PacketSled Launches First Network Monitoring Platform driven by Context-Aware AI, Changes name to MixMode

New Technology Reduces False Positive Alerts by 90%

Santa Barbara, Calif. — March 4, 2019 — PacketSled, the leading AI-driven Network Monitoring and Forensics platform, today announced its corporate name change to MixMode, reflecting the company's new Context-Aware AI (CAAI) technology that is reducing enterprise network False Positive alerts by 90%.

False Positives drain enterprise security resources and alert fatigue puts companies at risk of being non-compliant. 3 in 10 IT professionals admit that they ignore security alerts. According to a survey by the Ponemon Institute, "Organizations waste on average 395 man hours a week chasing erroneous alerts; Companies average 17,000 malware alerts weekly, only 4% are investigated and only 19% are reliable. 40% of infections go undetected."

In contrast with rule-based and regression-based AI systems that are reactive, MixMode uses a context-aware AI approach that maps a given network's behaviors influenced by operational rhythms and user actions on a specific network environment. MixMode better understands the network behavior, dynamically adapts to baseline changes and enables both misuse detection and anomaly detection, driving false positive alerts down dramatically. MixMode's platform also offers transparency to the customer on what is/is not being filtered so the customer can review and confirm the AI's results.

"Most security products rely on rules-based machine learning to drive their alerts. None of these products are effectively integrating the historical behavior of a given client's network, much less keeping it updated, because it is an enormous amount of data that would have taken server farms to address in the old world," said John Keister, CEO of PacketSled. "Most enterprises are totally overwhelmed with alerts for their security team, costing them billions of dollars per year. With our proprietary, AI-based platform, we want to help the security community take a massive step forward in addressing the alert fatigue problem."

"Network security systems need to become autonomous, and switch from passive tools to active participants in the security assurance process via the AI-human interaction. Current solutions including first wave AI (expert systems, rule-based) and second wave (statistics based, classification engines) approaches to network security have inherent issues with interpretability, *false positives, and dynamically changing data*. MixMode is the first to bring a third wave, context-aware AI approach that automatically learns and adapts to dynamically changing environments," said CTO and Chief Scientist Igor Mezic.

MixMode is based on technology developed by Chief Scientist Dr. Igor Mezic during a 10+ year period working with DARPA, DoD and other US government entities. Dr. Mezic joined MixMode in September 2018. For a look at Dr. Mezic's latest blog on the importance of context-aware AI, please go here.

MixMode's new platform offers multi-tenancy capability and easy API integrations. The MixMode CAAI system runs on top of the company's existing PacketSled system, used by enterprises and MSSPs for real-time network analysis, threat hunting and incident response.

About MixMode

MixMode is the first to bring a third-wave, context-aware AI approach that automatically learns and adapts to dynamically changing environments. MixMode's platform PacketSled, better understands network behavior as it adapts to baseline changes and enables both misuse detection and anomaly detection, as well as predictive maintenance. Used by enterprises and MSSPs for real-time network analysis, threat hunting and incident response, the platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics. Security teams can integrate PacketSled into their orchestration engine, SIEM, or use PacketSled independently to dramatically reduce false positive alerts and the resources required to respond to persistent threats, malware, insider attacks and nation state espionage efforts.

The company has been named an innovator in leading publications and by security analysts, including SC Magazine, earning a finalist award in 2018 and 2019 for "Best Computer Forensic Solution." Based in Santa Barbara with offices San Diego, the company is backed by investors including Keshif Ventures and Blu Venture Investors. For case studies, continuous product updates and industry news, please visit us at mixmode.ai.