Proactive approach to cybersecurity: Offensive Cyber Defense

USAID Cybersecurity for Critical Infrastructure in Ukraine Activity

Roman Sologub, CEO at ISSP

(Implementing Partner of USAID Cybersecurity Activity)

ACTIVITY SUMMARY

FUNDED BY:

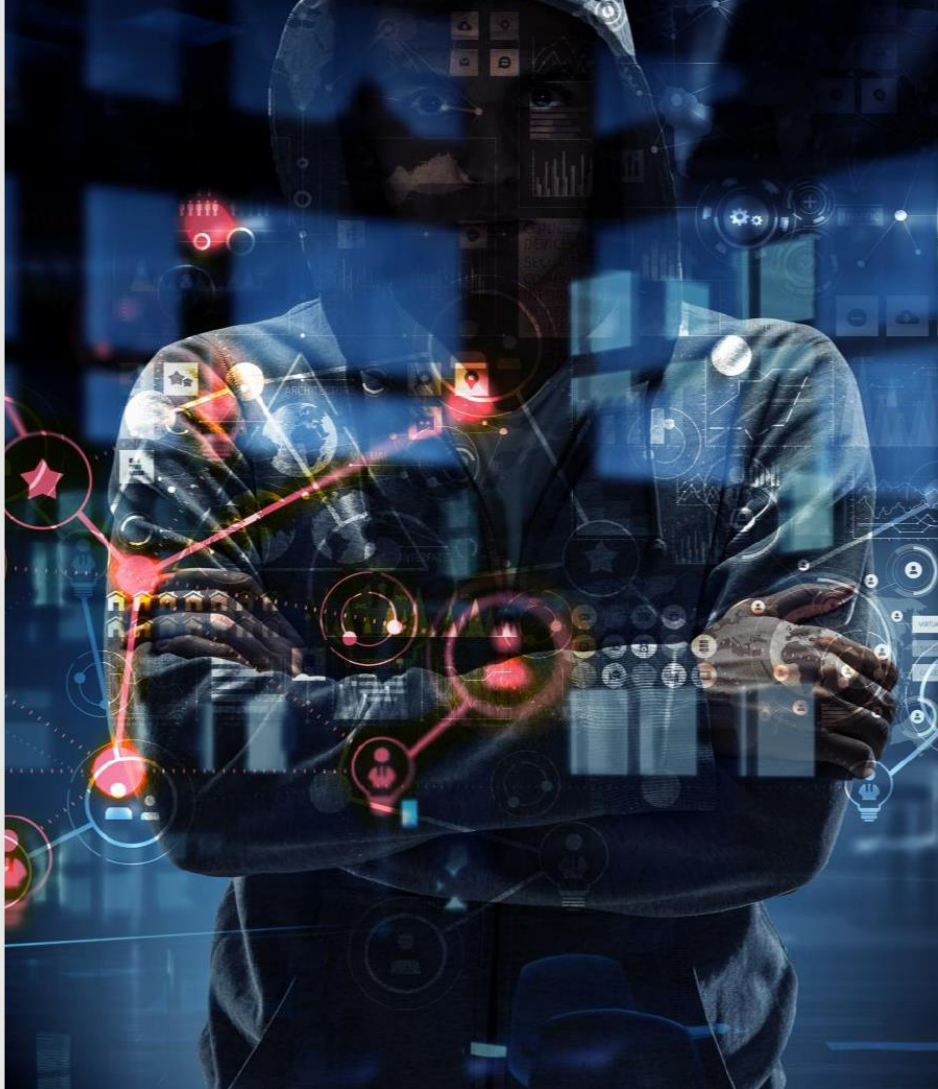
U.S. Agency for International Development

ACTIVITY DURATION:

May 2020 – September 2024

ACTIVITY GOAL:

Reduce cybersecurity vulnerabilities in critical infrastructure and transform Ukraine into a resilient, agile cybersecurity leader



COMPONENTS AND SUPPORTING TASKS:

1 ENABLING ENVIRONMENT

LEGISLATIVE REFORM AND CYBERSECURITY ROADMAP

- Laws, policies, and governance reforms

CYBER EXCELLENCE MECHANISM

- Communication, collaboration, and ad hoc assistance

NATIONAL PREPAREDNESS

- Critical infrastructure preparedness
- Threat information sharing
- National preparedness exercises

2 WORKFORCE DEVELOPMENT

HIGHER EDUCATION CAPACITY BUILDING

- Cybersecurity degree programs
- Practical training

UPSKILLING INDUSTRY PROFESSIONALS

- Professional training courses
- Practical training
- Peer mentoring

3 MARKET AND INDUSTRY DEVELOPMENT

CENTER FOR CYBERSECURITY INNOVATION

- Community building
- Partnerships and research support

CYBERSECURITY INVESTMENTS AND PARTNERSHIPS

- Facilitating investment

SMB ACCELERATION AND MENTORSHIP

- Growth and capacity building

EXCHANGE PLATFORM

- Market information and connections

National Preparedness

Create a safe and trusted environment to accelerate the development of people, processes, and technology in support of cybersecurity across critical infrastructure sectors and assets in Ukraine.

