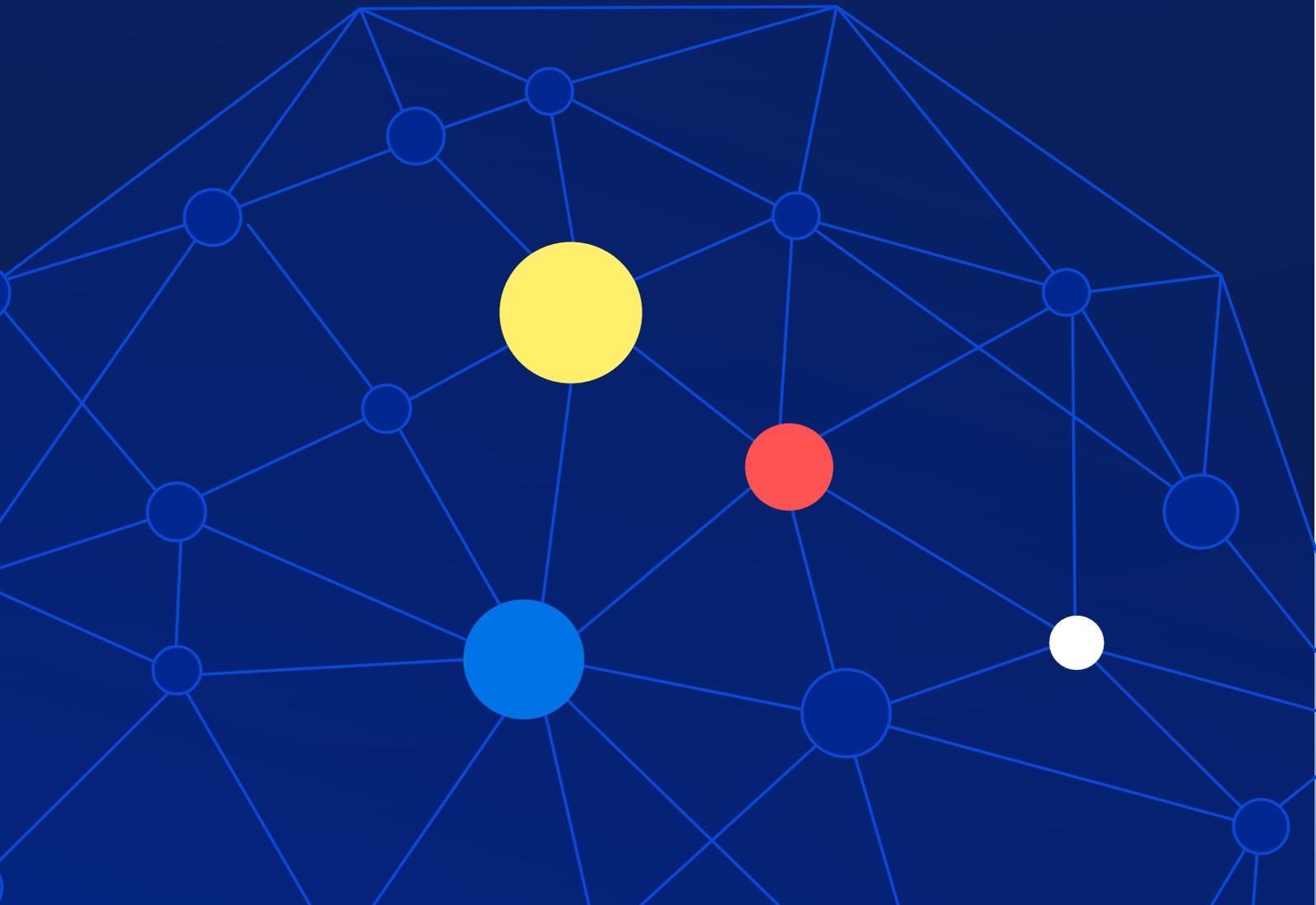




Knowledge Graphs: **The Secret of Google and now XDR**



Introduction

Threat detection is a key battleground in the ongoing battle against cybercrime. Unfortunately, the processes currently used to detect such incidents fall short in several areas:

Siloed: The processes depend on a wide variety of independent security products, with no shared context or correlation;

Manual: The processes are human-based, relying on analysts to sift through huge amounts of data trying to surface relevant issues;

Slow: Manually evaluating inconsistent data types across a complex environment is too slow and doesn't scale;

Knowledge-Limited: The analysts executing the process lack expertise in all the areas they encounter (applications, data, infrastructure, etc.).

