Fluency

Whitepaper

Elevating Security Operations with Fluency Security’s Advanced SIEM

A Look at the Standout Features Enabling More Effective Security Operations

Published September 2023

Introduction

As organizations face an increasingly complex and evolving threat landscape, security information and event management (SIEM) solutions have become a critical component of security operations. However, traditional SIEMs often struggle to provide the time-sensitive threat detection and efficient analyst workflows needed to keep pace with modern attacks. Fluency Security offers an innovative SIEM platform with built-in automated SOAR functionality designed to overcome these challenges through unique capabilities including real-time streaming analytics, intelligent and correlated alert clustering, flexible data access, and optimization for SOC operations. This whitepaper will examine how Fluency Security's approach differentiates it in the SIEM market and enables more proactive threat detection and automated response.

Watching vs. Searching: Alerting to Threats In-Motion

A key differentiation of Fluency Security's approach is that it analyzes and interrogates in-flight data streams as the data is ingested using streaming analytics. This enables SOCs to stop threats in their tracks the moment they detect anomalies, risk factors, or threats.

Other SIEM solutions work differently - they ingest data into a data lake first and then run searches and correlations afterwards. This means detection of critical threats happens after the fact, sometimes hours or days later depending on when searches are scheduled to run.

Fluency's live streaming analytics with commercial grade machine learning provides organizations with a much faster time-to-detect critical threats and security incidents as they are in-motion. Where legacy SIEMs rely on searching after data arrives, Fluency provides continuous monitoring and watching of data streams as they flow into the system.

Some benefits this enables:

- Timely alerting on threats as events happen, rather than after searching logs retroactively
- Delivering all relevant contextual information to analysts upfront for rapid investigation
- Greatly reducing noisy alerts by correlating related events in real-time

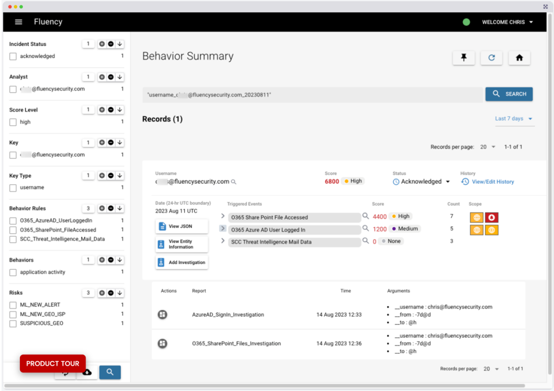
By using streaming analytics to watch and analyze data in motion, Fluency Security can achieve threat detection speeds that surpass traditional store-first, search-later SIEM architectures. This watch versus search differentiation allows SOC teams to respond swiftly to mitigate damages from attacks.

Alert Clustering

One of the biggest differentiators of Fluency Security's SIEM is its ability to cluster related alerts together into a single ticket, rather than creating separate tickets for each individual alert. For example, if there are 5 related alerts triggered by a security incident, other SIEMs would create 5 separate tickets that an analyst would need to handle. With Fluency Security, those 5 alerts are intelligently grouped together into a single ticket.

This alert clustering provides several major benefits:

- Reduces the number of tickets analysts need to handle daily. Rather than getting overwhelmed with thousands of alerts, the system condenses these down to the most important tickets.
- Groups all relevant information together, giving analysts the full context rather than just a single data point.
- Prioritizes the most critical and unique threats based on behavioral analysis across the environment.



Fluency — WELCOME CHRIS

Incident Status	1
☐ acknowledged	1
Analyst	1
☐ [redacted]@fluencysecurity.com	1
Score Level	1
☐ high	1
Key	1
☐ [redacted]@fluencysecurity.com	1
Key Type	1
☐ username	1
Behavior Rules	3
☐ O365_AzureAD_UserLoggedIn	1
☐ O365_SharePoint_FileAccessed	1
☐ SCC_Threat_Intelligence_Mail_Data	1
Behaviors	1
☐ application activity	1
Risks	3
☐ ML_NEW_ALERT	1
☐ ML_NEW_GEO_ISP	1
☐ SUSPICIOUS_GEO	1

Behavior Summary

"username_[redacted]@fluencysecurity.com_20230811" SEARCH

Records (1) — Last 7 days

Records per page: 20 1-1 of 1

Username: [redacted]@fluencysecurity.com — Score: 6800 High — Status: Acknowledged — History: View/Edit History

Date (24-hr UTC boundary): 2023 Aug 11 UTC

Triggered Events	Score		Count
O365 Share Point File Accessed	4400	High	7
O365 Azure AD User Logged In	1200	Medium	5
SCC Threat Intelligence Mail Data	0	None	3

Actions	Report	Time	Arguments
	AzureAD_SignIn_Investigation	14 Aug 2023 12:33	__username : chris@fluencysecurity.com __from : -7d@d __to : @h
	O365_SharePoint_Files_Investigation	14 Aug 2023 12:36	__username : chris@fluencysecurity.com __from : -7d@d __to : @h

