THE FAILED PROMISES OF SIEM:

How Next-Generation Cybersecurity Platforms are Solving the Problems Created by Outdated Tools

WHITEPAPER
CO-AUTHOR: GEOFF COULEHAN

www.mixmode.ai | +1 (858) 225-2352 | info@mixmode.ai | © 2022 MixMode, Inc.

Overview

While security information and event management (SIEM) vendors continue to insist their technology is sufficient to meet the dynamic challenges and exceptionally complex threatscape faced by cybersecurity teams today, their behavior in the marketplace and overall performance tells a different story.

If these platforms are as robust as vendors claim, it's puzzling why their approach is to continually tack on "features" that enable SIEM to perform somewhat adequately as effective security tools. If SIEM is effective, why do vendors recommend upgrading to network analysis or threat detection tools?

How can a SIEM offer real-time threat detection or predictive analysis, like some vendors claim, when these platforms rely on historic data logs that are outdated as soon as they are fed into the system? In truth, these systems are inadequate in their simple form and even when enhanced by add-ons. The answer to the issue of ineffective security solutions is not simply to increase cybersecurity spending. Surprisingly, the best solution for many organizations could be a lower overall cybersecurity investment.

The fundamental SIEM flaws lie in the platform's need for continual adjustment, endless data stores, and a tendency to create an overwhelming number of false positives. When organizations instead turn to a next-generation cybersecurity solution, which predicts behavior with an unsupervised (zero tuning) system, they are poised to save on both financial and human resources.

Contents

> ***“One of the most common failings I have seen is a SIEM overstuffed with useless data. A SIEM should augment analysis, not hinder it.***
>
> ***Put simply: less is more. The more data you have, the worse the SIEM performs.”***

Justin Henderson
SANS Institute

The Evolution of SIEM

It should be noted that SIEM platforms are exceptionally effective at what they initially were intended for: providing enterprise teams with a central repository of log information that would allow them to conduct search and investigation activities against machine-generated data. If this was all an enterprise cybersecurity team needed in 2020 to thwart attacks and stop bad actors from infiltrating their systems, SIEM would truly be the cybersecurity silver bullet that it claims to be.

The functionality of SIEMs does allow organizations to benefit from several significant features:

1. The ability to access historical data made it possible to comply with rapidly changing compliance requirements in an efficient, effective way.
2. Aggregating and analyzing network events captured by endpoints and machine-generated data sources to provide greater visibility into network infrastructure challenges.
3. Providing search and investigative capabilities.
4. Serving as a log collection point.

Over time, SOC teams recognized additional potential uses for the SIEM framework. But one of the fundamental foundations for the establishment and rise of the SIEM market was the compliance factor. The question now is whether these compliance platforms were built for modern cybersecurity challenges.

Gartner Defines SIEM

While SIEM-like processes were not entirely new among security operation centers (SOCs) in the early 2000s, the industry didn't recognize SIEM as a term until it was coined in 2005 by two Gartner security analysts, Mark Nicolett and Amrit Williams. Gartner's SIEM report, *Improve IT Security with Vulnerability Management*, proposed a new kind of security information platform based on two previous generations:

First-generation Security Information Management (SIM) approaches were built on top of traditional log collection and management systems. These systems benefitted from game-changing features like long-term storage and analysis capabilities. SIM also introduced the ability to evaluate combined logs with threat intelligence.

Security Event Management (SEM) second-generation platforms addressed security events. These systems could aggregate, correlate, and notify analysts about security events based on triggers from antivirus programs, firewalls, and intrusion detection systems (IDS). They could also handle events reported directly by authentication, SNMP traps, servers and network databases.

Over time, SOC teams recognized additional potential uses for the SIEM framework. Additional collections of queries, dashboards, and recording capabilities layered on top of the SIEM system allowed them to address specific user requirements.

NIST Identifies Benefits of SIEM Software

Later in 2006, NIST described SIEM in its *Guide to Computer Security Log Management*. The standards agency identified two main types of SIEM: agentless and agent-based.

