About the Interview

How can organizations move beyond a "reactive" cybersecurity mindset that only addresses breaches after they have caused damage?
By utilizing "Active Defense" and intelligence, companies can identify malicious infrastructure deployment weeks before an attack, allowing for preemptive disruption of network communication.
Shifting the industry standard from "detection" to "preemption" creates a powerful global deterrent by increasing the financial and operational costs for cybercriminals.

About the Interviewees

Luigi is a tech pioneer and strategist driven by curiosity and "predictive" foresight. With 40 years of PC experience, he evolved from MS-DOS tinkerer to VP roles at Dell and Quest, managing $350M+ P&Ls and 300-person teams. A master of scaling and M&A, he founded "Dell for Entrepreneurs" in France. Today, he disrupts the status quo at BforeAI, moving the industry from reactive "firefighting" to predictive behavioral AI to secure organizations before attackers can even strike.

About the Interviewer

Theodor Himmel connects students with experts in diplomatic and economic affairs. Together with his colleagues, he built EPIS Think Tank into one of the largest student-led think tanks in Europe and also initiated the EPIS Network. He currently serves as Chairman of EPIS. Alongside this, after completing an LL.M. at Leiden University, he is finalizing his legal training as a law clerk at the Regional Court of Baden-aden. Currently, he works as a consultant in a Munich-based family office.

The Mission: Predicting the Storm

Theodor Himmel

Luigi, you recently founded a cybersecurity company called Pre-Crime. You were selected as a World Economic Forum (WEF) Technology Pioneer in 2025—the only cybersecurity firm among the top 100. Tell us, what exactly do you do?

Luigi Lenguito

Think of us as a weather forecast for the internet. Most cybersecurity is reactive—detecting and responding to an attack that has already started. We identify the sources of attacks an average of three weeks before they happen, sometimes up to two years in advance. We then disrupt the network to isolate those sources and shut down the infrastructure before a single victim is made. Just yesterday, over 120 million people and businesses avoided becoming victims thanks to our technology.

Preemptive Defense: A security strategy that uses predictive data to identify and disrupt a threat actor's infrastructure and communication channels before an attack is actually launched.

Theodor Himmel

Are you focused on businesses or individuals?

Luigi Lenguito

Primarily large commercial organizations and critical infrastructure—banks like Volksbank, retailers like Primark, and manufacturing giants like Philips and Pirelli. By protecting these organizations, we naturally protect their millions of customers and suppliers at scale.

The Origin Story: From Formula 3 to Cybersecurity

Theodor Himmel

Tell us about your background. How did this journey begin?

Luigi Lenguito

I've been in front of computers since I was four years old. I spent 20 years in the corporate world, eventually serving as a VP at Dell. After retiring from M&A, I briefly returned to my other passion: racing as an ex-Formula 3 driver. But the "itch" to create returned. I saw that the cyber industry was trapped in a "reactive" mindset, essentially accepting that everyone would eventually be a victim. I wanted to build

something that stopped the crime before it started.

Theodor Himmel

And the name "Pre-Crime"? It sounds like something out of a movie.

Luigi Lenguito

Exactly. It's inspired by the "Pre-Cogs" in Minority Report. Interestingly, 20th Century Fox never trademarked the term, so I secured it. While the movie predicted this tech would exist in 2054, we are already doing it for cyber in 2026.

The Strategy: Preemptive vs. Offensive

Theodor Himmel

Is your approach a counteroffensive, or just a stronger defense?

Luigi Lenguito

We call it Preemptive Defense. Offensive defense—attacking the hackers back—is often illegal for private companies. Instead, we operate in an "active defense" gray area. We don't touch the criminal's PC; we simply create a "coalition of the willing" to ensure the "good guys" stop talking to the "bad guys."

By creating a coalition of the willing to isolate malicious sources, we move the defense line forward, ensuring that cybercrime is stopped before a single victim is ever made.

Theodor Himmel

Can you give a real-world analogy?

Luigi Lenguito

It's like the Iron Dome system. It predicts the trajectory of a rocket and intercepts it in the air. If no rocket is launched, the system stays quiet. We do the same: we see the "massing of troops" or the setup of malicious servers, and we disrupt the communication channels before the attack is ready.

Geopolitics and Global Impact

Theodor Himmel

As a think tank for foreign affairs, we are interested in the geopolitical side. How do state actors play into this?

Luigi Lenguito

We are largely agnostic. While state-sponsored attacks get the headlines, they are a minority. Most cybercrime is economic—the "Mafia of the 21st century." Interestingly, by volume, China is the most attacked nation in terms of its citizens, while the U.S. suffers the highest financial losses. Our goal is to increase the cost of an attack. If we make it too expensive and time-consuming for criminals to build infrastructure that never works, we create a global deterrent.

Advice for the Next Generation

Theodor Himmel

Finally, what is your advice for students and recent graduates entering the job market today?

Luigi Lenguito

Don't be intimidated by the "technical" label.

Cybersecurity is about governance, threat intelligence, and understanding human actors. The skills you learn in geopolitics and business are highly applicable to intelligence operations. With today's AI tools, you can bypass many of the traditional technical barriers. It is a purposeful, growing industry that needs the best minds to protect our future.

Theodor Himmel

Luigi, thank you for your time.