



Managing cyber security risks

ARE YOU READY FOR A STEP FORWARD?

CYBERSECURITY TODAY IS MUCH MORE THAN JUST PREVENTING CYBER ATTACKS, VIRUS INFECTIONS, OR RECEIVING FAKE EMAILS. TO SUCCESSFULLY PREVENT ATTACKS, IT IS NECESSARY TO HAVE ADVANCED TOOLS THAT ALLOW US TO HAVE INSIGHT INTO THE FUNCTIONING OF ALL CYBER SECURITY CONTROLS AND VARIOUS SECURITY SOLUTIONS, DETECT AND ASSESS RISKS AS SOON AS THEY APPEAR IN THE CYBER SPACE, AND TEST AND IMPROVE THE RESILIENCE OF OUR DEFENSE SYSTEMS.

■ By: Damir Muharemović
redakcija@asadria.com

“The Risk Management in Cyber Security: Are You Ready for a Step Forward?” was the title of an international professional conference organized by the Slovenian company CREAplus at the CUBO Golf course in Ljubljana. Managers for cyber security and experts from telecommunications, energy, financial, manufacturing, and IT companies were presented with advanced solutions and services for comprehensive risk management in their cyber space.

Successful prevention of multiple types of attacks

The solutions provided by Cynet and Perception Point for comprehensive visibility in all attack vectors, as well as for comprehensive detection, prevention, and response to cyber threats on endpoints, email, computer networks, and the cloud, generated interest among the attendees.

Their solutions effectively prevent phishing, ransomware, BEC (Business Email Compromise), ATO (Account Takeover), spam, malware, zero-day, and N-day attacks before they reach end users. This is precisely why Admiral Croatia, one of the largest regional gambling providers, is satisfied with their services. “We are currently using Cynet and Perception Point solutions. These are products that we are satisfied with, so it was a pleasure for us to be invited. We are always interested in new tools that can make our job easier, improve security, and so on. We have seen some things that we already have but are not using to their full extent. Practice is always lacking,” said Luka Pribanić, a system administrator at Admiral Croatia, adding that these companies, despite their relative youth, have been very suc-

cessful and pioneering in their respective fields of business.

An open and simple platform

Stellar Cyber has introduced an analytical solution for centralized performance monitoring and process management in all cybersecurity aspects of business and production information environments. The company offers an open platform for Extended Detection and Response (XDR). But what exactly does “extended” mean, or what do you need to have to achieve these extended functionalities? Usually, when working with a specific vendor, you need to purchase the entire solution to reach that level of XDR. However, difficulties arise when you have to integrate it with other security solutions. That’s why

Cybersecurity today means much more than just preventing cyber attacks, computer virus infections, or, for example, receiving fake emails.



Cybercrime is an industry

Speakers from Slovenia, Austria, the United Kingdom, and Israel, with extensive experience in the field of cybersecurity on the international stage, agreed that cybercrime has matured into an industry with its own operating principles. They operate on very similar principles to companies. In order to ensure a regular income for their criminal activities, they target not only wealthy enterprises but also attack and extort smaller businesses, schools, social, and medical institutions. Furthermore, smaller organizations are at greater risk than larger ones because they invest less in defense systems. "Today, we could see what a cybersecurity risk management system in the cyber space represents and why it is important for everyone to be aware of exposure, not just infrastructure and large manufacturing companies, banks, and government agencies. Almost every organization can be targeted by cybercriminals, including small and medium-sized enterprises. That's why it's even more important that we can provide affordable and quality cybersecurity protection to organizations of all sizes and activities, including manageable solutions," said Julianna Pihlar, Sales Director at CREApplus.

Stellar Cyber has opted for an open approach, independent of the manufacturer. Their XDR platform can be connected to any tool, firewall, Security Information Management (SIM) solution, etc., allowing it to ingest logs, telemetry data, and security alerts from any product. It

utilizes AI for analysis and correlation of collected data to identify threats in the cyber space, enabling security personnel to quickly respond to incidents. They see great potential in the regional market. "I started collaborating with CREApplus when I worked for Cynet, so I know most of the

partners and customers here. It's nice to see their progress in adopting new technologies from one conference to another. Customers in the Croatian market are becoming more professional, unafraid of new technologies, and willing to be visionaries in certain aspects. I am pleased to see this region developing," says Miri Varbitzky, Vice President of Sales for the EMEA region at Stellar Cyber.

Intelligence data in the service of protection

The cyber intelligence solutions provided by KELA drew special attention from over fifty guests from Slovenia, Bosnia and Herzegovina, Croatia, and Hungary. These solutions assist organizations in risk assessment and preparation of measures based on intelligence information from various sources where cyber criminal organizations and individuals operate. Among these data are those collected from the dark web, which surprised the end users present. Regional managers and information security experts were also introduced to the Picus platform for automated penetration testing of external cyber space and internal information and communication resources. In addition to software solutions, participants learned about crisis management approaches in the event of a successful cyber attack, as well as leading global educational services such as SANS Security Awareness for users.

"Today, cyber security means much more than just preventing cyber attacks, computer virus infections, or receiving fake emails. First and foremost, we need to have insight into the functioning of all cyber security controls and various security solutions in one place. We also need to be able to detect and assess risks as soon as they emerge in the cyber space, even before they reach the organization. Additionally, we must have tools that allow us to easily and continuously test and improve the resilience of our defense systems against new attacker techniques," said Miha Lavrič, Technical Director of CREApplus and a certified ethical hacker, who demonstrated a hacking attack example at the conference.

The overview of components of a comprehensive cyber security system was complemented by good cyber security practices from Admiral Croatia and ARES, a renowned Austrian company specializing in cyber incident response. ◀

