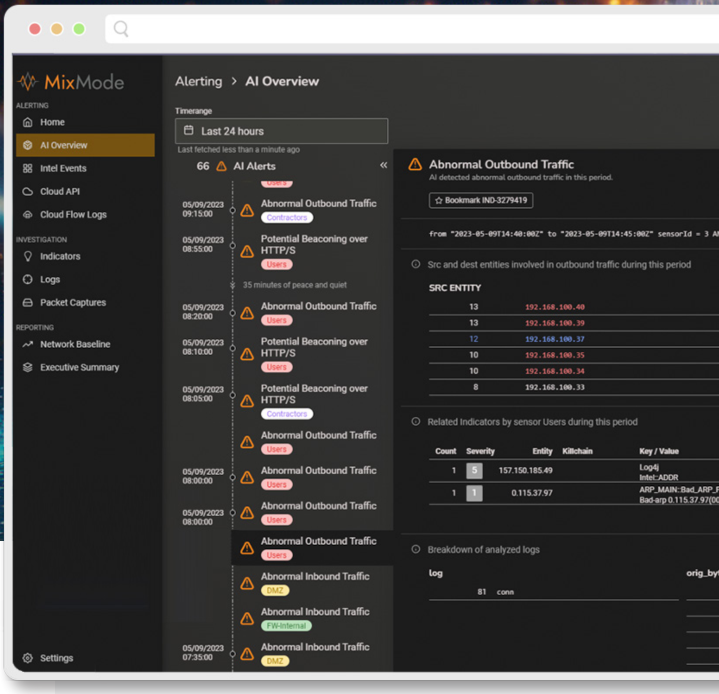
MixMode®

STRENGTHEN ZERO TRUST INITIATIVES WITH MIXMODE



Last fetched less than a minute ago

Users

05/09/2023 09:15:00 Abnormal Outbound Traffic Contractors

05/09/2023 08:55:00 Potential Beaconing over HTTP/S Users

35 minutes of peace and quiet

05/09/2023 08:20:00 Abnormal Outbound Traffic Users

05/09/2023 08:10:00 Potential Beaconing over HTTP/S Users

05/09/2023 08:05:00 Potential Beaconing over HTTP/S Contractors

Abnormal Outbound Traffic Users

05/09/2023 08:00:00 Abnormal Outbound Traffic Users

05/09/2023 08:00:00 Abnormal Outbound Traffic Users

Abnormal Outbound Traffic Users

Abnormal Inbound Traffic DMZ

Abnormal Inbound Traffic FW-Internal

05/09/2023 07:35:00 Abnormal Inbound Traffic DMZ

Abnormal Outbound Traffic

AI detected abnormal outbound traffic in this period.

```
from "2023-05-09T14:40:00Z" to "2023-05-09T14:45:00Z" sensorId = 3 A
```

Src and dest entities involved in outbound traffic during this period

SRC ENTITY

13	192.168.100.40
13	192.168.100.39
12	192.168.100.37
10	192.168.100.35
10	192.168.100.34
8	192.168.100.33

Related Indicators by sensor Users during this period

Count	Severity	Entity	Killchain	Key / Value
1	5	157.150.185.49		Log4j Intel::ADDR
1	1	0.115.37.97		ARP_MAIN::Bad_ARP_F Bad-arp 0.115.37.97(00

Breakdown of analyzed logs

log	orig_by
81 conn	

Detect Attacks in Real-time with MixMode

Organizations implementing a Zero Trust security framework face the challenge of ensuring continuous monitoring and threat detection across their networks to maintain high security. Another critical piece of solving for Zero Trust is to avoid bias that can accompany training data sets and human-written rules and thresholds. For most organizations, the path to Zero Trust is a transformational journey to prevent and manage risk.

Fortify Your Zero Trust Initiatives

By integrating The MixMode Platform into their zero trust architecture, organizations can quickly identify and respond to emerging threats that have successfully bypassed legacy security infrastructure.

The MixMode Platform utilizes self-supervised learning to forecast expected behavior and detect potential threats by analyzing network activity and extracting patterns and trends from the underlying time-stamped data without predefined rules or training. This proactive approach enables security teams to avoid bias, take immediate action, investigate incidents, and prevent potential breaches before they escalate.

MixMode's AI is driven by a generative model that initially takes no historical knowledge to function and is unbiased from human alteration.. The MixMode platform makes no assumptions about the data stream it analyzes out of the gate and everything must be continuously verified as expected behavior. Simply put, nothing is trusted and everything must be verified.

NO RULES. NO TUNING. NO DATA LIMITS. ANY ENVIRONMENT.

Key Capabilities:

Real-time Threat Detection: The MixMode Platform is the only generative AI cybersecurity solution built on patented technology purpose-built to detect and respond to threats in real-time, at scale to cut through the noise and surface critical threats, and improve overall defense against attacks.

Strengthen a Zero Trust Posture: Detects and prevents threats that bypass traditional rules-based security measures, including New Ransomware, Zero-Day, Insider Threats, "Living off the Land", Supply Chain, AI/ML Model Poisoning.

Detect at Scale: Easily monitor and protect the entire attack surface across cloud, on-prem or hybrid environments, to quickly detect and mitigate emerging threats without increasing spend.

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai | © MixMode, Inc.