Agentless SIEM, according to NIST, "receives data from the individual log generating hosts without needing to have any special software installed on those hosts." Then, the server "performs event filtering and aggregation and log normalization and analysis on the collected logs."

NIST concluded that the primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. However, NIST recognized that a "lack of filtering and aggregation at the individual host level could cause significantly larger amounts of data to be transferred over networks and increase the amount of time it takes to filter and analyze the logs."

Authentication, NIST, wrote, was another concern. If the agentless SIEM software needed to obtain authentication credentials for each logging host, an agent would likely need to be installed to remotely collect logs.

In the guide, NIST described Agent-Based SIEM as a program installed on the log generating host to "perform event filtering and aggregation and log normalization for a particular type of log, then transmit the normalized log data to a SIEM server, usually on a real-time or near-real-time basis for analysis and storage."

NIST explained that a SIEM server analyzes data from the various log sources, correlates events among the log entries, identifies and prioritizes significant events and can initiate responses to events.

The Failed Promises of SIEM

For all its promise, SOCs using SIEM inevitably face a clear and looming problem with this security advancement: to gain true visibility into network behavior, they must feed these systems a virtually endless stream of data.

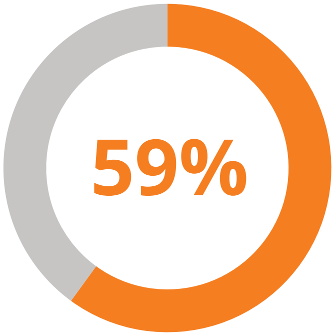
Because the fundamental nature of SIEM requires infinite amounts of data, security teams are forced to constantly wrangle their network data and faced with an unmanageable number of false positive alerts. This means they have to devise efficient ways to collect, organize and store data, resulting in an incredible investment in human and financial resources.

Worse, because SIEM relies on log data, its capability to respond to events is limited to the accuracy and scope of its latest view of a network's data. To be fair, SIEM has improved on this front since its inception in 2006. Today, SIEM software is quite capable of performing traditional searches and investigations.

However, the need to constantly add new sources severely restricts an organization's ability to take in a holistic view of events.

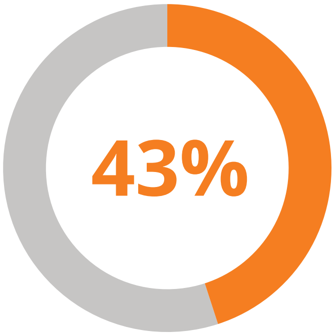
Vendors Capitalize on SIEM's Fundamental Flaws

SIEM customers often find themselves caught up in a never-ending cycle of collecting and storing data and then feeding it into the software quickly



59% of respondents report that they receive more than 500 alerts about public cloud security per day.

Thirty-eight percent report receiving more than 1,000 of these alerts each day.



43% — said that more than 40% of public cloud security alerts are false positives.

Four out of five respondents said that more than 20% of their alerts are false positives, meanwhile.

2022 Cloud Security Alert Fatigue Report enough to maintain an acceptable level of network security and regulatory compliance around data privacy.

In answer to these concerns, vendors present the doomsday scenario, telling customers: “If you don’t have all of your endpoint data, and all of your internal data, and all of the information from all of these sources, you are inherently vulnerable. And if you don’t save that information in perpetuity, and you have some critical incident that you don’t have the data saved, this could represent a compliance violation.”

And it’s true. SIEM is fundamentally limited by its insatiable, incessant need for fresh data. Once they are locked into a specific SIEM, however, it’s extremely challenging for security teams to see a way out. SIEM is a database for machine-generated data, one optimized for search and investigative capabilities.

In order to get a quick return on queries or to address functional requirements like incident management and threat detection, customers and vendors add to a constantly-growing collection of queries and reports. This is the only way to obtain the data the SIEM needs to compare against historical data to detect anomalies.

