O blog da AWS

DevSecOps: automatize práticas de segurança com uma biblioteca pronta do AWS Solutions

by AWS Admin | on 01 FEB 2021 | in DevOps, Security, Security, Identity, & Compliance | Permalink | Share

Por Bruno Lopes, Technical Trainer, AWS Training & Certification Team.

As ameaças à segurança da informação continuam evoluindo continuamente, tornando as tarefas de proteção e segurança proativas e reativas difíceis, com alto custo de implementação e gastando muito tempo dos profissionais de segurança. Definir rotinas automatizadas para estas respostas, seguindo boas práticas de segurança e de conformidade baseadas em padrões de mercado, é ao mesmo tempo um desafio a ser alcançado, e um objetivo na jornada de DevSecOps.

É sobre isso que iremos falar nesse blog post. Iremos descrever uma solução que faz parte da biblioteca de soluções da AWS, a AWS Solutions. Estas soluções foram projetadas para ajudar os clientes a solucionar problemas comuns e construir mais rapidamente usando a plataforma da AWS. Todas as soluções publicadas nesta plataforma são avaliadas por arquitetos da AWS e desenvolvidas para oferecer confiabilidade, eficácia, segurança e otimização de performance e custos, pilares fundamentais de arquitetura do *AWS Well-Architected Framework*.

Cada solução acompanha um *template* de IaC (*Infra-as-Code*, Infraestrutura como Código) criado em JSON ou YAML seguindo o formato de construção de infraestrutura como código na AWS, através do serviço AWS CloudFormation; e também um guia de implementação, com instruções adicionais, estimativa de custo, tempo de provisionamento e um diagrama da arquitetura implementada, afim de facilitar o seu entendimento e adoção.

A solução que iremos descrever aqui se intitula **AWS Security Hub Automated Response and Remediation**, e traz uma implementação avançada do AWS Security Hub, que traz atributos presentes em produtos como SIEM, CSPM e SOAR, que vão desde a detecção de ameaças, correlação de eventos, análise de conformidade, governança e automação de respostas a incidentes. Esta solução se baseia em componentes essenciais da infraestrutura AWS, como o AWS Config, e outros adicionais como o Amazon GuardDuty, o Amazon EventBridge, o AWS Organizations, etc.

Visão geral da solução

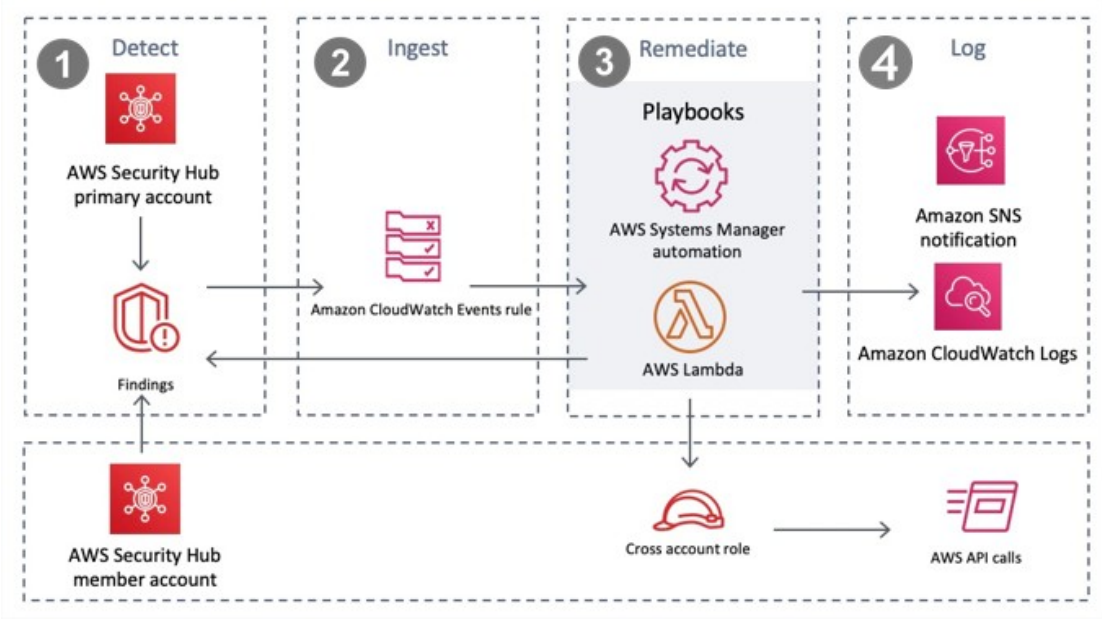

Figura 1 – Arquitetura completa da solução

A solução é composta por quatro estágios, descritos como “fluxos de trabalho”, que podem ser vistos na ilustração da arquitetura logo acima: **(1) Detecção, (2) Ingestão, (3) Remediação** e **(4) Logs**. Estas etapas podem ser implementadas em um ambiente de uma única

conta AWS, ou pode ser implementado em ambiente de múltiplas contas, uma novidade incluída na versão mais recente desta solução.

