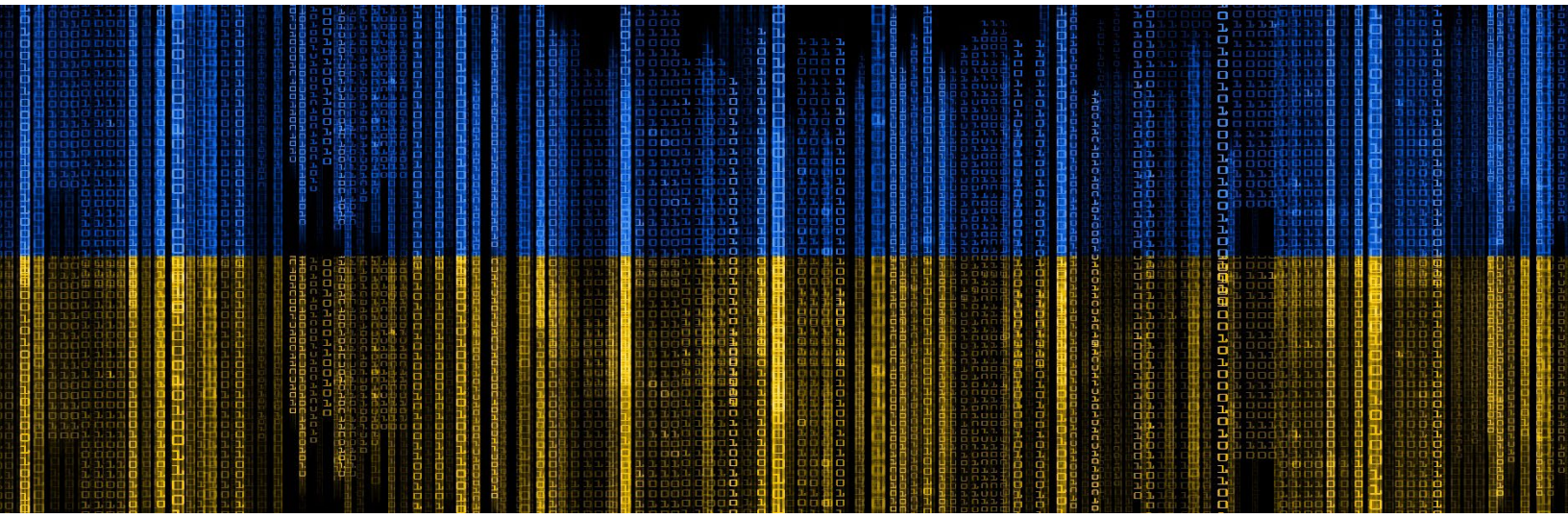

SUPPORTING PRIVATE SECTOR RESILIENCE IN UKRAINE THROUGH CYBER THREAT MANAGEMENT

A three-year, $3.75 million collaboration between Flare and Chemonics International is helping to enhance the resilience of Ukraine's critical infrastructure.

BACKGROUND

Russian cyberwarfare operations against Ukraine were evident both before and during the war, with Ukraine's private sector remaining highly susceptible to these threats. These operations specifically target and exploit Ukrainian critical infrastructure and business operations. For instance, Ukraine's financial sector was a key target in the 2022 cyberattacks that preceded the Russian invasion. Attacks on the financial sector can cripple economic growth and lead to social unrest. Similarly, Ukraine's information technology sector is a potential target for cyber threat actors. Disabling IT services can severely hinder the nation's ability to respond to cyber-attacks or maintain essential commercial and citizen services.

Furthermore, hijacking or dismantling telecommunications systems can be used by threat actors to slow response capabilities, disrupt business operations, and instill fear among the local populace. The economic and overall resilience of Ukraine is significantly dependent on its ability to protect, manage, and grow its industrial sector, making manufacturing firms prime targets for cyberattacks. Additionally, hijacking media and other public communication channels can be used to spread disinformation and propaganda.

To strengthen Ukraine's economic growth and enhance the resilience of its critical infrastructure, it is crucial to build the necessary skills and have access to tools that

About Flare

Since 2017, Flare has been building a threat-led cybersecurity program that combines proprietary world class collection from across the dark and clear web with radical ease of use. Flare can rapidly detect data leaks and stolen credentials, reduce noise through its AI-driven prioritization engine, and proactively detect and remediate many of the most common vectors leading to data breaches, ransomware attacks, and third-party exposures. Flare monitors 4,000 cybercrime forums and channels, 8 billion data points, and 28 million public GitHub repositories.

enable firms to effectively manage external threats. This will also enhance the confidence of Ukraine's commercial partners, such as prospective investors and importers in foreign markets, thereby safeguarding jobs and revenue.

CHEMONICS-FLARE COLLABORATION

This initiative leverages Chemonics International's extensive experience in supporting economic growth in Ukraine and Flare's commitment to enhancing the country's critical infrastructure cybersecurity resilience. Chemonics will utilize its broad network within Ukraine's business community to identify **24 firms that can apply to receive Flare's Threat Exposure Management (TEM) solution at no cost for three years.**

The solution integrates cyber threat intelligence, digital risk protection, external attack surface management, and other functions. This convergence enables organizations to proactively identify, prioritize, and respond to ransomware-related intelligence and threat exposures. Flare's TEM platform serves as the focal point for integrating exposure management throughout the security function creating continuous risk reduction.

EXAMPLES OF UKRAINIAN FIRMS TO BENEFIT FROM FLARE'S THREAT EXPOSURE

Critical Infrastructure

Emergency Services
Energy
Food and Agriculture
Healthcare
Transportation
Water and wastewater treatment

Financial Sector

Banks
Ukrainian Stock Exchange

Industrial Control Systems

Critical Manufacturing Firms
Manufacturing Plants

IT Sector

Cloud Service Providers
Cybersecurity Firms
Data centers

Media and Communications

News Organizations

Telecommunications

Internet Service Providers
Mobile Networks
Satellite Communications

MANAGEMENT SOLUTION

Chemonics will leverage relationships with targeted business organizations or associations in Ukraine to promote this initiative to suitable companies within their membership and stakeholder base. Chemonics will also publicize this initiative and suggest specific firms for Flare to consider in its selection process for the Flare TEM solution. Flare shall make the final determination of the selection of the firms.

Flare will undertake all outreach, technical presentations and communication pertaining to the identification and selection of the companies to receive the Flare TEM solution. Flare will conduct training for personnel of selected firms on cybersecurity needs and approaches to threat exposure prevention, management, and mitigation.