Records per page: 20 1-1 of 1

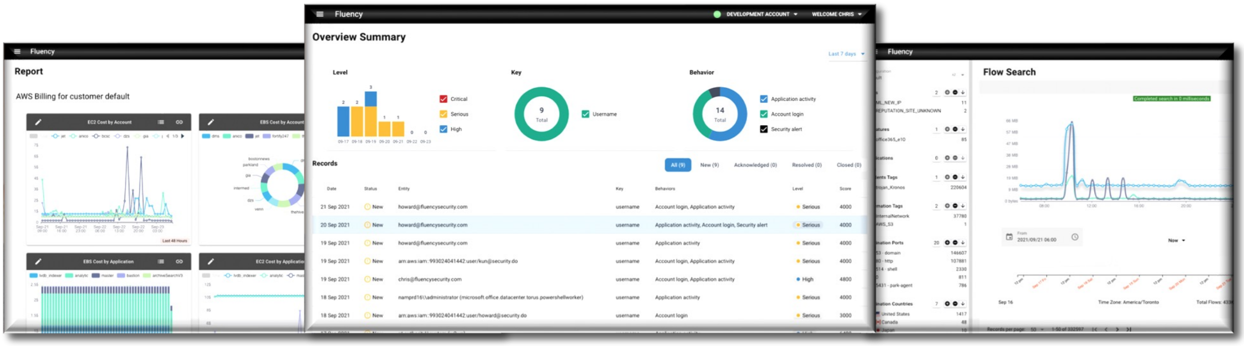
By reducing manual tedium for analysts and letting the system handle the clustering and prioritization, analysts can focus on higher-value security tasks.

Unified Data Access

Another key advantage of Fluency Security's SIEM is its Fluency Programming Language (FPL) that allows unified and federated access across all data sources. The system can query and correlate across log data, APIs, databases, and more, regardless of location.

For example, the SIEM could check Active Directory for a list of servers, and then query logs and endpoints to see which servers are missing critical software or falling out of compliance. This holistic viewpoint is difficult and time-consuming to achieve with traditional SIEMs.

FPL eliminates silos and gives analysts a single pane of glass across the entire environment. This enables more intelligent threat detection and faster investigation and remediation.



Overview Summary — DEVELOPMENT ACCOUNT — WELCOME CHRIS — Last 7 days

Records: All (9) New (9) Acknowledged (0) Resolved (0) Closed (0)

Date	Status	Entity	Key	Behaviors	Level	Score
21 Sep 2021	New	howard@fluencysecurity.com	username	Account login, Application activity	Serious	4000
20 Sep 2021	New	howard@fluencysecurity.com	username	Application activity, Account login, Security alert	Serious	4000
19 Sep 2021	New	howard@fluencysecurity.com	username	Application activity	Serious	4000
19 Sep 2021	New	arn:aws:iam::993024041442:user/kun@security.do	username	Account login, Application activity	Serious	4000
19 Sep 2021	New	chris@fluencysecurity.com	username	Account login, Application activity	High	4800
18 Sep 2021	New	namprd16\\administrator (microsoft.office.datacenter.torus.powershellworker)	username	Application activity	Serious	4000
18 Sep 2021	New	arn:aws:iam::993024041442:user/howard@security.do	username	Account login	Serious	3000

Report — AWS Billing for customer default

Flow Search — Completed search in 0 milliseconds — From 2021/09/21 06:00 — Now — Time Zone: America/Toronto

ML_NEW_IP	11
REPUTATION_SITE_UNKNOWN	2
office365_e10	85
trojan_Kronos	220604
InternalNetwork	37780
AWS_S3	1
53 - domain	146607
80 - http	107881
514 - shell	2330
0	811
5431 - park-agent	786
United States	1417
Canada	48
Japan	10

Records per page: 50 1-50 of 332597

Optimized for SOC Operations

Fluency Security designed its SIEM with security operation centers (SOCs) in mind. The system is optimized to reduce the time and effort required by Tier 1/2/3 analysts and the roles they play.

With the alert clustering and prioritization capabilities, the SIEM ensures analysts have a manageable workload each day. And the system learns from user feedback about false positives, constantly improving the signal-to-noise ratio. In fact, it’s not uncommon for Enterprise SOCs to reduce their alert volumes to highly manageable levels within a few months.

The SIEM is also designed to easily handle the scale required by large enterprise SOCs with tens of thousands of employees. It can correlate events across a wide international base to identify broader attack campaigns. And the unified data architecture works seamlessly across disparate environments with different data sources.

Conclusion

Fluency Security brings fresh thinking and advanced capabilities to the SIEM market. With strengths in live streaming analytics, unified data access, alert clustering, and SOC optimization, Fluency Security is well-positioned to improve the efficiency and effectiveness of security operations. Organizations looking to enhance their threat detection, investigation, and response should consider Fluency Security as a next-generation SIEM vendor that can provide greater context, focus, and productivity for analysts compared to traditional solutions. As threats become more dynamic and evasive, adopting an innovative platform like Fluency Security can provide the visibility and control today's security teams need.

ABOUT FLUENCY

Fluency is a live-streaming big data analytics company focused on cyber security. Analyzing terabytes of data-in-motion is a market capability that affords our clients time-sensitive visibility and alerting. Fluency’s global multi-tenant design is highly scalable and easily supports the largest of enterprise and MSSP needs. Observability is achieved with Fluency’s modern processing language (FPL) allowing analysis of streaming data. SOC teams benefit from the more than 2,000+ stateful behavioral models backed by proven machine learning and a proprietary risk-based scoring system to interrogate the data and determine if there is a threat that needs an analyst to review.

Find out how Fluency can help your organization at www.fluencysecurity.com
For more information, please email us at contact@fluencysecurity.com