É importante levar em consideração que há pré-requisitos para o funcionamento não apenas da solução, mas de alguns serviços nela utilizados, como o AWS Config para o AWS Security Hub entre outros. Veja na seção de pré-requisitos abaixo, afim de se preparar de forma mais adequada para sua implementação.

Logo após a execução do template de CloudFormation, são criados dois *Stacks*: o primeiro, para configuração da estrutura básica da solução, utilizando recursos como tópicos do **SNS**, Parâmetros do **Systems Manager**, chaves do **KMS** e funções/*roles* do **IAM**.

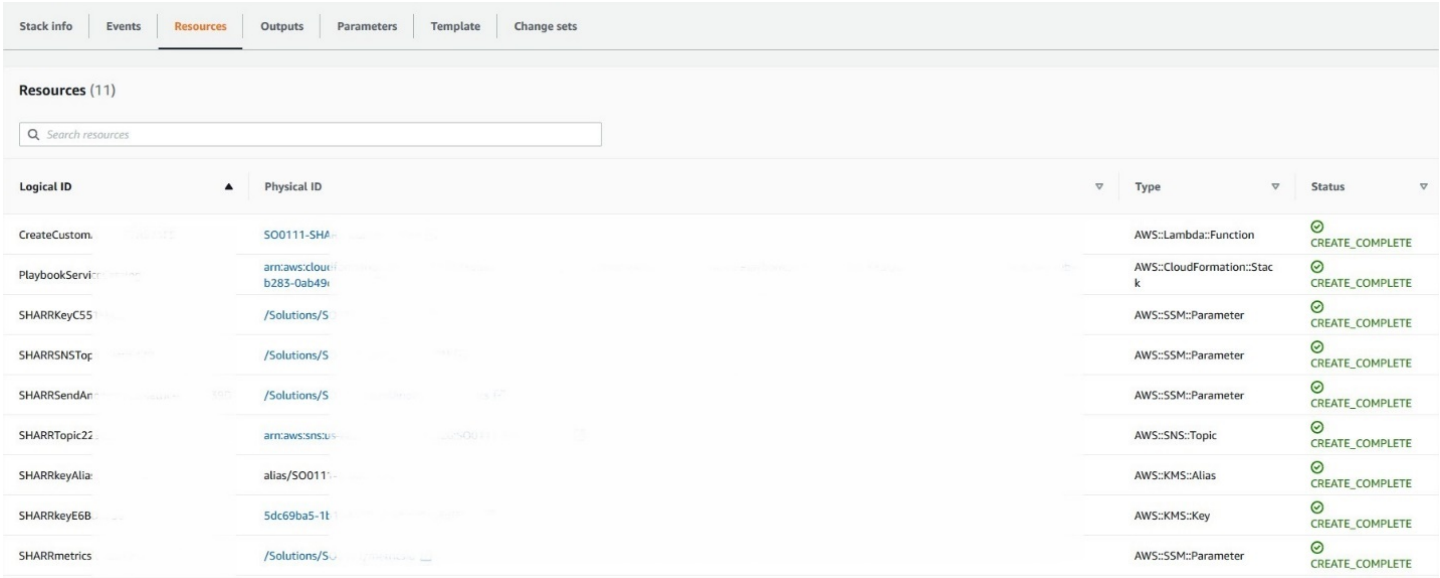

Figura 2 – Stack principal

Já no segundo *Stack* são configurados os *Playbooks*, um conjunto de tarefas de análise e remediação agrupados com o objetivo de organizar e facilitar a administração. Eles podem ser ativados ou desativados via AWS Service Catalog, e podem ser customizados ou até inseridos futuramente em novas versões desta solução. Na data da criação deste artigo, existiam cerca de 18 *playbooks* disponibilizados em um único Portfólio da solução, chamado *Security Hub Playbooks*.

