SIEM Evolution – Time to make the SIEM Smarter, Not Fatter

Decades ago, SIEMs operated solely on-premises, with legacy vendors employing a straightforward architecture typically consisting of a collector, logger, and an ESM. These systems focused primarily on enforcing compliance controls, employing simple rules to trigger actions. For CISOs at the time, purchasing software typically involved perpetual licenses, with on-prem deployment and a justified hardware cost spread over a five-year amortization period.

SO, WHAT CHANGED?

1. CLOUD ADOPTION AND NAVIGATING THE PRICE TAG OF CLOUD ADOPTION:

The widespread adoption of cloud technology has prompted SIEM vendors to transform. This shift has significantly impacted costs, with cloud SIEM vendors often needing to maintain margins typically 40% to 70% above the charges imposed by cloud service providers like AWS, Azure, or GCP. The proliferation of intermediaries has further inflated costs, creating a cascade effect with expenses at each step of data processing. While a few years ago, transitioning to the cloud seemed novel, it has now become a standard operating environment for most organizations.

2. SHIFTING PRIORITIES FOR SIEM/XDR

The threat landscape has undergone significant transformation, with cybersecurity breaches posing a substantial risk to companies. While meeting compliance requirements remains crucial, the primary focus for CISOs and SOCs is now safeguarding their organizations from reputational and financial damage resulting from cyberattacks. Additionally, the emergence of new regulatory mandates from entities such as the SEC has elevated cybersecurity to a board-level concern. In response to these evolving challenges, relying solely on a single system like a traditional SIEM is no longer sufficient. CISOs and SOCs recognize the need for a more comprehensive approach to cybersecurity, one that involves leveraging multiple tools and strategies to enhance threat detection and response capabilities. This multifaceted approach enables organizations to better mitigate risks and protect against a wide range of threat vectors, thereby reducing the likelihood of a cybersecurity breach and the associated reputational fallout.

3. CYBER SECURITY AND ITS HIGH VELOCITY DATA DELUGE

The current cybersecurity landscape is characterized by a high volume and velocity of data, which continues to grow exponentially. Gone are the days of simpler data environments confined within firewalls; today, organizations must contend with a myriad of data sources, including SaaS applications, 3rd party risk and cloud platforms. Moreover, with the increasing prevalence of supply chain attacks, the origin of threats is often difficult to ascertain. In response to these challenges, Security Operations Centers (SOCs) are dedicating more time and resources to integrating a broader range of data sources. They are transitioning from viewing compliance tools as mere checkbox exercises to leveraging them for cyber threat detection.

With the MITRE framework standardizing threat detections, companies are relying on SIEMs to provide comprehensive coverage.

4. DATA OVERFLOW: THE CHALLENGE OF RETAINING EDR, IOT/OT, AND CSPM DATA:

EDR, IoT/OT, and CSPM solutions often offer a standard data retention period of about 7 days before truncating the data. Despite the absence of active threat detection rules, organizations are reluctant to lose this valuable data. As a result, they resort to dumping these high-volume data sources into their SIEMs, as it remains the primary option for SOCs currently.

REDEFINING SIEM PRIORITIES

Shifting towards better Threat Detection and Response automation:

In response to the evolving threat landscape, SIEMs are shifting their focus towards prioritizing threat detection over simply generating alerts. This involves refining detection capabilities using ML/AI to reduce false positives and accurately identify genuine threats. With a focus on better detection, increased coverage from MITRE, and enhanced response automation, SIEM and XDR vendors view ingestion and data lake management as mere distractions.

Security Data Lake for Threat Hunting:

While threat detection is essential, it's not the only aspect of cybersecurity strategy. Many companies have implemented security data lakes to facilitate threat hunting activities, allowing analysts to conduct in-depth investigations. However, the integration of threat detection with a data lake may seem convenient on the surface, but it can mask underlying issues. Relying solely on a SIEM for both detection and investigation capabilities can be problematic. If detections consistently fall short, organizations may hesitate to replace their SIEM due to the need to retain historical data, which the SIEM holds as leverage. This situation is akin to keeping a malfunctioning car because it can still perform one task adequately opening the garage. With the emergence of Security Data Lake (SDL) solutions, organizations are reconsidering the relationship between their SIEM and data lake. Some are exploring options to decouple the two or, at the very least, route a copy of the data to their own data lake for cold storage. It's becoming increasingly apparent that separating the Security Data Lake from the Detection Layer is necessary for greater flexibility and control.

