Accelerating Incident Response with Distributed Graph Technology

By Pushap Goyal

Delhi Technological University

Conf42 Incident Management

2025

Disclaimer

The content presented here is based on my personal experience and publicly available information.

It has not been officially approved or endorsed by any organization.

Limitations of Traditional Incident Response Systems

Data Fragmentation

Scattered security data across disconnected systems that hinders timely aggregation and correlation.

Time Synchronization Issues

Timestamp discrepancies prevent accurate forensic timeline reconstruction.

Relationship Blindness

Traditional models fail to capture complex relationships between various entities.

Manual Correlation Overload

Manual correlation across dashboards is time-consuming and prone to error, scaling poorly.

These inherent limitations result in a fragmented understanding of security incidents, leading to extended detection and resolution times, incomplete investigations, and increased operational costs.

Ultimately, these challenges force security teams to react to incidents rather than proactively investigate. This highlights the critical need for a more advanced solution.

Graph Database for Incident Response

Graph databases fundamentally transform incident response by representing security data as:

- **Nodes:** Entities such as users, machines, IP addresses, processes.
- **Edges:** Relationships like "accessed," "created," "communicated with."
- **Properties:** Contextual information like timestamps, severity, classifications.

This structure enables relationship-based investigations that follow the natural progression of security incidents across system boundaries.

Unified Security Telemetry Integration

Network Security

Firewall logs, IDS/IPS alerts, DNS queries, and netflow data.

Application Security

Web application logs, database transactions, and API gateway metrics.

Endpoint Security

EDR telemetry, process creation events, file access records, and user session data.

Cloud Security

API calls, resource provisioning details, IAM changes, and service logs.

Identity & Access

Authentication attempts, privilege escalation incidents, and credential usage.

Graph Database can create unified semantic layer across these traditionally siloed data sources, enabling comprehensive analysis.

Google Spanner Graph is a natural fit

Google Spanner Graph is a globally distributed graph database, extending Spanner's capabilities for precise, reliable analysis of massive, distributed datasets. For incident response, Spanner Graph offers:

1

Global Consistency

Ensures consistent and immediately available data across regions.

2

TrueTime API

Enables precise, globally synchronized timelines, eliminating timestamp discrepancies for accurate forensic reconstruction.

3

Relationship Model

Define massive graph by edges across multiple nodes.

4

Scalability & Reliability

Inherits Spanner's horizontal scalability for petabytes of data, with automatic sharding and replication for high availability.

By combining these attributes, Spanner Graph transforms fragmented data into a cohesive, globally consistent, and relationship-rich view, accelerating investigations and strengthening security posture.

TrueTime API: Solving the Time Synchronization Challenge

In distributed environments, accurate incident reconstruction hinges on precise time synchronization—a notoriously difficult challenge. Spanner's TrueTime API provides a robust solution:

- **Globally Consistent Timestamps**
  Eliminates the "he said, she said" problem between logs from different systems.
- **Bounded Uncertainty**
  Provides precise knowledge of maximum time skew (typically within microseconds).
- **Causal Consistency**
  Guarantees that events are ordered correctly across all regions, preserving the true sequence of actions.

Relationship-Based Data Model

Google Spanner Graph's relationship-based approach fundamentally transforms security investigations. By modeling data as an interconnected web of entities and their interactions, it simplifies complex analysis, enabling incident responders to:

- Instantly identify the blast radius by quickly traversing connections from a breach point to all affected assets.
- Trace lateral movement patterns across diverse systems, revealing the attacker's path in detail.
- Discover hidden relationships between seemingly unrelated events, connecting dots traditional tools miss.
- Build comprehensive attack timelines with perfect sequencing, thanks to inherent temporal consistency and causal mapping.

This holistic view empowers incident responders to move beyond fragmented, alert-driven investigations, leading to faster, more accurate incident resolution and minimizing business impact.

