MixMode™

MIXMODE FREQUENTLY ASKED QUESTIONS

I ALREADY HAVE A SIEM NOW WHAT? / HOW DOES THIS WORK WITH MY SIEM?

The biggest difference between MixMode and a typical SIEM is that the SIEM collects logs of a limited set of data while wire data looks at all data and transactions on the network. Furthermore, a SIEM will never be completely configured as companies are constantly adding new devices, replacing old devices, etc. Oftentimes, companies rarely (or never) keep up on updating the configuration of the SIEM, further reducing their value. Challenges arise when relying solely on log data from a SIEM: Logs can be changed, altered, or adjusted to stop sending information.

HOW DOES YOUR API WORK?

Using our robust REST API, user can seamlessly integrate security stacks with MixMode by offloading data into SIEMs, orchestration engines and ticketing systems. We integrate with market-leading tools like Splunk, ServiceNow, LogRhythm, Demisto, ConnectWise, Pager Duty and more.

WHAT ARE THE SPECS ON YOUR APPLIANCE?

We are a software company. While we do have both SaaS and On-Premises options, we don't ship appliances as part of our standard course of business.

HOW IS IT DEPLOYED?

MixMode supports both on-premises and SaaS based employments.

HOW DOES THIS WORK WITH OUR SOAR?

MixMode can be integrated with your SOAR via our API. Automate and accelerate your search and investigations by using this integration to pull traffic flows, extracted files and PCAPs automatically.

HOW DOES MIXMODE MAKE ME MORE SECURE?

As cyber threats mature protection at the perimeter through traditional means is no longer sufficient. The goal has shifted from penetration prevention to rapid identification, remediation and response. MixMode's combination of AI anomaly detection and intel-based wire data detections give you visibility and confidence that you will never miss what matters.

DO I HAVE TO USE YOUR UI?

No. MixMode's AI can be integrated with your existing tooling to act as an intelligence layer and provide anomaly detection as well as alert reduction and precision. MixMode's AI can be used in traditional SIEMs like Splunk or Sumologic as well as SOARs like Demisto.

WHAT SOURCES OF DATA DO YOU INGEST?

MixMode can ingest all network data feeds including, Bro/ZEEK, SecurityOnion, Surricata & SNORT. In addition, MixMode can ingest CloudTrail Logs and AWS netflow data.

HOW IS YOUR AI DIFFERENT?

MixMode's AI is patented "Third-Wave AI" (as defined by DARPA). Most Cybersecurity solutions offering "AI-Enabled" systems are what DARPA would call "Second-Wave" or systems that require human rules and tuning. MixMode's AI was developed over 20 years by Dr. Igor Mezic. It can create a baseline understanding completely on its own in only 7 days (as opposed to 18 months which other systems require on average) and is fully autonomous in its ability to surface threats and anomalies.

WHERE DOES MIXMODE FIT IN MY WORKFLOW?

There are 2 common workflows for MixMode. 1) Proactive Alerting and 2) Reactive Investigations. MixMode ships with an action-based dashboard that will surface a combination of AI anomalies and intel-based detections that a security analyst should review each day. In addition, MixMode is a powerful forensic tool that can be used to research and identify the scope of a breach or detection from another platform.

DOES MIXMODE HELP WITH COMPLIANCE?

MixMode is a valuable tool for verifying your compliance status and ensuring that your tools and protocols are functioning properly. Customers routinely use us to verify their PCI, HIPAA and NIST compliance.

MORE QUESTIONS? CONTACT US!

Email info@mixmode.ai or Call (858) 225-2352. You can also send us a message at https://mixmode.ai/contact-us