Annex to the
CERTIFICATES of COMPLETION
of the courses within the 2021 Cybersecurity Summer Training Program
under the USAID Project
"Cybersecurity for Critical Infrastructure in Ukraine"

14 June – 23 July 2021

Course	Module	Hours
Malware Analysis	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
	Tests	10
	Total	**90**
Web security	Legacy and modern technologies for web applications	2
	Web application_server enumeration	2
	Web Servers Vulnerabilities	2
	Injections. 1. SQL Injections.	2
	Injections. 2. Function, code, command injections.	2
	Injections. 3. SSRF.	2
	Session security. 1. General session description. States in HTTP, HTTPS, WSS. Session storages.	2
	Session security. 2. Session attacks_ session fixation, session predicting, session hijacking. Mitigation.	2
	Scripting Attacks. CSP. CORS.	2
	Authentication vulnerabilities.	2
	Access control_Authorization issues	4
	XML vulnerabilities. 1. Introduction to XML and XML parsers. XML-based technologies_ SOAP, WSDL.	4
	XML vulnerabilities. 2. XML attacks_ reconnaissance, XML-poisoning, XXE	2
	Insecure Deserialization.	4
	General Web Application DOS_ slowloris, resource exhaustion.	2
	Business logic vulnerabilities	4
	Labs and Practices	40
	Tests	10
	Total	**90**

Security Audit and Risk Management	Place of audit and risk management in security	2
	Business processes and ICS	2
	Audit	2
	Risk assessment and evaluation	2
	Risk quantification	4
	Regulations	2
	Frameworks	4
	Ensuring professional opinion	2
	Creating solutions	4
	Continuity	2
	Reporting	4
	Communication in organisational structure	4
	Maturity models&criteria	2
	Continuous improvement activities	4
	Labs and Practices	40
	Tests	10
	Total	**90**
IoT Security and Privacy	Introduction to IoT	2
	IoT Platforms and Operating Systems	2
	Protocol Standards for IoT. Part 1	2
	Protocol Standards for IoT. Part 2	2
	An Overview of Cybersecurity Basics	2
	An Overview of Key Management. Part 1	2
	An Overview of Key Management. Part 2	2
	IoT Standards Security: WiFi Security. Part 1	4
	IoT Standards Security: WiFi Security. Part 2	4
	Application layer IoT Protocols and Privacy. Part 1	4
	Application layer IoT Protocols and Privacy. Part 2	4
	Application layer IoT Protocols and Privacy. Part 1	2
	Application layer IoT Protocols and Privacy. Part 2	4
	Summary of course	4

	Labs and Practices	40
	Tests	10
	Total	**90**
Cyber-physical System Security course	Introduction to Cyber-physical System	2
	Elements of a Cyber-Physical System	2
	SCADA Features	2
	System Architectures	2
	Industrial Network Protocols	2
	MODBUS	2
	DNP3. ICCP	2
	Attacks to ICS	4
	Major Security Issues	4
	SCADA Network Access	4
	Key Management Background	4
	Key Distribution Center	2
	Diffie-Hellman Algorithm	4
	Summary of course	4
	Labs and Practices	40
	Tests	10
	Total	**90**
Foundations of Computer and Network Security	Cybersecurity Essentials	2
	Understanding the Threat Landscape	2
	FIrewall Overview	2
	IDS/IPS Overview	2
	Suricata	2
	Snort IDS/IPS	2
	Network Analysis	2
	SOC Analyst	2
	Understands how to use wireshark to identify network traffic.	2
	PCAP Forensics: Wireshark	2
	Identifying Network IOCs: DNS Tunneling	2
	SSH Backdoor	2
	Carbon Black Endpoint Security	2
	CVE Overview	2
	SIEM & SOAR	4

	Splunk: Basics	4
	Introduction to Phantom Configuration	4
	Labs and Practices	40
	Tests	10
	Total	**90**

Timothy Dubel

Chief of Party USAID Cybersecurity Activity