ANALISTA SOC

Excel Management Conseil
PORTUGAL

O projeto está na fase de desenvolvimento, onde é necessária um consultor para desenvolver e construir os use case de Segurança no Cloud Público, os Playbooks de resposta, e realizar um plano de testes de ponta a ponta, incluindo os critérios de aceitação do usuário e o implantação em produção.

1.OBJETIVOS

Apoiar a entrega do projeto para expandir a plataforma de segurança global existente, Azure Sentinel, para monitorar logs e alertas do Cloud Público. Desenvolver e projetar as regras de detecção e os Playbooks de resposta alinhados com os use case de segurança selecionados.

2. PRINCIPAIS TAREFAS DO SERVIÇO

Trabalhando em estreita colaboração com a equipa do programa, a equipa existente de Defesa e os parceiros externos, as principais responsabilidades do consultor de segurança no Cloud Público serão liderar e apoiar as seguintes tarefas, seguindo a fábrica de use case internos do cliente destacada abaixo:

- Avaliar os use case do Cloud existentes
- Documentar as especificações dos use cases
- Construir as regras de detecção necessárias, quando necessário
- Desenvolver os Playbooks de resposta necessários para reagir aos incidentes detectados
- Construir e realizar o plano de teste de ponta a ponta e aceitação do usuário
- Reajustar as regras de detecção, os Playbooks conforme necessário
- Garantir uma aceitação tranquila do usuário e o deploy em produção

3.PRINCIPAIS ENTREGÁVEIS DO SERVIÇO

- Construir regras de detecção alinhadas com os use case selecionados para GCP e OpenShift, RedHat
- Construir o Playbook de resposta apropriado e o ticket Silva para gerir incidentes de segurança
- Construir e realizar um plano de testes detalhado para as regras de detecção e o Playbook de resposta desenvolvidos
- Coordenar e gerir a entrega técnica e os critérios de aceitação do usuário para passar para produção/Business As Usual

4.EXPERTISE NECESSÁRIA

- Desenvolvimento de use case no Azure Sentinel
- Redação de Playbooks associados
- Experiência em provedores do Cloud e soluções de segurança associadas: AWS, Azure, GCP, Azure Security Center; Guard Duty
- Experiência em atividades de SOC: triagem, investigação e resposta
- Abordagem de testes e aceitação de usuários
- Técnicas Mitre ATT&CK

SOC ANALYST

The project is in development phase where a resource enforcement is needed to develop and build the Public Cloud Security use cases, response Playbooks and perform end-to-end test plan including user acceptance criteria and deployment to production.

1.OBJECTIVES

- Support the project delivery to extend the existing Global Security Platform Azure Sentinel to monitor the Public Cloud logs and alerts
- Develop and design the detection rules and response Playbook in alignment with the selected security use cases

2. SERVICE MAIN TASK

Working closely with both the program team, the existing Cyber Defense team and the external partners, the main duties of the Public Cloud Security service will lead and support the following tasks following the client internal use case factory highlighted below :

- Assess the existing Cloud use cases
- Document the use cases specifications
- Build the required Detections rules when it's needed
- Develop the response Playbooks needed to react on detected incidents
- Build and perform the end-to-end test plan and user acceptance
- Fine-tune and readjust the Detection rules, Playbooks as needed
- Ensure a smooth user acceptance and production deployment

3.SERVICE MAIN DELIVERABLES

-Build detection rules in alignment with the selected use cases for GCP and OpenShift, RedHat
-Build the appropriate response Playbook and Silva ticket to manage security incidents
-Build and perform a detailed test plan for the developed detection rules and response Playbook
-Coordinate and manage the technical handover and user acceptance criteria to move to production/Business As Usual

4.REQUIERED EXPERTISE

-Use Case development in Azure Sentinel
-Associated playbook writing
-Expertise of cloud provider and associated security solutions: AWS, Azure, GCP,
Azure security Center; Guard Duty
-Expertise of SOC activities: triage, investigation, and response
-Testing approach and user acceptance
-Mitre Att&ack techniques.