Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Implementing Runtime Security Monitoring for AWS Container Clusters

By: David Williams Supervisor: Hisain Elshaafi

4th year Cybersecurity & IT Security

C00263768

Introduction

This research is dedicated to exploring the critical intersection of security and containerized environments within AWS cloud computing. With a particular emphasis on Falco, a leading security tool for cloud containers, the study delves deep into cybersecurity considerations in modern cloud infrastructures.

The escalating demand for enhanced cloud container security globally, particularly accentuated in Europe, has driven the increasing adoption of AWS cloud services. This increases the critical role of security needed in shaping the expansion of AWS infrastructure across European regions. Furthermore, the pivotal role of AWS Elastic Kubernetes Services (EKS) in modern cloud architecture is highlighted, alongside the emergence of Falco as a leading runtime threat detection tool. This convergence underscores the critical importance of implementing robust security measures within cloud container environments, with a particular emphasis on the effectiveness of solutions like Falco. As cloud container demands increase, so too the role of Falco as a leading runtime threat detection tool becomes increasingly pivotal. Therefore, there is a pressing need for further exploration of AWS services and security solutions like Falco to effectively address evolving security challenges in cloud containerisation.

The key focus to this research is the exploration of Falco, a runtime threat detection in real time security and AWS Elastic Kubernetes Services (EKS), a cornerstone of contemporary cloud architecture. Understanding its operational intricacies, configurations, and pivotal features is paramount to grasping its potential impact. Furthermore, the investigation extends to prospective tools like Falcosidekick UI, shedding light on its significance in bolstering cloud security and operational efficiency within AWS environments.

Research

How does the growing presence of AWS cloud services in Europe correlate with the increasing emphasis on enhanced security measures?

What are the operational intricacies, configurations, and pivotal features of Falco, and how does it contribute to real-time threat detection in AWS cloud environments?

What role does AWS Elastic Kubernetes Services (EKS) play in contemporary cloud architecture, and how does its integration with Falco enhance security in containerized environments?

How does the Falcosidekick UI contribute to enhancing security and operational efficiency within AWS environments, particularly in conjunction with Falco and AWS Elastic Kubernetes Services (EKS)?

