

Desenhada desde o início como uma aplicação em cloud. BugScout oferece a possibilidade de analisar grandes aplicações acabando com uma das maiores limitações dos arquiteturas SAST tradicionais.

Resolve os erros de raiz

BugScout, a ferramenta de análise estática de códigos (SAST) de última geração revenda exclusiva da NalbaTech se integra com o ciclo de vida de desenvolvimento, aumentando a eficiência e verificando a segurança do código antes da implantação ou compilação.

As investigações do setor confirmam que a eliminação de vulnerabilidade em fase de desenvolvimento é 7 vezes mais barato durante a fase de testes e 15 vezes mais barato do que após a implantação.

O que é bugScout?

bugScout é uma plataforma SAST de última geração de detecção de vulnerabilidades na aplicação e no código fonte de páginas web. BugScout foi desenhado por hackers e analistas de segurança do Centro Europeu de Operações e Segurança (SOC).

Atualmente os auditores de segurança de código fonte são imagens que definem o estado da aplicação em um determinado momento, ao mesmo tempo que se criam relatórios. eles já estão desatualizados. dada a natureza do processo contínuo da fase de desenvolvimento.

Graças a seu rápido comportamento e escalabilidade, bugScout permite análises contínuas do código fonte: as auditorias de segurança seguem o mesmo ritmo do processo de desenvolvimento. Os relatórios adaptados a cada rol facilitam a comunicação entre analistas de segurança e desenvolvedores na hora de identificar vulnerabilidades. apontar as causas e corrigir os problemas.

Características

- ✓ Desenhado por hackers éticos e auditores de segurança para automatizar suas melhores práticas.
- ✓ Escalável sendo possível analisar, inclusive, as grandes aplicações.
- ✓ Robusta detecção de vulnerabilidades para as linguagens de programação mais utilizadas (Java, PHP, .NET).
- ✓ Combine segurança com qualidade de software.
- ✓ A menor taxa de falsos positivos do mercado.
- ✓ Simplifica e agiliza os ciclos de vida das aplicações.
- ✓ Múltiplas políticas de detecção.
- ✓ A solução de segurança mais rápida do mercado, capaz de analisar milhões de linhas de código por hora.
- ✓ Ferramenta disponível em cloud para rápida utilização. sem a necessidade de equipamento físico.



Como funciona o bugScout?

Unifica SAST do código fonte e desenvolvimento, obtendo um único fluxo de trabalho para todos os departamentos da empresa.

Motor próprio de análise de código Fonte, rápido e eficiente: analisa milhões de linhas de código em poucos minutos, com grande eficácia.

Sua rápida e fácil integração possibilita a análise contínua do ciclo de vida de desenvolvimento: verifica a segurança do código antes da implantação ou compilação, com as mais baixas taxas de Falso positivos e o melhor índice de velocidade/ precisão do setor.

Plataforma comum para todos os membros da equipe, o que facilita a centralização e a gestão, ao mesmo tempo que melhora a comunicação entre os departamentos: ajuda os desenvolvedores a compreender as vulnerabilidades indicando as causas e permitindo corrigi-las de maneira eficiente.

Economize tempo e dinheiro: encontra e corrige vulnerabilidades na Fase de desenvolvimento o que e 15 vezes mais barato do que na fase de implantação.

Aprendizado automático (machine learning), integração com WAF e múltiplas políticas de detecção incrementam a eficiência.

Tecnologia flexível com múltiplas opções de configuração: eleje a melhor política de detecção para cada análise com a menor taxa de falsos positivos do mercado. O bugScout aplica a aprendizagem automática a partir de suas decisões e as análises lançadas: quanta maior seja o uso da ferramenta. maior será sua precisão.

Integração com sistemas AF: configure de forma automática as políticas de bloqueio e monitoramento para o firewall de aplicações, baseando-se em análises de código-fonte.

Robustas bibliotecas e detecção das vulnerabilidades causadas pela integração de distintas linguagens de programação: suporte para as linguagens de programação mais utilizadas. incluindo Java, PHP e .NET. assim como conhecimento dos problemas causados pela integração dos mesmos.

Suporte a múltiplas listas de vulnerabilidades open source e proprietárias: CWE. OWASP. CPE. CVSS. WASC. e SANS Top25.



das aplicações
tem vulnerabilidades.



das vulnerabilidades
se encontram
nas aplicações.

”

“A investigação de Verizon mostra que as ferramentas de AppSec atuais não são suficientes e que é necessária uma ferramenta de última geração”

Francisco Bernabeu
CEO and Founder of NalbaTech

Ferramenta em cloud, rápida e escalável para infraestruturas e grandes aplicações

Escala até analisar por completo grandes aplicações: desenhado desde o início como um app em cloud, bugScout acaba com uma das maiores limitações das arquiteturas SAST tradicionais.

Início rápido: sistema em cloud para um início simples, sem necessidade de equipamentos nas instalações.

Modelo de appliance virtual opcional: para aquelas empresas que não desejam ter seu código fonte fora de suas instalações.

Gerador de relatórios completo

Os documentos são 100% personalizáveis, fornecem informações detalhadas para relatórios executivos, de cumprimento normativo, assim como relatórios para os usuários de equipes técnicas.

O que é Penetration Testing?

O teste de penetração é um método de avaliação da segurança de um sistema, rede ou uma organização inteira, emulando um cenário de ataque real. O objetivo final é ajudar a identificar riscos específicos, que quando abordados, terão impacto positivo na segurança geral da sua empresa.

O teste de penetração simula o comportamento de um criminoso cibernético real, a fim de identificar problemas na integridade de seus sistemas e aconselha como corrigi-los antes de serem explorados de forma real. Os testes de penetração podem ser realizados fora ou dentro de sua rede para simular ameaças internas. Se você tomar a segurança cibernética a sério, então o teste de penetração é vital.

Acerca de NalbaTech

Nascemos em 2010 com uma missão, **quebrar o paradigma de complexidade que envolve soluções de TI, oferecendo soluções de alta performance, flexibilidade e custo adequados.**

Acreditamos que o negócio deve ser o protagonista da proposta de valor para uma empresa, e que a tecnologia deve ser uma ferramenta agregadora ao seu serviço e não o contrário.

Soluções tecnológicas para problemas complexos.



Segurança global de aplicativos contra fraudes na Web e e-Commerce

Proteção de ataques cibernéticos em sistemas, informações e ativos de negócios.

Utilizamos as melhores ferramentas em sofisticadas infraestruturas de clientes internacionalmente.



Proteja os benefícios e a reputação de sua empresa, evitando desastres financeiros e publicidade negativa associados ao comprometimento de seus sistemas.