Google Cloud | Deloitte.

Chronicle

Chronicle SIEM

Reducing total cost of ownership (TCO)

Deloitte's Chronicle SIEM (Security Information and Event Management) enablement services can help your organization to enhance environment visibility by leveraging our Alliance relationship with Google Cloud and decades of cyber industry experience to unlock the fullest value from your Chronicle SIEM deployment.

Legacy SIEM challenges and how Chronicle can help

License model is compelling organizations to filter ingested logs, introducing new blind spots

→ **Unlimited ingestion of data**, scaling with your business to unlock visibility

Manual threat hunting can be slow and time consuming

→ **Continuous indicators of compromise (IoC) matching** and **retro hunts** assist in automation of detections

Many **proprietary data formats** and **separate data indices** introduce needless time and effort into investigation cycles

→ **Unified Data Model** with consistent correlation across disparate data types

Force Multipliers

Up to 6x reduction in TCO[1]

Compared to equivalent legacy SIEM ingestion-based models

Security Operations Center (SOC) analysts empowered

Through leveraging embedded platform automations, removing the need for many previously manual, quotidian tasks

Enhanced environment visibility

Store petabytes of data while keeping it "hot" searchable for 365 days. With zero rate limiting or restrictions on data ingestion, security analysts have the benefit to perform sub-second searches against their data in a single platform.

1 Enterprise Strategy Group, Analyzing the economic benefits of Google Chronicle Security Analytics Platform, 2020.

Chronicle SIEM features

Detect Engine gives the flexibility to use advanced rules out-of-the-box, build your own custom, and migrate rules from legacy tools.

Stitches ingested data into a timeline, allowing you to quickly view events as you pivot between users, hosts, and log sources during investigation.

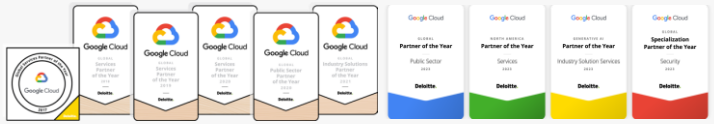
Correlate assets and their associated metadata to singular cohesive entities, constant through search and detection to better understand user and machine relationships and the actions they take.

Empower security analysts using context-aware analytics to better prioritize alerts during investigation through assigning scores based on contextual vulnerability and business risk.

Deloitte's Accelerators

Log ingestion	• Custom parsers for numerous unsupported log types • Ingestion architecture frameworks
Detection Use Cases	• Deloitte Cyber Chronicle and Google Cloud labs to accelerate use cases • Content repository of pre-built use cases, and framework for translation from legacy SIEMs
Third-party Integrations	• Custom integrations for numerous information technology service management (ITSM), security orchestration, automation and response (SOAR), and threat intelligence platforms (TIP)
Deloitte-Google Cloud Alliance	• Strong alliance with Chronicle engineering supporting early preview access, as well as development requests and prioritized feedback on platform features

Why Deloitte & Google Cloud



Four-time Global Services Partner of the Year
Services Partner of the Year – North America
Specialization Partner of the Year**, Security**
Industry Solution Services Partner of the Year**, Generative AI**
Two-time Public Sector Partner of the Year

Google Cloud **Security Specialization**

Google Cloud **Chronicle SecOps Delivery Partner**

5,100+
Google Cloud Globally Certified Professionals
Including architects, security engineers, and developers

Deloitte's Approach

Co-Operation

Augmenting *your existing SIEM with Chronicle's capabilities:*

- **Gather** information regarding the current technology stack and data sources to determine quick win gains in visibility
- **Define** the intended systems use, goals, and boundaries for each system in a collaborative model
- **Deploy** the log forwarding and aggregation infrastructure to support both platforms

Migration

Replacing *your legacy SIEM with Chronicle through full cutover:*

- **Develop** execution plan to minimize impact to day-to-day operations to gracefully transition security operations
- **Transfer** log sources through dual feeding where possible, followed by hard cutovers
- **Achieve parity** with and **enhance security posture** upon existing detection and reporting content

Sample Case Studies

By **augmenting** their legacy SIEM with Google Chronicle, a client was able to achieve a **57%** cost reduction and…

10x decrease
in mean time to detection/remediation

75% increase
in fidelity and detection capabilities

By **replacing** their legacy SIEM with Google Chronicle, a client was able to achieve a **70%** cost reduction and…

11x increase
in hot data retention

30x reduction
in analyst time spent on alert triage

200% increase
in data ingested

100x reduction
in analyst time spent on investigations

CONTACTS

Upen Sachdev
Principal
Deloitte & Touche LLP
usachdev@deloitte.com

Chris Trollo
Lead Sales Executive
Deloitte Services LP
ctrollo@deloitte.com

Ryan Lee
Alliance Manager
Deloitte Services LP
ryanlee8@deloitte.com