Daniele Mucci

Staff Security Engineer

✉️ daniele@mucci.me 📞 (+372) 55964972 🌐 daniele.mucci.me

Work Experience

Form3

Staff Cloud Security Engineer   *Apr 2025 - current*

I moved to a technical leadership position, taking the role of Staff Engineer with a focus on the Kubernetes and platform area.

Form3

Lead Cloud Security Engineer   *Dec 2022 – Apr 2025*

I took the lead the Platform Security team, whose main responsibilities involved creating and implementing security standards and guidelines for many platform components.
- SME for Kubernetes, Linux and containers security and main security contact for the engineering platform teams, performing many ad-hoc investigations, threat modeling activities, evaluations and generally contributing to the platform design.
- Lead a team of up to 4 people.
- Artifact attestation and admission control in Kubernetes using Sigstore tooling (support and experimentation).
- Lead internal initiatives to raise standards (e.g., knowledge management and documentation).

Form3

Senior Cloud Security Engineer   *Apr 2022 – Dec 2022*

I joined Form3 as a cloud security engineer and worked on designing, implementing, maintaining and configuring the CNAPP solution for a multi-cloud platform. I have also worked on some internal Go tooling for managing accesses to production environments.
- Rollout of CNAPP solution across multiple clusters.
- Runtime security for Kubernetes via falco/Kyverno (custom) rules/policies, in multi-cloud and baremetal environments.
- Developed just in time access capability to GCP.

Coolbet

Lead Security Engineer   *Nov 2021 – Apr 2022*

I led the Security Engineering team within the company. The main tasks included supporting the company's compliance objectives by recommending, designing and implementing security controls. These controls ranged from network to Kubernetes security, including securing the development pipeline, championing secure software development and application security practices. I designed, coordinated and implemented the vulnerability management program. In addition to the technical responsibilities, I managed my team resources, budget, prioritization and internal training.
- Supported the Terraformation for the self-managed identity provider
- Implemented from scratch in-house vulnerability scanner integrating FOSS tooling
- Hardened Kafka deployment using Vault

Coolbet

Information Security Engineer   *Jan 2020 – Nov 2021*

I moved my focus fully on security, assisting in developing the Information Security Program and policies for the organization, implementing technical controls for Kubernetes clusters and the development pipeline, and performing targeted penetration tests.

Coolbet

Security Operations Engineer   *Oct 2018 – Jan 2020*

In addition to the previous responsibilities, I investigated and resolved recurring issues and security incidents and worked on securing the Kubernetes clusters.

Coolbet

System Administrator   *Sep 2016 – Oct 2018*

I performed standard Linux administration tasks, including servers deployment and maintenance while managing multiple Kubernetes clusters.

Licenses and Certifications

CKS - Certified Kubernetes Security Specialist   *Certificate URL*
The Linux Foundation   *Jan 2024*

Linux/UNIX Network Programming   *Certificate URL*
man7.org   *Jan 2024*

System Programming for Linux Containers   *Certificate URL*
man7.org   *May 2023*

CKA - Certified Kubernetes Administrator   *Certificate URL*
The Linux Foundation   *May 2023*

eWPT - Web Application Penetration Tester   *Certificate URL*
eLearnSecurity   *Mar 2023*

CCSE - Certified Container Security Expert   *Certificate URL*
Practical DevSecOps   *Feb 2023*

OSCP - Offensive Security Certified Professional   *Certificate URL*
Offensive Security   *Nov 2021*

eXDS - Certified eXploit Developer   *Certificate URL*
eLearnSecurity   *May 2021*

eCPPT - Certified Professional Penetration Tester   *Certificate URL*
eLearnSecurity   *Sep 2020*

Education

Tallinn University of Technology (TalTech)
Master's Degree in Cyber Security   *Sep 2015 – Jun 2018*
- **Score**: 5/5
- **Courses**: Information System attack and defense, Malware I and II, Secure Software Development

La Sapienza University of Rome
Bachelor's Degree in Computer Engineering   *Sep 2012 – Jun 2015*
- **Score**: 110/110 cum laude

Skills, Languages, Interests

- **Languages**: Italian (Native), English (Professional), Russian (Elementary)
- **DevSecOps**: Kubernetes (advanced), containers (advanced), Linux (intermediate), Terraform (intermediate), Ansible (intermediate), AWS/GCP/Azure (basic), Hashicorp Vault (intermediate)
- **Offensive Security**: Exploit development (basic), web applications (basic), penetration testing (intermediate)
- **Defensive Security**: Access-control (intermediate), falco (advanced), Kyverno/admission controls (intermediate), security design (advanced), threat modeling (intermediate), network security (intermediate), eBPF (basic)
- **Tools**: Grafana/Prometheus, Elastic/Kibana/Logz, Chronicle SIEM, Github Actions, Jenkins, Flux, Helm, Git, Logstash, Fluentd, Fluentbit, Kafka, Cilium
- **Programming Languages**: Go, Rust, Python, Bash

Projects

Homelab   Jan 2018 - current

I run and develop for years a small homelab, including Mikrotik network appliances, VLANs, Wireguard VPN, NAS devices and a 4-nodes Kubernetes cluster to host various services for the family. The whole lab is managed via Ansible, Terraform and Flux.
- Manage and secure k0s-based cluster.
- Hashicorp Vault integration for CA (SSH) and secrets management.
- Developed custom tool to backup Kubernetes persistent volumes (Rust).

Research and Publications

TED - A Container based Tool to Perform Security Risk Assessment for ELF Binaries
Published on *Proceedings of ICISSP 2019, Prague*   *Oct 2014*
D. Mucci, B. Blumbergs. ISBN 978-989-758-359-9