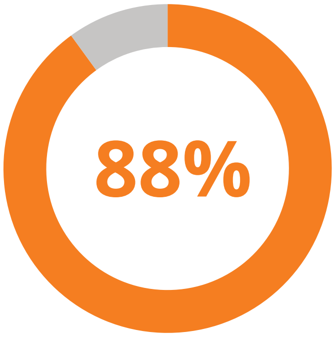
Vendors fully understand how vital it is for organizations to adhere to today’s customer data compliance requirements. Their platforms are positioned in a way that requires customers to aggregate and format data into the vendor’s exclusive, proprietary format.

In the meantime, when organizations rely solely on SIEM, security lags behind modern, real-time solutions that feature predictive threat detection. SIEM data, by nature, has latency built in. It cannot provide real-time threat detection because of the time it takes to process, move, aggregate and normalize data.

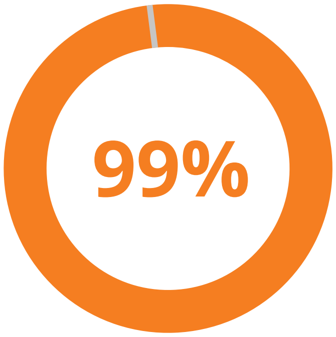
Vendors understand this SIEM flaw, too, as evidenced by the advent of what they describe as “supplemental approaches to complement security information and event management systems.”

Gaps in the “Next-Generation” SOC

Customers have a clear interest in securing their networks against a quickly evolving modern threatscape where bad actors are on constant watch for the chance to exploit vulnerabilities in SIEM setups. Savvy hackers use sophisticated AI designed tactics to work around rules-based security approaches.



88% of organizations have challenges with their current SIEM platform.



99% would like additional SIEM automation.

35 stats that matter to your Security Operations team

If they hope to keep their networks shored up, they have little choice but to sign on for supplemental features like NDR and NTA that allow their expensive software to perform fundamental security functions.

As SIEM evolved, vendors began bolting on NDR (network detection and response) and NTA (network traffic analysis) to their base SIEM offerings. The hope (and promise) was that these tools would add the real-time security solution that was lacking with SIEM technology.

Instead, this ad hoc approach compounded the issue by forcing data into siloed platforms and increasing data overload. Because these platforms used SIEM data, the promise of real-time threat detection and network analysis was doomed from the start.

Still, organizations are hurting for these capabilities. No longer are they content with relying on historic log aggregate data as their primary system of record for threat detection and analysis.

Real-time information provides the granularity necessary to truly understand network behavior. This is where SIEM falls flat. Taking all of these concerns into account, it becomes clear that SIEM is inherently flawed in several important ways:

1. It is additive in nature — to make it function as a security tool, customers must add additional solutions like NDR and NTA.
2. Even when customers opt for these additive solutions, the system is ineffective as a modern, real-time, self-adapting security offering.
3. They need continual monitoring and an endless supply of data, which organizations must store indefinitely.

In short, SIEM is not an inclusive approach. Rather, customers must add functions to benefit adequately from this software, a fact vendors are happy to exploit.

