VIAVI Solutions

Folheto

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

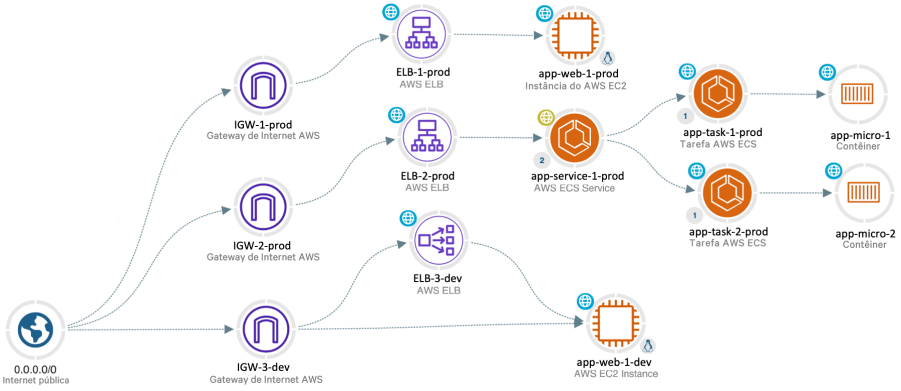
O Observer Sentry permite que você veja seu ambiente da perspectiva do invasor

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 – com frequência implementando mudanças 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 da AWS em constante mudança.



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

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. Usando a integração de detalhes de configuração e dados de tráfego fornecidos pela AWS, os usuários podem ver duas perspectivas criticamente importantes: o que a configuração permitirá (o que é possível) e o que está realmente acontecendo. Isso revela se os criminosos comprometeram recursos expostos ou exploraram vulnerabilidades conhecidas.

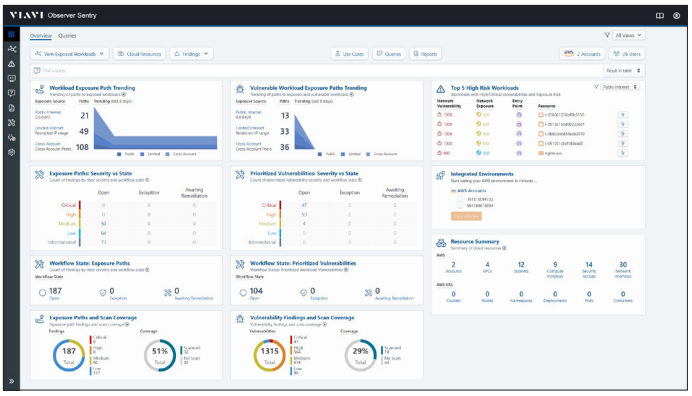
Gerenciamento de superfície de ataque e caminho de ataque

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.

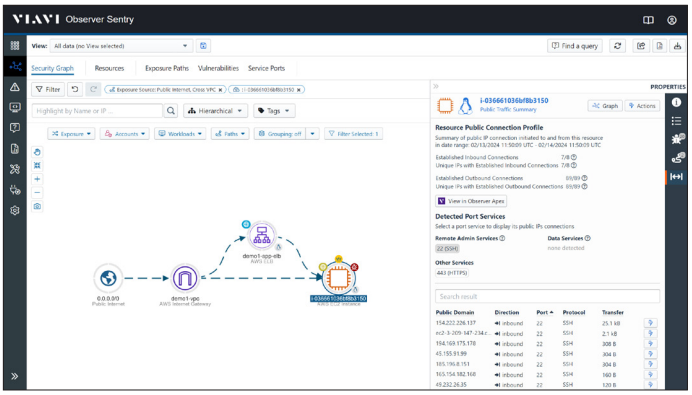
Caminhos de ataque são a combinação perigosa de exposição, vulnerabilidades de rede exploráveis e configurações arriscadas que fornecem os caminhos de menor resistência a recursos de alto valor dentro do seu ambiente. O Attack Path Management fornece contexto acionável para seus problemas mais críticos,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

Integração de dados de tráfego

Quando exposições não intencionais ou vulnerabilidades não corrigidas são identificadas, não é suficiente entender o que poderia acontecer ou o que pode já ter acontecido – você precisa saber o que realmente aconteceu. Por meio da integração de dados de tráfego fornecidos pelos logs de fluxo do VPC da AWS, os usuários do Sentry ganham visibilidade das tentativas de conexão de entrada e saída e conexões estabelecidas por porta e protocolo, bem como com o volume de dados associados a uma conexão. Os usuários podem, então, passar do Observer Sentry para o Observer Apex para realizar uma análise forense detalhada do tráfego de qualquer conversa de interesse ou preocupante.



Identifique exposições não intencionais e priorize cargas de trabalho de alto risco rapidamente



As equipes de segurança obtêm as informações necessárias sobre exposições de alta prioridade integrando um histórico detalhado de tráfego e conversação

Respostas do Observer Sentry:

Como os invasores veem meu ambiente da AWS?
Onde tenho configurações incorretas?
Quais caminhos os invasores podem explorar?
Onde meus ativos de nuvem estão em risco?
Onde tenho configurações excessivamente permissivas?
Como priorizo a mitigação de riscos?
Algum recurso exposto foi comprometido?
Alguma vulnerabilidade conhecida foi explorada?

Observabilidade e priorização baseada em risco da AWS

Conecte-se ao seu ambiente da AWS e aos clusters Elastic Kubernetes Services (EKS) e Elastic Container Service (ECS) em minutos. O Observer Sentry verifica continuamente seus ambientes da AWS e gera diagramas altamente intuitivos entre ambientes que ajudam a identificar rapidamente configurações incorretas e excessivamente permissivas, bem como 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/node/113528

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

VIAVI Solutions

Contato +55 11 5503 3800

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

observer-sentry-br-ec-pt-br
30193968 901 0224