



විද්‍යාලීකරණ අමාත්‍යාංශය
டிஜிட்டල් பொருளாதார அமைச்சு
Ministry of Digital Economy



1101, 11 වන මහල, වත්තේල් ලේස්, # 1A, මැද පාර, කොළඹ 02
1101, 11 வது மாடி, வந்தகோல் பேஸ், # 1A, சென்டர் வீதி, கொழும்பு 02
Unit 1101, 11th Floor, One Galle Face Tower, # 1A, Centre Road, Colombo 02

/modesrila
mode.gov

මගේ අංකය
எனது இல
My No.

MODE/DEV/GENERAL/SLCERT

ඔබේ අංකය
உமது இல
Your No.

දිනය
திகதி
Date

03 .03.2026

Circular No: MODE/2026/01

Secretaries of Ministries,
Chief Secretaries of Provincial Councils,
Heads of Departments and Statutory Organizations.

Implementation of the Malware Analysis & Threat Hunting (MATH) Lab Established under Sri Lanka CERT

Sri Lanka CERT, under the guidance of the Ministry of Digital Economy is implementing the Information and Cyber Security Policy for the government organizations as approved by the cabinet of ministers. As instructed by the Cabinet of Ministers, all government organizations defined as public authorities under the Right to Information Act are required to implement this policy to protect digital infrastructure of the government from unauthorized access, misuse, disclosure, disruption, or destruction (Circular No : MOT/2023/01, dated 02.05.2023).

2. To facilitate the implementation of this policy, Sri Lanka CERT under the guidance of the Ministry of Digital Economy has initiated Malware Analysis and Threat Hunting (MATH) Lab to improve the cyber security readiness of the government organizations with the approval of the Cabinet of Ministers.
3. MATH Lab consists of an advanced solution that has Attack Surface Monitoring (ASM), which is used to identify potential weakness of the public facing digital infrastructure before they are exploited, and a Cyber Threat Intelligence (CTI) platform which is used to understand attackers' behavior, indicators of compromise, and threat actor infrastructure. Such a solution would provide government organizations with enhanced visibility into their external threat landscape, enable early detection of emerging cyber threats, support proactive risk mitigation, and strengthen overall cyber resilience.
4. Sri Lanka CERT has identified many government organizations are critical, and therefore ASM and CTI facility will be provided. To ensure accuracy and effectiveness of providing ASM and CTI services, complete visibility of all internet-facing digital infrastructure is mandatory.
5. Therefore, please provide details for validation and confirmation of identified digital infrastructure such as domains and sub-domain names of websites, public IP addresses, login portals, official mobile apps and cloud storage buckets.

6. Upon completion of validation of such digital infrastructure, each government organization will receive a comprehensive Threat Landscape Report, which includes vulnerabilities and mitigation strategies to strengthen the organizational cyber security posture.
7. Therefore, this Ministry requests your active engagement for this national initiative by providing the necessary information as requested above.
8. To ensure smooth coordination, your organization is requested to nominate a dedicated Point of Contact (PoC) for all matters related to MATH Lab engagement. The nominated officer should directly coordinate with Mr. Senalike Devalawatte, Manager – Information Security (email: senalike@cert.gov.lk, mobile: 076-3605905) of Sri Lanka CERT. PoC shall be Director of IT, Information Security Officer (ISO) or Assistant Information Security Officer (AISO).
9. A list of organizations that are identified as critical to providing ASM and CTI facilities are annexed hereto.
10. Your cooperation is vital to strengthening Sri Lanka's national cyber resilience.

Waruna Sri Dhanapala
Secretary

Copy: Secretary to the President, Presidential Secretariat - f.y.i. please
Secretary to the Prime Minister, Prime Minister's Office - f.y.i. please
Auditor General, National Audit Office of Sri Lanka - f.y.i. please