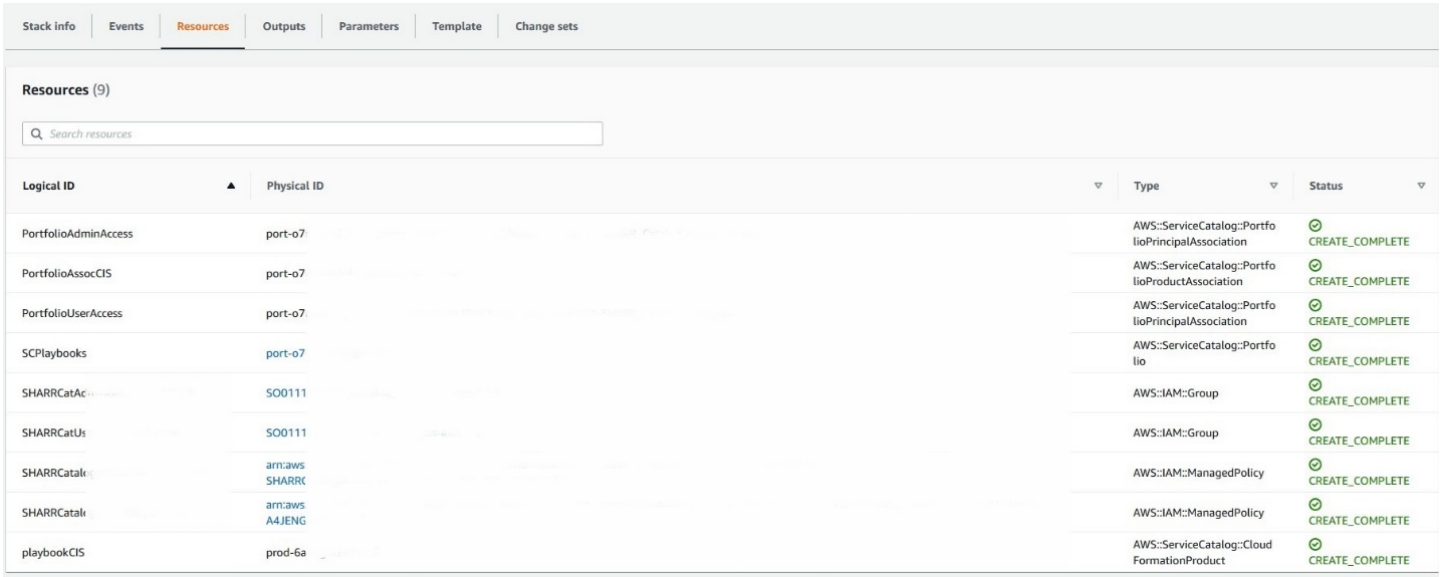

Figura 3 – Stack secundária

O AWS Service Catalog pode ser usado para criar um “catálogo de produtos” na AWS, onde você poderá ofertar neste catálogo serviços provisionados na AWS Cloud utilizando os *templates* de CloudFormation, já devidamente configurados com as suas melhores práticas, requisitos de conformidade e regulações, e oferecer tudo isso aos seus usuários através de um Portfólio, publicados em um portal próprio.

