UNDERSTANDING RISK

IVAN DOLENSKY (SENIOR VICE PRESIDENT -INTERNATIONAL SALES), FIDELIS CYBERSECURITY, ON THE THREAT-RISK LANDSCAPE AND THE ROADMAP FOR THE REGION.

What do you see as the key trends in market?

Digital transformation, COVID, and more sophisticated cyber adversaries in dynamic and more complex IT environments will continue to be trends worldwide.

> **"FIDELIS CYBERSECURITY HAS ALWAYS MAINTAINED A STRATEGY OF PRESERVING RESOURCES CLOSE TO OUR CUSTOMERS AND PARTNERS. FIDELIS WILL ADDRESS AND WORK CLOSELY WITH COMPANIES LOOKING TO ADD PROACTIVE CYBER DEFENSE CAPABILITIES TO BETTER SAFEGUARD THEIR DATA, ASSETS AND SERVICES. "**

Digital transformation enables massive scalability and agility, as well as cost advantages. But it also increases IT complexity. SOC teams need to ensure data and assets are secure no matter where they reside on your networks.

While digital transformation has dispersed data to new place, COVID has pushed our people to working from new places. Instead of securing one corporate environment with 500 people, we're securing 500 "offices" of one person each. Classic phishing tactics thrive on naivety. COVID also limited budgets and the resources we have available.

Cyber adversaries are getting more sophisticated and are using more advanced tools, neural networks, AI tools, automated analytics to achieve their goal. They have found new ways in, penetrate environments deeper and linger longer. These threat actors are bringing global organizations and supply chains to a halt.

In short, complicated environments, limited resources, against very well-prepared adversaries is yielding 1M new threats discovered in the world every day.

Modern cyber defenders/security teams must have deep visibility across hybrid and multi-cloud environments coupled with rich analytics to protect all data, assets, and services and better safeguard their IT environment.

Ivan Dolensky

What expansion and growth plans do you have for the region? What are the priorities for customers?

Fidelis Cybersecurity has always maintained a strategy of preserving resources close to our customers and partners. Fidelis will address and work closely with companies looking to add proactive cyber defence capabilities to better safeguard their data, assets and services. That strategy means we will continue to invest in local resources based in the region, as well in local partner ecosystem. Quality alliances in the region are critical to our business success. We will continue knowledge transfer and trainings locally to enrich existing and simplify new partnerships and provide customers and partners the tools they need for success.

What strategic relationships are important to you in the region?

Fidelis Cybersecurity recently sign very strategic and important local MSSP partnerships to help customers who want the value we offer delivered as a service. Work closely with these MSSPs to develop and deliver a unique managed security services value-based offering, and this will continue to be a key priority in the local market.

Can you tell us about the roadmap for Fidelis Cybersecurity and the value it will provide to customers?

Fidelis Cybersecurity portfolio is designed to deliver the proactive defence capabilities you need to safeguard your data, assets, and services – no matter where they are on your networks. Already, we provide proactive and defence-in-depth security that spans endpoints, network, and hybrid and multi-cloud environments.

We acquired CloudPassage in May, which is allowing us to further evolve our XDR platform with a solution that keeps pace with our customers' needs as they migrate more and more of the business to the cloud.

Our customers have a choice to use our XDR platform as a comprehensive offering, or they can deploy it as an open platform leveraging integrations with existing tools in their environment. We will continue to deliver integrations and functionality our customers need from an Active XDR platform to detect, respond, and neutralize threats earlier in the attack lifecycle.

Finally, cyber threats succeed when they can detect and exploit risks and vulnerabilities. Fidelis starts by understanding the current environment and risk, allowing the security team to address risk prior to an exploit. Risk has traditionally been based on vulnerability scans that are run periodically - daily or weekly, however risk changes immediately when threats are activated - through phishing, malware, user impersonation, etc. We will combine detections from endpoint, network, and cloud in a way that immediately changes risk, automatically responds, and constantly evolves the security of the enterprise.

What do you see happening with the cloud and on prem offerings and private cloud?

Digital transformation is happening. Data centers are moving to the cloud. Security needs to also move. These hybrid environments are more complicated to secure, and each enterprise must decide for themselves how to proceed. If they decide to use on-prem data centers, private cloud or public cloud, security must view this as a deployment strategy without any loss of capability. Fidelis will allow our customers to deploy security to match their enterprise environment, including cloud, on-prem, or hybrid without loss of detection capabilities.