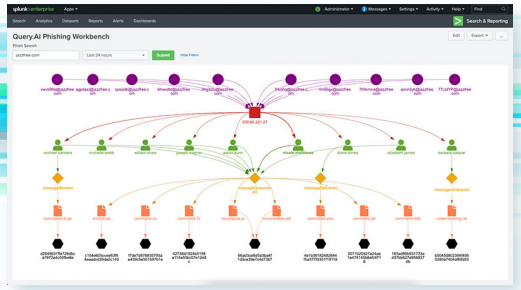
Query.ai

Datasheet

Accelerate Phishing Investigations with Query.AI Federated Search for Splunk®



Phishing threats have been around for a long time. Yet, despite existing defenses, they reach employee inboxes at an alarming rate. Phishing is so prevalent that security operations center (SOC) teams spend **23 percent of their total activity** on managing these email threats.[1]

Where is most of that time spent? **Investigations.**

In fact, nearly half (46.9%) of the time is attributed to the "swivel chair" investigation challenge of analyzing attachments, investigating senders, and identifying other recipients.[2] That's the **manual and time-consuming process** typically required to gain access and insights into crucial data located in silos across the organization.

Query.AI gives SOC teams a faster way to gather investigation entities in a single search—right from their existing Splunk console.

Product overview

Query.AI Federated Search for Splunk unlocks access to, and value from, cybersecurity data wherever it is stored, regardless of vendor or technology, **without requiring centralization**. An app that provides a new way for companies to consume the powerful Query.AI Security Investigations Platform, Query.AI Federated Search for Splunk **plugs into disparate security technologies quickly and easily using APIs**. It displays real–time and historical data in the Splunk console, empowering teams to make timely and accurate decisions on phishing investigations with high confidence in the outcomes.

Key Benefits

Access and search across data silos

Gain **real-time insights** to **decentralized data** that resides **outside the Splunk platform**, without any data movement or transfer.

Expedite phishing investigations

Visualize the relationship between phishing-related data sources to quickly assess which emails are suspicious.

Increase SOC team efficiency

Streamline investigation processes, directly within Splunk, **without ripping and replacing existing technologies**.

Retain control of the indexed Splunk data

Gain flexibility to decide to **index any returned data** to the Splunk platform.

[1] Infosec. SOCs spend nearly a quarter of their time on email security. June 2021.
[2] Ibid

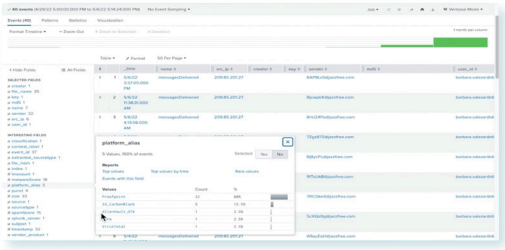
©2022 Query.AI, Inc. • All rights reserved • QDS-0003

How it works

Query.AI extends a company's Splunk platform with access to **investigate siloed data across cloud, third-party SaaS, and on-prem environments, without transferring or moving data**. With a single, federated search from within the Splunk console, security analysts get the insights they need to quickly and accurately complete their phishing investigations.

Search on data sources outside of Splunk

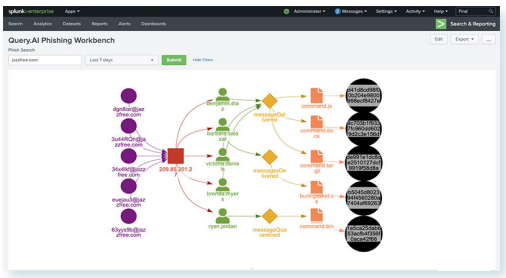
Phishing investigations can start from any threat indicator such as an alert, user submission, or MD5 hash. Using Query.AI Federated Search for Splunk, **teams can simultaneously search on the MD5 hash across multiple data sources.** Say "goodbye" to swivel chair searches.



Security analysts will gain **immediate insights** from the APIs connected to Query.AI, such as Active Directory, email security solutions, ticketing systems, endpoint protection technologies, and cloud infrastructure.

Visualize the relationship between entities

Query.AI Federated Search for Splunk enables security teams to **easily see the relationship** between phishing-related data sources. This allows them to **quickly understand** if the threat is real—and if it is quarantined or sitting in a user's inbox.



The visual map enables teams to:

- View email sources from different senders that are coming from the same gateway.
- Identify all users who received the email.
- Identify the file attachments.
- Assess which suspicious emails are quarantined or delivered.

SOCs gain **more value from the Splunk console** by enriching it with a **complete picture** of the organization's decentralized environment to **expedite phishing investigations**.

Learn More

Ready to see how Query.AI Federated Search for Splunk can **supercharge your phishing investigations**?

Request a Demo

©2022 Query.AI, Inc. • All rights reserved • QDS-0003