INSIGHT ENGINES

Cyber Security Investigator™ for Splunk™ Enterprise by Insight Engines

Natural language search for modern cyber operations

Accelerate productivity

Expand your hiring pool and accelerate your training

Enable *everyone* to accomplish more in less time (no matter how technical they are)

Generate advanced optimized SPL in real-time, *everytime*

Reduce enterprise risk

Increase accessibility and expand capabilities of your team

Spend more time hunting and less time searching

Make smarter decisions *faster*

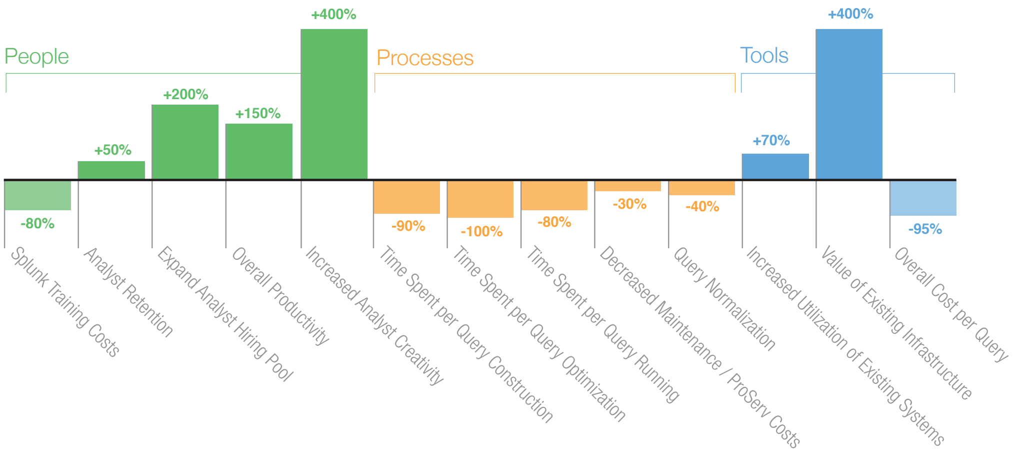
Security operations teams are drowning in machine data and strapped for people who can make sense of the signals coming from it. In today's rapidly evolving threat landscape, quickly drawing actionable insights from the data is **the key to reducing risk**.

Cyber Security Investigator (CSI) for Splunk enables your analysts at any level to harness the power of natural language search, be significantly more productive, and think strategically, as they investigate complex data. In many cases, CSI enables you to investigate over 10x faster, which reduces both the actual and potential risk to the enterprise.

Basic Query	Insight Engines Query
`tag=authentication action=failure | stats count by user | search count>=10`	`"Show users with greater than 10 failed logins"`
Query for 24hrs can take 10 minutes or more to run and requires advanced technical knowledge	Insight Engines Query can generate answers in <10 seconds with basic understanding of security concepts

Splunk Enterprise has become the nerve center of the most forward-thinking security operations teams–with Insight Engines CSI, these teams become even more agile. Teams spend less time searching and more time analyzing, as CSI fosters organic knowledge discovery through an already familiar interface.

Do More: CSI accelerates your People, Processes, & Tools



INSIGHT ENGINES

Technical requirements

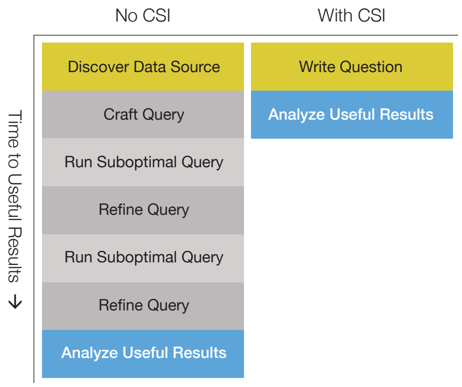
- CSI Readiness app
- Splunk Enterprise 6.3 or greater
- Splunk Common Information Model (CIM)
- Splunk Enterprise Security (optional)
- 2GB of Disk Space per Search Head

Get a Demo

Contact us to get the Insight Engines CSI Readiness App
info@insight-engines.com

Accelerate productivity

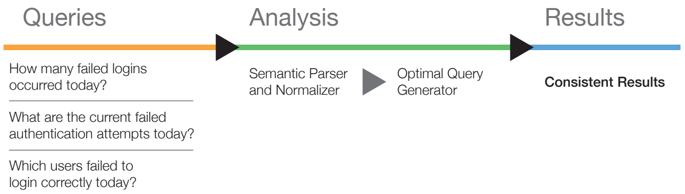
CSI is your analysts' intelligent assistant, empowering them to be more insightful and productive. It enables your team to use their words to run ad-hoc queries, explore data, and test out ideas without getting bogged down by code syntax. In seconds, it generates multiple visualizations and tables for the trained eye to examine, and simplifies the creation of custom dashboards and new alerts. This decreases training time for your new hires from months to days, as your lower-level analysts become more effective, and your higher-level analysts can mitigate more complex threats while gaining more time to hunt for new threats.



No CSI	With CSI
Discover Data Source	Write Question
Craft Query	Analyze Useful Results
Run Suboptimal Query	
Refine Query	
Run Suboptimal Query	
Refine Query	
Analyze Useful Results	

Reduce enterprise risk

With CSI, your analysts can now perform complex correlations and compare/contrast across wider time ranges, data sources, and event types than ever before. CSI translates freeform questions into highly optimized Splunk queries that would ordinarily take the most sophisticated Splunk experts hours or days to craft. By intelligently leveraging the capabilities of the Splunk query language (SPL) and built-in Splunk data model accelerations, CSI empowers everyone within your organizations to generate more meaningful results over larger data sets, with less CPU load, in a fraction of the time it takes them today. Ultimately, this enables your team to discover and mitigate existing threats faster, while providing them more time to proactively focus on new threats—thereby reducing your overall risk profile.


Queries
Analysis
Results
How many failed logins occurred today?
What are the current failed authentication attempts today?
Which users failed to login correctly today?
Semantic Parser and Normalizer
Optimal Query Generator
Consistent Results

Deploy quickly and securely

CSI is a Splunk app that deploys in hours, is currently offered on-premise, and runs 100% inside your existing Splunk deployment. Designed with the most secure and sensitive customer environments in mind, CSI does not require any new hardware, new infrastructure, or downtime of your Splunk system. It increases load by less than 1% per search, and adds less than 100 milliseconds latency at search time. After CSI is installed, your Splunk system is immediately ready.

About Insight Engines

The Insight Engines team has been building intelligence augmentation and natural language search technologies for 8 years. Insight Engines' flagship product is Cyber Security Investigator (CSI) for Splunk, which empowers your security investigation and hunting teams to more quickly and effectively mitigate serious cyber threats.

Their Investors include Google Ventures, Data Collective, several prominent angel investors, and leading security experts. It's an extremely talented team lead by CEO: Grant Wernick (Angellist, Kauffman Foundation), CTO: Jacob Perkins (NLTK Cookbook, O'Reilly's "Bad Data Handbook"), and VP of Technology: Darien Kindlund (FireEye, AWS, and MITRE). They are located in San Francisco and Washington, DC.