databricks

# Modernizing Government Security Operations Centers With A Cybersecurity Lakehouse

Government IT leaders understand the importance of a strong cybersecurity posture, but they've been stuck fighting modern adversaries with outdated tools.

The urgency to tackle that challenge has intensified in recent years given the July 2023 release of the National Cybersecurity Strategy Implementation Plan that furthers the prior Executive Order on cybersecurity and the M-21-31 memorandum.

But it's not just a matter of executive mandate. Multiple high-profile security breaches have shone a spotlight on the need for federal agencies to modernize Security Operations Centers (SOCs) to ensure their cyber posture can adequately protect valuable data and other assets against a dynamic array of threats. The SolarWinds hack, Microsoft IIS exploit, and Log4j vulnerability made it crystal clear that legacy tools and processes are not up to the task of protecting valuable agency systems and data.

## Legacy security tools can't keep up

These hacks — coupled with the Executive Order — reveal that a 90-day audit trail is insufficient, especially given the complexity of modern IT infrastructure and software supply chains. Federal IT teams must operate with a mindset that assumes breach — and that gives them the proper tools and processes to detect, mitigate and audit security incidents whenever and wherever they occur.

Legacy SIEM tools and architectures, however, weren't designed for this modern paradigm. In particular, they're not good at separating compute from storage — a necessity for teams that want to be able to look back a year (or more) at their security data. They also struggle with modern federation requirements, and typically lack the advanced analytics capabilities including AI/ML that more and more IT teams want.

Yet budget and other operational constraints means federal CIOs can't simply replace and modernize their SOC overnight.

Fortunately, there's a way for agencies to modernize now while also creating a migration path to next generation security architecture when they're ready.

## Modernize with a Cybersecurity Lakehouse from Databricks

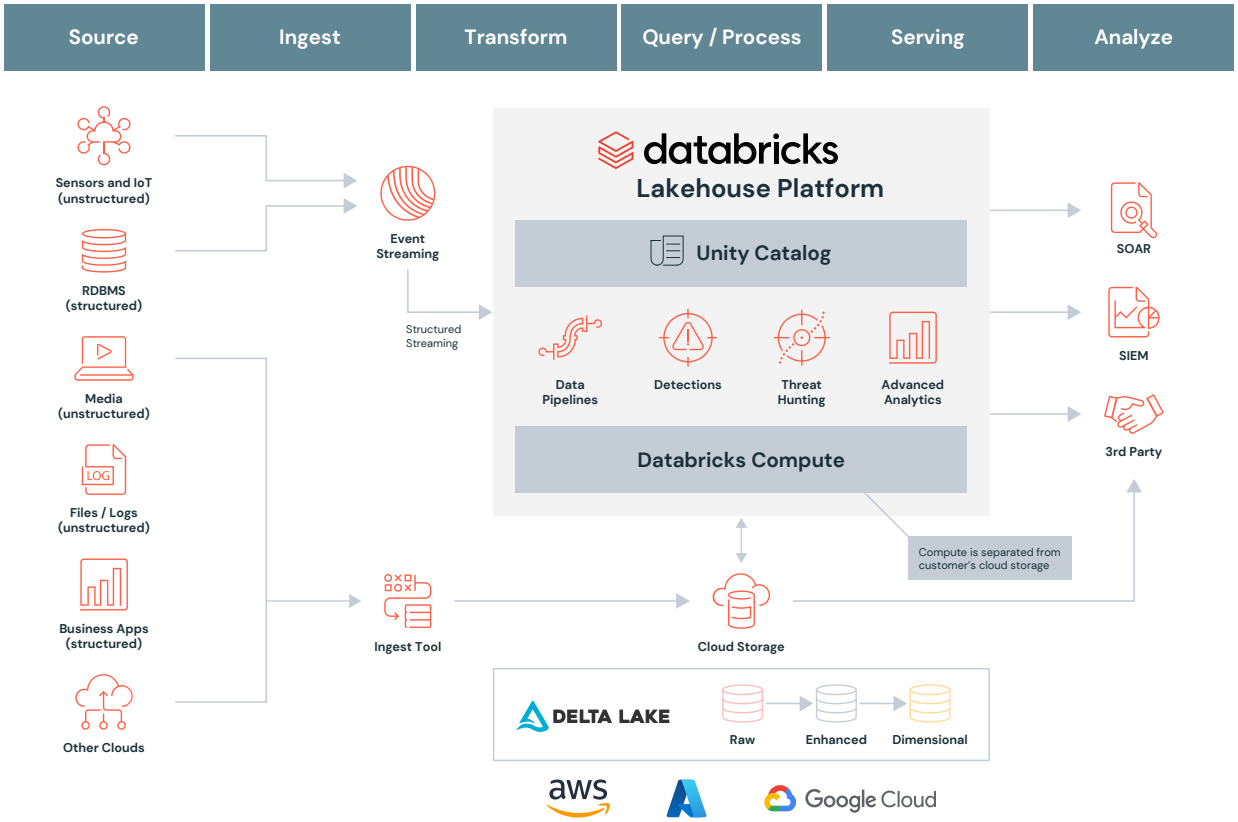
The Databricks Lakehouse Platform is a combination of the best elements of data lakes, data warehouses, data engineering and data science/ML in a secure, reliable, and compliant solution. The Cybersecurity Lakehouse approach can collect and ingest any data into a single platform for secure data pipelines, data normalization, incident response, threat hunting and advanced analytics — in a scalable manner that can support retention and audit periods of more than one year.