Outcomes:

1. Reduced CI cybersecurity vulnerabilities over short and long term

2. Trusted communication and information sharing between stakeholders

3. Institutions capable of managing cybersecurity of CI

National Preparedness: Implementation Plan

REPLAY

Communication, Coordination, Reporting

Cybersecurity Exercises

COORDINATE

Collaborative cybersecurity

Threat Intelligence Sharing Mechanism

IMPROVE

Cybersecurity capacity improvement process

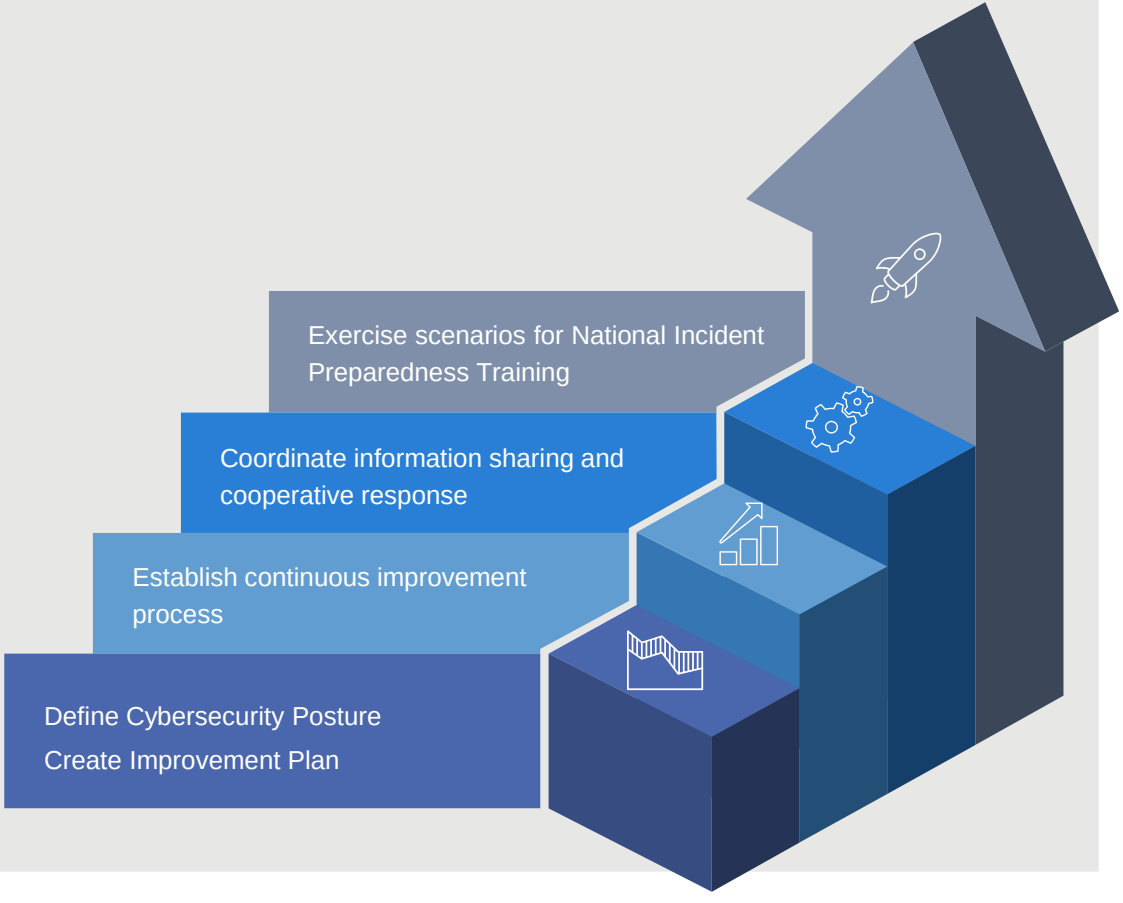
Cyber Maturity Model

Professional Workforce

BASELINE

Cybersecurity Incident Preparedness Diagnostics

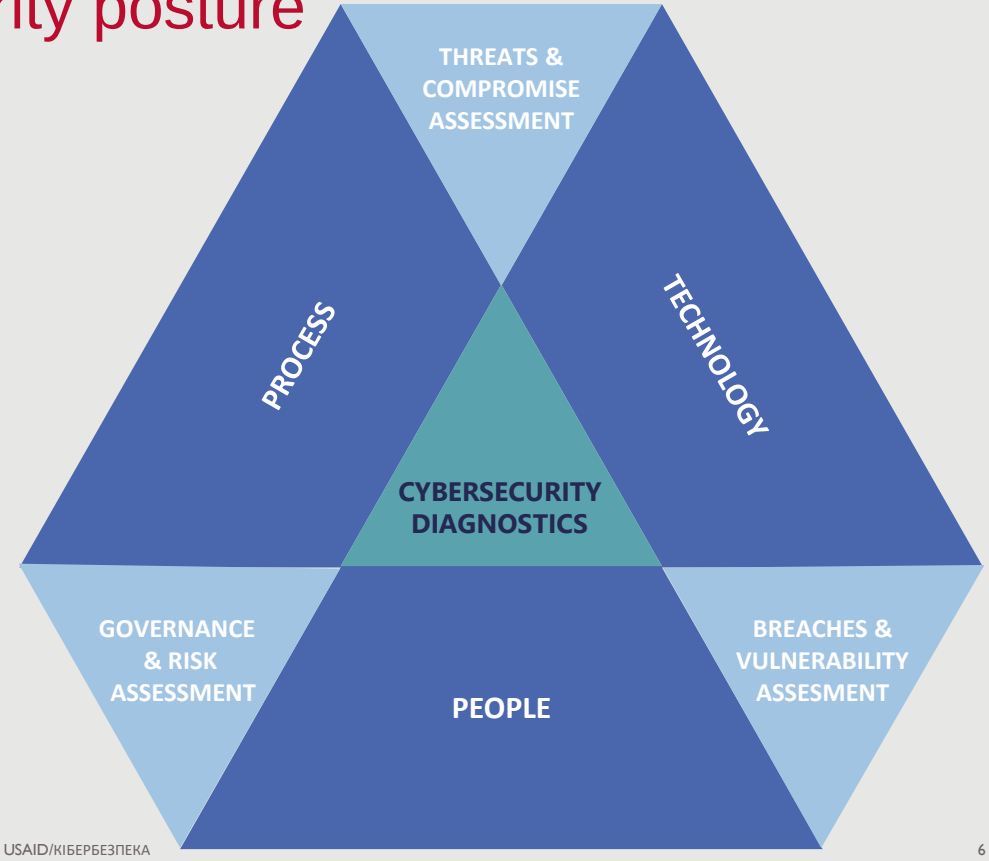
Improvement Plan



Pentest – the essential component to evaluate the organizational cybersecurity posture

PENTEST:

- Highlights Specific Risk Factors
- Enables a Continuous Security Stance
- Provides You with Valuable Insights
- Ensures Regulatory Compliance
- Helps with Training Implementations



The approach to grow resilient cybersecurity capability

Effective cybersecurity operations utilizes a mix of offensive and defensive actionable tactics to provide cybersecurity

Defensive:

Uses a reactive approach to security that focuses on prevention, detection, and response to attacks.

Uses a proactive approach to identify cyberthreats through use of threat hunting (internal vector) and threat intelligence (external vector).

Offensive:

Deploys a proactive approach to security through the use of ethical hacking, application security techniques and user awareness evaluation technologies.

Working together towards proactive cybersecurity approach

	Enterprises	GOU Institutions
 PEOPLE	Investment in talent development programs, certifications and training. Deploy interactive online training for people across the organization	Recognize new cybersecurity professions: Threat Hunters, DevSecOps, IoT/OT Sec Architects, Penetration Testers.
 PROCESS	Independent “second line of Defense” capabilities. Effective resilient and ongoing supply chain risk management function.	Build effective early prevention and response capabilities. Develop ongoing cybersecurity awareness campaigns
 TECHNOLOGY	Adopt proactive technologies such as penetration testing, cyberattack simulation testing, threat hunting, threat intelligence management.	Develop end-to-end capabilities for threat research, vulnerability discovery and threat information sharing.

www.usaid.gov

www.facebook.com/CyberActivityUA

www.issp.com

rsologub@issp.com

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