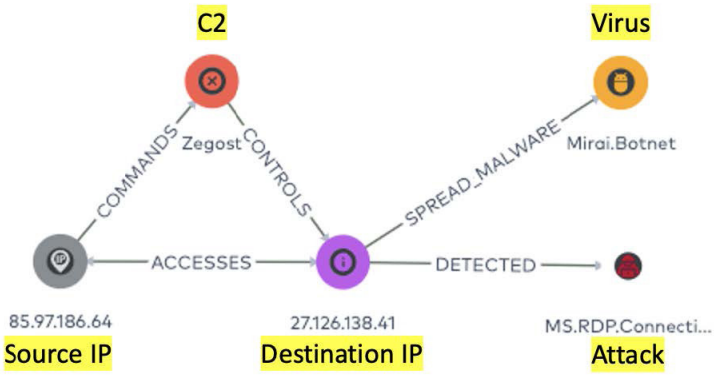
Explore: Cybersecurity

Let Gemini Explore connect the dots between your organization's data.

Overview

As companies continue to become more dependent on technology, they become more vulnerable to security breaches in their network. The current cybersecurity systems generate hundreds of thousands of alerts daily on average.

A network breach can be detrimental. For example, a botnet can give a hacker the ability to automate a large-scale attack. In this case, the attacker will execute a coordinated action from their botmaster to all of the individual devices under their control simultaneously.



Organizations can be at risk of losing critical data, distributing malware, or launching Distributed Denial of Services (DDoS). This will greatly disrupt a business' normal operations as long as the network has been infiltrated.

Currently businesses struggle with the inability to:

- Review high volume amounts of alerts generated by security software.
- Process unstructured and rapidly changing in real-time.
- Visualize their entire network traffic to spot unusual activity.
- Quickly identify the origin of a network breach and the machines / devices affected.

Solution

Gemini Explore connects data stored in SQL, Splunk, JDBC, or CSV sources and provides the contextualization that enables staff to make faster, better-informed decisions in near real-time.

Investigations in cybersecurity become simple and intuitive. A complex investigation can be easily done with few clicks of a mouse to reveal relationships that were hard to visualize before, and no specialized skills or query knowledge are required to gain valuable insights.

Analysts can connect the dots and develop a shareable story to be reviewed with other colleagues. This maximizes the value of the data collected by existing security systems in the company.

Benefits of using Gemini Explore

Data visualization with Gemini Explore can cut manual review time in half, allowing analysts to quickly understand the relationships, saving both money and time in the process. In addition, with the ability to spot more compelling stories previously hidden within their data, analytics teams begin to see possibilities far beyond their typical investigation routines.

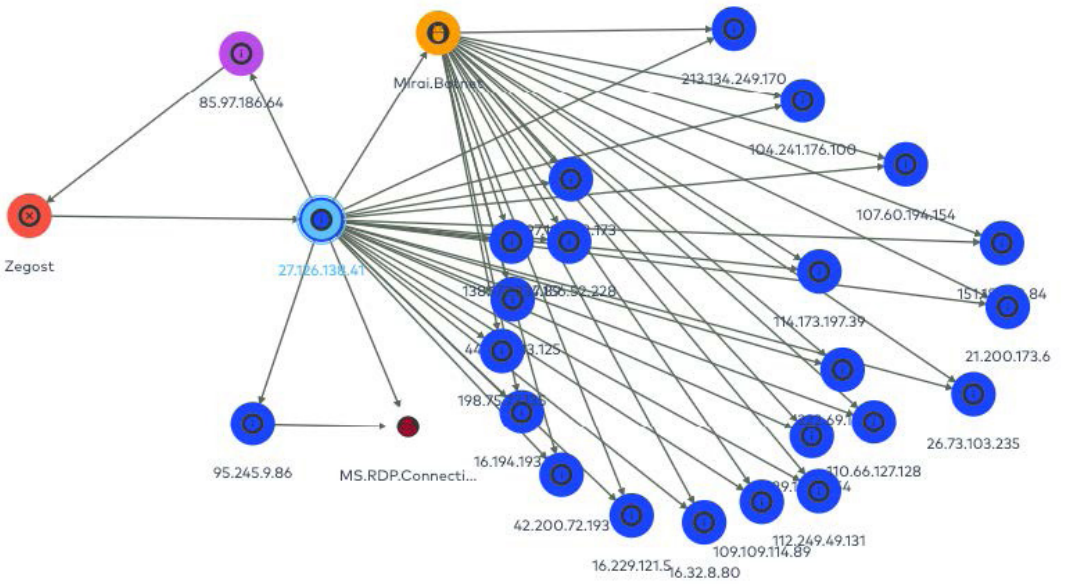
- View information from disparate data sources, in-house departments, and external sources all in one place.
- Learn the hidden stories and reveal the context between multiple data sources.
- Reveal patterns of network behavior and use this to develop a better security strategy.
- Quickly identify super-spreader nodes and the popular method of infiltration used by attackers.

How it Works

Gemini Explore creates an end-to-end solution that presents data as a set of nodes and edges instead of tables, rows and columns.

This enables insights from the relationships between data elements such as devices, IP addresses, viruses, attacks, and malwares.

When ingesting multiple data sources, Gemini Explore makes it easy to cross-reference by normalizing similar data fields using tags.



Why use Gemini Explore for Cybersecurity?

- **Contextualize data – add real meaning and unlock further insights**
  Correlate and contextualize multiple datasets for rapid decision-making .
- **The ability to go from raw data to an 'aha!' moment in a few simple steps**
  Ingest data from multiple sources, choose the significant fields/headers which will become nodes, create edges to show relationships between them, and quickly view the results on the canvas.
- **The 'no-code' advantage**
  Gemini Explore can be used by technical and non-technical users alike. No specialized skill or knowledge of query languages is required, removing the barriers to produce deeper insights.