

Gerenciamento de exposição a ameaças para Amazon Web Services (AWS)

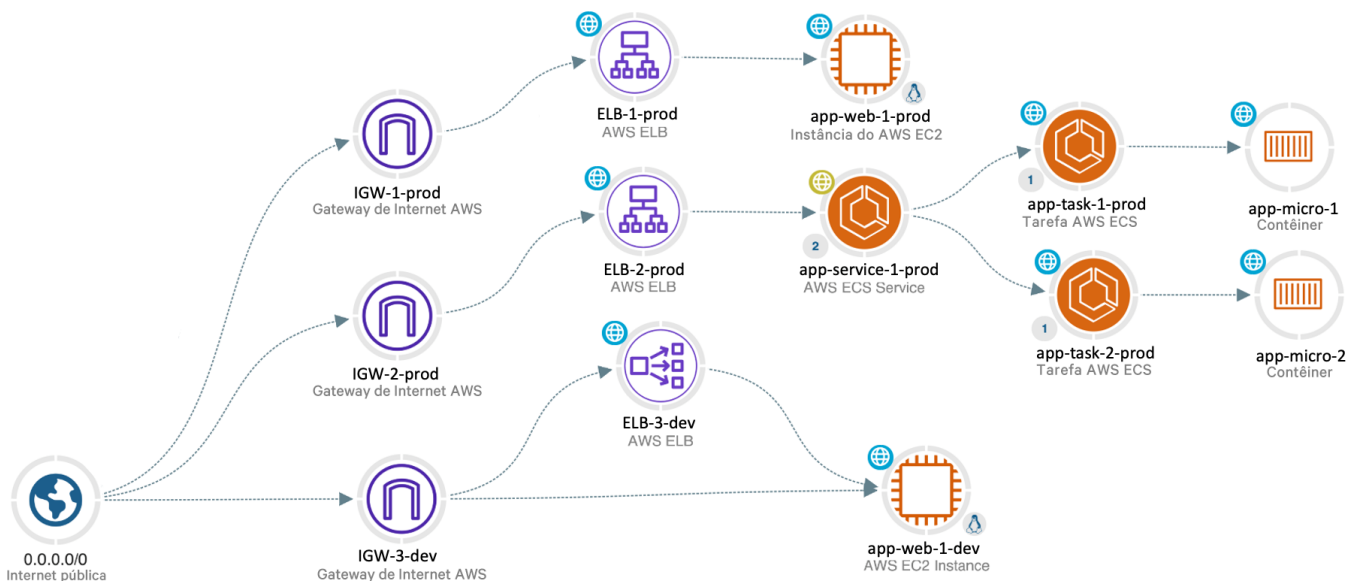
O Observer Sentry permite que você veja seu ambiente da perspectiva do invasor

O Desafio

Em um esforço para melhorar e expandir continuamente a prestação de serviços e aproveitar totalmente os avanços tecnológicos, as arquiteturas de prestação de serviços baseadas em nuvem estão em constante mudança. As pressões comerciais e competitivas forçam muitas organizações a reagir rapidamente—implementando mudanças com frequência o mais rápido possível. As consequências? Identidades de nuvem excessivamente permissivas, aplicativos de contêiner de terceiros com vulnerabilidades de segurança e ativos críticos que são expostos externamente. Esses problemas generalizados resultaram em um crescimento dramático nos casos de exploração de nuvem e violações de dados.

A solução

O Observer Sentry da VIAVI Solutions oferece gerenciamento de exposição a ameaças baseado em software como serviço, oferecendo aos arquitetos de SecOps, DevOps e nuvem a tão necessária visibilidade de ameaças em ambientes AWS em constante mudança. Ao descobrir e combinar caminhos de ataque internos com varredura de superfície de ataque externo focada, o Observer Sentry identifica exposições de segurança, analisa o impacto nos negócios e ajuda a priorizar atividades de remediação.