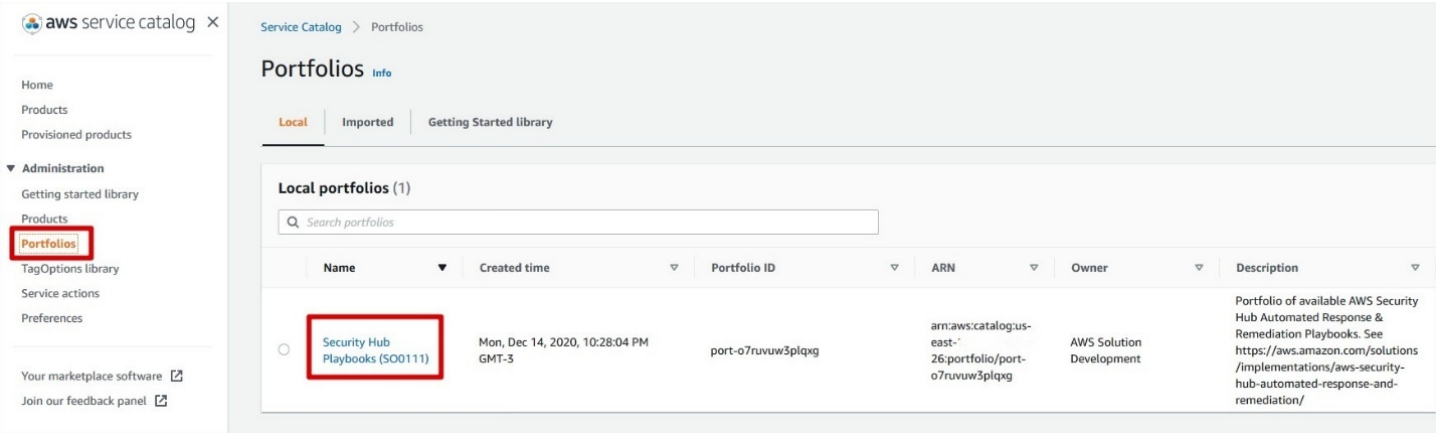

Figura 4 – Portfólio do Service Catalog

Vamos então aos estágios:

1. **Detecção**: Nesta fase, o recurso principal da solução, que é o AWS Security Hub, trabalha na coleta dos eventos e dados provenientes de diversas fontes como AWS Config, GuardDuty, Firewall Manager entre outros. Você pode habilitar outros serviços adicionais no Security Hub, que não estão listados na solução, como o serviço de detecção e proteção de dados confidenciais do Amazon Macie, o novo Amazon Audit Manager para automação de auditorias, o IAM Access Analyzer para verificações de permissões excessivas e até soluções de parceiros do Marketplace. Nesta etapa, ele também irá correlacionar estes eventos com os "pacotes de conformidade" que fazem parte do Security Hub e dão maior abrangência na sua atuação de verificações de segurança. No caso desta solução, o utilizado é o **CIS AWS Foundation Benchmark**. No final deste artigo vamos falar um pouco sobre ele na seção de recursos adicionais.
2. **Ingestão**: Logo após a detecção, é iniciada a parte do processamento e início do fluxo de trabalho dentro da solução. Os eventos do **Amazon EventBridge** (aka CloudWatch Events) serão acionados pelas customizações do Security Hub, na seção *Custom Actions*. Estes eventos servirão como gatilhos para **Lambda** *Functions* ou documentos de *Automation* do **Systems Manager**. Interessante notar aqui que os clientes podem definir se querem automatizar o processo de remediação, ou se querem manter manual.

