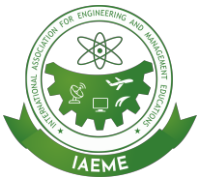
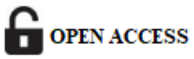
Journal of Computer Engineering and Technology (JCET)
Volume 6, Issue 2, July-December 2023, pp. 14-18, Article ID: JCET_06_02_002
Available online at https://iaeme.com/Home/issue/JCET?Volume=6&Issue=2
ISSN Print: 2347-3908 and ISSN Online: 2347-3916
Impact Factor (2023): 18.14 (Based on Google Scholar Citation)





FORTIFYING CYBER DEFENSE: THE CRITICAL ROLE OF SECURING SIEM DATA PIPELINES

ShivaDutt Jangampeta
Senior Manager of Security Engineering
JPMorgan Chase, Plano, USA

ABSTRACT

Data has become a crucial part of the data-driven business landscape, but as it travels through complex pathways, there's a hidden danger. This report explores the imperative of securing data pipelines within Security Information and Event Management (SIEM) systems. Exploring SIEM data pipelines, we uncover challenges from using multiple tools and dealing with scattered data. This includes cases where credentials were exposed due to misconfigurations. The paper also highlights the vital role of strong security practices, proper setup, and regular updates in securing data pipelines within the dynamic SIEM environment.

Keywords: SIEM, Data pipelines, Security, Threat Detection, Log management, Incident Response, Compliance reporting, Forensics, Data Security, Cyber Defense, Data fragmentation, Cyber adversaries

Cite this Article: ShivaDutt Jangampeta, Fortifying Cyber Defense: The Critical Role of Securing SIEM Data Pipelines, Journal of Computer Engineering and Technology (JCET) 6(2), 2023, pp. 14-18.
https://iaeme.com/Home/issue/JCET?Volume=6&Issue=2

I. INTRODUCTION

Security platforms gather a lot of data. For example, SIEM might ingest endpoint events, a variety of application logs, firewall logs, and threat detection results from various other products. However, logging everything to SIEM is a bad approach as it's expensive and noisy. The security data pipeline minimizes the log size and routes events intelligently to the security data lake.

Some organizations still lack robust security monitoring and detection controls. However, surviving without employing the best data engineering practices around business-related data is risky in today's digital world. That said, strongly engineering data pipelines should be a fundamental function for companies relying on data analytics to keep their data secure.

Global data breaches in the first quarter of 2023 resulted in the exposure of over 6 million data records, according to Statista. [1]

Acquiring, preparing, and managing data requires modern technology stacks with mature processes. The adoption of data pipelines in security coexists with the maturation of the industry. The first step to overcome the issue is running two solutions in parallel, the legacy SIEM and data pipelines. But that too comes with certain challenges.

Let's explore the criticality of securing data pipelines within Security Information and Event Management (SIEM) systems, recognizing that data demands a protected pathway. [2]

II. WHAT IS SIEM?

Security Information and Event Management (SIEM) is a security solution that helps organizations identify and mitigate potential security threats and vulnerabilities proactively. SIEM systems aid in preventing disruptions to business operations.

Key features of SIEM include:

Log Management: SIEM systems gather and consolidate log data produced across the organization's technological framework, encompassing host systems, applications, as well as network and security devices.

Correlation: SIEM tools correlate and analyze the log data to identify patterns, detect anomalies, and highlight potential security incidents.

Alerting and Notification: SIEM systems can generate alerts and notifications in real-time when they detect events or patterns that may indicate a security threat or policy violation.

Incident Response: SIEM facilitates incident response by providing detailed information about security incidents, allowing security teams to investigate and respond quickly.

Compliance Reporting: SIEM tools often include reporting features that help organizations demonstrate compliance with industry regulations and internal security policies.

Forensics and Analysis: SIEM solutions enable forensic analysis by providing a historical view of security events, aiding in the investigation of past incidents. [3],[4], [5]

III. UNDERSTANDING THE DATA PIPELINE IN SIEM

A data pipeline integrates a variety of tools and processes to transfer data from one system to another, facilitating storage and subsequent processing. Conventional SIEM architectures incorporate this concept but in a basic and straightforward manner. Typically, log shippers are responsible for transmitting data to a designated SIEM database or index as the final destination, concluding the process.

