PROTECTING DATA AND INTELLECTUAL PROPERTY FROM CYBERTHREATS

"Our value is tied directly to the speed at which we can react. If we can move quickly, we can prevent the spread, which means less data is infected, and fewer resources have to work on cleanup. MixMode AI quickly identifies anomalies so we can alert our clients and start our investigations."

Technology-enabled Cybersecurity Expertise

Established by former officers from the U.S. intelligence community, Nisos provides technology-enabled cybersecurity services and investigations. The company is a trusted partner to many Fortune 500 firms that need to secure their on-premise and Cloud-based assets to avoid existential threats to their businesses.

Relying on a cross-functional, expert-driven culture built on diverse backgrounds and skill sets, Nisos quickly responds to complex threats across a wide range of networks. The firm partners with industry leaders and ground-breaking technology companies to address platform abuse, supply chain integrity and nation-state level hacking, among other issues.

An important tool in its fight against cybercrime is MixMode, the leading provider of comprehensive network traffic analysis powered by the most advanced AI in cybersecurity.

Developed for projects at DARPA and the DoD, MixMode's third-wave AI needs no human training and can baseline client networks in only seven days, enabling 95 percent alert precision and reduction and identification of zero-day attacks.

With MixMode, Nisos is using best-in-class, context-aware AI to create evolving baselines of its clients' networks. Through the combination of threat-intel and sophisticated anomaly detection, Nisos predicts and identifies threats in real-time.

Using MixMode Nisos can:

- **Predict and identify threats in real-time**
- **Ingest and analyze CloudTrail logs**
- **Need no human training and can baseline client networks in seven days**
- **Enable 95 percent alert precision and reduction and identification of zero-day attacks**

About Nisos

Nisos is a technology-enabled, cybersecurity services and investigations company. It tailors its services to provide clients with a holistic approach that addresses their highest priority risks. Based on years of experience, the company has found that these risks nearly always connect to the digital world, even if the connection isn't obvious or is difficult to frame at first glance.

Challenge: Manual Audits Impact Efficiency

After suffering a possible breach, a client approached the team at Nisos for help evaluating the security of its AWS environment. The client was concerned about possible malicious activity on the part of a former employee who had maintained an AWS Identity and Access Management (IAM) account after being separated.

To understand the scale of the possible breach, Nisos needed to export and manually review all of the client's CloudTrail logs, a resource-intensive and time-consuming exercise.

"Speed and accuracy are important in our investigations. This AWS account had roughly 10 to 15 API calls every second. Just manually exporting the CloudTrail logs was killing our machine. It took hours, and we finally ran out of inodes, so we couldn't cease and write to disk."

Creating a Single View to Drive Productivity

Based on input from Nisos, MixMode now addresses the challenges that Nisos faced analyzing CloudTrail data logs: the lack of intelligent analysis behind CloudTrail and the fact that CloudTrail information is presented across multiple screens.

With its patented, context-aware AI, MixMode ingests and analyzes CloudTrail logs, correlates events, and presents the results in an intuitive interface. Rather than manually reviewing data logs for days, Nisos can now quickly report anomalous activity, like the deletion of an EC2 instance or a change to MLA keys, back to its clients.

About MixMode

MixMode is a revolutionary AI focused Cybersecurity Company using patented third-wave AI originally developed for projects at DARPA and the DoD. MixMode's AI-Powered Network Traffic Analytics Platform provides deep network visibility and predictive threat detection capabilities, enabling your security team to efficiently perform real-time and retrospective threat detection and visualization. Used by breach response teams worldwide, security analysts and SOC teams can integrate MixMode into their playbooks, SIEMs, or utilize MixMode on a standalone basis to dramatically reduce investigation time, cost and expertise required to respond to persistent threats, malware, insider attacks and nation state espionage efforts. Based in Santa Barbara with an additional office in San Diego, the company is backed by investors including Keshif Ventures and Blu Venture Investors.