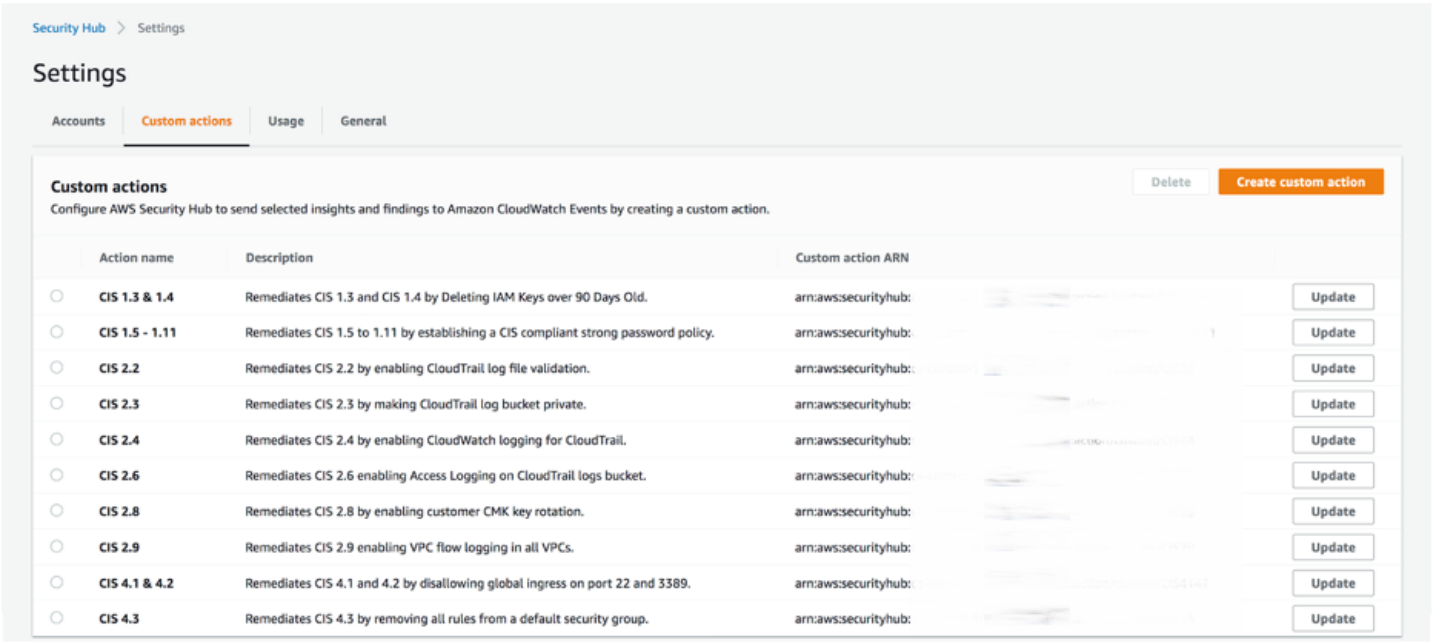

Figura 5 – Custom Actions do Security Hub

3. **Remediação**: Aqui serão executados os processos definidos pelas tarefas de reparação das configurações detectadas como *non-compliant*. Dependendo do item a ser reparado, pode-se utilizar uma função Lambda ou um documento de automação do Systems Manager. As Lambdas são comumente utilizadas quando há necessidade de interação entre contas AWS *(cross-account)*, afim de centralizar o gerenciamento da solução para ambientes de múltiplas contas.