[Hunters](#) set out to solve this challenge. Our mission is to revolutionize SOC detection & response by creating a new standard for cyber knowledge automation. This whitepaper will describe the key technological element that differentiates our approach, to explain why we will succeed where so many other solutions have failed.

HIGHLIGHTS

Cybersecurity threat detection tools have done little to improve the slow, manual approaches used by most SOCs.

Behavioral-based machine learning is not a panacea, given the wide variety and dynamic nature of attacker TTPs.

Hunters' approach to threat detection leverages a Knowledge Graph, a key technology driving Google's search engine.

Unlike SIEMs or behavioral ML, the Graph provides the environmental context required to reliably surface true threats and get better with time.

The Hunters Vision

Knowledge Graph Based Machine Learning - Technological Leap for the SOC

The Hunters vision for extended threat detection and response is based on a novel use of a technical approach already proven in other applications. Competing threat detection solutions suffer from heavy silos between them. In addition, they typically use behavioral analysis, looking for statistical deviations to surface indicators of compromise. These suffer from low fidelity (false negatives and positives) and high operational overhead (triage, data collection and system tuning).

In contrast, Hunters' approach combines several technologies that deliver high-fidelity and accuracy heretofore unavailable. The most important of these is the use of a Knowledge Graph – the same technology that powers Google Search. A Knowledge Graph is a structured representation of knowledge, architected for flexibility and compatibility with scalable analytical algorithms. As an example, consider a big city subway system. A Knowledge Graph of the system would include detailed, continuous object attribute and interaction data on the tracks, vehicles, signals, stations, riders, employees, environment, and more. The interaction aspect cannot be overemphasized: The graph would detail how all these objects communicate and relate to each other, rather than just recording an event log related to each object type. The graph also would allow all public agencies (Transport, Finance, Public Works, Police, etc.) to apply their own analysis tools to the graph to do whatever they require. There would not be a constrained list of supported analytics tools or algorithms the agencies had to pick from.



CONSIDER A CITY SUBWAY SYSTEM. ITS KNOWLEDGE GRAPH WOULD INCLUDE DETAILED, CONTINUOUS OBJECT ATTRIBUTE AND INTERACTION DATA ON TRACKS, VEHICLES, SIGNALS, STATIONS, RIDERS, EMPLOYEES, ENVIRONMENT, AND MORE.

In the case of Google Search, a massive Knowledge Graph is what powers the “Knowledge Graph Panels” that often appear in the upper right corner of a search result. Search for “Michelangelo” as an example.

Hunters has developed the technological application for extended threat detection, by building a cloud-based Knowledge Graph specifically designed to host and maintain cyber security knowledge. Hunters’ Graph is much more than just a model of the environment or a database of events. It is a representation of objects and entities, their behaviors, and interactions over time. At a high level the Graph contains:

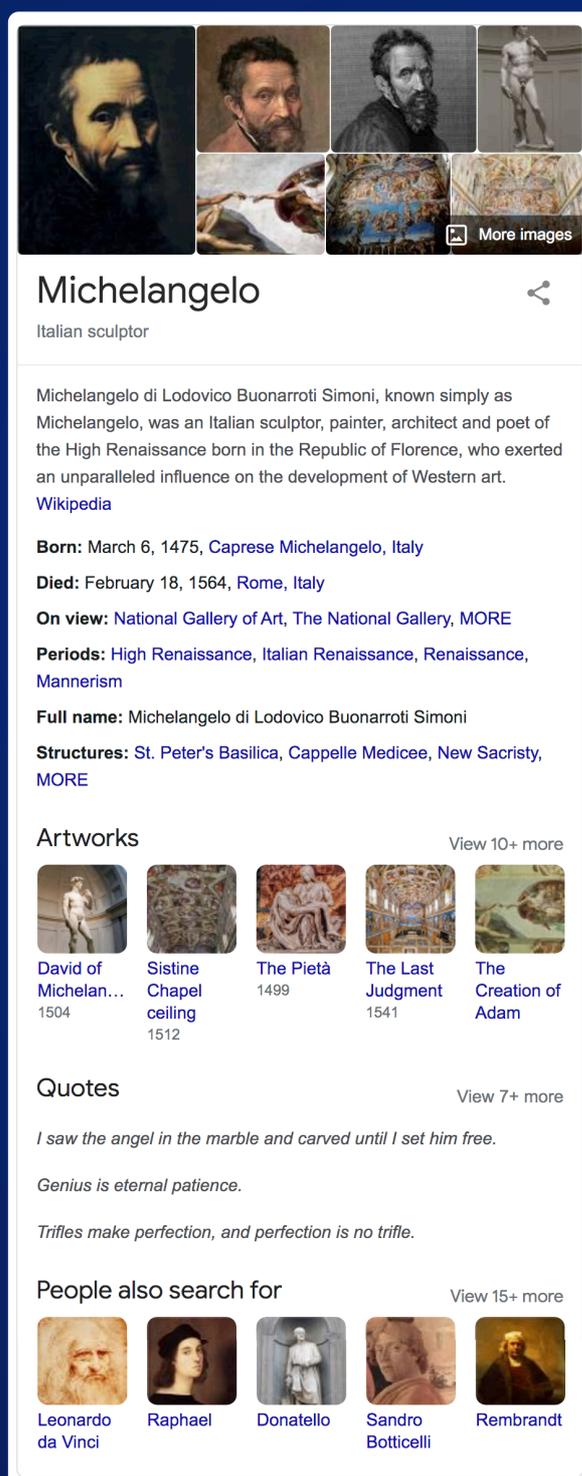
Organizational Context: Users, servers, data stores, applications, etc.

Threat Intelligence: Adversaries, campaigns, targets, methods, etc.

Events detected from existing security products and infrastructure: Alerts and logging

Adversary Detection Modeling Data: Knowledge suggestive of adversarial activity curated using our TTP Extraction Engine and autonomous investigations.

It should be noted that the Hunters’ Knowledge Graph focuses on modeling attacker behavior, and less on user behavior. Our design philosophy is that better fidelity is achieved by identifying the techniques used by the adversaries, rather than modeling the user community and looking for “deviations”. It’s just too noisy an approach.



Michelangelo
Italian sculptor

Michelangelo di Lodovico Buonarroti Simoni, known simply as Michelangelo, was an Italian sculptor, painter, architect and poet of the High Renaissance born in the Republic of Florence, who exerted an unparalleled influence on the development of Western art.
[Wikipedia](#)

Born: March 6, 1475, Caprese Michelangelo, Italy
Died: February 18, 1564, Rome, Italy
On view: National Gallery of Art, The National Gallery, [MORE](#)
Periods: High Renaissance, Italian Renaissance, Renaissance, Mannerism
Full name: Michelangelo di Lodovico Buonarroti Simoni
Structures: St. Peter's Basilica, Cappelle Medicee, New Sacristy, [MORE](#)

Artworks [View 10+ more](#)

- [David of Michelangelo](#) 1504
- [Sistine Chapel ceiling](#) 1512
- [The Pietà](#) 1499
- [The Last Judgment](#) 1541
- [The Creation of Adam](#)

