

Cyber Analytics & AI Engine

Deloitte offers a new analytics platform for long-term storage and Artificial Intelligence (AI) threat alerts.

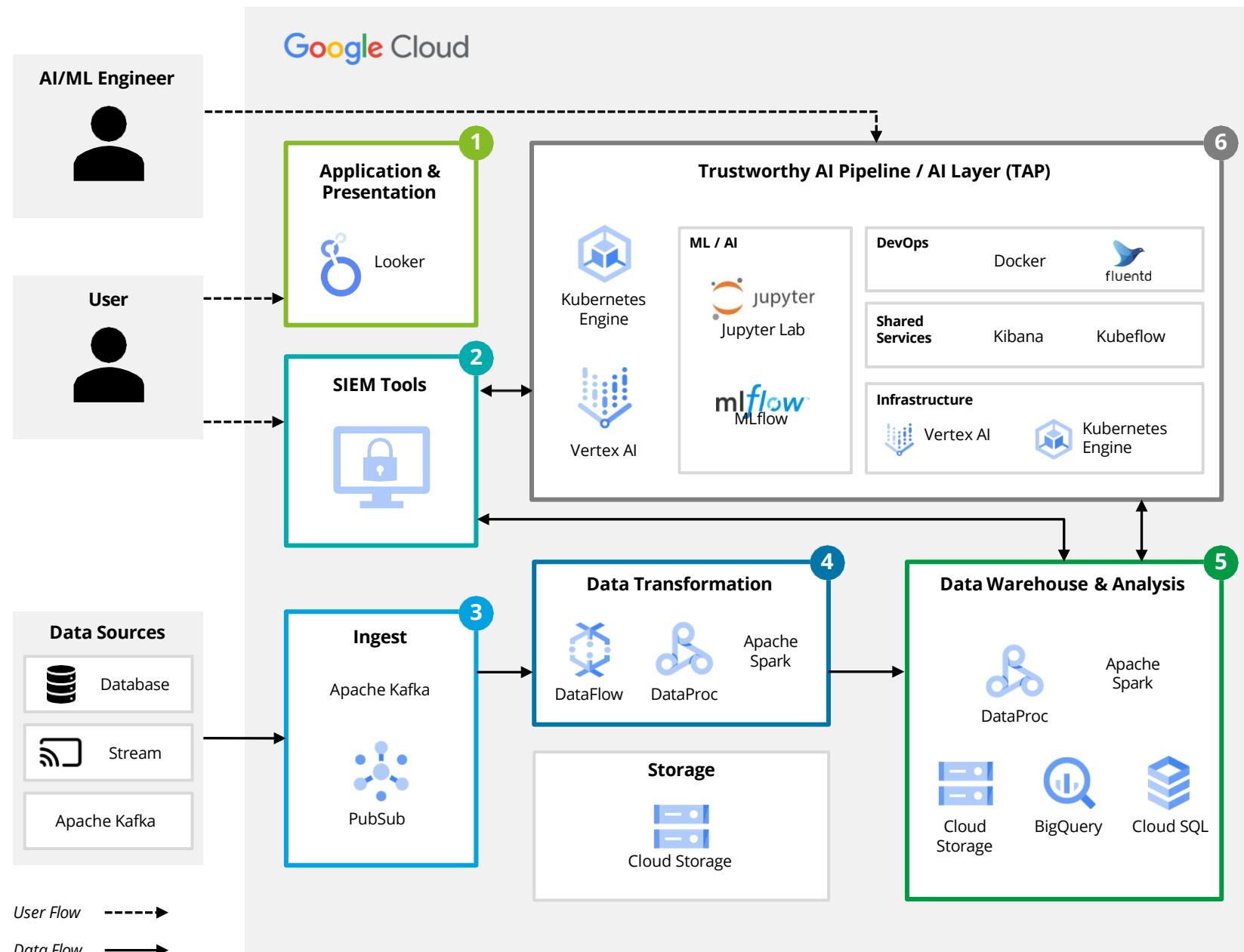
Deloitte is adding the Advanced Cyber Analytics & AI Engine (CAE) module to its capabilities. CAE integrates data from cloud, enterprise, and other assets while leveraging AI for deep analysis. This enables proactive threat hunting and rapid incident response. The enhanced visibility and alert system are designed to help organizations bolster their cyber defenses. As a result, clients can more effectively meet their cybersecurity goals with scalable, enhanced security.