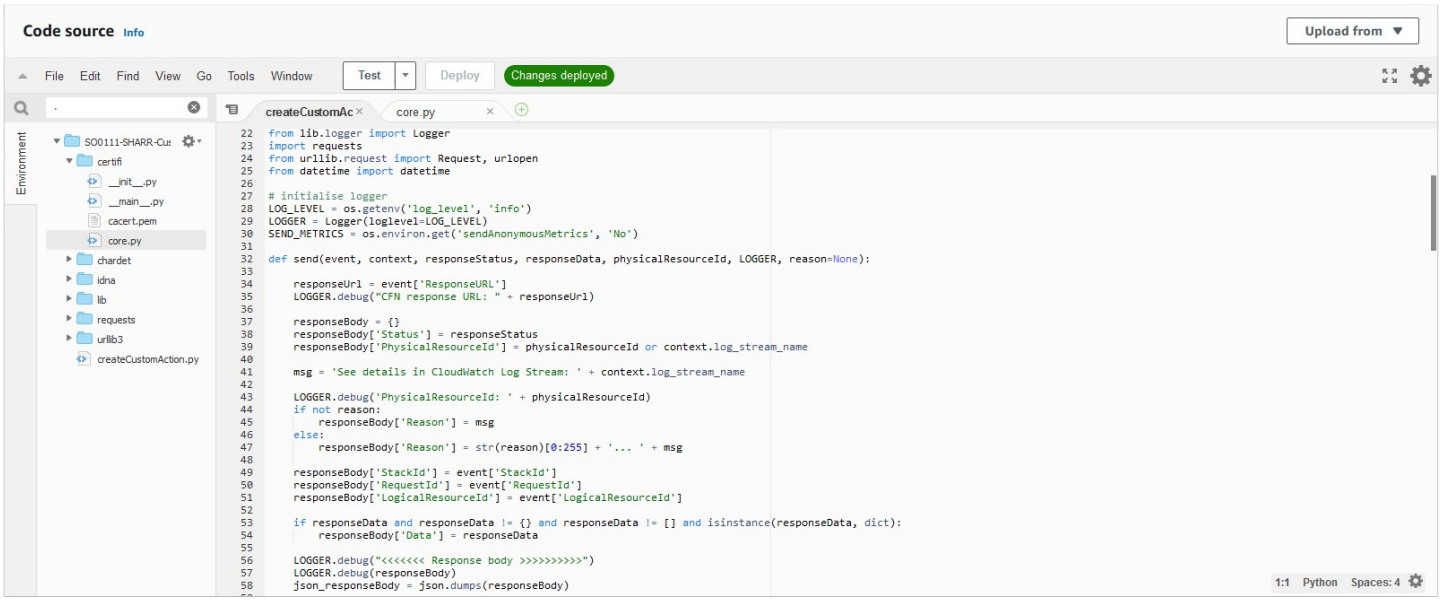

Figura 6 – Lambda function do SHARR

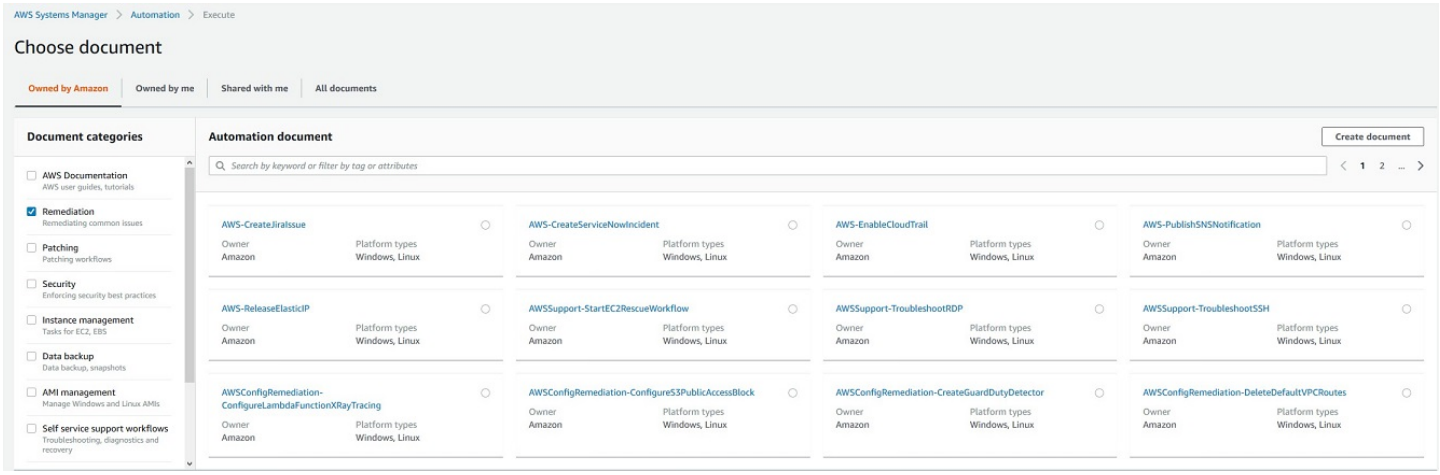

Figura 7 – Documentos do Systems Manager Automation

4. **Logs**: Depois que as medidas são tomadas para remediar os eventos encontrados, os *playbooks* retornam com o resultado das ações e as armazenam em detalhes no CloudWatch Logs. Isso possibilita a obtenção de detalhes para análise póstuma e auditoria, de cada item mitigado, e das respectivas ações que foram realizadas. O processo também aciona um tópico do SNS para envio de notificações aos administradores, ou até mesmo outras ações, como por exemplo o envio de um chamado para o Zendesk. É necessário também notificar ao Security Hub, para que os eventos alarmados no painel sejam resolvidos. Então, o fluxo também altera o status das descobertas *(findings)* do Security Hub para **"RESOLVED"**.