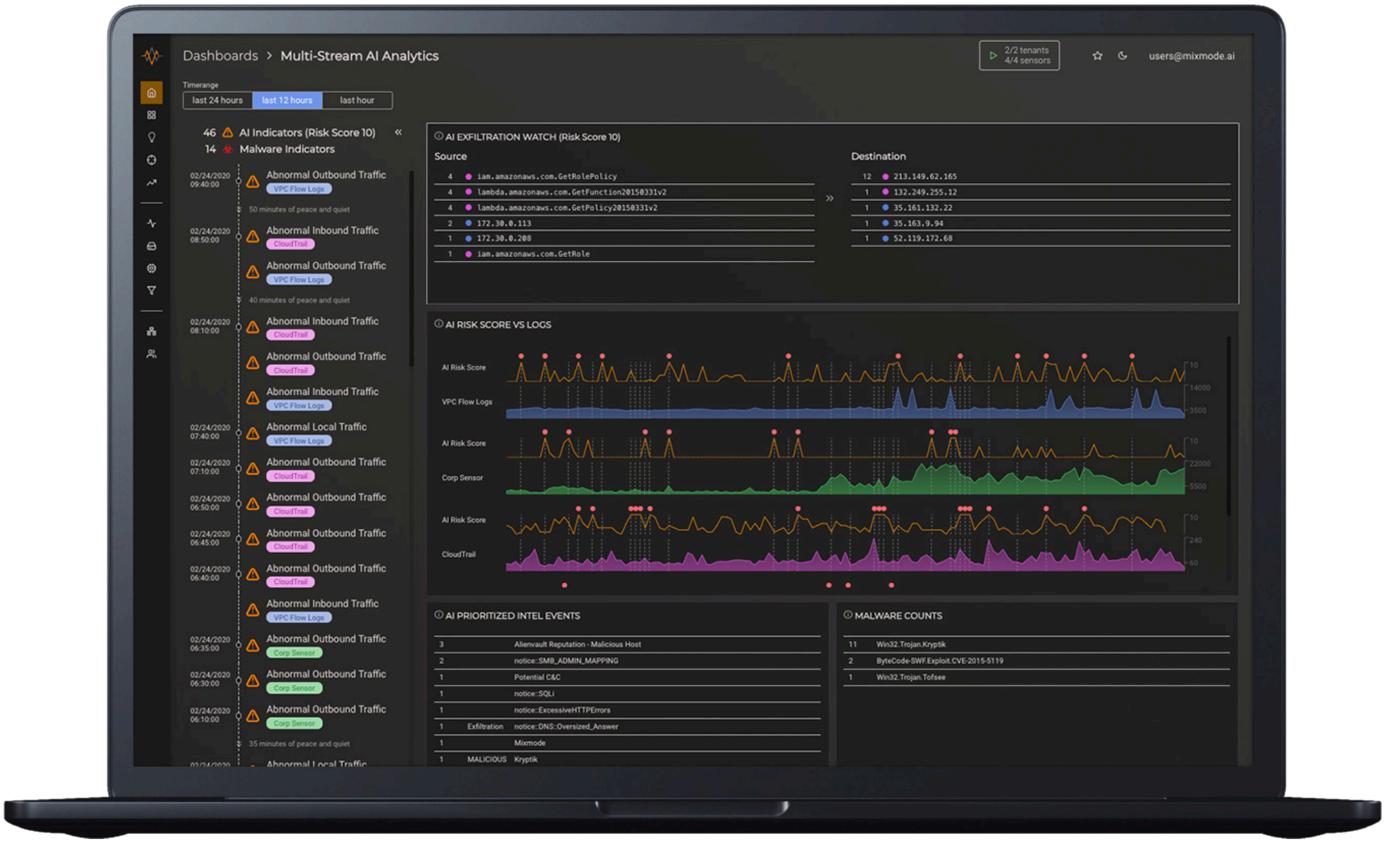
> ***"Billions are spent on products like an SIEM or SOAR that do not operate efficiently because they are ingesting too much data and an overwhelming number of false positives. "Garbage in, garbage out."***
>
> - Industry AI and Automation Analyst

Improving on the Typical SIEM Model

Despite its inherent flaws, today's SIEM software solutions still shine when it comes to searching and investigating log data. One effective, comprehensive approach to network security pairs the best parts of SIEM with modern, AI-driven predictive analysis tools. Alternatively, organizations can replace their outdated SIEM with a modern single platform self-learning AI solution.

MixMode vs. Legacy SIEM

With a SIEM, customers face a prevalent inherent shortcoming: Analysts must spend hours on fruitless manual investigations into alerts based on an inaccurate baseline. When vendors push NTA add-ons to "complement" their SIEM platforms, it is often an attempt to overcome this significant limitation.



