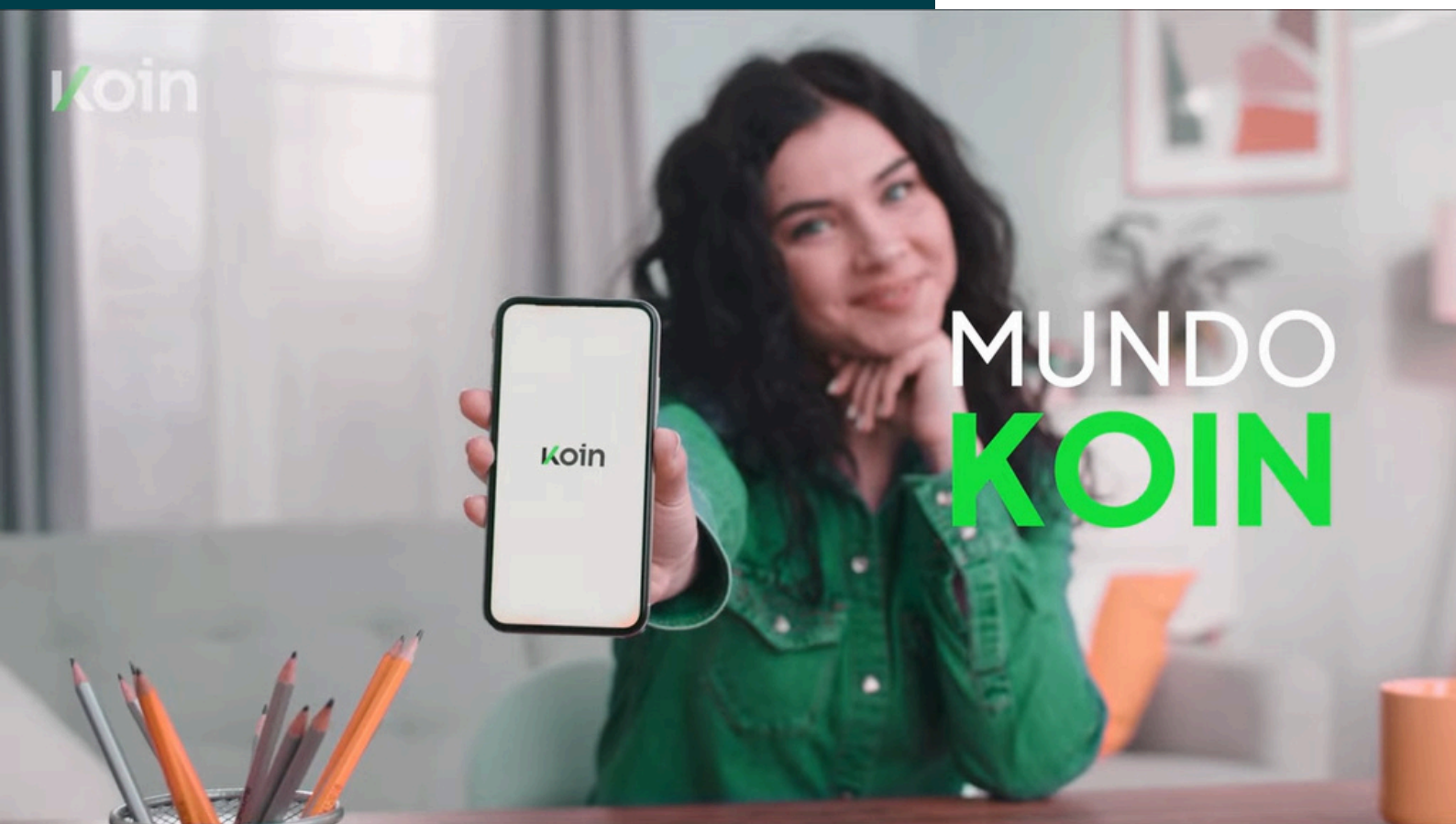
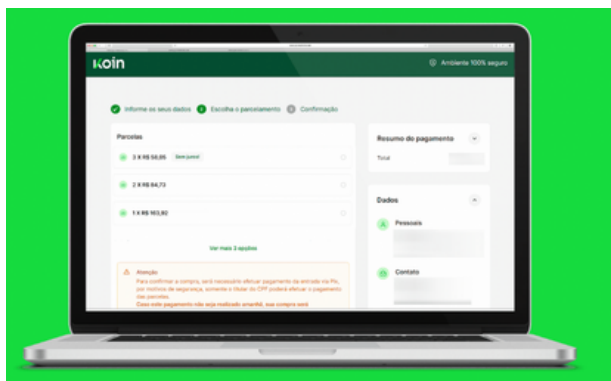


Koin & RealCloud: Proteção em runtime com visibilidade e segurança em cloud com Upwind Security



A Koin

A Koin é uma fintech brasileira pioneira em soluções de pagamento como serviço, com destaque para o modelo BNPL (Buy Now, Pay Later). Com foco na democratização do acesso ao crédito e na simplificação da experiência financeira, a empresa atende tanto consumidores quanto negócios por meio de soluções digitais acessíveis.



A Infraestrutura em Cloud da KOIN

A infraestrutura cloud da Koin é baseada majoritariamente em ambientes AWS e estruturada em três organizações distintas: BNPL (legada), Unified (modernizada) e PCI (voltada à conformidade). Essa divisão permite segmentação operacional e aderência a requisitos específicos de segurança, escalabilidade e governança. A organização BNPL utiliza workloads em EKS com instâncias EC2 e ECS Fargate, enquanto a Unified — que adota melhores práticas e automação via Terraform — vem absorvendo progressivamente os serviços legados.

