GEMINI DATA

GEMINI ENTERPRISE:

Getting to Cyber Security Situational Awareness

Situational awareness (SA) for cyber security is critical for the reduction of business risk. Attaining SA means understanding the implications of potential threats from inside and outside the organization at all times in the context of what they mean to the business. In support of this ideal, many organizations have implemented big data solutions as a foundation to ingest and organize security relevant data for search and analysis. Often added to this foundation is an analytics layer supporting visualizations for threshold based alerting. Advanced searches are often written to monitor for specific conditions. When set conditions are met or a risk threshold is reached, a security professional is alerted.

To support situational awareness, a big data foundation has to be deployed and managed in a way that allows an implementation to grow and expand as data volumes increase without performance degradation. Many big data vendors tell us that a successful implementation means:

- proper implementation and ease of management for linear scalability,
- mastery of the search language, and
- moving from reactive forensic investigation to continuous monitoring.

This is more complex than it seems. There are pitfalls along the journey to situational awareness that can slow or stop it in its tracks.

THE PROBLEM

Often, the journey to situational awareness is impeded by:

1. big data solution management that becomes fragmented into several management silos,
2. a key employee who had mastered the search syntax has left the company, and
3. the realization that creating searches that result in positive correlations, and crossed risk thresholds doesn't address the challenges of analysis.
4. commodity hardware and home-grown management that don't scale to meet use case demands for continuous simultaneous searches,

THE SOLUTION

Cyber security situational awareness can best be attained through the use of a tightly integrated solution—an analysis stack that seamlessly works to address all four of these problems. Gemini Investigator uses artificial intelligence (AI) and your data to create situational awareness and analysis at scale without the need for additional searches. Even for the most experienced search language specialist, searching and manually pivoting through different data types, looking for all connections and relationships between IP addresses, email addresses, MD5 hashes, identities, vulnerabilities, etc., is exhausting time-consuming work. Relationships between these entities are not explicit in your data, yet they are the key to complete understanding of a security incident and your

geminidata.com | contact@geminidata.com | (415) 826 - 7269 | 15 Funston Ave, San Francisco, CA 94129

ability to convey a narrative about why it happened. Investigator uses machine reasoning (a form of AI), a relationship schema, and an ontology of over 2,000 data objects to intelligently organize your data into entities and relationships. Investigator also uses AI to infer and display entities for which it has no data, but should be present based on other entity data and relationships. The interactive user interface lets you create a visual narrative to which you can add notes or manually create relationships as needed. Use any part of an alert from any system for which data has been collected as a starting point and follow multiple investigation paths without pivoting across data types.

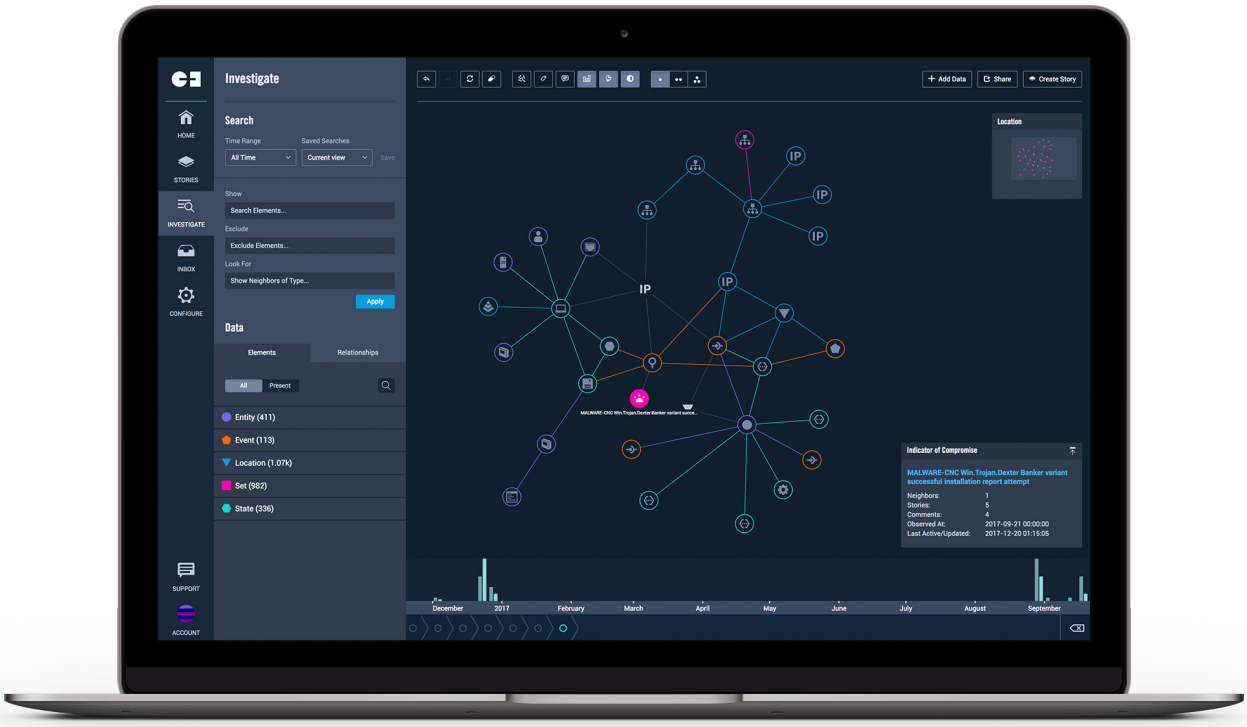
Among the many possible use cases for Investigator are:

- security incident investigation,
- phishing and malware attacks,
- fraud investigations
- compliance management
- any other use case where root cause analysis is needed.

Custom physical and virtual hardware appliances with a hardened operating system tuned for big data deployments are the the foundation of your big data analysis stack. Gemini's Manager software automates node and cluster management, provides visualizations of your deployment, and gives you all the tools you need to successfully manage and monitor your big data deployment in a single user interface. You have the ability to add more indexers, search heads, and forwarders as fast new use cases are created data volume grows.

SUMMARY

Maturing the use of your big data solution with purpose-built hardware and big data management software allows a use case owner (security or IT operations) to successfully manage a big data implementation at scale, or move it to IT Operations with the smallest possible impact. Using AI, Gemini Investigator matures and scales analysis capacity, speed and accuracy by dramatically reducing the time-consuming activity of manually searching and pivoting through your data. With entities and relationships already defined by Investigator, you can know what happened, how it happened, and can present a complete story across teams and up to the C-suite. These stories can be saved for training purposes or communicated as visual representation of an incident across the enterprise. Gemini Enterprise provides an easy way to accelerate your journey to situational awareness.



Gemini provides Continuous Data Analysis. We translate data into knowledge using machine reasoning. With Gemini Enterprise, gain enterprise knowledge and awareness, accelerate analysis with AI, and simplify management of big data platforms. Designed for modern architectures, Gemini Enterprise reduces complexity in the cloud or on premises. Gemini Data was founded and built by experts from Splunk, ArcSight, and AppDynamics that understand the importance of building awareness across the enterprise. Find more information at geminidata.com or follow us on Twitter @geminidataco.