46 AI Indicators (Risk Score 10)
14 Malware Indicators

02/24/2020 09:40:00 Abnormal Outbound Traffic VPC Flow Logs
50 minutes of peace and quiet
02/24/2020 08:50:00 Abnormal Inbound Traffic CloudTrail
Abnormal Outbound Traffic VPC Flow Logs
40 minutes of peace and quiet
02/24/2020 08:10:00 Abnormal Inbound Traffic CloudTrail
Abnormal Outbound Traffic CloudTrail
Abnormal Inbound Traffic VPC Flow Logs
02/24/2020 07:40:00 Abnormal Local Traffic VPC Flow Logs
02/24/2020 07:10:00 Abnormal Outbound Traffic CloudTrail
02/24/2020 06:50:00 Abnormal Outbound Traffic CloudTrail
02/24/2020 06:45:00 Abnormal Outbound Traffic CloudTrail
02/24/2020 06:40:00 Abnormal Outbound Traffic CloudTrail
Abnormal Inbound Traffic VPC Flow Logs
02/24/2020 06:35:00 Abnormal Outbound Traffic Corp Sensor
02/24/2020 06:30:00 Abnormal Outbound Traffic Corp Sensor
02/24/2020 06:10:00 Abnormal Outbound Traffic Corp Sensor
35 minutes of peace and quiet
02/24/2020 Abnormal Local Traffic

AI EXFILTRATION WATCH (Risk Score 10)

Source		Destination	
4	iam.amazonaws.com.GetRolePolicy	12	213.149.62.165
4	lambda.amazonaws.com.GetFunction20150331v2	1	132.249.255.12
4	lambda.amazonaws.com.GetPolicy20150331v2	1	35.161.132.22
2	172.30.0.113	1	35.163.9.94
1	172.30.0.208	1	52.119.172.68
1	iam.amazonaws.com.GetRole		

AI PRIORITIZED INTEL EVENTS

3		Alienvault Reputation - Malicious Host
2		notice::SMB_ADMIN_MAPPING
1		Potential C&C
1		notice::SQLi
1		notice::ExcessiveHTTPErrors
1	Exfiltration	notice::DNS::Oversized_Answer
1		Mixmode
1	MALICIOUS	Kryptik

MALWARE COUNTS

11	Win32.Trojan.Kryptik
2	ByteCode-SWF.Exploit.CVE-2015-5119
1	Win32.Trojan.Tofsee

MixMode mitigates this issue by changing the fundamental way the SIEM establishes the baseline while providing the standard security features of a SIEM including search and investigate functionality. Legacy NTA solutions rely on a historical analysis of network traffic and comparing behavior anomalies against one another. Rules and alerts based on a historical, non-evolving baseline are limited in their effectiveness.

Network conditions are constantly shifting and along with them, expected baseline behavior. An anomaly today may not be an anomaly tomorrow. For example, when a significant percentage of workers abruptly switched to remote work arrangements, unprepared companies were hit with a mountain of false positive alerts.

MixMode removes the siloed nature of additive NTA baselines with an adaptive approach that is responsive to rapidly evolving network baselines.

Context-aware insights result in fewer false positive alerts, while AI-prioritized reports decrease demands on analyst time. Instead of spending hours sifting through SIEM logs, analysts can address genuine security vulnerabilities.

MixMode vs. Next-Generation SIEM

MixMode is built around robust predictive analytics capabilities, an area where SIEM lags far behind. Instead of relying on historical log data, MixMode constantly updates expected baseline network behavior. The result is authentic real-time threat detection and predictive analysis based on actual, current network behavior.

MixMode can be used as a standalone solution or in parallel with a traditional SIEM. In either case, upgrading will help organizations reduce overall cost and resource requirements. In fact, MixMode offers real-time and predictive threat detection, noise reduction, and deep investigation at a fraction of the cost of a typical SIEM.