The Pitfalls of Data Lake dependence in the SIEM:

SIEM and XDR Bring Your Own Data Lake strategy is not working. Fewer SIEM vendors may claim that the data remains accessible in the organization's data lake even after severing ties with the SIEM. The proprietary format of the data may render it practically unusable without significant expertise in deciphering and querying it. This underscores the importance of evaluating not just the capabilities of the SIEM itself but also the implications for data accessibility and portability when considering cybersecurity infrastructure.

Unveliing Data Value: The reality of irrelevant data in Cyber Security:

The reality in cybersecurity is that not all data collected by SIEMs is equally valuable. In fact, a significant portion—around 45%—of the data collected may have zero security relevance. This means that only a fraction, roughly 20%, of the data collected is utilized for security purposes. As organizations increasingly adopt Cloud SIEM solutions, they often find themselves facing unexpected costs associated with data ingestion. Many Cloud SIEMs charge based on usage or total data ingested, directly tying costs to the volume of data processed. This can catch customers off guard, especially after the initial allure of first-year free offerings wears off and data volumes begin to accumulate. Given the high volume of irrelevant data collected, effective data filtering becomes imperative. However, traditional SIEMs may not excel in this regard. While they are proficient at collecting and processing data, they may lack the sophisticated filtering capabilities necessary to efficiently separate relevant security events from noise. In response to these challenges, organizations may need to explore complementary solutions or enhancements to their SIEM infrastructure to improve data filtering and reduce costs. This could involve leveraging specialized data analytics tools or investing in SIEM platforms that incorporate advanced filtering algorithms to streamline data processing and enhance the efficiency of threat detection efforts.

Data Ingestion and Orchestration is a "Means to an End":

In the contemporary cybersecurity landscape, customers are increasingly prioritizing smarter detection capabilities, enhanced threat coverage, and seamless integration with Security Orchestration, Automation, and Response (SOAR) systems for rapid automated response and containment. However, there has been a noticeable shift in focus away from data ingestion and management, with SIEM and Security Data Lake (SDL) vendors dedicating minimal effort to integrating with newer data sources and neglecting to address issues such as schema drift and observability. While AI and machine learning-based detection mechanisms are gaining traction, there remains a critical need for SIEM vendors to continuously improve threat coverage and adapt to evolving cyber threats. This requires ongoing research and development efforts to expand detection capabilities and integrate with emerging security technologies. Moreover, the integration of SOAR functionalities within SIEM platforms has become essential for enabling faster response and containment of security incidents. Customers expect seamless integration between their SIEM and SOAR solutions to streamline incident response workflows and automate repetitive tasks. However, despite the growing demand for comprehensive data integration capabilities, many SIEM and SDL vendors have limited their efforts to a select few commonly requested connectors. This narrow focus hampers organizations' abilities to effectively leverage data from diverse sources and limits the overall effectiveness of their cybersecurity posture. Furthermore, the lack of proactive measures to address schema drift—the gradual evolution of data structures within source telemetry—and the absence of robust observability features around cybersecurity solutions are significant gaps in current offerings. Without mechanisms in place to detect and adapt to schema drift or to provide visibility into the performance and effectiveness of cybersecurity solutions, organizations may struggle to effectively manage and secure their digital assets.

Cost, Margin and Attrition Challenges – Struggles Facing MSSPs and MDRs:

The rise of Managed Detection and Response (MDR) services and Managed Security Service Providers (MSSPs) has transformed how organizations approach cybersecurity operations. While some businesses choose to outsource all or part of their Security Operations Center (SOC) functions, MSSPs are facing challenges in managing the costs associated with traditional SIEM solutions.
The advent of cloud technology has streamlined deployment processes, prompting many MSSPs to leverage cloud-based SIEM solutions instead of maintaining on-premise data centers. However, despite the benefits of cloud SIEMs, MSSPs are encountering pressure on their profit margins due to intense competition and pricing pressure within the industry.

The competitive landscape among MSSPs has led to a race to the bottom in terms of pricing, with providers striving to offer the most cost-effective solutions to attract clients. As a result, cloud SIEMs, with their ease of deployment and scalability, are gaining traction among organizations seeking cost-effective cybersecurity services.

