BASE4 SECURITY

Ajudando a construir um ecossistema digital mais seguro.

Application Security

DATA SHEET

Aspectos gerais da área

A **Base4 Security** acompanha as empresas na automação dos controles de segurança dentro do SDLC de seus projetos, onde as ajudamos a integrar a segurança no DevOps através da colaboração contínua entre as equipes de desenvolvimento, operações e segurança. Incorporando a segurança no ciclo de vida do desenvolvimento de software.

É um método que faz parte de um desenvolvimento ágil de software e é uma evolução para uma responsabilidade compartilhada pela segurança. Isso envolve levar em conta a segurança do software desde o início, bem como automatizar os processos para não retardar o fluxo de trabalho DevOps dentro do pipeline de desenvolvimento de aplicações de acordo com seu nível de maturidade.

Meta

Nosso objetivo é conseguir entregas de software mais rápidas e seguras, sem transformar a segurança em um gargalo de estrangulamento. Em outras palavras, a DevSecOps tenta assegurar uma entrega rápida e segura, resolvendo problemas comuns entre desenvolvimento e segurança. Para isso, conta com ferramentas como o Veracode.

Visibilidade

Realizamos a Análise GAP baseada na estrutura OWASP SAAM como

uma forma eficaz e mensurável para sua organização analisar e melhorar sua postura de segurança de software.

Benefício

- Ganhe visibilidade do atual estágio de maturidade da segurança de seu pipeline de desenvolvimento dentro do SDLC.
- Obtenha um plano preciso de crescimento e investimento em segurança de aplicação cobrindo níveis de criticidade.
- Cobertura das últimas vulnerabilidades globais constantemente carregadas em sua nuvem sem a necessidade de instalar patches.

Pontos de verificação

Executamos serviços One Shot como pontos de verificação de segurança em sua aplicação, como Agile Ethical Hacking, Static Code Scanning, Análise de bibliotecas de terceiros e Análise Dinâmica.

Meta

- Serviços rápidos e limitados para medir o grau de risco de sua aplicação tanto externamente como a partir do código fonte.
- Encontrar as vulnerabilidades mais importantes e separá-las por nível de criticidade para poder consertá-las rapidamente e obter um melhor time-to-market.
- Remediação de acompanhamento até que a aplicação atinja 100% de estabilidade antes de entrar em produção.
- A implementação centralizada de políticas dá maior foco e orientação à análise e controle da segurança de TI sem influenciar o processo de desenvolvimento.
- Analisar todo o projeto compilado em nível de código, bem como ter integrações com as IDEs mais relevantes do mercado, ferramentas de integração contínua e gerenciamento de projetos.
- Mostrar um grau de severidade encontrado sob a restrição política aplicada é mais severo no sentido de indicar vulnerabilidades e problemas encontrados.

Funcionários

Terceirizamos perfis 5x8 DevSecOps para proporcionar melhoria contínua da segurança no pipeline de desenvolvimento, bem como visibilidade das melhorias comerciais.

Meta

- Ter uma pessoa dentro do mundo DevOps com experiência e capacidade em segurança cibernética.
- Evitar a rotatividade de pessoal em posições semelhantes.
- Melhoria dos pontos de controle de segurança nas aplicações.
- Maior integração com a área de ciber-segurança.
- Treinamento para a equipe de desenvolvimento.
- Apoio na implementação de tecnologias e integrações.
- Criação e automatização de análises.
- Apresentações de vulnerabilidades e recomendações de melhores práticas.
- Criação de Métricas e Indicadores.

Tecnologia

Comercializamos tecnologia para fornecer segurança cruzada automatizada em todos os tipos de aplicações com controle independente da área de desenvolvimento sob políticas de segurança cibernética.

Meta

- Melhorar o time-to-market.
- Reduz os custos de tempo de desenvolvimento.
- Reduzir os custos de Ethical Hacking.
- Automação de processos.
- Otimizar a segurança e os processos de desenvolvimento.
- Ensinar boas práticas de segurança para as diferentes equipes.
- Avaliar os riscos e definir planos de contingência.
- Identificar as ameaças e vulnerabilidades antes de entrar em produção.

Por que aplicar DevSecOps?

A integração da segurança em todo o processo de desenvolvimento e não apenas no final permite que DevOps e profissionais de segurança tirem o máximo proveito das metodologias ágeis, removendo obstáculos para a segurança do código.

Estes são os principais benefícios da adoção do DevSecOps:

- Desenvolver software seguro por projeto.
- Identificar vulnerabilidades de código e ataques mais cedo.
- Implementar a segurança de forma mais rápida e rápida.
- Responder rapidamente às mudanças e exigências.
- Melhorar a colaboração e a comunicação entre as equipes.
- Gerar maior conscientização de segurança entre todos os membros.
- Foco na geração do maior valor comercial.

