April 2023

NAVY SBIR TRANSITION PROGRAM SPOTLIGHT

Company: La Jolla Logic, Inc.
Website: www.lajollalogic.com
POC: Karina Arushanyan
Phone: (619) 535-1121
Address: 444 West C Street, Suite #220
San Diego, California 92101

La Jolla Logic Uses Artificial Intelligence and Machine Learning to Identify Network Threats

By Jennifer Reisch

La Jolla Logic, Inc. (LJL) developed Cognitive Autonomous Artificial System Intelligence (CAASI), a tool designed to detect anomalous communication on networks. CAASI identifies potentially malicious activity, whether from direct hack attempts, viruses, bots, or even insider threats. It improves the speed and accuracy of responses to cyber threats.

CAASI uses artificial intelligence (AI) and machine learning (ML) to identify anomalous communication on networks. "CAASI listens to networks for their heartbeat; it learns how that heartbeat of communications works and then identifies—after its learning period—when there are irregularities. It identifies anomalous communication and can cue alerts for operators to closely examine what's happening," explained Brian Brethen, operations manager at LJL.

La Jolla Logic, Inc. developed Cognitive Autonomous Artificial System Intelligence (CAASI), a tool designed to detect anomalous communication on networks. CAASI identifies potentially malicious activity, whether from direct hack attempts, viruses, bots, or insider threats.

Because CAASI is an unsupervised ML tool, it can detect previously unseen threats and determine something is wrong. "When you think about traditional antivirus programs or intrusion detection systems, they're always after the fact; somebody got breached somewhere. Then forensics came in and identified what code cracked open the system. And then you start looking for that code being injected into your system so you can prevent the same intrusion from occurring," Brethen explained. CAASI adds a new capability to existing cyber security tools through its anomalous behavior detection. Unlike traditional antivirus programs, which are reactive and only identify threats after a breach has occurred, CAASI uses unsupervised ML to identify anomalous communication within a network and can identify threats without requiring a fingerprint or previous knowledge of the threat, drastically limiting the ability of malware to propagate and compromise complex networks.

When it detects unusual communication patterns, it flags potential threats and alerts operators to investigate the issue. “CAASI looks at how a network communicates from some very complex combinations of factors. And when the network begins to communicate in an unusual fashion—two systems that don’t normally connect do so, or a system sends a message to an unexpected and unidentified asset—CAASI notes it right away. Based on its unsupervised learning, it determines whether this is within reason or not within reason and should be flagged,” Brethen said. The software can also take action in addition to sending out an alert. For example, it can be configured to automatically intercept communications and take the individual out of the process, countering hostile actions before any damage is done.

“One of the key exciting parts of CAASI is it functions exceptionally well on industrial control system [ICS] networks, where one of the great concerns we were faced with was false positives because that’s really the biggest challenge with unsupervised machine learning. In La Jolla Logic’s test environment we were getting 100% detection of bad behaviors with only four false positives a year, which is well within the acceptable tolerance limit for false positives and allows for timely intervention to prevent breaches. These were exceptionally amazing results for an unsupervised machine learning tool, and the Navy said, ‘We can really use something like this.’”

The Navy also conducted its own tests in their own cybersecurity lab. “That process involved us providing an installation kit and user guidelines to the Navy technical point of contact for CAASI; then the government scientists and engineers did their own deployment and ran their own tests in their own environment. While our engineers remained on call in San Diego, the test was run independently by the Navy on the East Coast,” Brethen said. The software demonstrated impressive results in the government test environment as well, which led the Navy to work with LJL to integrate CAASI into the Navy’s existing network security tool suite to enhance their detection and response capabilities.

Despite the extraordinary success of the software tests and the Navy’s interest, it took a while to get the product into Navy systems. “The moment we had the test results, we were told that they were going to put us on contract, but it did take several months," he said. The Navy needed to find the funds and then determine the best way to integrate it into some existing programs with their other detection tools, and also determine the best vehicle to contract with LJL under SBIR rules. Under the SBIR Phase III transition, LJL has an engineering services contract and the Navy has a license to use the software.

LJL has also reached out to other military branches, federal agencies and commercial organizations with critical infrastructure and ICS networks that could benefit from this software. CAASI is broadly applicable to any computer network system for detecting unknown anomalous activity, including potential security threats. It can also be adapted to specific industries, such as public water distribution and energy sector utilities, to analyze detected anomalies and indicators that a system is acting abnormally and may be about to fail. CAASI's ability to detect abnormal behaviors on ICS networks can inform condition-based maintenance models to improve accuracy and reliability of predicted failures.

As a participant in the Navy STP, "The quad chart was hands down the most valuable communication tool we developed throughout the entirety of the program. That was more important than building call lists and writing a plan because the quad chart was the document we could hand to every potential contact with an environment where CAASI could be a fit. When we were talking to some of the large primes it provided a succinct tool that gave us a clear set of communication points we could elaborate on in a conversation. Navy STP forced us to think in different ways about commercializing the product, about how to frame and tell our story. It also helped us shape how we intended to market CAASI, and that was vital for overall success," Brethen said.

LJL is an advanced security solutions and technology business working across all service branches of the DoD as well as other agencies and with commercial organizations. LJL is an SBA certified 8(a) woman owned small business (WOSB).

Capabilities:

- Cybersecurity Engineering Services
- Cross Domain Solutions
- Artificial Intelligence / Machine Learning
- Secure Software Engineering (DevSecOps)

For more information, visit the company website at www.lajollalogic.com.

LA JOLLA LOGIC