USAID
FROM THE AMERICAN PEOPLE

Annex to the

CERTIFICATE of COMPLETION

of the course

Advanced Malware Analysis

within the 2022 Cybersecurity Summer Instructor Training Program

under the **USAID Cybersecurity for Critical Infrastructure in Ukraine Activity**

11 July – 31 August 2022

Module	Hours
History of malware	2
Classification of cyber threats. Naming conventions	1
Attack vectors and MITRE ATT&CK model	2
Phishing	2
Malware detection technologies: deterministic vs probabilistic	2
Exploits. Demo: How buffer is overflowed	2
Analysis of malicious office documents (e.g. DOCX, XLSX)	2
Malware passive and active self-defense (packing, obfuscation, anti-debugging, anti-VM, anti-AV)	1
Supply-chain attacks (NotPetya attack)	2
Ransomware. History and encryption schemes	1
Ransomware. Ransomware-as-a-Service model	1

Ransomware. Double-extortion approach	1
Ransomware. Defense evasion techniques	1
Machine learning for malware analysis, detection, and attack simulation	2
Phishing detection	4
Malware detection with Yara	2
Static malware analysis	2
Dynamic malware analysis	2
Analysis of web exploits	2
x86 Disassembly: Analysis of DLL Side-Loading Attack	2
x86 Disassembly: Unpacking	4
Decrypting files encrypted by ransomware	2
Analysis of Android ransomware	2
Phishing detection with ML	4
Labs and Practices	32
Self-study	90
Tests	10
Total	**180**

Petro Matiaszek

Chief of Party, USAID Cybersecurity for Critical Infrastructure in Ukraine Activity