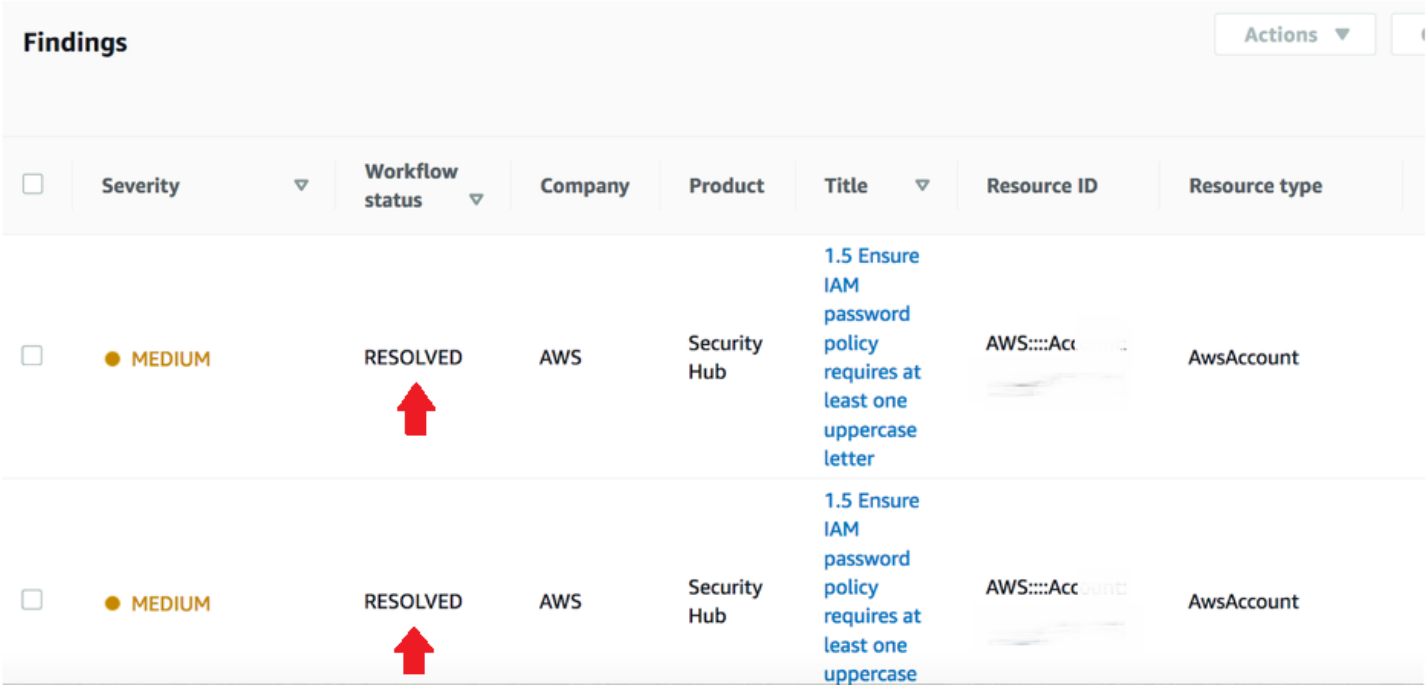

Figura 8 – Painel Security Hub

Pré-requisitos e serviços AWS

Para a configuração desta solução, alguns serviços são necessários como pré-requisitos para a configuração, e outros serão usados como parte da construção da solução final.

- **AWS Config** precisa ser habilitado previamente, como requisito para o AWS Security Hub. Interessante citar que mesmo o AWS Config tendo custo na utilização, neste caso especificamente os clientes não serão cobrados por se tratar de uma configuração habilitada pelo Security Hub, como podemos ver aqui.
- **AWS Security Hub** precisa estar ativo na região de implementação da solução;
- **AWS CloudFormation** e **AWS CDK**, para provisionamento e automação da infraestrutura necessária para implementação e customização da solução;
- **AWS IAM** Roles, políticas e tokens STS para todo o processo de segurança e permissionamento da solução, principalmente quando usada entre contas AWS *(cross-account)*;
- **AWS Systems Manager** para remediação de algumas situações, através dos documentos de automação;
- **AWS Lambda** para remediação de outras situações com maior nível de customização e interação com os SDKs da AWS, por exemplo;
- **Amazon EventBridge** (aka **Amazon CloudWatch Events**) que servirá como gatilho para iniciar os processos de remediação da fase três;
- **Amazon SNS** para fornecer tópicos de notificações, que podem ir de simples ações de envio de emails para times de NOC/SOC, ou até mesmo enviar uma requisição HTTP para um sistema de tickets para encerrar um chamado crítico em aberto, por exemplo.

Recursos adicionais

Para configuração dos *playbooks*, foram usadas as recomendações previamente descritas no *CIS AWS Benchmark*, que possuem diversas práticas recomendadas para segurança dentro dos ambientes em nuvem da AWS.

- **CIS AWS Foundation Benchmark** – Este documento fornece orientação detalhada para configurar as opções de segurança para um subconjunto específico de serviços da Amazon Web Services, com ênfase em configurações fundamentais, testáveis e de arquiteturas agnósticas. Este *benchmark* foi criado por meio de um processo de revisão consensual, composto por especialistas no assunto. Os participantes fornecem perspectivas de um conjunto diversificado de *backgrounds*, incluindo consultoria, desenvolvimento de software, auditoria e conformidade, pesquisa de segurança, operações, governo e jurídico. Cada *CIS benchmark* passa por duas fases de revisão. A primeira fase ocorre durante o desenvolvimento inicial de *benchmark*. Durante esta fase, os especialistas no assunto (*SME – Subject Matter Expert*) se reúnem para discutir, criar e testar rascunhos de soluções do *benchmark*. Essa discussão ocorre até que se chegue a um consenso sobre as recomendações documentadas. A segunda fase começa após a publicação do *benchmark*.

Durante esta fase, todos os feedbacks fornecidos pela comunidade da Internet são revisados pela equipe, para incorporação no *CIS benchmark*.

