HAARETZ Labels
Commercial Content

EFFECTIVE MULTI-LAYERED DEFENSE BEGINS WITH INTELLIGENCE-LED PREVENTION

Roni Roytman, co-founder and CEO of INTENSITY GLOBAL, a serial entrepreneur and cybersecurity expert, presents HUNTER 1, a platform that shifts the defense paradigm from reactive detection to proactive prevention. "Our defensive perspective comes from the attackers' point of view," he says. "We operate with a proactive hunting strategy: locating attackers before they act and staying several steps ahead of them."

Shutterstock

Yoel Tzafrir, in cooperation with INTENSITY GLOBAL from the Accel Solutions Group

Feb 12, 2026, 4:22 pm IST

Roni Roytman | Photo: Shlomi Perry

Cyberattacks are no longer isolated incidents but an ongoing process, in which skilled attackers operate quietly over extended periods, beneath the radar of organizational security systems. In this reality, a defense approach based on perimeter walls and isolated technical alerts struggles to provide an adequate response. While it may detect symptoms, it does not always present the full story of the attack.

This is where HUNTER 1 enters the picture — a platform that advances detection to an earlier stage, before the threat materializes. The system combines external intelligence with behavioral analysis of network traffic and user activity within the organization, in order to connect isolated data points and expose emerging attack patterns before they are translated into real damage.

"HUNTER 1 is an AI platform for cyber-threat prediction, cyber intelligence and operational forensic analysis of incidents," says Roni Roytman, co-founder and CEO of the INTENSITY GLOBAL Group, who developed the system together with Dan Fromovich, the Group's CTO.

"The platform enables organizations to anticipate threats and significantly strengthen their defense posture and response capabilities," he adds. "Instead of waiting for after-the-fact alerts, we aim to identify attack patterns at an early stage and build an operational picture from them. Put simply, we hunt the attackers and enable our customers to stay two steps ahead of them."

According to Roytman, most organizations today are coping with the phenomenon of isolated islands. Security systems — from firewalls and EDR to the Microsoft 365 environment — generally operate in isolation from one another, without synchronization or continuous information sharing. This gap creates blind spots, since in many cases even systems such as SIEM and SOC fail to generate timely alerts regarding the presence of an attacker on the network. Within these blind spots, skilled attackers can operate almost without disturbance. The HUNTER 1 platform helps bridge this gap through a comprehensive, active and operational approach that controls all digital assets, from endpoints to mailboxes, and performs full integration between the various systems.

"Our goal is to transform dispersed information and big data, which include numerous alerts, into a single, complete and active intelligence picture that enables unified visibility and immediate response to any threat," notes Roytman.

Surfacing the significant threats

Attack prediction in advance is carried out both within the organization's internal environment and in the external arena. Outside the organization, the platform operates a large-scale monitoring array that spans the entire internet space, far beyond the Dark Web alone. "The system continuously tracks more than 200 attack groups that pose a direct and relevant threat to Israeli targets, and enables organizations to understand the attacker's TTPs (tactics, techniques, and procedures) already at the planning stages," emphasizes Roytman.

At the same time, the system performs a deep dive into the organizational network and exposes quiet attackers and hostile actors operating covertly, beneath the radar of standard security tools. Correlating data from internal organizational

systems (logs and communications) with the platform's external and unique data enables the organization to discover the unseen and thwart even highly sophisticated threats, shifting from a reactive posture to proactive prevention.

"The system performs comprehensive correlation across all defense systems and the organizational network, with full automation that enables surfacing critical threats from within the big data of the security systems," he explains. "Using artificial intelligence that we developed, which governs the entire organizational operation, the platform generates forensic insights and precise prediction, turns raw information into an active prevention tool in the hands of the organization, and also significantly reduces the burden on security teams."

How does this manifest in practice?
"Beyond 'dry' data collection, the LLM embedded in the system makes it possible to generate a complete end-to-end attack narrative. While most security systems see only isolated fragments of information, HUNTER 1 is capable of following the entire attack chain — from the initial intrusion, through the stages of lateral movement across the network, and up to identifying the attacker's intent."

"In other words, instead of settling for a technical alert about a suspicious IP address, the system provides security teams with a holistic picture: how the attack started, which segments it traversed, and what its current status is. Connecting all the dots enables the organization to see the full picture, one that eludes other cyber tools."

Led the breakthrough into the international market
Roni Roytman is a high-tech entrepreneur with 26 years of experience in the cyber domain, during which he accumulated expertise as a senior strategic advisor to company and organizational managements and as a mentor to start-ups. About eight years ago, he founded INTENSITY GLOBAL, a company specializing in offensive and defensive cyber operations and strategic consulting, and led its expansion into the international market. As a serial entrepreneur, he also co-founded Cycon Security together with Dan Fromovich. Together they developed the HUNTER 1 platform, which, as noted, operates from both the attacker's and the defender's points of view. Today, INTENSITY GLOBAL represents the platform in Israel.

Over the years, Roytman has founded and partnered in additional operational cyber companies. The most significant recent structural change occurred in July 2024, when the public company Accel Solutions acquired 51% of INTENSITY GLOBAL. Following the acquisition, the Accel Cyber Group was established, bringing together under one roof the solutions of the Accel Group's information security and cyber companies: INTENSITY GLOBAL (operational cyber and IR), Danet Communications (integration and information security), and Cyber Hive (SOC and monitoring services). All of this is intended to offer very high-quality, end-to-end information security solutions and deliver real added value to organizations. "Our central goal is to expand into international markets, a process that has already begun and is gaining momentum," he says.

A full, multi-layered defense envelope
The INTENSITY GLOBAL GROUP manages complex cyber-attack incidents on a weekly basis in Israel and around the world. It provides a full and comprehensive defense envelope, including IR (Incident Response) teams — technological response teams that are deployed to the incident scene to halt the attack and manage the crisis at both the managerial and technological levels.

Alongside crisis management, the company provides year-round protection services (Managed Services). The purpose is to strengthen the organization in advance, provide strategic guidance to senior management, and prevent future attacks through gap analysis and active intelligence.

What is your customer profile?
"Our customer base consists of companies across all sectors, including enterprise organizations and critical infrastructures that form the backbone of the Israeli and global economy. This includes hospitals and medical institutions, leading fuel and energy companies, high-tech companies and start-ups, banks and financial institutions, as well as leading defense and government bodies."

As a cyber expert and senior advisor, what is your key message to the market ahead of CyberTech 2026?
"My message is simple. There is immense importance to a full, multi-layered defense envelope. While there is no hermetic protection, our goal is to make every attack economically unviable for the attacker. Organizations must stop viewing security as isolated islands of technology and begin looking at the complete picture. From our experience managing cyber incidents, we have learned that only the combination of active intelligence, AI-based prediction, and immediate technological response (IR) can minimize damage and build long-term organizational resilience.

"Ultimately, the ability to get ahead of the attacker and understand the full picture is what differentiates a proactive organization from any point-solution response system."

https://tinyurl.com/haaretz-labels