Checkmarx | nova8 CYBERSECURITY | aws

O mundo depende de código. Nós o protegemos.

Estudo de caso

Pismo protege seu pipeline de desenvolvimento de software com a Checkmarx

> *Nós levamos a segurança a sério, e nossos clientes confiam em nossa proteção. Nós precisávamos de ferramentas dinâmicas o suficiente para nossos processos, que mudam continuamente; ferramentas comprovadas, estáveis e adaptáveis em termos de escala. Tivemos a sorte de encontrar a Checkmarx, que nos ajudou a melhorar o SLA de identificação e correção de riscos, reduzir o risco e o número de vulnerabilidades e eliminar problemas de alto e médio risco.*

- Ubirajara Aguiar Jr.
Líder de Tecnologia, Red Team/DevSecOps, Pismo

pismo

A exigência: AppSec em um estágio mais inicial do desenvolvimento e ferramentas e processos fáceis de usar

Fundada em 2016, a ***Pismo*** é uma empresa de tecnologia que fornece uma plataforma completa para operações bancárias e processamento de pagamentos. A Pismo evolui e inova continuamente para atender às necessidades de seus clientes com a plataforma de processamento financeiro mais avançada do mercado.

Uma vez que a Pismo é uma plataforma nativa da nuvem na AWS, ela oferece APIs para os aplicativos web ou móveis dos clientes, de modo que eles podem usar a infraestrutura da Pismo como back-end. A base de clientes da Pismo, que consiste em bancos, empresas de tecnologia financeira (fintechs) e instituições não financeiras, usa a tecnologia inovadora da plataforma para lançar e ampliar rapidamente suas soluções digitais de banco e pagamentos, tudo com alta segurança.

Por outro lado, a expectativa de alta segurança implica grande responsabilidade pela redução dos riscos e das vulnerabilidades nas ofertas da empresa.

Para fazer frente à exigência de maior segurança, a empresa contratou Ubirajara Aguiar Jr. dois anos atrás, com a missão de desenvolver e liderar a Red Team/DevSecOps na Pismo. Logo no início, ele avaliou o estado da segurança de aplicativo (AppSec) da Pismo e constatou que os processos existentes e a cultura de segurança de desenvolvimento demandavam melhorias.

"Nós nos demos conta de que era preciso fazer as verificações de segurança em um estágio mais inicial do ciclo de vida de desenvolvimento de software (SDLC), o que é sempre mais fácil, mais rápido, mais barato e mais eficaz que fazê-las posteriormente", observa Aguiar. *"E, para isso, nós precisávamos adotar ferramentas mais completas e mais adaptáveis em termos de escala. Para começar, nós definimos um novo processo e novos critérios de sucesso para a seleção de ferramentas.*

A equipe passou a criar um roteiro de segurança, que incluía não só práticas recomendadas, como fazer a varredura de todos os repositórios, como ainda a escolha de membros para serem embaixadores de segurança e terem acesso inicial às novas ferramentas.

A solução: SAST e SCA da Checkmarx

Aguiar observou que a solução escolhida precisaria ser compatível com várias linguagens de desenvolvimento, oferecer integração bidirecional com ferramentas de monitoramento de erros, abrir e fechar chamados automaticamente e identificar falso-positivos recorrentes.

Além disso, era importante que as ferramentas pudessem ser facilmente integradas nas rotinas dos desenvolvedores para encorajar a adoção e minimizar o atrito ou resistência. *"Sempre temos nossos desenvolvedores em vista ao considerar novas ferramentas. Queríamos que a transição fosse tranquila e transparente, sem que eles se precisassem se preocupar com o processamento de chamados ou de cartões. Estávamos em busca especificamente de ferramentas que tornassem o trabalho dos desenvolvedores mais fácil e mais produtivo."*

Acima de tudo, as ferramentas deveriam permitir que a equipe *"quebrasse o pipeline"*, visto que o objetivo era eliminar vulnerabilidades de alto e médio risco no código nos repositórios principais. Com os critérios em mãos, Aguiar consultou a Gartner para identificar possíveis fornecedores, escolhendo inicialmente oito deles, depois reduzindo-os a três, inclusive a Checkmarx, para uma POC com uma simulação de um pipeline de desenvolvimento real.

A Pismo escolheu o Static Application Security Testing (SAST) da Checkmarx, uma solução de segurança de aplicativo para uso corporativo, que fornece análise rápida, completamente automática, flexível e precisa do código-fonte a fim de identificar falhas de segurança com o potencial de criar vulnerabilidades em códigos personalizados. Com a flexibilidade para executar varreduras completas e incrementais sempre que necessário, o SAST da Checkmarx fornece relatórios completos e altamente precisos, que priorizam vulnerabilidades conforme a gravidade para orientar os desenvolvedores quanto aos problemas a serem solucionados primeiro. O SAST da Checkmarx é compatível com uma ampla gama de linguagens de programação e frameworks. Ele também se integra completamente com o Software Composition Analysis (SCA) da Checkmarx, que a Pismo está usando na nuvem para fornecer grande cobertura de segurança para códigos personalizados e códigos abertos.