A operação envolve workloads efêmeros em Auto Scaling Groups, instâncias com diferentes versões de kernel Linux e ambientes críticos em produção e homologação. A instalação de agentes para visibilidade e segurança exigiu soluções adaptadas, como uso de agentes BCC, ajustes em templates de ASG, e otimização do uso de memória em instâncias pequenas como t3.small. A equipe de InfraSec e AppSec da Koin mantém um controle apurado sobre a rede, detecção de vulnerabilidades e automação de respostas, integrando ferramentas como Upwind e Jira para garantir agilidade e rastreabilidade em todo o ciclo de vida da infraestrutura cloud.

Desafios

O crescimento da Koin e a complexidade crescente de seus workloads geraram desafios relevantes para os times de InfraSec e AppSec. Entre os principais estavam a dificuldade em obter visibilidade em tempo real sobre a superfície de ataque em workloads distribuídos, a baixa rastreabilidade de eventos em instâncias efêmeras oriundas de Auto Scaling Groups, a superficialidade das detecções apresentadas por ferramentas tradicionais, e a limitação de integrações eficientes com ferramentas de remediação, como o Jira. Também se destacava a necessidade de monitorar workloads sem acesso à internet, além de alertas excessivos sobre recursos intencionalmente expostos, como buckets S3 públicos utilizados para hospedar websites estáticos.

A Solução

A Koin optou por adotar a plataforma Upwind Security, ferramenta capaz de fornecer visibilidade contextualizada e em tempo real de riscos e vulnerabilidades em workloads vivos. Sua abordagem baseada em tempo de execução prometia dar à Koin um entendimento mais aprofundado sobre o comportamento real dos recursos em produção, superando as limitações das soluções tradicionais de segurança em nuvem.

A Implementação

A RealCloud deu suporte ao time de segurança da Koin na implementação da solução Upwind, com acompanhamento técnico próximo e colaborativo, contribuindo nos testes, ajustes e validação durante a integração de múltiplos workloads. A instalação dos agentes foi realizada em instâncias EC2, clusters EKS e tarefas ECS Fargate, utilizando a versão BCC do agente em kernels compatíveis.

A integração com o CloudTrail central da Koin foi aplicada para detecção de eventos maliciosos em nível de nuvem, como acessos e modificações indevidos, complementando a visibilidade aprofundada já oferecida em nível de workload por meio do sensor. A integração com o Jira foi aprimorada para garantir que os tickets de vulnerabilidades fossem automaticamente abertos e associados ao time responsável por meio de tags por namespace. Avanços técnicos relevantes também incluíram a instalação do agente em instâncias t3.small com apenas 2GB de RAM, o mapeamento de eventos de rede em tempo real e a adaptação de alertas com base no contexto real do ambiente da Koin, como no caso de buckets S3 públicos usados intencionalmente.

A equipe superou desafios como a instalação em instâncias por trás de Load Balancers e a compatibilidade em ASGs, ajustando templates e estratégias de implantação.

"O apoio técnico da RealCloud foi determinante para o sucesso da nossa POC. A equipe atuou lado a lado com nosso time de engenharia e segurança, acelerando a instalação dos agentes, destravando obstáculos com a Upwind e garantindo que conseguíssemos ver valor desde os primeiros dias de uso."

Fabio Franchi, Head de Infraestrutura & Segurança na Koin.

O Papel da RealCloud

A RealCloud desempenhou um papel estratégico durante todo o processo, atuando desde o desenho da arquitetura de integração da Upwind até o "troubleshooting" de agentes e ajuste fino das configurações.

Com conhecimento do ambiente AWS da Koin e da operação da Upwind, a consultoria foi essencial para permitir uma implementação eficiente e alinhada aos objetivos técnicos e de compliance da empresa. A RealCloud facilitou a comunicação entre os times da Koin e da Upwind, contribuindo ativamente para a evolução da maturidade em segurança da organização.

Resultados

A visibilidade obtida marcou a evolução da jornada de segurança da Koin. A Upwind detectou vulnerabilidades com precisão em workloads vivos, contextualizando com base no comportamento real das aplicações. Integrada ao Jira, acelerou a remediação e ajudou a priorizar ações críticas. A plataforma identificou falhas desde pipelines CI/CD até workloads efêmeros, elevando a maturidade da operação.

Com o apoio do time de Customer Success da RealCloud, a Koin acelerou a adoção da plataforma e transformou a operação em resultados práticos. "Reduzimos em mais de 30% o tempo médio de resposta às vulnerabilidades mais críticas após a adoção da Upwind e sua integração ao nosso Jira. Esse resultado só foi possível graças ao acompanhamento próximo da RealCloud em cada etapa do processo", destaca Fabio Franchi.



+55 (21) 2179 7788

Sobre a RealCloud

A RealCloud é líder em soluções de gestão e otimização de nuvem na América Latina, ajudando empresas a alcançar eficiência operacional com redução de custos e aumento de performance. Com clientes como Koin, VTEX, iFood e Hotmart, a RealCloud já auxiliou na economia de mais de US\$ 340 milhões em gastos com nuvem. Saiba mais em: realcloud.systems



RealCloud

© 2025 por RealCloud