Adrian Furo

aady81@outlook.com | +400770872200 | Timisoara, Romania | https://adrianfuro.com/about

EDUCATION

BS Computer Science [redacted]

Polytechnic University of Timisoara, Timisoara, Romania

WORK EXPERIENCE

DevSecOps - Security Engineer

December 2022 - Present

Resideo, Bucharest, Romania (REMOTE)

- Write and maintain Terraform code to provision and manage cloud infrastructure, while ensuring compliance through Policy as Code (Hashicorp Sentinel) scripts
- Manage the security of Docker containers and Kubernetes clusters using Prisma Cloud Compute Edition (formerly Twistlock) by Palo Alto
- Fine-tune runtime policies/rules for Prisma Cloud to optimize security and performance
- Develop custom scripts for Multi-Cloud environment.
- Write Open Policy Agent scripts to ensure code compliance in CI/CD pipelines

DevOps Engineer

August 2022 - December 2022

Atos, Timisoara, Romania

- Automated the build and deployment of cloud infrastructure using Jenkins, Terraform, Ansible
- Developed Python tools that automated the process of deploying secure cloud infrastructure
- Managed and monitored on-prem Linux instances
- Deployed applications using Docker containers and ensured high-availability with K8S
- Configured Web-Apps on Linux servers with full SSL encryption and containerized them

Cloud Security Engineer

April 2021 - August 2022

Atos, Timisoara, Romania

- Managed Microsoft Azure resources by improving the overall Security Posture
- Monitored security related events on cloud using SIEM technology
- Developed Python scripts to aid Cloud related tasks
- Experimented with HSM's

SKILLS

Programming Languages	Python, Bash, Yaml, Rego, Golang
Tools	Git, Terraform, Ansible, Prisma Cloud
Soft Skills	Leadership, Critical thinking, Flexibility and adaptability, Teamwork
Platforms	GitHub, GitLab, AWS, Azure, GCP, OCI
Technologies	Docker, K8S, Linux
Domains	DevOps and DevSecOps, Cloud Security, Cybersecurity, Offensive Security

PROJECTS

2048 & The Aviator *JS, Python, HTML & CSS, SQL*
Two web-based games to enhance the company's promotional efforts, utilizing JavaScript, HTML, CSS, and Python for backend development. To ensure a containerized environment, I created custom Docker images for both games. These games featured leaderboards that fetched data from a MySQL database, also hosted within a Docker container.

Azure Resources and Security Analysis Automation *Python, Azure CLI* https://github.com/adrianfuro/azure_helper
Developed an automation script using Python and Azure CLI to streamline data collection and security analysis of Azure resources. The script conducts comprehensive vulnerability scans within the Azure environment, integrating with Azure Defender to generate actionable security recommendations. Key features include automated data gathering, reducing manual input errors, and exporting data and analysis results to CSV for simplified data management and reporting.

PCMan's FTPD 2 Exploit *Python, Immunity Debugger, MSF Console* https://github.com/adrianfuro/exploit_pcmanftpd2
I engineered a Python script designed to exploit a buffer overflow vulnerability in a specific FTP server application, PCman's FTPD 2 server. The focus of this project was to investigate how such vulnerabilities can be manipulated to execute arbitrary code, thereby highlighting the potential severity of such security gaps. The script works by manipulating memory, specifically targeting stack registers such as EIP and ESP. This manipulation allows for the execution of arbitrary code, demonstrating the potential risks associated with buffer overflow vulnerabilities. This project underscored the importance of secure coding practices and robust security measures in software applications, while also enhancing my technical prowess in Python scripting and cyber security

Terraform Apache-Tomcat Deployment on Azure *Terraform* https://github.com/adrianfuro/terraform-assessment
I developed a Terraform module specifically for Azure, designed to automate the provisioning of an entire infrastructure. The infrastructure built by this module includes key components such as a Virtual Machine Scale Set and a Load Balancer, ensuring the efficient distribution of network traffic and the capability to handle fluctuations in workload. The primary application served by this infrastructure is Apache Tomcat, a widely-used open source implementation of the Java Servlet, JavaServer Pages, and Java Expression Language technologies. This project not only showcases my expertise in infrastructure as code (IaC) and cloud services but also demonstrates my ability to automate and optimize complex infrastructure setups

VM Provisioning - IaC Automation (Security Implementation Lead) *Terraform, Open Policy Agent, Hashicorp Sentinel, GitHub Actions, Jenkins, Ansible AWX, HCP Packer*
As the Security Implementation Lead for the Corp-IT IaC Automation project, my responsibilities encompassed the implementation of all security measures within an automated pipeline. This pipeline was activated when a user raised a ticket on ServiceNow (SNOW). The project involved a seamless integration of SNOW, Terraform, and Jenkins. SNOW communicated with Terraform via Jenkins, parsing the input from the ticket request to initiate the provisioning process. This process was designed to be multi-cloud, supporting Azure, AWS, and VMWare vSphere. A crucial part of the infrastructure in Jenkins was the deployment of HCP Packer. This tool was utilized to create Golden Images, ensuring the delivery of secure, custom-built VM images across all cloud platforms. During the VM provisioning process on Terraform.io, policy compliance checks were conducted by Open Policy Agent and Hashicorp Sentinel. These checks were performed on the Terraform plan (tfplan), a component I was personally responsible for. My role involved the creation and implementation of the security check policies. Upon the completion of provisioning, Terraform.io communicated with Ansible AWX via a REST API. This interaction was designed to transmit the output of the run, which included details such as the VM's IP and ID, to commence the patch management phase. During the patch management phase, I integrated Open Policy Agent within the Github Actions workflow for the repository where Ansible playbooks were stored. This resulted in security scans being triggered after each merge or pull request. This project showcased my proficiency in security implementation, automation, and infrastructure management across multiple cloud platforms. It demonstrated my capability to integrate various tools and platforms to create a secure, efficient, and automated multi-cloud IT infrastructure.