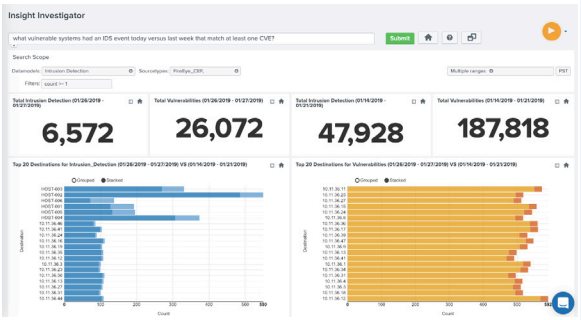
Quickly ask questions to get the insights that secure your organization.

INSIGHT INVESTIGATOR FOR SPLUNK

The Challenge

Cybersecurity teams need better ways to detect, investigate, and visualize threats. By the time an analyst creates a complex query to access their machine data, that data is already outdated. Cybersecurity leaders know they need new ways to arm everyone on their team to more quickly extract timely insights from their ever-growing data store.

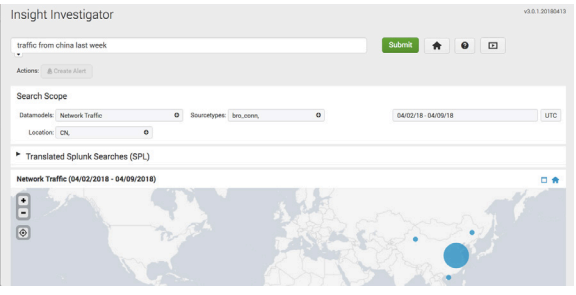
The Solution



Insight Investigator for Splunk enables people to easily ask questions of their machine data for the use cases they need. Powered by Insight Engines' unique Natural Language Processing (NLP) technology, Insight Investigator allows analysts to type their questions in plain English, (not complex data store specific query languages). Entry-level analysts can quickly add value by investigating and mitigating threats. Senior cyber-security analysts can focus on advanced threat hunting and complex query development.

Natural Language Processing

Insight Engines' NLP search technology is much more than keyword lookups from a dictionary. It is a real-time parser that examines the language within a question to understand meaning, intent, and context.



For example, Insight Investigator can understand if a search centers around location and will automatically show accompanying geo-IP maps. In seconds, it translates plain English questions to complex database queries to produce accurate results, and powerful visualizations.

The Insight Engines Advantage

Solve the Skills Gap

Junior analysts are effective on day 1 and advanced analysts are freed of mundane tasks to make the best use of their expertise.

Reduce Risk

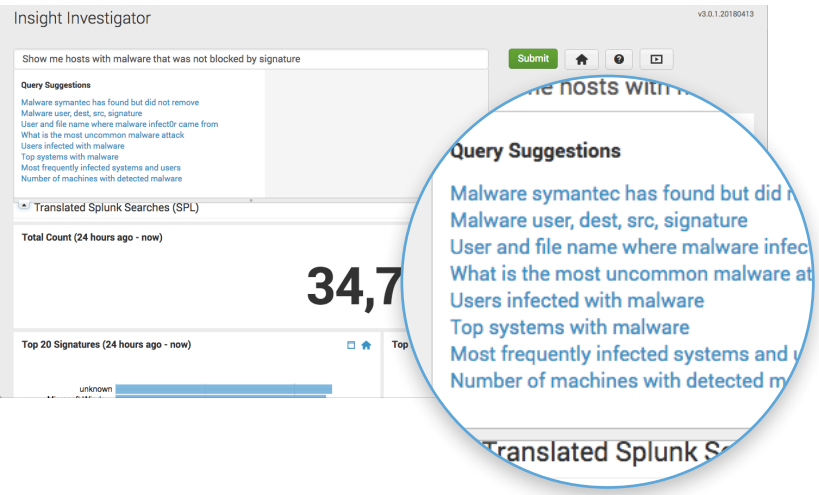
Investigate, mitigate and proactively eliminate threats beyond your SIEM.

Accomplish 10x more Every Day

Instead of spending hours crafting queries, get answers in seconds.

Right-size your data

Log what you need so your costs reflect what matters to you.

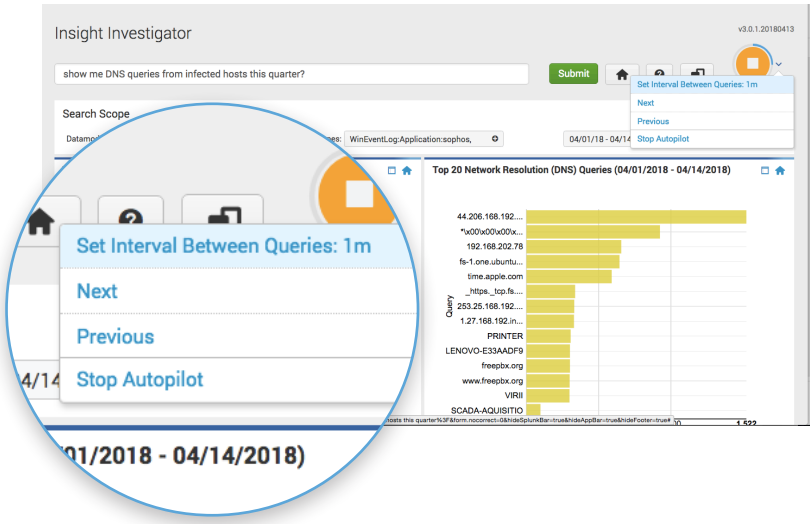


Search Recommendations

Investigator offers rich capabilities to augment security intelligence with comprehensive and relevant search suggestions via the Insight Recommendation Engine that is constantly getting smarter.

AutoPilot Insight

AutoPilot auto-asks questions of your data for you based on timely threat intelligence and common security controls to uncover previously unthought of issues outside of the standard SIEM. It is dynamic and fluid, replacing static dashboards containing outdated data and surfacing new anomalies quickly.



Technical and Installation Details

- 100% self-contained Splunk App
- Can install in minutes
- No additional hardware required
- Installs on a search head or search head cluster
- Requires only Splunk Enterprise
- Leverages Splunk Common Information Model (CIM)

ABOUT INSIGHT ENGINES

Insight Engines is the Cyber Security Investigation Platform that enables cybersecurity teams to know the data that matters, ask the questions they need and get answers to use cases at scale in seconds. With its patented natural language processing (NLP) technology, Insight Engines enables analysts to easily ask security questions from complex data. The company's products unlock the value of data by making it available, understandable, and actionable to anyone in an organization.

www.insightengines.com **sales@insightengines.com**