Deloitte.

snowflake

Enhancing Cybersecurity through Data Analytics in the Cloud with Deloitte and Snowflake

Cybersecurity teams face a complex and dynamic cyber threat landscape, and the legacy of working may no longer be up to the task of ensuring a robust security posture.

Part of the challenge owes to how security operation centers (SOCs) have adopted technologies. In many cases, security tools with narrow capabilities were acquired to address discrete challenges. Over time, this approach can lead to a multitude of tools with disjointed data and limited scale. Cybersecurity is a challenge of data analysis and visibility, and siloed data and poorly aligned tools can inhibit insights, delay resolutions, and even allow compromises to go unseen.

At the same time, security leaders are challenged to maximize capabilities given a limited budget. With traditional security information and event management (SIEM) solutions, high licensing costs based on ingestion volume come alongside limited data retention. Because legacy SIEMs are challenged to handle the scale of today's data volumes and cloud data sources, security teams often face tradeoffs in how much data can be analyzed, leading to security blind spots and other risks.

With novel threats, myriad attack vectors, and a constantly changing security environment, sophisticated SOCs are looking to innovate and create new approaches to meeting cybersecurity threats. Traditional SIEMs may enable real-time monitoring for security events, but they can also constrain creativity and may not be able to accommodate advances in data science and artificial intelligence (AI).

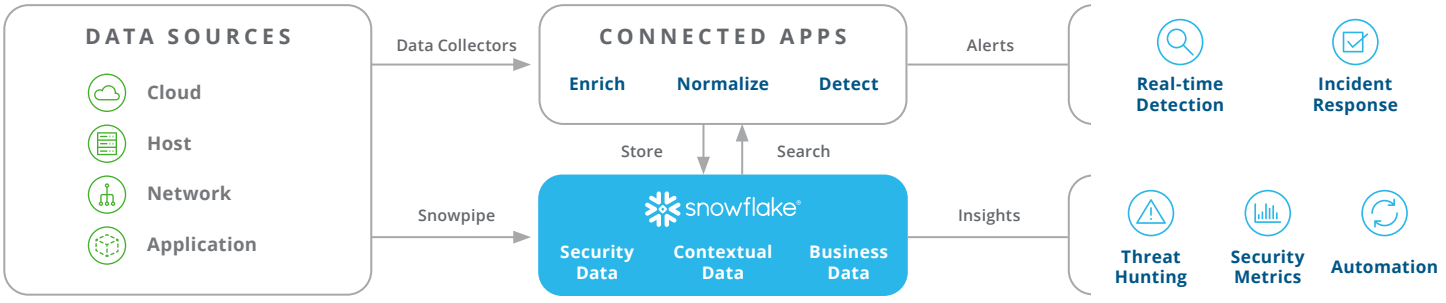
Ultimately, there is a need to adapt security operations and threat monitoring to today's cybersecurity environment and to prepare for tomorrow's. Fortunately, there are solutions available that can consolidate capabilities and data, enhance threat visibility and response, and open the door to innovation with cutting-edge technologies.

Taking a new security approach in the cloud

Today, cloud data lakes are infrequently used in security, in part because of hard lessons learned related to governance, cost, and the high skill level required to manage them. Yet, the technology and associated problems of yesterday are giving way to new approaches and solutions. A modern security lake (such as that powered by the Snowflake Data Cloud) consolidates data and allows the organization to connect security applications, creating a single source of truth that can illuminate more threats, drive keener insights, which can deliver better security results.

A modern security lake is not a one-to-one replacement of tradition SIEMs. Instead, it unlocks a different approach to security monitoring and event adjudication. The potential is founded on the capabilities of a modern data cloud and off-the-shelf applications that turn a petabyte-scale data platform into a solution that can address fast-moving, complex security challenges.

One of the greatest advantages is the ability to bring analytics to bear, solving for cybersecurity as a data challenge, rather than a search challenge. Combining data sets and leveraging an ecosystem of applications and automations can drive metrics and deliver deep insights for security stakeholders in a self-service manner. Developing this environment from scratch would likely be difficult, costly and time-consuming. With a security solution like that from Snowflake, organizations can access cloud capabilities and an ecosystem of applications in days or weeks, rather than years.



Snowflake's Security Data Lake

No SOC wants to make compromises when it comes to their security posture. As such, what's needed are enhanced capacity in data collection, retention, and scalable compute. Snowflake's Cybersecurity workload can natively handle structured and unstructured logs and unite security and enterprise data to enable detection and investigation. Importantly, SOCs can work with the security data lake in universal languages (e.g., SQL, Python), overcoming the challenge with solutions that require an obscure proprietary query language. This also opens the possibility of enabling the organization's data scientists and analysts to work with security data and create visualizations. In this, data teams help build data pipelines and visualizations while the security team focuses on detection and remediation.

This approach to cybersecurity monitoring and detection also sets up the enterprise to address a broader range of use cases and technologies. A modern data lake with an ecosystem of out-of-the-box applications can support things like security compliance, identity verification, and vulnerability management. It also positions the organization for a future with artificial intelligence (AI).

The advent of Generative AI is permitting capabilities that can empower SOCs to discover insights and vulnerabilities. Security organizations can be challenged to build expertise in highly technical areas (e.g., detection engineering), but with the aid of a large language model (LLM), security users can query enterprise data in natural language, lowering the technical bar to working with the data. At the same time, an LLM trained on secure and governed enterprise data consolidated in a modern cloud can help users interpret security events or insights, offering natural language outputs that allow the SOC to richly understand the issue and reduce the time needed to triage a problem. With Generative AI as a security co-pilot and a modern security data lake enabling vast storage, scalable compute, and powerful analytics, organizations have an opportunity to enable participation in cybersecurity across the business.

Accessing a modern data ecosystem with Deloitte and Snowflake

Transforming the organization to use a modern data ecosystem is more than just a technology endeavor. It takes enterprise-wide transformation, with essential adjustments to processes, workflows, change management, security, and compliance. To rapidly access the value and capabilities in modern data security platforms, like Snowflake's, you need to work with an organization with both the technical capacity to implement a data modernization effort as well as the industry and domain experience to do so in a way that can limit disruption and orient the business for new ways of working and decision making.

Deloitte offers the rich experience, trained talent, and subject matter experience that can help SOCs access cloud-based modern security solutions. We help reduce risk by taking an automation-led approach with our accelerators and Migration Factory offering, and we help you use Snowflake to fuel your AI programs.

Beyond our technical experience, Deloitte also holds a deep understanding of end-to-end complexities in the cloud environment and the business realm more broadly. Our clients count on our knowledge and advisory services across cybersecurity, compliance, and risk management. It is why we have one of the largest Snowflake practices among professional services firms and why Snowflake named Deloitte the 2022 GSI Partner of the Year.

With Deloitte's capabilities across security operations, organizational design, risk, workforces, regulations, and data security, we can help you modernize data and applications in a way that is fast, efficient, and secure.

Ready to get started?

Please get in touch! Deloitte is eager to learn about your priorities and help you chart your path to a modern data environment with Snowflake.

Matt Wallbrown
Snowflake Lead Alliance Partner
Deloitte Consulting LLP
mwallbrown@deloitte.com

Rupesh Dandekar
Chief Technical Officer for Snowflake
Deloitte Consulting LLP
rudandekar@deloitte.com

Dave Mattox
Senior Solutions Architect
Deloitte Consulting LLP
dmattox@deloitte.com

Anthony Ciarlo
Alliances Relationship Executive
Deloitte Consulting LLP
aciarlo@deloitte.com