**Highlights of the the platform include:**

- True multicloud support
- HiddenLayer for thwarting adversarial attacks on AI/ML models
- Large Language Model (LLM) explainability — no black boxes
- Zero trust architectural support
- Advanced data science & analytics capabilities
- A robust partner ecosystem ready to support agencies' specific needs

databricks

## Databricks for SOC Modernization




The Lakehouse approach also gives your agency the flexibility and scalability required to modernize on your schedule. Since the Databricks Lakehouse is fundamentally a data integration platform, you can ingest data incrementally — on your timeframe — while simultaneously enhancing and modernizing your SOC and cyber posture.

This approach lets you migrate from legacy to modern in a very stage-and-phase manner. Over time, the Cybersecurity Lakehouse becomes your modern data platform and modern integration platform, creating the foundation for modern tooling and architectures.

## Advantages of the Cyber-security Lakehouse approach

The overarching benefit for agencies is the ability to respond to growing pressure to boost your cybersecurity, on a timeline that is actually attainable. It's a cost-effective method of meeting recent cybersecurity directives while also enabling future modernization.

**Cybersecurity Lakehouse advantages include:**

- **Build a migration bridge from legacy to modernization:** Take a phased approach to modernization that doesn't require ripping-and-replacing your existing SIEM and other SOC tooling
- **Dramatically lower TCO:** Support high-velocity data growth needs for ephemeral compute and cloud object storage — at agency level scale — while actually lowering costs
- **Gain flexibility in architecture:** Keep sensitive security data within your agency's own cloud account in an open format that facilitates integration with various SIEMs and Security Operations tools
- **Extend and enhance search retention periods:** Monitor data with long retention periods at agency data scale (Petabyte+), without additional storage architecture or significant costs
- **Add AI security analytics:** Implement advanced analytics today's federal IT pros need, such as anomaly detection using Databricks' leading data science and machine learning platform
- **Ensure explainability:** Eliminate data silos black box security algorithms