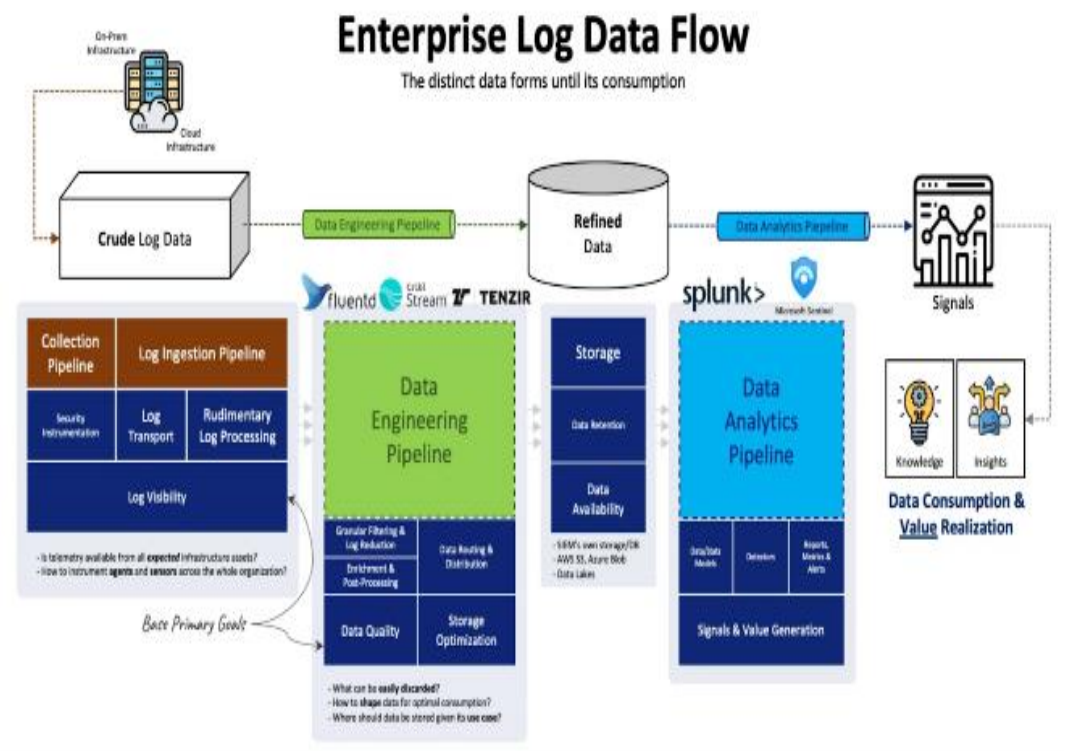


FIG. 1

Ultimately, there is minimal emphasis on refining the data before it reaches the SIEM storage layer. This lack of refinement gives rise to well-documented challenges, ranging from high licensing expenses to performance deterioration and data security issues. [6]

IV. THE SIGNIFICANCE OF SECURING A DATA PIPELINE IN SIEM

Securing data pipelines in SIEM confronts challenges due to the widespread use of multiple tools, as shown in the figure below. Varied responsibilities among groups lead to adopting diverse SIEM platforms, hindering standardization. This multi-tool approach results in fragmented data sources, making it challenging to integrate and maintain.

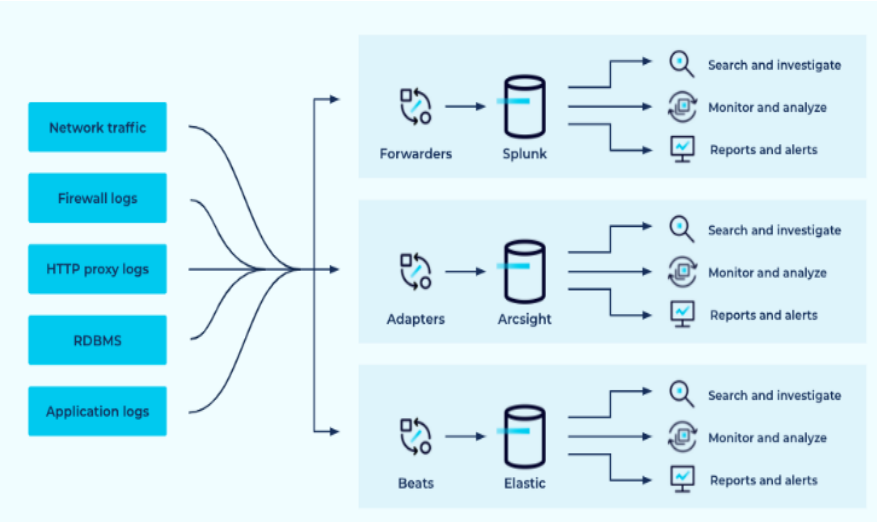


FIG. 2

The difficulties extend to introducing new tools and shifting workloads between them. Also, the complexities in standardization, data fragmentation, and managing diverse tools highlight the importance of addressing these issues to enhance the overall security posture of data pipelines within the SIEM environment.