Expected Benefits

Client Problem	High cost of storage in traditional Security Information and Event Management (SIEM) tools, especially for Big Data. Lack of centralized raw log repositories accepting multiple data streams.	Lack of a centralized data analytics platform, especially for AI detections. Complex searches across distributed/ multi-cloud storage with constrained bandwidth.	Shortage of analysts and increasing pressure on existing analysts. Average malware dwell time of 21 days in an enterprise network. ¹
CAE Benefit	CAE offers accessible and cost-effective long-term storage in Google Cloud. Our architecture can provide significant cost reductions when compared to traditional SIEM products, thanks to file compression and the price advantages of the cloud. Security data can be ingested at a scale of over 15 terabytes (TB) daily and stored over 18+ months. Data in storage can be accessed by multiple data visualization tools.	Leading-practice AI goes beyond simple responses built on existing rulesets to uncover new and unseen threats and attack vectors. AI-based analytics detect different kinds of threats as compared to signature-based methods due to their less mechanistic approach to threat detections, while lowering false positives.	Threat correlation across network and endpoint data increases threat detection accuracy and speed, reducing pressure on overstretched analysts. For example, Lateral Movement (LM) is an AI model that detects malicious remote authentication events without requiring pre-existing threat intelligence, shielding against the rise in identity attacks.

Sources: 1. Kevin Townsend, Security Weekly, "Attacker Dwell Times Down, But No Consistent Correlation to Breach Impact", April 19, 2022



Why Deloitte & Google Cloud

In 2026, Deloitte was named the Partner of the Year for Artificial Intelligence (North America & APAC), Gemini Enterprise (Global), Industry Solutions (Global), Managed Security Service Provider (Global), and Infrastructure Modernization (Oracle).

[Learn More](#)



CONTACTS



Eric Dull

Managing Director
Deloitte & Touche LLP
1919 North Lynn Street, Arlington, VA
Mobile: +1.571.882.7436
edull@deloitte.com



Scott Riede

Specialist Leader
Deloitte & Touche LLP
1919 North Lynn Street, Arlington, VA
Phone: +1.571.882.6256
jscottriede@deloitte.com

1 SIEM Integration

Bring Your SIEM

Writeback support facilitates the integration of our custom platform with Google Chronicle Security Operations, enabling users to send data back to these systems for enhanced security analysis and incident response.

2 Visualization

Custom Dashboarding

Google's Looker™ application programming interface (API) allows users to customize dashboards, define layouts and data visualization, and integrate custom JavaScript modules.

3 Durable ingestion

Reliable and Flexible

CAE is rigorously tested and can support various data formats including JSON, XML, and log files; it effectively handles and streams **data volumes exceeding 15 TB/day**.

4 Enhanced query ability

Cross-Dataset

This module accommodates various cyber data formats, enables efficient cross-dataset querying, and helps you handle the challenges of aligning different features or event types from multiple sources.

5 Long term storage

Big Data

CAE has demonstrated its capability to manage and maintain petabyte-scale storage efficiently, helping users to conduct in-depth **historical data analyses over 18+ months** without compromise on performance or accuracy.

6 Supports custom and Deloitte pre-built analytics

Anomalous Threat Detection

Auto-encoder model detects threats based on network flow data using generalized anomaly score for suspicious network behavior.

Lateral Movement

Non-parametric and deep learning models detect malicious remote authentication events shielding against the rise in identity attacks without the need for threat intelligence feeds.

Deloitte's Malware Behavior Prediction™

Convolutional neural network model detects malicious network traffic behavior in network log data trained on over 6 million samples of malware.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.