditoria Periódica de Sistemas

Embora a maioria das organizações possua algum conhecimento sobre o desenvolvimento de uma estrutura de segurança cibernética, muitas delas reconhecem não estar preparadas para a contratação interna de uma força de trabalho disponível 24 horas por dia, 7 dias por semana, para o Centro de Operações de Segurança (SOC). A segurança cibernética é uma das áreas mais procuradas atualmente e enfrenta uma grave escassez de recursos, o que impacta a capacidade de muitas organizações de recrutar os profissionais qualificados adequados.

A cibersegurança é uma atividade colaborativa, e é por isso que a Beyondsoft desenvolveu um ecossistema de especialistas que unem as suas diversas especialidades em prol dos nossos clientes. Reconhecemos que nenhuma organização pode se proteger de forma isolada. Assim, como ecossistema, dependemos uns dos outros para partilhar, aprender e oferecer conhecimento especializado. É praticamente inviável enfrentar os desafios do atual panorama de ameaças de forma solitária. Acreditamos

Estrutura do Sucesso

Centro de Operações de Segurança

Ajudamos a configurar o seu Centro de Operações de Segurança (SOC), disponibilizando uma variedade de especializações, serviços e suporte ao longo de todo o processo. Um SOC é um elemento fundamental da infraestrutura de segurança cibernética da sua organização, encarregado de monitorizar e responder a ameaças de segurança em tempo real. Consulte a nossa estrutura:

Avaliação e Planeamento

Realizamos uma avaliação preliminar da sua postura e infraestrutura de segurança cibernética atuais. Colaboramos consigo para compreender as suas necessidades de segurança, perfil de risco e objetivos empresariais. Com base nessa avaliação, elaboramos um plano abrangente para a implementação do seu SOC, delineando os processos necessários, as plataformas tecnológicas e, acima de tudo, os recursos qualificados.

Design e Arquitetura de SOC

Projetamos a arquitetura do SOC para assegurar um desempenho e escalabilidade ideais. Levaremos em conta fatores como a coleta de dados, correlação, análise e fluxos de trabalho de resposta a incidentes para desenvolver um design de SOC robusto e eficiente.

Seleção de ferramentas e tecnologia

Projetamos a arquitetura do SOC para assegurar um desempenho e escalabilidade ideais. Levaremos em conta fatores como a coleta de dados, correlação, análise e fluxos de trabalho de resposta a incidentes para desenvolver um design de SOC robusto e eficiente.

Processos e fluxos de trabalho

Apoiamos a elaboração de planos de resposta a incidentes, procedimentos operacionais padrão (POPs) e fluxos de trabalho para a equipa do SOC. Isso assegura que os analistas do SOC possam reagir de forma eficaz a incidentes de segurança de maneira oportuna e coordenada.

Implementação e Integração

Com quase três décadas de experiência em implementações de soluções, apoiamos a implementação e integração das tecnologias e ferramentas de segurança selecionadas. A nossa equipa de especialistas configurará os sistemas para que operem em perfeita harmonia, assegurando que todas as fontes de dados necessárias estejam conectadas ao SOC para um monitoramento eficaz de ameaças.

Governança e Aperfeiçoamento Contínuo

Apoiamos o seu SOC na otimização contínua das suas operações. Isso implica concentrar-se em avaliações regulares, monitorização de desempenho e aperfeiçoamento de processos com base nas lições extraídas de incidentes anteriores.

Próxima etapa

Além de auxiliar os nossos clientes na configuração do seu SOC, também disponibilizamos serviços geridos para operações de segurança. Oferecemos serviços de SOC geridos, nos quais a operação integral do seu SOC será administrada por nós ou em colaboração com parceiros dedicados. Esta abordagem permite que você se concentre no seu negócio principal, enquanto conta com a expertise em segurança cibernética da Beyondsoft e dos nossos parceiros.

Vamos colaborar para reforçar a sua postura de segurança.

Sobre a Beyondsoft

Como uma empresa global de TI com mais de 30.000 colaboradores, a Beyondsoft emprega tecnologias emergentes e um método de entrega comprovado, permitindo que clientes de diversos setores adotem uma abordagem ágil e inovadora nos negócios. Há quase três décadas, a Beyondsoft oferece uma vasta gama de serviços de TI de alta qualidade, incluindo inteligência artificial, computação em nuvem, big data e análise, terceirização de processos de negócios, soluções de software personalizadas, automação de testes, capacitação digital e outros serviços de engenharia de software.

DESENHO POR
ZAMSTARS