Cyber adversaries may find internally developed data pipelines appealing due to their access to sensitive data. Furthermore, these pipelines often operate independently of regular engineering protocols. Internal security teams may lack awareness of the associated risks and the tools necessary to monitor potential data leakage from within the pipeline. [7]

Moreover, instances have been identified where self-hosted pipelines, like those in Apache Airflow [8], exposed numerous credentials due to misconfigurations, hardcoded passwords, and outdated security updates. This scenario directly correlates with the challenges faced in securing data pipelines within SIEM.

The vulnerabilities highlight the importance of robust security practices, emphasizing proper configuration and regular updates within the SIEM environment to mitigate potential risks in data pipelines. [9]

V. BENEFITS OF SECURING DATA PIPELINES

A secure data pipeline is essential for maintaining customer trust. It demonstrates a commitment to protecting sensitive information and fostering positive customer relationships.

Here are a few benefits of securing data pipelines.

Cybersecurity Protection: Enhanced security measures in a data pipeline act as a crucial component of an organization's overall cybersecurity strategy. They protect against cyber attacks and mitigate the risk of sensitive data breaches.

Abnormal Behavior Detection: A secure data pipeline enables the detection and response to abnormal network behavior promptly. Proactive measures to identify potential security threats contribute to a more resilient cybersecurity posture.

Improved Data Quality: Ensuring the security of a data pipeline enhances data integrity, resulting in improved overall data quality. It guards against data corruption, tampering, or unauthorized modifications. [10]

VI. CONCLUSION

This report highlights the imperative need for securing data pipelines within Security Information and Event Management (SIEM) systems. Security professionals must recognize the critical importance of security data pipelines in SIEM.

The key takeaway is clear: Robust security practices, proper configuration, and regular updates are necessary to strengthen the overall security posture of data pipelines within the dynamic and complex SIEM environment. Awareness, adherence to best practices, and proactive measures are critical to secure sensitive information and maintain the integrity of data pipelines. [11]

REFERENCES

[1] A. Petrosyan, “Quarterly Online Data Breaches 2022,” Statista, Nov. 29, 2022. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

[2] R. Haleliuk, “Security is about data: how different approaches are fighting for security data and what the cybersecurity data stack of the future is shaping up to look like,” ventureinsecurity.net. https://ventureinsecurity.net/p/security-is-about-data-how-different

[3] IBM, “What is Security Information and Event Management (SIEM)?,” IBM, 2022. https://www.ibm.com/topics/siem

[4] Microsoft, "What is SIEM? | Microsoft Security," www.microsoft.com, 2023. https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

[5] "What is SIEM and Why is it Important?," Search Security. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

[6] A. Teixeira, "Why you need Data Engineering Pipelines before an enterprise SIEM," Medium, Oct. 17, 2023. https://detect.fyi/why-you-need-data-engineering-pipelines-before-an-enterprise-siem-0be553584aa9

[7] "SIEM Optimization for Better Cyber Security," Confluent. https://www.confluent.io/blog/siem-optimization-for-better-cyber-security/

[8] Misconfigured Apache Airflow servers leak thousands of credentials," Bleeping Computer. https://www.bleepingcomputer.com/news/security/misconfigured-apache-airflow-servers-leak-thousands-of-credentials/

[9] T. Conklin, "Leaky Data Pipelines: Uncovering the Hidden Security Risks," The New Stack, Jul. 27, 2023. https://thenewstack.io/leaky-data-pipelines-uncovering-the-hidden-security-risks/

[10] Д. Врачарић, "How to Enhance Security and Access Controls with Data Pipeline - FotoLog," Apr. 18, 2023. https://www.fotolog.com/enhancing-security-and-access-controls-with-data-pipeline/

[11] GDT, "The Importance of Protecting SIEM Data | Enhancing Cybersecurity," GDT, Feb. 19, 2020. https://gdt.com/blog/the-importance-of-protecting-siem-data/

Citation: ShivaDutt Jangampeta, Fortifying Cyber Defense: The Critical Role of Securing SIEM Data Pipelines, Journal of Computer Engineering and Technology (JCET) 6(2), 2023, pp. 14-18.

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/JCET/VOLUME_6_ISSUE_2/JCET_06_02_002.pdf

Abstract Link:
https://iaeme.com/Home/article_id/JCET_06_02_002

✉ editor@iaeme.com