Strengthening South Africa's Malware Defense Capacity

Introduction

South Africa has become an increasingly attractive target for cybercriminals, with malware and ransomware attacks on critical national infrastructure and public institutions rising in both frequency and severity. High-profile incidents, such as ransomware attacks on Transnet, the Department of Justice, and the Government Employees Pension Fund (GEPF) highlight the scale of the threat. These attacks result in severe operational disruption and financial losses, often due to inadequate readiness and response mechanisms.

Despite legislative advancements in South Africa such as the establishment of the Cybercrimes Act (Act 19 of 2020), and National Cybersecurity Hub (CSHUB), systemic gaps remain in malware threat intelligence sharing, malware analysis capacity, and the integration of hands-on training. These challenges signify the need for improved national malware threat intelligence, stronger national coordination, and investing in hands-on cybersecurity training to develop skills in digital forensics, malware analysis and open-source intelligence.

Tasks and Objectives

You are a Cyber Resilience Task Force appointed by the South African Cybersecurity Hub. Your mandate is to design a national "Malware Readiness" blueprint that enables local organisations – from SMMEs to critical state entities – to identify threats before major attacks occur.

Key Tasks

Your 3-minute video proposal must cover the following:

1. Examine Global Models: Analyse successful models of national cyber resilience and malware intelligence sharing from other regions (e.g., the EU or Australia). Identify which components of these models are applicable to the unique challenges of the African context, such as risk concentration in large single-operator entities like national electricity or transport companies.
2. Capacity Building & Hands-on Training: Outline a plan for workforce development that emphasises practical skills in malware analysis and digital forensics. How can public-private partnerships be leveraged to create a sustainable pipeline of cybersecurity professionals to support state-level crisis response?
3. Intelligence Sharing & Coordination: Design a model for a National Cyber Threat Exchange. How will this platform facilitate the real-time sharing of Indicators of Compromise (IoCs) between the public sector and private enterprises? Recommend a mechanism for effective national coordination. How should the CSHUB and private sector entities share threat indicators without compromising sensitive data, ensuring that an attack on one entity allows others to prepare and defend immediately?

Final Requirement

Your plan should be simple, practical, and realistic, helping the company protect its systems while ensuring that operations remain safe and uninterrupted.

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

The CSIR is a leading scientific and technology research organisation that researches, develops, localises and diffuses technologies to accelerate socioeconomic prosperity in South Africa. The organisation's work contributes to industrial development and supports a capable state. The CSIR was established through an Act of Parliament in 1945 and the organisation's executive authority is the Minister of Science, Technology and Innovation. The organisation plays a key role in supporting public and private sectors through directed research that is aligned with the country's priorities, the organisation's mandate and its science, engineering and technology competences. For more information, visit www.csir.co.za.