Contribution ID: **313** Type: **Paper presentation**

Optimizing Configuration and Monitoring of Test Environments for Cybersecurity Assessments

Thursday 18 September 2025 16:30 (15 minutes)

Abstract—The increasing complexity and scale of cyber threats demand optimized and reproducible testing environments for security evaluations. This paper proposes a set of best practices for configuring and monitoring such environments to ensure effective and realistic vulnerability scans, penetration tests, and compliance audits. Key contributions include the use of Infrastructure as Code (IaC) for automating the provisioning of virtual and physical instances, applying network and security policies, and integrating advanced logging and real-time monitoring mechanisms. The proposed methodology addresses major challenges such as configuration drift, poor visibility, and lack of scalability by leveraging tools like Terraform, Ansible, ELK Stack, and Prometheus/Grafana. The paper also discusses the integration of these environments in CI/CD pipelines and the potential of AI/ML in anomaly detection. Future directions include self-healing test environments and deeper AI integration.

Keywords—cybersecurity, test environments, Infrastructure as Code, monitoring, reproducibility, CI/CD, AI/ML

Author: Mr ABOTEZĂTOAEI, Daniel

Co-authors: Mr ARGINT, Cornel; Mr NISTOR, Cristian

Presenters: Mr ARGINT, Cornel; Mr NISTOR, Cristian; Mr ABOTEZĂTOAEI, Daniel

Session Classification: Security & Resilience in Cyber-Physical Systems

Track Classification: Security & Resilience in Cyber-Physical Systems