SANS

Analyst Program

Self-Supervised Learning Cybersecurity Platform for Threat Detection

SPONSORED BY

MixMode

A SANS First Look

Written by **Matt Bromiley** | March 2023

Introduction

Let's face it—cybersecurity analysts have far too much data to analyze these days. We've written time and time again how complex the modern enterprise is getting. Today, organizations scale hybrid environments across the globe and support an equally complex remote workforce. Security analysts are charged with protecting these complicated environments. However, many large enterprises are not performing real-time analytics of their largest data environments.

In this SANS First Look, we examine MixMode, a platform designed to focus on providing cybersecurity teams full visibility and real-time threat detection—at enterprise scale. Via its proprietary artificial intelligence (AI), MixMode boasts a self-learning platform that can ingest various data types, from cloud to network to endpoint, and help analysts identify adversarial threats, from run-of-the-mill known attacks to never-before-seen novel attacks. MixMode can significantly reduce false positives and noisy data, allowing analysts to focus on the threats that matter now.

Bring All Your Data

The folks at MixMode know that enterprise security teams have large amounts of data to monitor as part of their daily jobs. And we mean a lot of data. Think about all the data the modern enterprise generates:

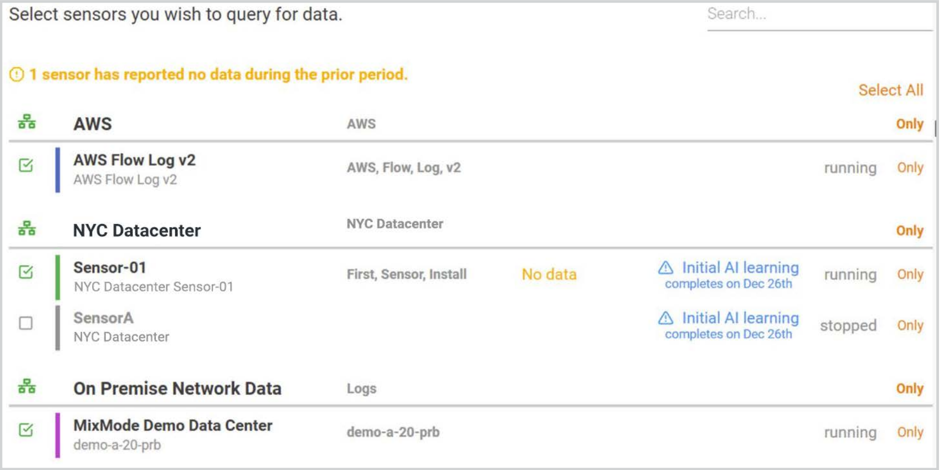
- On-prem network data, ranging from NetFlow to full packet capture (PCAP) from multiple geographic locations
- Network device data, to support physical and virtual assets
- Endpoint telemetry, including endpoint detection and response (EDR) data and raw system logs
- Cloud-centric logs and telemetry streams, ranging from logs to third-party outputs

However, collating, correlating, and wrangling all this data into one place is much easier said than done. And this is where many organizations simply stop and rely on limited data to hopefully detect threats to the environment. Additionally, even with "all" the data in one place, security analysts must still be able to find threats among the noise. Unfortunately, missed or overwhelming data means adversaries can slip through.

> **We have been saying for years that the more data, the better. However, standard cybersecurity programs often fail as organizations can't make sense of it all. MixMode's AI lets you jump that barrier to find threats among all the noise, including novel attacks designed to bypass legacy detection systems.**

For this reason, MixMode encourages organizations to bring all data to the table—the more context, the better. Couple that strategy with its advanced AI detection capabilities and security analysts no longer must rely on signature-based detection systems. Meaning, detection at *enterprise scale* is achievable. Figure 1 provides a view of a MixMode multitenant sensor dashboard, highlighting some of the various sources it can incorporate.

As soon as data is ingested into the MixMode platform, the AI automatically begins learning so it can discover potential threats to the environment across the organization's various data feeds. The more data brought into MixMode, the more comprehensively its generative model can learn on its own.



Select sensors you wish to query for data. Search...

ⓘ 1 sensor has reported no data during the prior period.