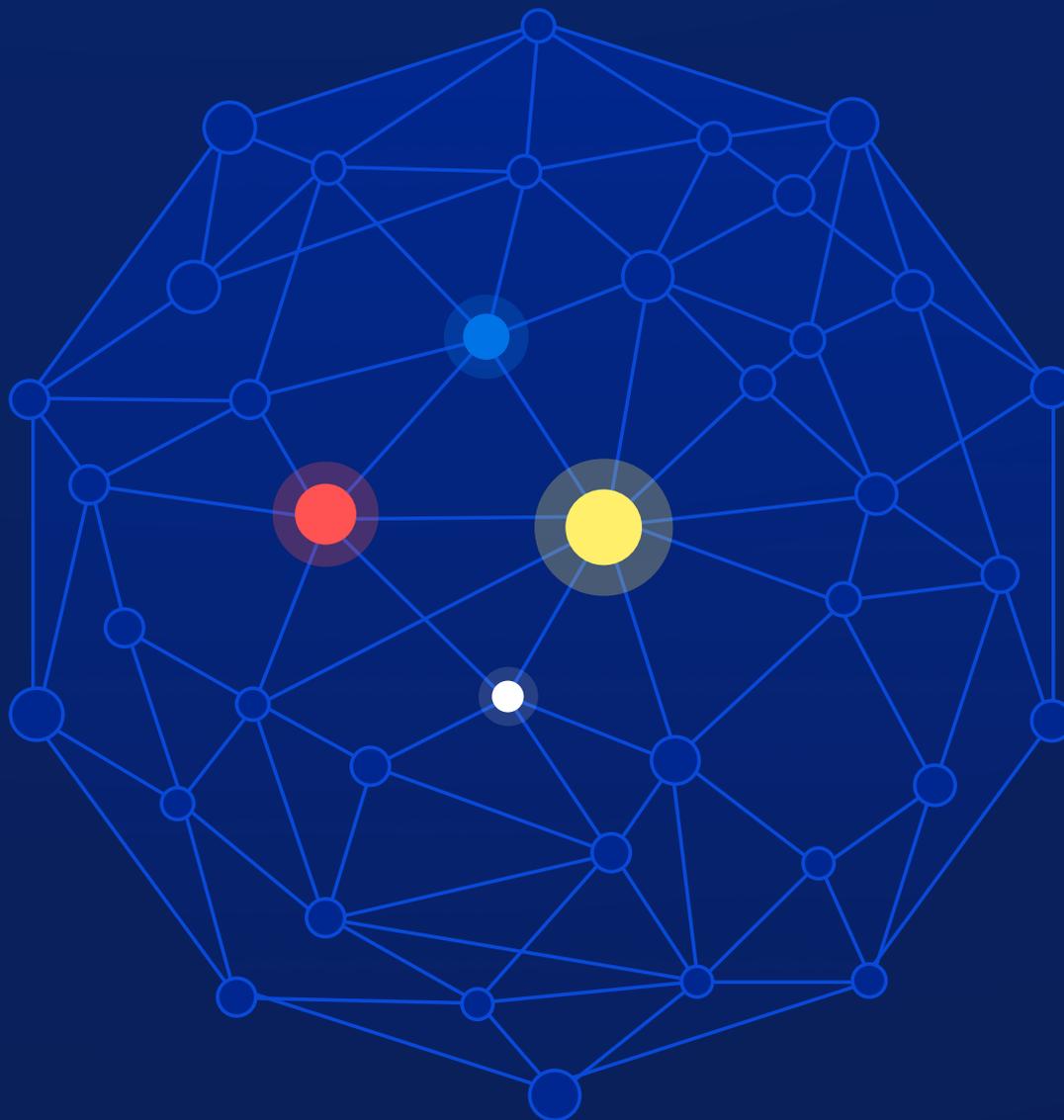
Quotes [View 7+ more](#)

- I saw the angel in the marble and carved until I set him free.*
- Genius is eternal patience.*
- Trifles make perfection, and perfection is no trifle.*

People also search for [View 15+ more](#)

- [Leonardo da Vinci](#)
- [Raphael](#)
- [Donatello](#)
- [Sandro Boticelli](#)
- [Rembrandt](#)

“Knowledge Graph Panels” that often appear in the upper right corner of a search result. Search for “Michelangelo” as an example.



**HUNTERS' GRAPH IS MORE THAN JUST A MODEL OF
THE ENVIRONMENT OR A DATABASE OF EVENTS.**

Knowledge Graphs and XDR

So how does Hunters' Knowledge Graph improve detection scope and fidelity?

Ever-Evolving Detection Context

The Graph provides environmental attribute context to our unsupervised machine learning. This makes it possible to build an intelligent system to autonomously correlate different findings and detect malicious activity. Just as a human learns over time, new knowledge added to the Graph continuously improves the accuracy of the solution. In addition to Hunters' mentioned TTP-based algorithms, knowledge in the Graph is also aggregated across the Hunters' customer base, greatly increasing the breadth of experience our machine learning can leverage in its analysis.