databricks

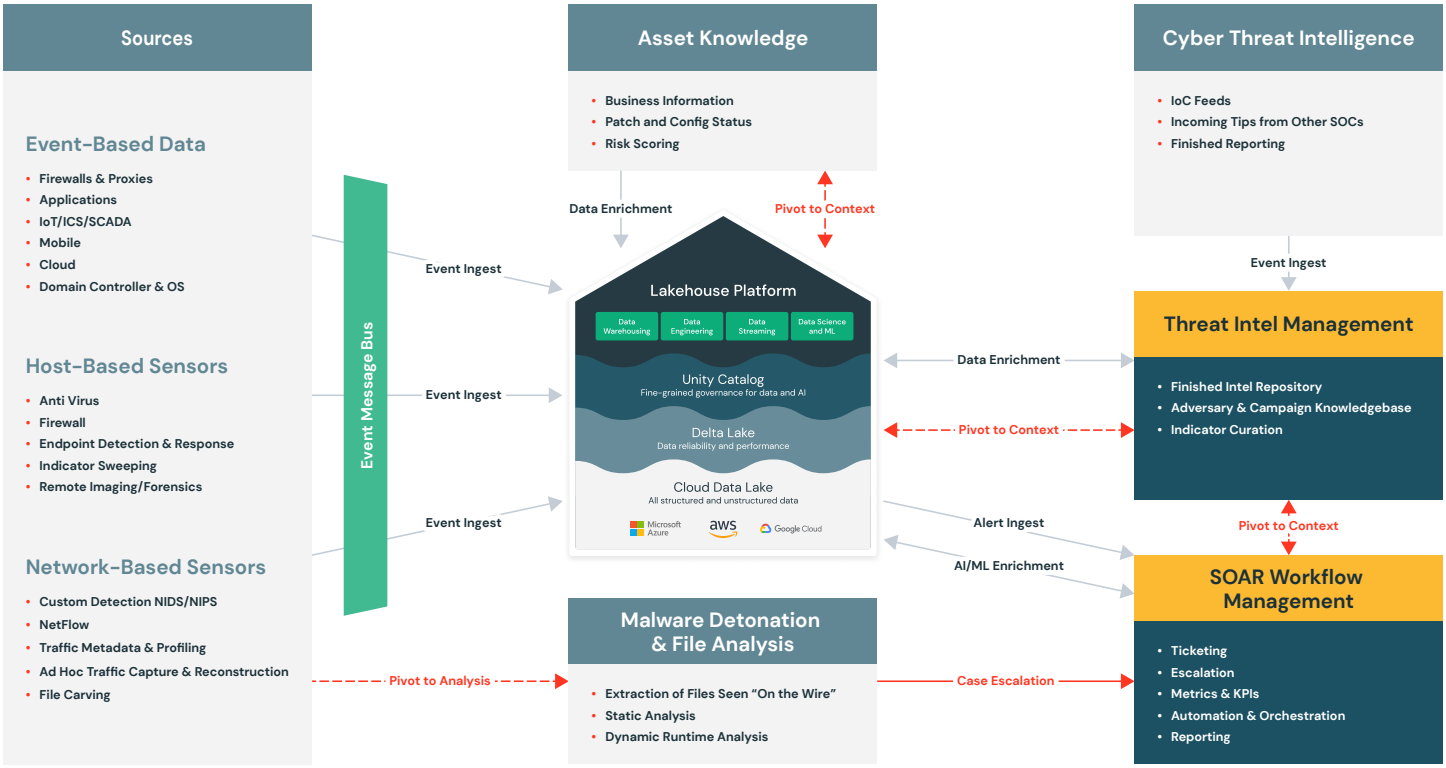
# Meeting M2131: Paving the road from legacy tools to the modern SOC

The recent executive directives on cybersecurity aren't surprising — they're necessary. The modern threat landscape is too complex and dynamic for legacy architectures and tools. But there's no time-warp that can take you from legacy to super-modern overnight. Your IT teams must work within their operational mission — and their operational challenges — to take a phased approach that stays within budget.

Building a Cybersecurity Lakehouse on the Databricks platform allows exactly that: A cost-effective, flexible and scalable approach to SOC modernization that can work alongside your existing SIEM and other tools.

As MITRE notes in its "11 Strategies of a World-Class Cyber-security Operations Center," the practice of running a modern data & ML platform alongside a legacy SIEM has become popular enough that it has a name: the "dual stack" approach.

Think of it as a best-of-both-worlds strategy, one that empowers agencies to meet recent directives and modernize their security operations in a pragmatic manner. That's the Databricks Lakehouse Platform.




Original Source: Mitre, 11 Strategies of a World-Class Cybersecurity Operations Center

Learn more

**Ready to start your SOC modernization journey?**
**Learn more at databricks.com/cybersecurity-analytics.**