Technologies

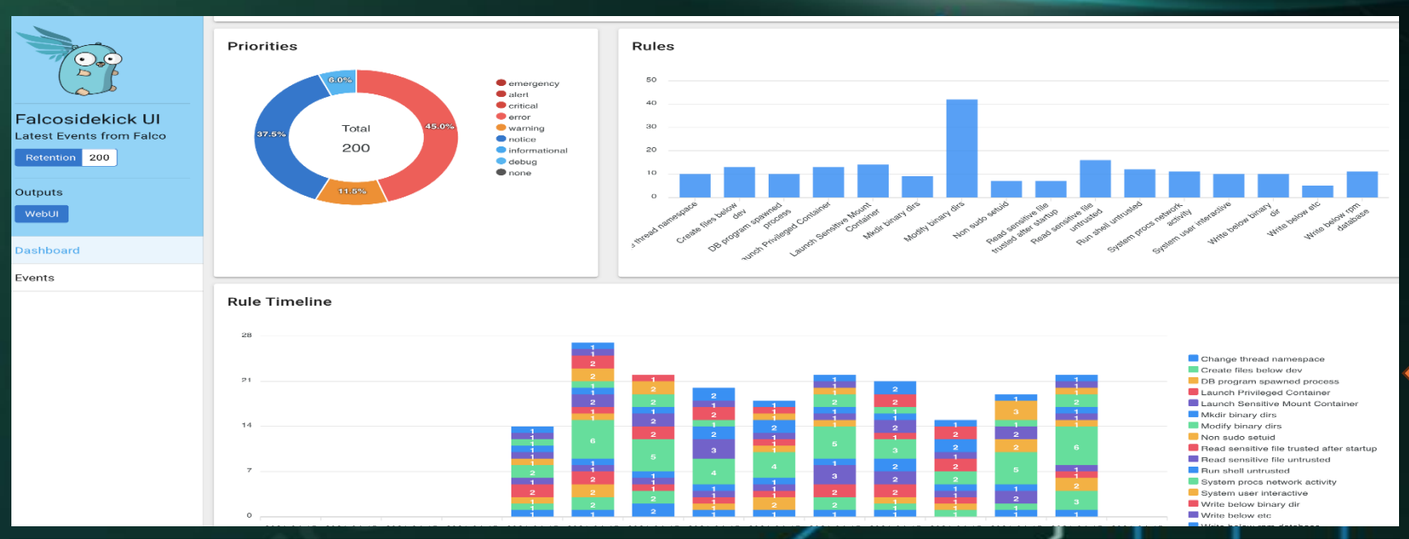
Amazon EKS

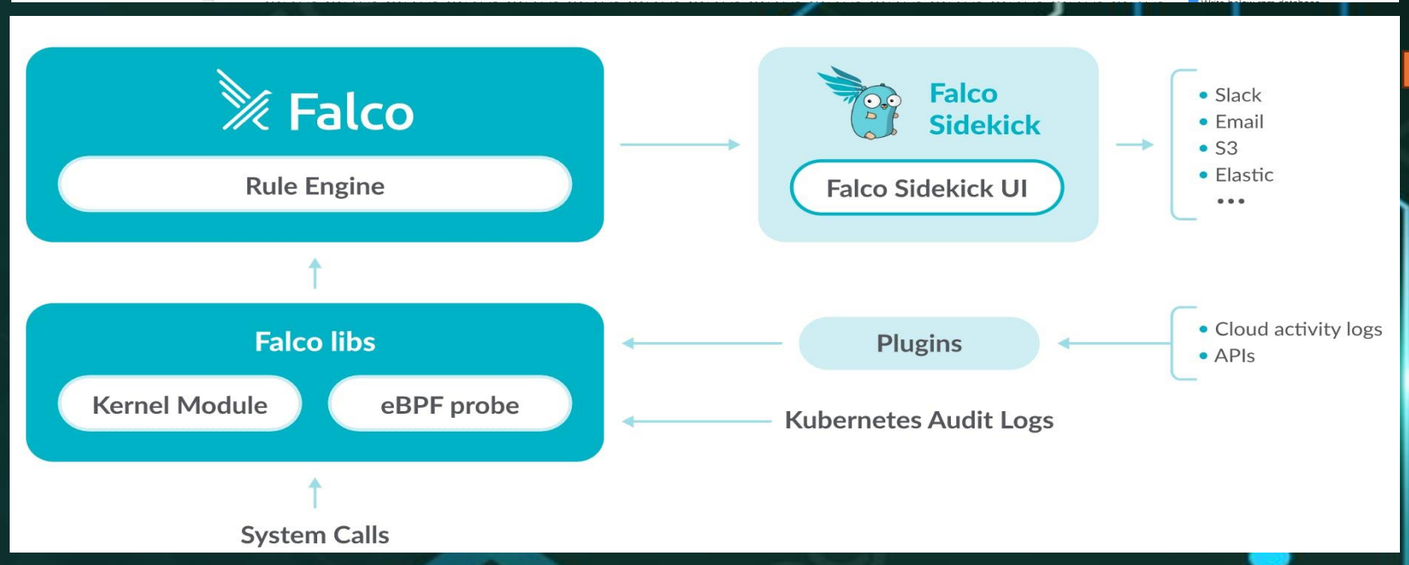
AWS Lambda

Falco

aws

ubuntu





Events

- Unauthorized Access
- Anomaly Detections
- Privilege Escalation
- File System Modification

Methodology

Research: Conduct extensive research on AWS cloud computing, containerization, security measures, and tools like Falco and Falcosidekick UI.

Gather empirical data from various sources including documentation, industry reports, and case studies to understand current practices and challenges.

Hypothesis: My hypothesis is that the seamless integration of Falco and Falcosidekick UI with AWS services will improve threat detection capabilities and operational efficiency in containerised environments.

Experiment: Design and implement experiments to evaluate the performance of Falco and Falcosidekick UI within AWS environments.

Set up test environments using AWS resources and containerized applications to simulate real-world scenarios.

Configure security configurations and operational parameters to measure the impact of Falco and Falcosidekick UI on security and efficiency metrics.

Analysis: Analysing the collected data using statistical methods and qualitative analysis techniques.

Evaluate the effectiveness of Falco and Falcosidekick UI in detecting and mitigating security threats.

Assess the impact of integration with AWS services on operational efficiency and resource utilization.

Conclusion: Summarize findings and draw conclusions based on experimental results.

Provide insights into the potential benefits and challenges of integrating Falco and Falcosidekick UI with AWS cloud services.

Offer recommendations for leveraging these tools to enhance security and operational efficiency in containerized environments within AWS.