Accurate Analysis

The Hunters Graph acts as the intelligence source for all threat detection, incident response, and threat hunting use cases, delivering an unprecedented level of breadth and accuracy. To use a cooking analogy: The statistical learning approach used by alternative products looks at a dirty kitchen floor and concludes "I believe a cake was baked here". In contrast, the Hunters Graph provides the recipe for baking cakes, monitors the activity of the cook, and concludes "I saw behavior that's consistent with the cook baking a cake". This approach is far more accurate.

Explainability

Another Knowledge Graph benefit is "explainability": it can map its findings back to the knowledge in the graph and summarize the rationale for its attack classification conclusions. This is tremendously valuable for both threat detection and hunting, as security analysts and compliance audits need to know how controls have been circumvented, to speed up and justify response and remediation. Lastly, the Knowledge Graph improves manual investigations and workflows. Rather than combing through log data from isolated sources, the Graph allows analysts to work with contextualized data, rich with relationships and attributes. This dramatically improves the efficiency of investigative teams and threat hunters.

Three additional elements support the Hunters knowledge graph architecture. **First**, our flexible, cloud-based Ingestion Engine is the conduit between the graph and customer environments. To provide high quality XDR (Extended Detection and Response) capabilities, robust data ingestion and timely support for new data types is essential. Security data sources and infrastructure are complex, heterogeneous and constantly evolving. Our strategy is to focus on the most popular product categories and common infrastructure components:

Security solutions: EDR, firewall, CASB, web and email gateways, threat intelligence

Infrastructure and identity APIs: Cloud IaaS (AWS), Okta, Cisco Meraki

Applications and Data: S3, Azure Blob, Office365, ADP

The ability to accommodate these sources while maintaining both flexibility and scaling is essential to build out the Knowledge Graph.

Second, our TTPs (Tactics, Techniques and Procedures) operate on this raw extracted data to put it in context. Building on years of expertise in offensive and defensive cyber security, Hunters provides out-of-the-box advanced detection based on proprietary adversary modeling of attack TTPs, IOCs, and threat intel feeds. Hunters identifies threat signals across the environment, feeds them into the graph, and thoroughly investigates and ranks them to spot high fidelity threat “leads” from siloed systems. It links them together and transforms them into actionable attack “stories” - multi-dimensional views of incidents. Since attack methods change daily, the Hunters cyber threat research team continuously updates the models to include newly seen techniques.

Finally, the Hunters solution includes a Continuous Investigations and Scoring component. These machine learning algorithms operate continuously on both the graph itself, and upon extracted threat signals prior to graph insertion. This dynamic, context-dependent process operates as relationships change or new signals are extracted, and performs a number of critical tasks, including:

- Data enrichment from both external and internal sources
- Entity relationship management
- Retro threat hunting
- Risk-rated prioritization and scoring

The algorithms are constantly updated, maximizing the solutions’ ability to differentiate high-risk activity from benign.



**FLEXIBLE, CLOUD-BASED INGESTION, ADVERSARY
MODELING, AND ML-BASED INVESTIGATIONS
SUPPORT HUNTERS' KNOWLEDGE GRAPH
ARCHITECTURE.**

The Hunters Advantage

Cybersecurity threat detection continues to vex organizations of all types and sizes. Hunters' approach to threat detection combines a Knowledge Graph with machine learning. The Hunters approach has been shown to deliver:

A

Improved SOC efficacy and efficiency;

B

Better business transparency and compliance.

C

Synergetic leverage of existing security and infrastructure solutions

D

Faster, more accurate detection;

E

Easy, low risk deployment;

SUMMARY

THE ARCHITECTURE IS PURPOSE-BUILT FOR THREAT DETECTION AND ANALYSIS AT SCALE, MAKING HUNTERS XDR A CENTRAL SOC PLATFORM IN THE ONGOING BATTLE AGAINST CYBERSECURITY THREAT ACTORS.

Get more info:

Website: <https://hunters.ai> | **Contact:** info@hunters.ai