Select All

AWS	AWS				Only
☑ **AWS Flow Log v2** AWS Flow Log v2	AWS, Flow, Log, v2			running	Only
NYC Datacenter	NYC Datacenter				Only
☑ **Sensor-01** NYC Datacenter Sensor-01	First, Sensor, Install	No data	⚠ Initial AI learning completes on Dec 26th	running	Only
☐ SensorA NYC Datacenter			⚠ Initial AI learning completes on Dec 26th	stopped	Only
On Premise Network Data	Logs				Only
☑ **MixMode Demo Data Center** demo-a-20-prb	demo-a-20-prb			running	Only

Figure 1. Multitenant Sensor Dashboard

Detecting and Investigating Threats

Of course, ingesting data into a centralized location and layering it with efficient AI capabilities is only half the battle. Once a threat has been detected, that's where humans "take over" to review and triage. For this reason, the MixMode platform is broken into three high-level functions that represent various stages of security operation center (SOC) detection and analysis:

- **Alerting** is the initial view and includes the various types of telemetry brought into the organization, the status of AI, and threat intelligence associated with observed telemetry.
- **Investigation** allows analysts to view indicators of detection in a timeline manner, query logs, and review packet captures as observed from network telemetry.
- **Reporting** is exactly as it sounds—reports and insights into the platform, including data ingestion and bandwidth statistics.

We envision that analysts will spend most of their time between the **Alerting** and **Investigation** options, reviewing alerts and conducting further analysis to determine impact and response options. The **Alerting** screen, shown in Figure 2, provides high-level details analysts can drill into to gain more context.

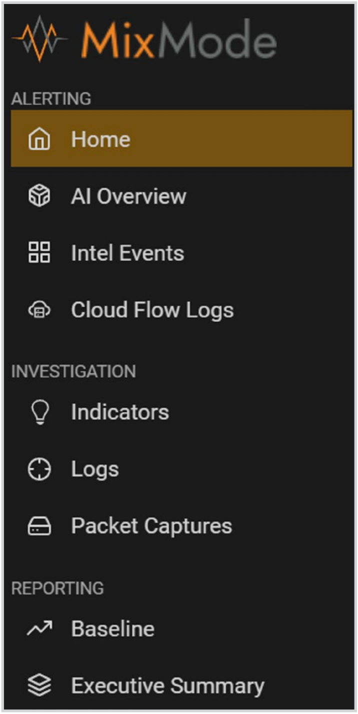
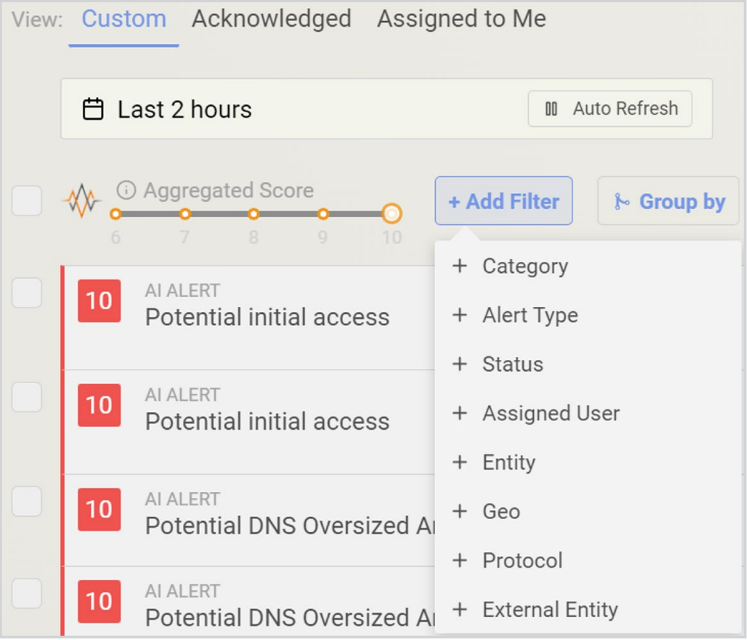


Figure 2. MixMode Alerting Screen

Notice in Figure 3, the **Alerting** screen is coupled with various filtering and assignment options. These allow SOC analysts and managers to assist alerts, escalate if necessary, and utilize the platform in daily ticket management and response.

Beyond alerting, analysts can use the **Investigation** options to triage various datasets in the platform to gain more context around alerts. Figure 4 provides a snippet of network data as observed and categorized by the MixMode platform.

During our First Look of MixMode, we continually saw examples of significant data reduction and alerting that would serve many enterprise security teams very well. As we've stated before, finding signals among the noise is paramount, especially within extremely large datasets. MixMode's AI platform is constantly learning as new data is brought in, giving cybersecurity analysts the advantage they need to detect all types of attacks in real time.