This shift towards cloud SIEMs has forced MSSPs to reassess their business models and pricing strategies to remain competitive in the market. Some MSSPs may choose to innovate by offering value-added services on top of cloud SIEM platforms, while others may explore alternative revenue streams to offset declining margins.

Decoupling Ingestion for Next-Gen Cyber Security Solutions:

The cybersecurity industry is experiencing a surge in the emergence of AI vendors, offering innovative solutions powered by advanced machine learning algorithms and natural language processing. Many organizations are eager to adopt these new-age technologies, which often necessitate redirecting cyber telemetry data to the AI-based solutions. However, customers are increasingly wary of deploying multiple agents or collectors to route the same data to multiple destinations. This approach not only adds complexity to their infrastructure but also raises concerns about potential performance impacts and security vulnerabilities. As a result, there is a growing recognition of the need to separate the data ingestion process from the specific cybersecurity solutions consuming the data. By decoupling ingestion from consumption, organizations can streamline their data collection mechanisms and avoid the need for redundant agents or collectors. This separation allows organizations to centralize their data ingestion processes, consolidating data from various sources into a single repository or pipeline. From there, the data can be efficiently distributed to different cybersecurity solutions, including both traditional SIEMs and emerging AI-based platforms, without requiring redundant data collection mechanisms.

Navigating Challenges in Inter-team data sharing:

Sharing data with peer organizations has become a challenge despite the initial intent of data lakes to centralize data for multiple uses. Cybersecurity SOC teams often refrain from sharing data with counterparts like compliance, insider threat, and IAM teams due to the sensitive nature of the monitored data. As a result, separate mini data repositories or "swamps" are spun up by these teams, leading to fragmentation and duplication of data.

Efforts to waterfall data from the data lake or SIEM to these mini repositories have proven ineffective. In response, organizations have begun exploring the development of homegrown data routers. However, over time, managing and maintaining these routers becomes burdensome and inefficient.

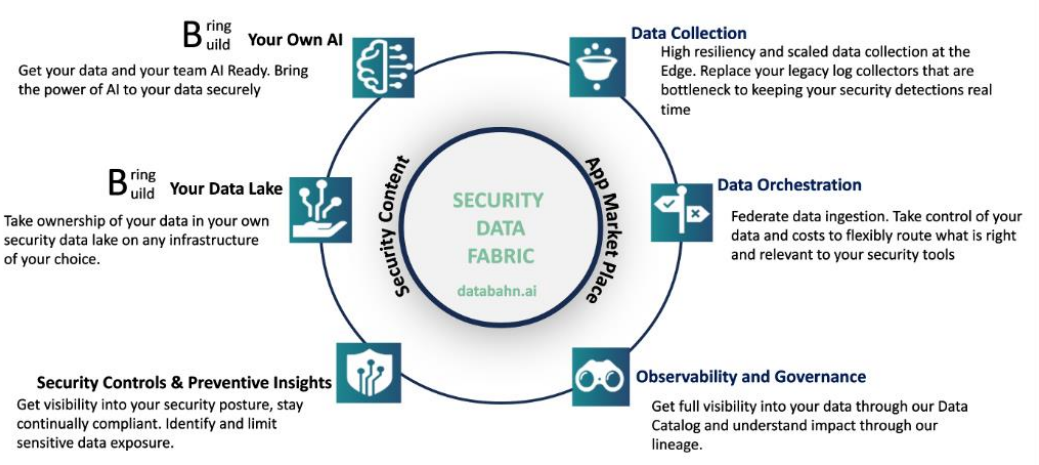
This fragmentation not only hampers collaboration and data sharing but also complicates data governance and compliance efforts. To address this challenge, organizations need to find efficient and secure methods for sharing data across teams while maintaining data privacy and security. This may involve implementing robust data governance policies, deploying centralized data sharing platforms, or adopting standardized data sharing protocols to streamline collaboration and ensure data integrity.