- **Playbooks da versão 1.0** – ações de monitoria e remediação criadas para automação das tarefas detectadas pelo AWS Security Hub. Abaixo podemos ver uma lista de cada um deles, e o link para a documentação na respectiva numeração:

1.3 – Certifique-se de que as credenciais não utilizadas por 90 dias ou mais estejam desativadas

1.4 – Certifique-se de que as chaves de acesso sejam rotacionadas a cada 90 dias ou menos

1.5 – Certifique-se de que a política de senhas do IAM requer pelo menos uma letra maiúscula

1.6 – Certifique-se de que a política de senhas do IAM exige pelo menos uma letra minúscula

1.7 – Certifique-se de que a política de senhas do IAM requer pelo menos um símbolo

1.8 – Certifique-se de que a política de senhas do IAM requer pelo menos um número

1.9 – Certifique-se de que a política de senhas do IAM requer um comprimento mínimo de 14 ou mais

1.10 – Garantir que a política de senhas do IAM evite a reutilização de senha

1.11 – Certifique-se de que a política de senhas do IAM expire as senhas em 90 dias ou menos

2.2 – Certifique-se de que a validação do arquivo de log do CloudTrail esteja habilitada

2.3 – Certifique-se de que o bucket S3 do CloudTrail não esteja publicamente acessível

2.4 – Certifique-se de que os logs do CloudTrail sejam integrados aos logs do Amazon CloudWatch

2.6 – Certifique-se de que o log de acesso ao bucket S3 esteja habilitado no bucket do CloudTrail

2.8 – Certifique-se de que o rotacionamento para CMKs criadas pelo cliente esteja habilitada

2.9 – Certifique-se de que os logs do VPC Flow Logs estejam habilitados em todas as VPCs

4.1 – Certifique-se de que nenhum grupo de segurança permita a entrada de 0.0.0.0/0 para a porta 22

4.2 – Certifique-se de que nenhum grupo de segurança permita a entrada de 0.0.0.0/0 para a porta 3389

4.3 – Garanta que o grupo de segurança padrão de cada VPC restrinja todo o tráfego

Customizações e Desinstalação da solução

Os recursos para esta solução foram criados utilizando o AWS CDK, uma forma diferente e eficiente de escrever Infraestrutura como Código para a AWS. Podem ser facilmente customizáveis para adequar a sua necessidade de implementação, inclusive tendo o código da solução aberto e disponível no repositório do GitHub da AWS Labs.

Se não houver mais interesse em manter a solução, você pode efetuar a remoção da mesma através da interface do CloudFormation, pela qual fez o provisionamento. Basta excluir a *Stack* principal, e será iniciado o processo de desprovisionamento dos recursos. Lembre-se que alguns recursos criados manualmente podem não ser removidos juntamente com a *Stack*. Outros serão mantidos propositalmente, como os logs do **CloudWatch Logs**, a fim de manter as políticas de conformidade das organizações de acordo com as suas preferências.

Conclusão

Neste blog post, explicamos sobre a solução **SHARR** – *AWS Security Hub Automated Response and Remediation*, criada pela AWS com intuito de auxiliar na parametrização do AWS Security Hub, oferecendo oportunidades de automação e remediação de situações de não-conformidade descritas no guia de referência do *CIS AWS Foundation Benchmark*.

Explicamos também quais as fases que a solução contempla, e quais ações e serviços são usadas em cada uma delas. Pudemos entender quais benefícios essa estratégia pode trazer para auxiliar as estratégias de DevSecOps dentro das nossas organizações, trazendo segurança sem comprometer a agilidade e os processos.

Sobre o autor

Bruno Lopes é Technical Trainer no time da AWS LATAM. Trabalha com soluções de TI há mais de 12 anos, tendo em seu portfólio inúmeras experiências em *workloads* Microsoft, ambientes híbridos e capacitação técnica de clientes. Como Trainer, já está há mais de 6 anos dedicando seus dias a ensinar tecnologias de ponta aos clientes da América Latina.

Revisores

Caio Ribeiro Cesar atualmente trabalha como arquiteto de soluções especializadas em tecnologia da Microsoft na nuvem AWS. Ele iniciou sua carreira profissional como administrador de sistemas, que continuou por mais de 13 anos em áreas como Segurança da Informação, Identity Online e Plataformas de Email Corporativo. Recentemente, se tornou fã da computação em nuvem da AWS e auxilia os clientes a utilizar o poder da tecnologia da Microsoft na AWS.

Daniel Garcia é arquiteto de soluções especialista em segurança com experiência de mais de 20 anos em tecnologia e segurança da informação. Daniel trabalha continuamente para ajudar companhias de vários segmentos e abrangências geográficas a definir, planejar e implementar com sucesso suas estratégias de cibersegurança.

TAGS: AWS, devops, Segurança