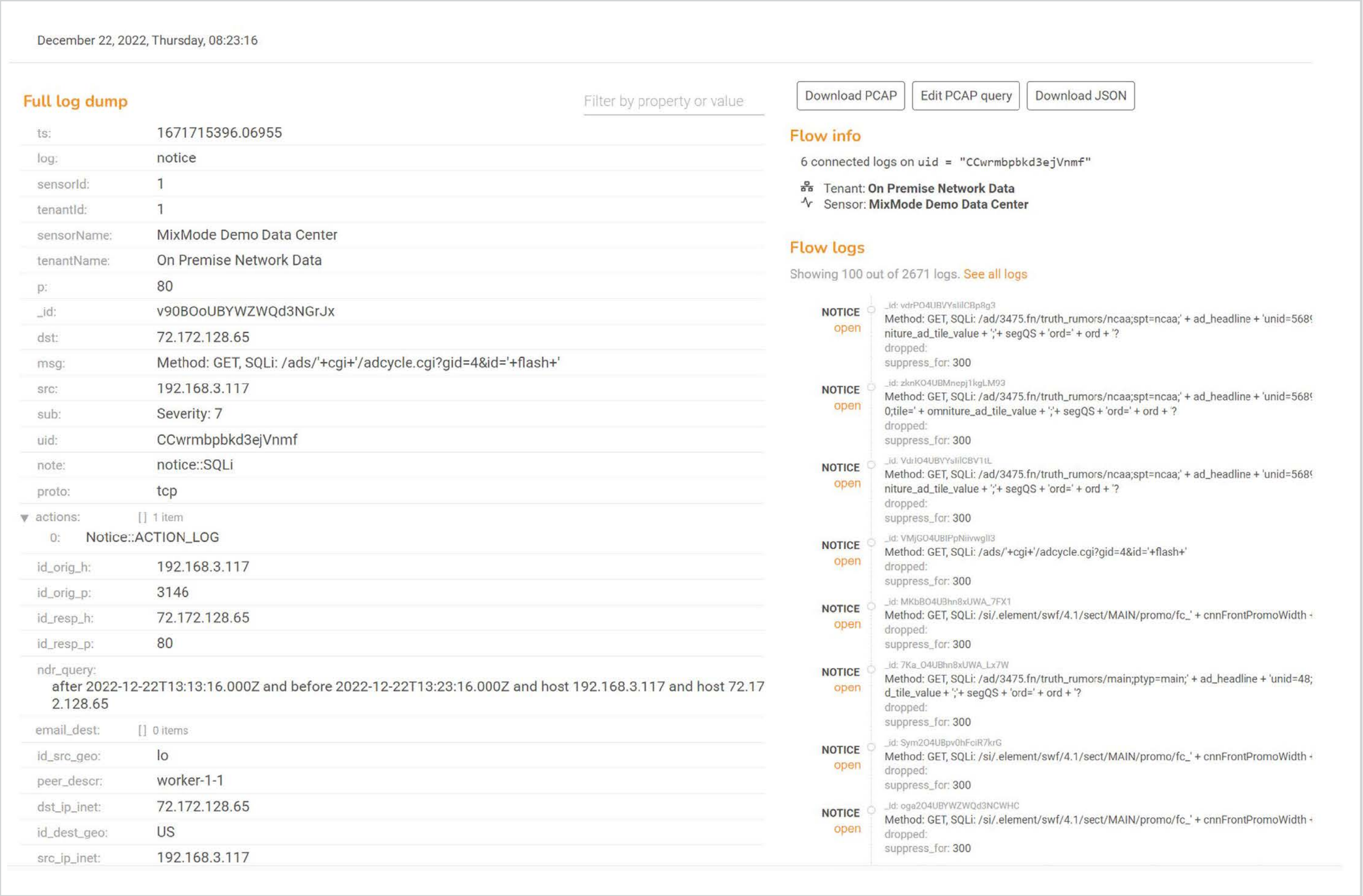
10 AI ALERT Potential initial access

10 AI ALERT Potential initial access

10 AI ALERT Potential DNS Oversized A

10 AI ALERT Potential DNS Oversized A

Figure 3. Alerting Function Filtering Options



December 22, 2022, Thursday, 08:23:16

Full log dump

```
ts:            1671715396.06955
log:           notice
sensorId:      1
tenantId:      1
sensorName:    MixMode Demo Data Center
tenantName:    On Premise Network Data
p:             80
_id:           v90BOoUBYWZWQd3NGrJx
dst:           72.172.128.65
msg:           Method: GET, SQLi: /ads/'+cgi+'/adcycle.cgi?gid=4&id='+flash+'
src:           192.168.3.117
sub:           Severity: 7
uid:           CCwrmbpbkd3ejVnmf
note:          notice::SQLi
proto:         tcp
▼ actions:     [] 1 item
    0:     Notice::ACTION_LOG
id_orig_h:     192.168.3.117
id_orig_p:     3146
id_resp_h:     72.172.128.65
id_resp_p:     80
ndr_query:
  after 2022-12-22T13:13:16.000Z and before 2022-12-22T13:23:16.000Z and host 192.168.3.117 and host 72.17
  2.128.65
email_dest:    [] 0 items
id_src_geo:    lo
peer_descr:    worker-1-1
dst_ip_inet:   72.172.128.65
id_dest_geo:   US
src_ip_inet:   192.168.3.117
```

Flow info

6 connected logs on uid = "CCwrmbpbkd3ejVnmf"

Tenant: **On Premise Network Data**
Sensor: **MixMode Demo Data Center**

Flow logs

Showing 100 out of 2671 logs. See all logs

```
NOTICE  _id: vdrPO4UBVYslilCBp8g3
open    Method: GET, SQLi: /ad/3475.fn/truth_rumors/ncaa;spt=ncaa;' + ad_headline + 'unid=568
        niture_ad_tile_value + ';'+ segQS + 'ord=' + ord + '?
        dropped:
        suppress_for: 300
NOTICE  _id: zknKO4UBMnepj1kgLM93
open    Method: GET, SQLi: /ad/3475.fn/truth_rumors/ncaa;spt=ncaa;' + ad_headline + 'unid=568
        0;tile=' + omniture_ad_tile_value + ';'+ segQS + 'ord=' + ord + '?
        dropped:
        suppress_for: 300
NOTICE  _id: VdrIO4UBVYslilCBV1tL
open    Method: GET, SQLi: /ad/3475.fn/truth_rumors/ncaa;spt=ncaa;' + ad_headline + 'unid=568
        niture_ad_tile_value + ';'+ segQS + 'ord=' + ord + '?
        dropped:
        suppress_for: 300
NOTICE  _id: VMjGO4UBIPpNiivwgll3
open    Method: GET, SQLi: /ads/'+cgi+'/adcycle.cgi?gid=4&id='+flash+'
        dropped:
        suppress_for: 300