Melhores práticas DevSecOps

Estas seriam boas práticas na implementação do DevSecOps:

- Otimizar a segurança e os processos de desenvolvimento.
- Ensinar boas práticas de segurança para as diferentes equipes.
- Gerenciar e melhorar os controles de acesso.
- Automatizar processos repetitivos.
- Avaliar os riscos e definir planos de contingência.
- Usar ferramentas de segurança.
- Identificar proativamente ameaças e vulnerabilidades.
- Realizar auditorias de segurança com regularidade.

Recomendações do Gartner

A integração da segurança no DevOps requer uma mudança na mentalidade, nos processos e nas tecnologias. Gartner faz uma série de recomendações para a prática bem sucedida do DevSecOps:

- Adaptar ferramentas e processos aos desenvolvedores e não o contrário.
- Não tente eliminar todas as vulnerabilidades durante o desenvolvimento.
- Foco na identificação e eliminação de vulnerabilidades conhecidas de código aberto primeiro.
- Adaptar as análises de testes estáticos e dinâmicos (SAST /SCA/ DAST) à nova realidade.
- Treinar os desenvolvedores em segurança, sem esperar que eles se tornem especialistas.
- Adotar um modelo de Security Champion (especialista em segurança que orienta as outras equipes) e implementar uma ferramenta simples de levantamento de requisitos.
- Garantir e aplicar a mesma disciplina operacional aos scripts de automação e à infra-estrutura de segurança.

Implementar um controle de versão robusto em todos os códigos e componentes.

- Implementando a gestão de segredos.
- Adotar uma mentalidade de infra-estrutura imutável.
- Repensar como os incidentes na prestação de serviços, incluindo a segurança, são tratados.
- Usar o provisionamento de acesso dinâmico para os desenvolvedores no DevSecOps.

OWASP DEVOPS Auditoria

Riscos de auditoria no processo de desenvolvimento, arquitetura e comunicações para compreender a maturidade da segurança cibernética do gasoduto.

O processo é realizado através de reuniões a fim de ver o GAP entre as melhores práticas do mercado e o que o cliente está fazendo sob um plano de trabalho detalhado. Posteriormente, a execução envolve a revisão de uma ou várias aplicações, entrevistas com desenvolvedores, revisão de inventários de ferramentas, oleodutos, melhores práticas, resultados de pentestarias anteriores, entre muitas outras.

Você receberá um relatório com detalhes dos controles, estatísticas e recomendações de implementações e melhores práticas no uso de ferramentas, documentos, lista de verificação de validação, wiki online com recomendações de práticas de desenvolvimento na organização, conselhos subseqüentes, entre outros.

O serviço é orientado para obter um melhor ROI, aumentando a segurança das aplicações a partir de seu próprio desenvolvimento, automatizando-o, ganhando tempo de comercialização contra sua concorrência e evitando riscos na produção que possam ter um impacto negativo sobre a economia e a imagem do cliente.

Modelagem de ameaças

Proteja suas aplicações desde o início para evitar riscos futuros. O objetivo é que a segurança de tal aplicação seja implementada desde o início, modelando as ameaças futuras.

A implementação da modelagem de ameaças ocorre nos estágios iniciais do projeto do software. O objetivo é assegurar que a área de desenvolvimento seja clara sobre as possíveis ameaças que a aplicação pode ter desde a concepção e idéia do negócio até sua execução em células de desenvolvimento, bem como a arquitetura validada do ponto de vista da segurança cibernética.

Através de reuniões com os interlocutores validados, será elaborado um documento com a topologia da aplicação e as recomendações de melhores práticas a serem consideradas no momento do início de seu desenvolvimento, tanto por áreas de desenvolvimento como de infra-estrutura.

O objetivo do serviço é contemplar os maiores riscos que a aplicação pode ter de acordo com seu uso, conexões, arquitetura, design e linguagem. Isto reduzirá estes riscos durante o processo de desenvolvimento, de modo que sua passagem para a produção seja acelerada, para ganhar tempo para o mercado, reduzir os tempos de desenvolvimento e envolver a área de segurança cibernética desde o início.

A **BASE4 Security** também comercializa a tecnologia Threat Modelling para automatizar o processo dentro das empresas.

Escaneamento de código

Ganhe visibilidade das vulnerabilidades atuais em seu código fonte com este serviço One Shot, que ajudará a antecipar e pesar os riscos antes de passar para a produção.

Usando ferramentas de primeira classe de nuvem, a BASE4 Security fornece o serviço Static and Dynamic Code Scanning para descobrir as vulnerabilidades atuais no código.

O serviço tem uma curta duração e ajuda a prever ameaças e riscos antes das aplicações entrarem em produção, sendo uma ferramenta muito produtiva para reduzir os ataques às aplicações.

Um relatório das vulnerabilidades segregadas pela criticidade será entregue aos clientes, bem como uma recomendação sobre a remediação das mesmas.

BASE4
SECURITY

www.base4sec.com