Graph Query Capabilities for Incident Investigation

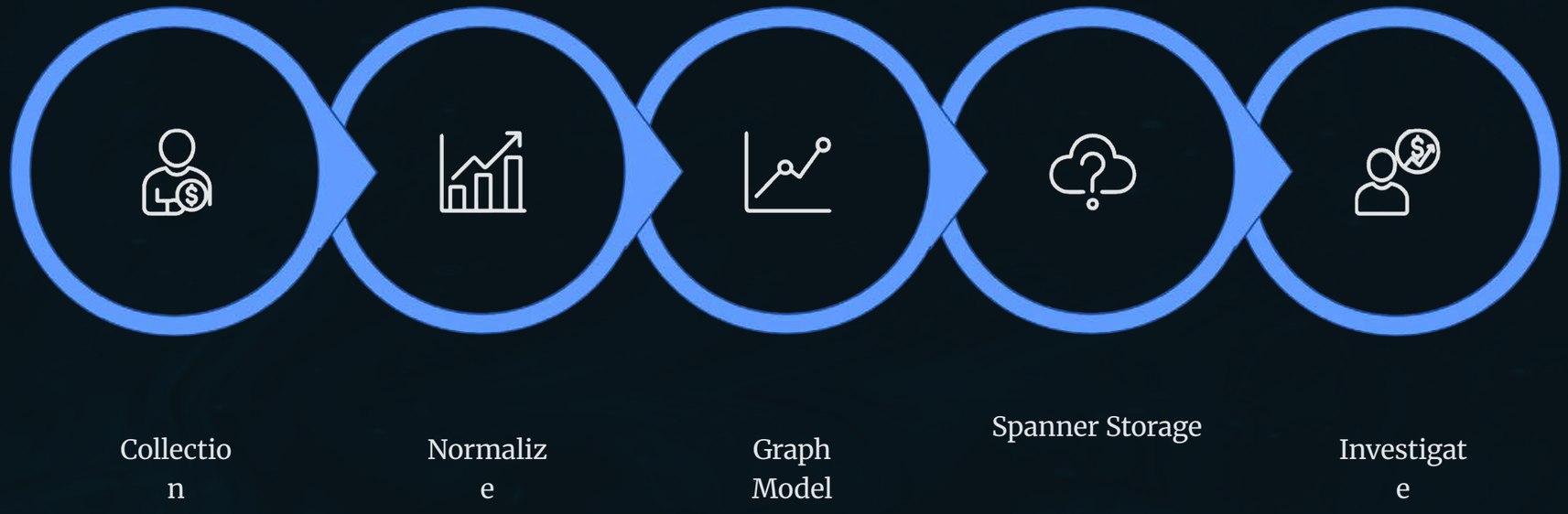
Spanner Graph supports powerful query capabilities that transform incident investigations:

- **Path Analysis:** Find all possible connections between compromised assets.
- **Pattern Matching:** Identify known attack patterns across the environment.
- **Centrality Measures:** Identify critical assets and choke points in attack paths.
- **Community Detection:** Group related activities to identify campaign scope.

These capabilities enable dramatically faster investigations by allowing responders to ask sophisticated questions about relationships in their data.

Implementation Architecture

A successful implementation requires careful planning to ensure data quality, performance, and usability for incident responders. This architecture outlines the journey of security telemetry into Spanner Graph, from raw data to actionable insights:



This architecture begins with **Data Collection** from diverse security sources, followed by **Normalization & Enrichment** to standardize formats and add context. Data is then transformed into **Graph Models** of nodes and edges, stored securely in **Spanner Storage**, leveraging its global distribution and TrueTime API. Finally, **Investigation & Analysis** provides powerful query interfaces for rapid incident resolution.

Technical Implementation Considerations

Schema Design

Properly modeling security entities and relationships requires careful consideration of:

- **Entity Granularity:** Balancing detail to optimize performance.
- **Relationship Types:** Defining directional versus bidirectional connections.
- **Property Indexing:** Strategizing for efficient query optimization.

Ingestion Pipeline

Building reliable data pipelines that maintain consistency involves:

- **Real-time vs. Batch:** Deciding between immediate and scheduled processing.
- **Out-of-Order Events:** Strategies for handling non-sequential data.
- **Data Enrichment:** Integrating and normalizing disparate datasets.

Query Optimization

Ensuring optimal performance for complex incident queries requires:

- **Query Planning:** Developing efficient execution strategies.
- **Pattern Caching:** Storing frequently accessed query results.
- **Response Time:** Balancing query complexity with real-time needs.

Key Takeaways

Spanner Graph transforms incident response by providing:

- A unified, time-synchronized view of security events across global infrastructures
- The ability trace attack progression through complex, multi-hop relationships
- Precise time coordination that eliminates timestamp discrepancies
- A relationship-based data model that reveals the full scope of compromise

By implementing this approach, organizations achieve faster incident triage, more comprehensive forensic analysis, and improved post-incident reporting.

Thank You !