NOTICE  _id: MKbBO4UBhn8xUWA_7FX1
open    Method: GET, SQLi: /si/.element/swf/4.1/sect/MAIN/promo/fc_' + cnnFrontPromoWidth +
        dropped:
        suppress_for: 300
NOTICE  _id: 7Ka_O4UBhn8xUWA_Lx7W
open    Method: GET, SQLi: /ad/3475.fn/truth_rumors/main;ptyp=main;' + ad_headline + 'unid=48;
        d_tile_value + ';'+ segQS + 'ord=' + ord + '?
        dropped:
        suppress_for: 300
NOTICE  _id: Sym2O4UBpv0hFciR7krG
open    Method: GET, SQLi: /si/.element/swf/4.1/sect/MAIN/promo/fc_' + cnnFrontPromoWidth +
        dropped:
        suppress_for: 300
NOTICE  _id: oga2O4UBYWZWQd3NCWHC
open    Method: GET, SQLi: /si/.element/swf/4.1/sect/MAIN/promo/fc_' + cnnFrontPromoWidth +
        dropped:
        suppress_for: 300
```

Figure 4. Investigation Screen Showing Network Data

Takeaways

Conquering the vast amounts of data generated by the modern enterprise is something many SOC teams have only dreamed of. The data is there, and they know the value of good telemetry, but it is too much manual effort to sift through it all to try to make sense of the noise. This approach also can be costly, as analysts take time to determine what data is useful, all the while racking up ingestion and storage fees.

Armed with a platform like MixMode, this problem is no longer as massive as it seemed. With MixMode, organizations can:

- Bring any and all data to the table—from cloud providers to network devices to endpoint—and use it to detect both known and novel threats within the environment.
- Identify the *threats that matter* using its proprietary AI algorithms and bring those to the surface for analysts.
- Make their analysts' lives easier with a single point of analysis and triage, allowing them to focus on responding to threats rather than swimming through data.

It should come as no surprise that enterprises will continue to generate more and more data, especially as we see integration of new products and migration to cloud providers. Don't let your security team fall behind all these changes. A platform like MixMode will help ensure that a complex environment doesn't prohibit the detection and prevention of threats to the environment.

SANS would like to thank this paper's sponsor:

MixMode