This company aims to protect connected cars from cyberattacks

September 7 2022, by Breana Noble

Credit: Pixabay/CC0 Public Domain

Half of all auto cyberattacks in history occurred in 2021 alone—up nearly 140% from 2020.

That's according to Upstream Security Ltd., a startup offering a cloud-based automotive cybersecurity and data analytics platform that's opening its first vehicle security operation center outside of its native

Israel in Ann Arbor, Michigan.

The number of connected vehicles on the road has jumped, and automakers, including the Detroit Three, have plans to add millions more over the rest of the decade offering over-the-air updates, on-demand features and technology perks that customers demand.

That, however, also means they can be vulnerable to cyberattacks that can steal personal information, take control of vehicle functions and even potentially provide hackers access to the greater electric grid. And those threats are growing with automakers and smart mobility providers accounting for 6% of the targets of attacks so far in 2022 compared to 2% last year.

"The auto industry is at a point now where autos and trucks and vehicles are really becoming just another device," said Richard Forno, assistant director of the Center for Cybersecurity at the University of Maryland, Baltimore County. "You have smart phones, Amazon Alexas, autos are now just another smart device. As such, they are always connected. There are a range of security concerns for any other always-on device. With any new technology that becomes popular, you are going to see an increase in attacks."

That's where Upstream comes in. Working with automakers, it offers a layer of protection to identify and fight against attackers that is a requirement of service regulation, says CEO Yoav Levy.

"This is critical infrastructure (that) should be taken very seriously not only by the car company or the fleet owners," he said, "but also by the government."

Hackers may seek private information like credit card numbers, to unlock and start vehicles to be stolen and to access electric-vehicle

charging stations to install ransomware, shut them down as a means of cyberwarfare or even access the greater electric grid, Levy said. Additionally, there's the potential for disrupted supply chains, deliveries and other services.

"The impact is much more than if someone had an enterprise and stole their data," Levy said. "The brand damage is very big."

Additionally, he said, vehicles are more vulnerable when they use public charging stations or are receiving over-the-air updates, which the industry is rapidly expanding.

Upstream has the ability to cover 90% of potential security attacks on a vehicle, he said. From its customers, it obtains information coming to and from connected vehicles, charging stations and other digital applications being collected in the cloud. Upstream's platform does security analysis and uses machine learning models to look for known and unknown anomalies in the data.

The company has hundreds of playbooks generated from various use cases from when anomalies are detected on actions that can be taken to protect the vehicle or information. Depending on the type of attack, some actions are automatic, while others may take longer. Actions may also include disabling the SIM card in a vehicle, working with the automaker's cybersecurity team and contacting the driver.

"We provide some kind of bird's eye view of the entire fleet," Levy said. "And it's being monitored by cybersecurity experts. Once they detect a threat or an anomaly, they can actually respond in close to real time with playbooks and actually mitigate the risk."

In this way, Upstream not only has been able to offer defenses to new vehicles, but also existing connected vehicles already on the road, which

was one of the company's goals when it launched in 2017.

Upstream today monitors around 12 million vehicles. Its Ann Arbor center will be responsible for a few million.

Levy declined to specify if Upstream works with one of Detroit's automakers, citing the sensitive nature of cybersecurity. It has, however, received more than $100 million over four financial rounds. Supporters include the alliance between Renault, Nissan and Mitsubishi, the Volvo Group, BMW and Hyundai Motor Co. as well as insurance companies, mobility firms and other investors. Levy declined to discuss the firm's financial details.

The Ann Arbor center will be a 24/7 operation. Upstream is training 10 people for the center, but it's hiring both full-time and part-time positions. It has 130 employees globally today. Levy recommends computer science degrees for those interested in the work, though it's not required for the job.

Upstream chose Ann Arbor for access to customers and Southeast Michigan's autos knowledge base. In Israel, where there is a military service obligation for its citizens, many people have experience in cybersecurity, and Upstream offers training for its application for autos.

In Michigan, it's the opposite. Upstream hopes to benefit from the deep-rooted knowledge of the industry in the state and offers training on the work of cybersecurity for it.

"We can learn a lot from them around their deep experience in automotive," Levy said. "We don't have any car company in Israel that builds cars, so our knowledge in automotive is very narrow."

The center is another testament to how Michigan's expertise in

automotive transportation gives it an advantage for fostering an ecosystem supporting the cars of the future.

"Companies continue to invest in Michigan because of our world-class talent, quality of life, low cost of doing business and culture of innovation," Trevor Pawl, Michigan's chief mobility officer, said in a statement. "Michigan remains committed to being the global epicenter of the next revolution of the automotive industry and we applaud Upstream's continued success and investment in Michigan's autonomous and electrified future."

Upstream expects its Ann Arbor center to be fully operational by the end of the year. It is looking to open a vehicle security operation in center in Japan, as well.