A Pismo trabalhou com um parceiro da Checkmarx, a NOVA8, para implantar e obter serviços profissionais para as novas ferramentas. *"A Nova8 é um parceiro importante"*, afirma Aguiar. *"Sempre que precisamos, eles estão prontos para nos ajudar. Eles possuem uma ótima base de conhecimento e profissionais experientes que trabalharam em várias implantações diferentes e que nos ajudaram a solucionar problemas que não poderíamos nem sequer nos imaginar resolvendo por conta própria."*

"A Checkmarx oferece ferramentas incríveis, que são dinâmicas o bastante para apoiar nossas várias implantações, nossos vários desenvolvedores e nossas várias APIs", observa Aguiar. *"É muito importante para nós podermos corrigir erros já no desenvolvimento, não em um ambiente de produção, o que poderia afetar substancialmente nossos clientes. Uma das grandes vantagens do SAST da Checkmarx é que o processo de abertura e fechamento de chamados é completamente automático, o que alivia a carga de trabalho de nossos desenvolvedores e nos permite auditar esse mesmo processo."*

Aguiar menciona que a implantação das soluções da Checkmarx se deu em fases.

> ***"Começamos com a instalação das ferramentas, criação dos ambientes necessários e apresentação de uma avaliação inicial. Depois, passamos a integrar nossas APIs, o que levou cerca de 90 dias. Em seguida, possibilitamos a integração com a ferramenta de monitoramento de erros, que aliás impede que os desenvolvedores quebrem pipelines nos repositórios. Ao final, tínhamos tudo pronto, desde a criação de cartões até a quebra de pipelines."***
>
> - Ubirajara Aguiar Jr., Líder de Tecnologia, Red Team/DevSecOps, Pismo

Os resultados: programa robusto de DevSecOps, SLA melhor de correção de erros e redução de riscos e vulnerabilidades

Com 130 desenvolvedores em diferentes países, cerca de 40 deles (entre profissionais de segurança e engenharia) usuários da Checkmarx, Aguiar observou que os desenvolvedores gostam de usar as ferramentas. *"Por se integrarem tão bem a nossos processos e a nossa cultura de segurança, as ferramentas facilitam que os desenvolvedores corrijam os problemas identificados pela Checkmarx. Estamos satisfeitos com as taxas de adoção e de uso e com o fato de que alguns funcionários já integraram por conta própria a ferramenta em seus fluxos de trabalho."*

"Pudemos definir nosso SLA como apenas 14 dias para a correção de qualquer vulnerabilidade do SAST. A equipe corrige somente problemas de baixo risco, e a Checkmarx bloqueia a combinação de quaisquer novos problemas de alto ou médio risco. TÉ uma ótima sensação." A equipe também está trabalhando assiduamente na estratégia do Software Composition Analysis da Checkmarx. *"Agora, estamos focados em avaliar as vulnerabilidades e classificá-las em quatro categorias: primeiro, as vulnerabilidades mais críticas; segundo, possíveis vulnerabilidades, porém com informações ausentes; terceiro, o uso de pacotes com vulnerabilidades conhecidas, porém em condições não vulneráveis; quarto, o uso de pacotes desatualizados sem vulnerabilidades"*, conta Aguiar. Aguiar e sua equipe agora podem mostrar ao Chefe de Segurança da Informação da Pismo, Leonardo Carmona, e aos executivos da empresa métricas e KPIs importantes, que deixam ver o progresso desde a adoção das soluções da Checkmarx.

"Criamos um gráfico representando riscos e vulnerabilidades; inicialmente, havia um grande número de problemas de alto risco. Agora, todos estão no nível zero, uma vez que foram corrigidos, e não há problemas adicionais. É exatamente o que queríamos. E em um curto período, nossos fundadores e diretores reconheceram que o dinheiro investido na Checkmarx foi bem utilizado," conclui ele.

A conclusão: os desenvolvedores da Pismo adoram usar as ferramentas de AppSec da Checkmarx

- Fortalecimento da cultura de segurança da Pismo
- Eliminação de vulnerabilidades de alto e médio risco
- Correções mais rápidas
- Menos vulnerabilidades não corrigidas

Solução da Checkmarx

- SAST da Checkmarx
- SCA da Checkmarx

Parceiro da Checkmarx

nova8 CYBERSECURITY

Hospedagem na Nuvem

aws

Saiba mais aqui: ***Checkmarx, estudos de caso de clientes da Checkmarx, SAST da Checkmarx, SCA da Checkmarx***