MixMode vs. False Positives

Based on validated data, both customers profiled in our real-world examples were able to achieve greater than 95 percent suppression of false positives in the first week, compared to the false positive rate delivered by their outdated, rules-based SIEM approaches.

Fewer false positive alerts leads to a decreased workload for employees who have been tasked with combing through all those alerts. Instead of applying their own experience and human intelligence to the monotonous task of threat hunting, these analysts can prioritize their time on true threats and anomalies.

MixMode in the Real World

How a Top 5 US City Used MixMode to Overcome the Shortcomings of their SIEM

Over time, most organizations will come to the realization that they will never achieve a full enterprise deployment of their SIEM. By its very nature, SIEM is always “in process.” It’s not unusual for an organization to have an SIEM in process for a full decade.

Along the way, these organizations will be hit with ever-increasing costs for additional applications to address the shortcomings of SIEM, as well as astronomical licensing and data ingest costs. This is an unsustainable situation that becomes more difficult to justify as time goes on.

Many customers come to MixMode with a very specific business problem: “I’m trying to address the same functional requirements today that I was trying to address 15 years ago and these systems have proven ineffective at addressing not only my functional requirements but they’ve also created operational and technology costs that are unsustainable.”

It’s a sobering reality that the functional limitations of a SIEM identified 15 years ago are the same functional limitations of a SIEM today.

These customers need an alternative, and in one recent example, MixMode was able to demonstrate better granularity and authentic visibility into both real-time threats as they occurred as well as network and operational configuration challenges.

It’s understandable that these customers come to MixMode frustrated and in search of a viable alternative. In one recent example where the customer was a large city, MixMode made all the difference. The platform was able to demonstrate better granularity and authentic visibility into real-time threats as they occurred.

The customer was also able to address network and operational configuration challenges that had gone previously unnoticed — despite a three-year SIEM deployment and a two-year UBA deployment that had been in production.

> ***“MixMode, where the SIEM solutions were originally put in place to address, is now able to do so literally at a fraction of the cost of those systems. They were able to get that visibility in one week without any resource involvement whatsoever, purely based on the artificial intelligence-informed insights that they were able to achieve.”***

Gaining this level of visibility allowed the customer to become more agile and responsive, so much so that they decided to decommission both the UBA and SIEM systems in favor of a next-generation SOC powered by MixMode.

MixMode, where the SIEM solutions were originally put in place to address, is now able to do so literally at a fraction of the cost of those systems. They were able to get that visibility in one week without any resource involvement whatsoever, purely based on the artificial intelligence-informed insights that they were able to achieve.

As a municipality, the customer had a unique need to comply with requirements like PCI and HIPAA. With MixMode, they were able to meet these requirements with ease, using a single platform. MixMode allowed them to demonstrate they had the capability to go back and access required data and provide forensic-level detail about it. The customer had put into place a large collection of rules-based alerts, queries and dashboards that had been designed to provide threat intelligence via the SIEM. Because that information was based on legacy log data, they had no visibility into real-time threats and anomalies.

Insider threat prevention was another major challenge for this customer. Despite the presence of their UBA platform, the customer suspected they were increasingly coming under attack by adversarial AI and state-sponsored probes for vulnerabilities. They also had to deal with related misconfigurations and network configuration optimization challenges.

MixMode was able to identify active attacks and probes that were taking place that the customer's existing tools had no visibility into, confirming the customer's suspicions. Insider behaviors, in particular, came into clear view.

Within a week, MixMode was able to address the immediate functional requirements related to security challenges as well as addressing the previously unknown network configuration and optimization challenges, without any operational resources, predefined queries, pre-existing intel feeds or rules-based alerts.

Customers routinely encounter aggressive SIEM vendors who encourage them to consider adding IT operational intelligence as an additional SIEM platform deliverable. They do this by creating layer upon layer of abstraction, normalization, reporting, queries, thresholds-based alerts, dashboards...all at a premium.

