MixMode™

PREDICTIVE SECURITY MONITORING FOR YOUR AWS CLOUD ENVIRONMENT

According to SANS Institute, the lack of integration & visibility across Cloud Platforms and Hybrid Environments is one of the main problems plaguing enterprise cybersecurity teams today. The inability to understand what is normal behavior in a cloud environment – and therefore recognized the existence of an anomaly – is the main reason for this challenge.

Using our patented unsupervised AI originally built for DARPA and the DoD, MixMode helps enterprise security teams all over the world monitor their AWS network traffic and API calls in real-time to shore up the gap in their security posture.

Deploy MixMode within your AWS environment to surface anomalies and correlate alerts across VPC Flowlogs, AWS Cloudtrails logs and on-premise network data. Additionally, MixMode give you access to a host of forensic investigation tools that allow you to search and investigate your cloud infrastructure like never before.

AWS CloudTrail

AWS VPC Flow Logs

Key Benefits

CORRELATION OF AMAZON CLOUDTRAIL DATA AND VPC FLOWLOGS

MixMode offers the ability to correlate AWS CloudTrail traffic with VPC Flowlogs and/or SIEM logs to identify IPs that cause issues across these data streams.

VISIBILITY INTO CLOUDTRAIL AND VPC FLOW LOGS ON A SINGLE SCREEN

VPC Flow Logs provides access to IP traffic in and out of your AWS VPC. CloudTrail monitors the API calls into your AWS environment. To secure your AWS cloud infrastructure requires leveraging both tools with visibility on a single platform.

CLOUD AI BASELINE AND ANOMALY DETECTION

MixMode's unsupervised AI can baseline your CloudTrail and FlowLog activities in as little as 7 days. This baseline allows you to understand what is "normal" in your AWS environment so when a threat occurs you will know.

COMPARE CT AND VPC FL TO SECURITY INTEL AND USER-DEFINED RULES

In addition to AI baselining and anomaly detection, MixMode will also compare your CloudTrail and Flow Log traffic against our database(s) of known intel feeds. This combination of anomaly detection and traditional threat detection gives you a comprehensive picture of your current security posture.

FORENSIC SEARCH AND CORRELATION ACROSS CT AND VPC FL

Once ingested into the MixMode Platform, our powerful forensic search tools give you the ability to search across an unlimited history of your data. These tools are critical to your ability to investigate potential threats and see the scope and origination of an attack. What's more by preserving a forensic record outside of your AWS environment, you can be assured that your data cannot be tampered with.

PREDICTIVE THREAT MONITORING

Using a combination of MixMode's baseline and a variety of threat and intelligence feeds, our Unsupervised AI compares expected behavior with anomalies to pinpoint and surface threats in your AWS environment real-time.

POWERFUL PATENTED AI

By delivering an ongoing and predictive baseline of your normal cloud behavior, our AI can accurately assess which alerts should and should not be fired. The AI will continue learning and defining what is normal over time as behavior changes for better anomaly detection.