ENDGAME.

Artemis:
An Intelligent Assistant for Cyber Defense

SERIES ONE, VOLUME ONE

BOBBY FILAR + RICH SEYMOUR

You've used them for directions, to order pizza, to ask about the weather.

You've called them by their names Siri, Alexa, Cortana... You speak to them like you know them, like they can understand you. Why? Because they usually can. Intelligent assistants are on the rise and increasingly supporting our lives. In large part, this is driven by the user's desire for ever more efficient querying and frictionless action. Instead of muddling through bloated interfaces, simply speaking or typing your queries or commands through a bot is often easier, faster, and seamless.

Bots aren't just useful for helping us plan our day and listen to music. They are increasingly implemented across a wide range of industries, and have been introduced by companies to market and provide customer/sales support and recommendations. They can automate large portions of many data-driven tasks, correlating data, and providing context. They can go even further and suggest what you may want to do next.

In short, bots can take care of the data gathering, munging, and routine analysis that previously consumed significant resources. This is especially pertinent for the information security mission. Security operators and analysts encounter simple tasks and actions daily while executing their complex higher order work. Unfortunately, the elementary tasks currently consume an inordinate amount of time. With that in mind, we created Artemis, an intelligent assistant for cyber defense.

Background

In contrast to other fields where bots are ubiquitous, bots have yet to make a major impact in the information security industry. Due to the talent shortage and the vast and diverse array of data in information security, there is a unique opportunity for intelligent assistants to help improve the workflow of operators and analysts. Resource-constrained security teams may rely on alerts generated by security platforms, but these alerts often lack context and require additional collection and correlation to make a solid analytic judgement. Intelligent assistants can help automate repetitive tasks and provide a natural language interface to streamline workflows for interacting with endpoint data.

By removing friction inherent in accessing information during an investigation, we can free up the responder to focus on the core investigatory analysis which is difficult to automate. Questions like "Is this artifact present on other systems?", "What does this file do?", "Is this artifact malicious?", and "What strings are present in this process's memory?" require additional querying and collection as well as enrichment from other available sources. Today, this process often demands an intimate understanding of multiple data schemas to effectively derive meaning from the mountains of data available during an investigation.

Artemis, An Intelligent Assistant

Endgame introduces Artemis, a first-of-its-kind intelligent assistant for cyber defense operations with these challenges in mind. Artemis is the ideal enabler for an organization's information security mission, allowing analysts, hunters, and forensic personnel to use natural language to perform precision-guided analytics on endpoint data. The following are some of the intelligent assistant's key features.

A Conversational Interface to Your Endpoints

The user interface is simply a chat window we've been familiar with in tools from IRC to Slack. The user merely asks a question and the intelligent assistant surmises what needs to happen next. This leads to a natural and fluid two-way conversation towards the analyst's objectives without needing to learn a complex query language to formulate the perfect query in one go.

Expert Recommendations and Rapid Contextualization

Less experienced analysts may have difficulty knowing how to pivot through data in response to an event or alert. They may make the common mistake of pulling in so much data that it becomes overwhelming and the malicious activity is lost in the noise. Artemis solves this by helping answer questions about what to search for, during what timeframe, and from which endpoints to extract data. The experience of our subject matter experts who've worked as hunters and DFIR experts in government, military and financial sectors is baked directly into the technology and guides the workflow. For a given alert or issue, Artemis immediately suggests logical and effective next steps or actions.

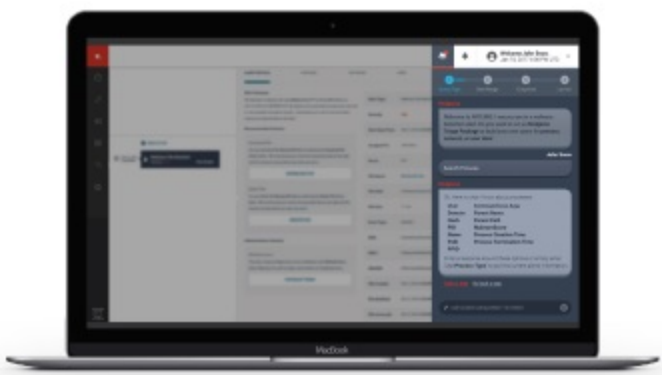
Focused Collection and Efficient Operation

The conversational interface of Artemis creates the query logic that runs on each targeted endpoint, culling data there instead of returning mass amounts of data to be centrally processed. In this way, the results of an Artemis conversation turn a big data problem into a good data solution. This lessens the physical resource strain in storage and network bandwidth, as well as the mental strain on analysts who have a helpful assistant guiding them, as needed, through the process.

User Directed Workflows

The conversational interface of Artemis streamlines workflows and

enhances junior level analysts as well as power users. Importantly, analysts do not relinquish control. They remain in the driver's seat. Furthermore, the power of Artemis' advanced query and aggregation capabilities can be accessed via Endgame's open API, allowing power users to derive many of the benefits of Artemis as they directly access their endpoint data programmatically.



Artemis, the intelligent assistant for cyber defense

Conclusion

Intelligent assistants offer great promise to expedite security analysis and operations, save time and resources, and help strengthen defense. Artemis is capable of doing all these things, ultimately reducing the frequency and impact of significant cyber intrusion. In an accompanying post, we will dig deeper into the bot architecture, including the natural language processing, algorithms, and user experience features. If you'll be attending RSA, you can also swing by our booth #1739 and hear our talk about bots for security.

ENDGAME.

 | 3101 Wilson Blvd, Arlington, VA 22201 | 844-357-7047