While MixMode engages primarily at the tip of the spear with SOC teams, network operation teams often notice the level of visibility, granularity and business benefits they can pull from real-time insight, as well.

> ***"Ultimately, what we see are customers able to address a host of challenges with a single platform solution that is attractive for both security operation teams and network operation centers. Traditional SOC, UBA, and SIEM challenges, alongside traditional network operation center challenges, are all overcome with the singular MixMode platform."***

Ultimately, what we see are customers able to address a host of challenges with a single platform solution that is attractive for both security operation teams and network operation centers. Traditional SOC, UBA, and SIEM challenges, alongside traditional network operation center challenges, are all overcome with the singular MixMode platform.

How a Customer Used a MixMode Empowered Program to Enhance their SIEM

With our large city MixMode customer example, the SIEM deployment was a shared resource among network operation center team members and security operations team members. Together, they had full budgetary authority over the system, but this is not always the case.

However, many of our customers have SIEM deployments shared across multiple business lines beyond security and network operations teams, or need to address multifaceted challenges like internal compliance audits. The MixMode solution provides a central hub for these distributed needs customers.

A recent MixMode client using SIEM across multiple business units wanted to retain the SIEM exclusively for its historic search and investigation capabilities in order to meet compliance requirements. By shifting all of their security and network operation center functional deliverables to MixMode, they were able to achieve two significant accomplishments:

- The customer was able to decrease their total SIEM deployment cost by decreasing the amount of traffic that needed to be aggregated and stored. MixMode took on these data-rich tasks.
- The customer was able to shift from a dependency on rules- and threshold-based approaches for security operations teams on the front line to turning all of that functional responsibility to MixMode.

The customer now benefits from having MixMode play the role of the security operations center in front of the existing SIEM. They can also maintain the SIEM system on the back end to accommodate multiple lines of business requirements for historic compliance search and investigative capabilities.

MixMode has been able to empower the customer to achieve all of this while decreasing overall costs. Within a week, MixMode was able to:

- Identify policy violations and active adversarial AI attacks.
- Identify state-sponsored attacks from foreign entities that they had no visibility into with their SIEM-based rules and threshold-based approach.

Looking Ahead

The industry idea of what the ideal cybersecurity solution should look like is fundamentally flawed. In reality, these solutions, including SIEM, cause data overload, increased costs and the need for more human operators. These solutions are simply unsustainable in the modern environment.

Looking ahead to the next-generation of SOCs, it is clear that the time has come to rethink this model. By leveraging new forms of self-supervised AI that deliver unique functionality like predictive threat detection, significant decreases in false positive alerts, zero day attack identification, and AI-powered threat monitoring, enterprises will be able to stop threats and attacks more efficiently.

This is showing that major improvements are ahead for SOC visibility and productivity, coupled with decreased costs for storage, detection and time spent combing through false positive alerts.

MixMode™

www.mixmode.ai

+1 (858) 225-2352 | info@mixmode.ai | © 2022 MixMode, Inc.

About MixMode

MixMode is a next-generation, AI-powered cybersecurity platform focused on solving two primary issues for the Security Operations Center: providing next-generation threat detection, surfacing zero-day attacks and improving false-positive alert fatigue. MixMode allows security teams to dramatically increase productivity and efficiency while significantly decreasing the wasted time, effort, and resources associated with legacy cybersecurity tools.

MixMode's AI intelligently creates and updates the network baseline, then provides security teams with sophisticated functionality like predictive attack detection, 95% false-positive alert reduction, and all the tools necessary to investigate a threat. SOC teams can easily integrate MixMode into their security stack to dramatically reduce the investigation time, cost, and expertise required to respond to persistent threats, malware, insider attacks, and nation-state espionage efforts. MixMode's core AI algorithm is patented and was utilized over the past 20 years on projects for DARPA and the DoD. MixMode is headquartered in Santa Barbara, CA.