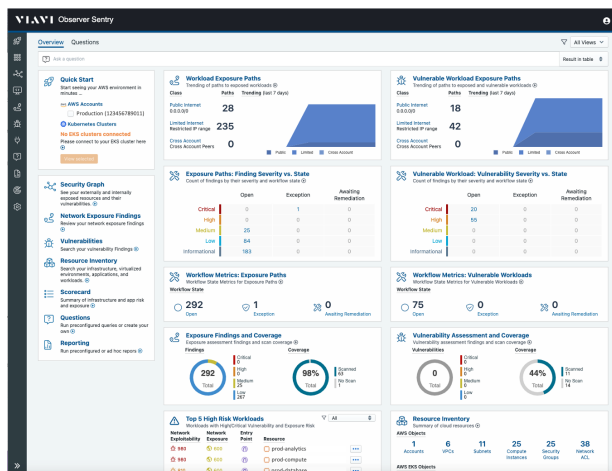


“Os defensores pensam em listas. Os invasores pensam em gráficos. Enquanto isto for verdade, os atacantes vencem.”
John Lambert – Microsoft Threat Intelligence Center

Gerenciamento de superfície de ataque e caminho de ataque

O Observer Sentry cria um inventário detalhado dos ativos da nuvem e, em seguida, realiza uma análise para determinar a superfície de ataque, a exposição e o risco. Essa análise também pode ser aplicada coletivamente a agrupamentos lógicos de ativos que compõem aplicações ou cargas de trabalho específicas. Esses agrupamentos podem ser rastreados em scorecards de risco e visualizados em mapas de superfície de ataque.

Caminhos de ataque são a combinação perigosa de exposição, vulnerabilidades de rede exploráveis e configurações arriscadas que fornecem os caminhos de menor resistência a recursos de alto valor dentro do seu ambiente. O Attack Path Management fornece contexto acionável para seus problemas mais críticos, para que suas equipes possam melhorar de forma proativa e contínua sua postura de segurança na nuvem.



Respostas do Observer Sentry:

Como os atacantes veem meu ambiente AWS?

Onde tenho configurações incorretas?

Que caminhos os atacantes podem explorar?

Onde meus ativos de nuvem estão em risco?

Onde tenho configurações excessivamente permissivas?

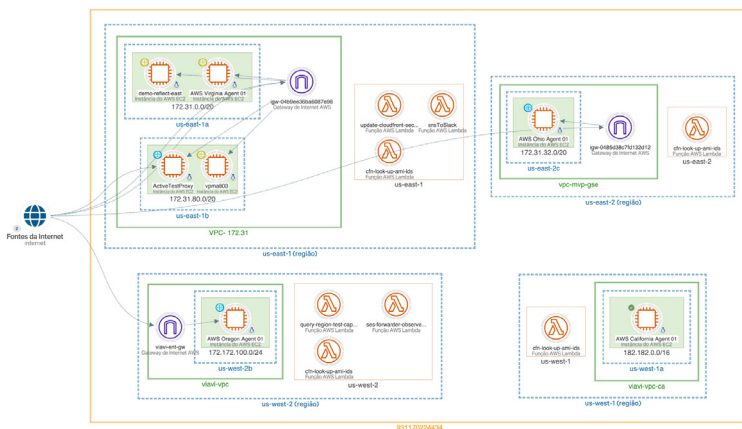
Como priorizo a mitigação de riscos?

Observabilidade da AWS e priorização baseada em risco

Conecte-se ao seu ambiente AWS, aos clusters Elastic Kubernetes Services (EKS) e Elastic Container Service (ECS) em minutos. O Observer Sentry verifica continuamente seus ambientes AWS e gera diagramas altamente intuitivos entre ambientes que ajudam a identificar rapidamente configurações incorretas, configurações excessivamente permissivas e exposições não intencionais.

O Observer Sentry prioriza riscos críticos com base na análise de configurações incorretas, exposição à rede, vulnerabilidades e outros fatores para fornecer uma visão priorizada do risco para seu ambiente de nuvem.

Saiba mais: viavisolutions.com/pt-br/sentry



Experimente o serviço Observer Sentry, sem riscos, em seu ambiente. A ativação típica da conta e a configuração inicial levam menos de 15 minutos.



Contato +55 11 5503 3800

Para encontrar o escritório mais perto de você, visite viavisolutions.com.br/contato

© 2023 VIAMI Solutions Inc. As especificações e descrições do produto neste documento estão sujeitas a mudanças sem aviso prévio. observer-sentry-br-ec-pt-br.30193968.900.0923