SUMMARY:

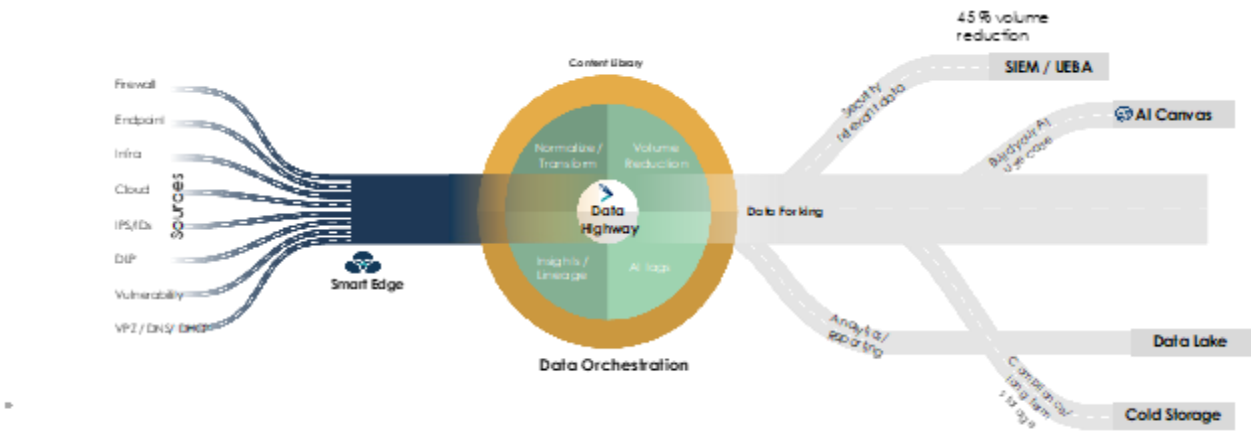
- Cloud Adoption Impact: SIEMs have adapted to the rise of cloud technology, adjusting cost structures and deployment methods. However, these changes have led to increased expenses and margins, requiring a predictable cost model.
- Evolving Threat Landscape: Organizations prioritize comprehensive cybersecurity strategies beyond compliance due to increasingly sophisticated threats. Next-gen SIEMs and XDRs play a crucial role in providing enhanced visibility, reducing the need for frequent SIEM replacements.
- Data Explosion and Management Challenges: The exponential growth of data poses significant challenges in management, ingestion, and filtering within Security Data Lakes (SDLs).
- Focus on Threat Detection: SIEMs now prioritize threat detection over simple alert generation, aiming to reduce false positives and enhance capabilities to address the evolving threat landscape.
- Integration Challenges and the Rise of AI Vendors: Integrating new AI-based technologies requires separating data ingestion from consumption to streamline processes and avoid redundancy.
- Challenge of Data Sharing: Despite centralizing data for multiple uses, cybersecurity teams hesitate to share sensitive information, highlighting the need for more efficient and secure data sharing mechanisms.

SOLUTION - INTRODUCING DATABAHN SECURITY DATA FABRIC:

Databahn's Smart Edge and Highway platform is specifically crafted to address the intricate challenges of handling "big data" within the realm of cybersecurity. By adopting a strategy of federating and decoupling data ingestion from platforms such as SIEM and Security Lakes, our platform not only streamlines processes but also significantly slashes costs associated with steep subscription and license fees.



Our innovative approach ensures that only relevant data is directed to downstream platforms, thus consolidating your tools and enhancing data quality and governance. This, in turn, expedites the analysis process within your SOC. Our Security Data Fabric framework integrates several pivotal components:



- Data Collection: Seamlessly aggregate data across cloud and on-premise sources with the highest levels of resiliency.
- Orchestration: Employ intelligent data pipelines to streamline and route only the most pertinent data to your security tools, thereby reducing costs and enhancing performance.
- Observability and Governance: Implement robust oversight mechanisms to provide clear visibility into the health of your telemetry.
- Security Controls and Preventive Insights: Offer proactive security controls and insights to comprehensively understand your overall security posture.
- BYO-AI (Bring Your Own AI): Provide flexibility to integrate your own AI models without compromising sensitive information.
- BYO-SDL (Bring Your Own Security Data Lake): Empower customers to build their own Security Data Lake equipped with comprehensive insights into their data posture.

Our customers have experienced remarkable benefits, including:

- A 40% reduction in SIEM costs within the first month of deployment.
- Replacement of legacy log collectors and forwarders with our highly resilient edge collectors.
- Establishment of their own data lakes to assert ownership and control over their data.
- Consolidation and reduction of tool sprawl, optimizing infrastructure spending.
- Gain of visibility and insights into the overall security logging posture.

This comprehensive solution is tailored to revolutionize your cybersecurity operations while delivering tangible cost savings and operational efficiencies.