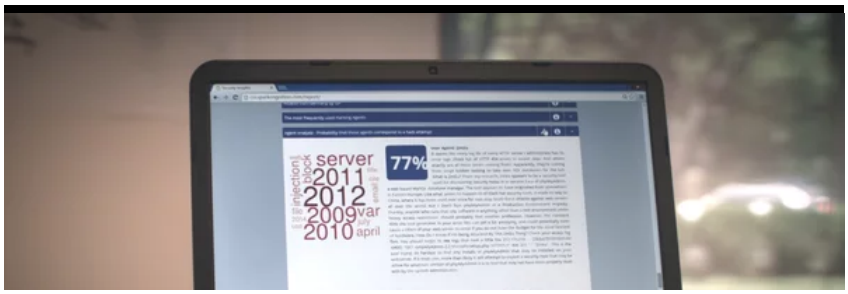
sparkcognition

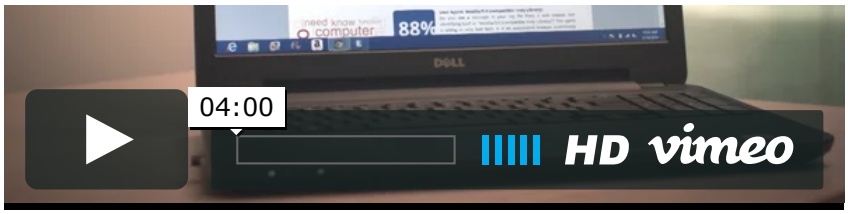
Home Products Solutions Press About Careers

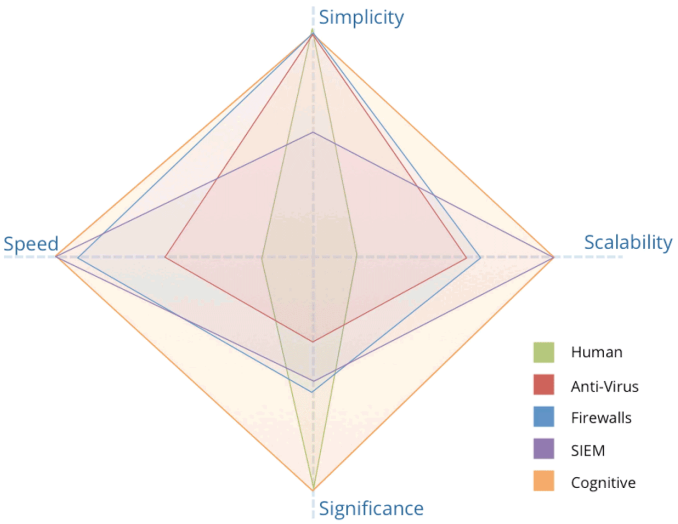
Human Intelligence at Machine Scale

SparkSecure™ Cognitive Insights add a cognitive layer to traditional security solutions, increasing the operational efficiency and knowledge



retention of your security analyst team. Essentially, Cognitive Insights does much of what a human security analyst can do, but at machine speed and Big Data scale.





We Can Identify New Attacks Automatically

With over 45,000 zero-day attacks occurring every day, solutions that rely solely on signature matching are behind the times. Literally, a threat that is brand new has no known signature, so it can't be caught by systems that simply look for signatures. Cognitive Insights does more.

Some SIEM systems claim to use machine learning, but all SIEMs still require the security analyst to do a lot of work in formulating the right queries, on the right data. But human security analysts simply can't research all threats, determine their validity and priority, and plot remediation steps. The number of false positives and SIEM tickets associated with these alerts can be overwhelming. Cognitive Insights can help.

360° Protection

- Identifies unknown, zero day attacks including insider threats
- Minimizes human errors with accurate and trustworthy information
- Delivers consistent & accurate remediation answers that can be applied consistently throughout the environment

Reduces costs associated with security teams

- Reduces time to close a SIEM ticket through automated research
- Minimizes the number of tickets to close/research
- Scales security admins research capabilities via in-context advice

Improves knowledge retention

- Watson trained on “tribal” knowledge reduces impact of attrition

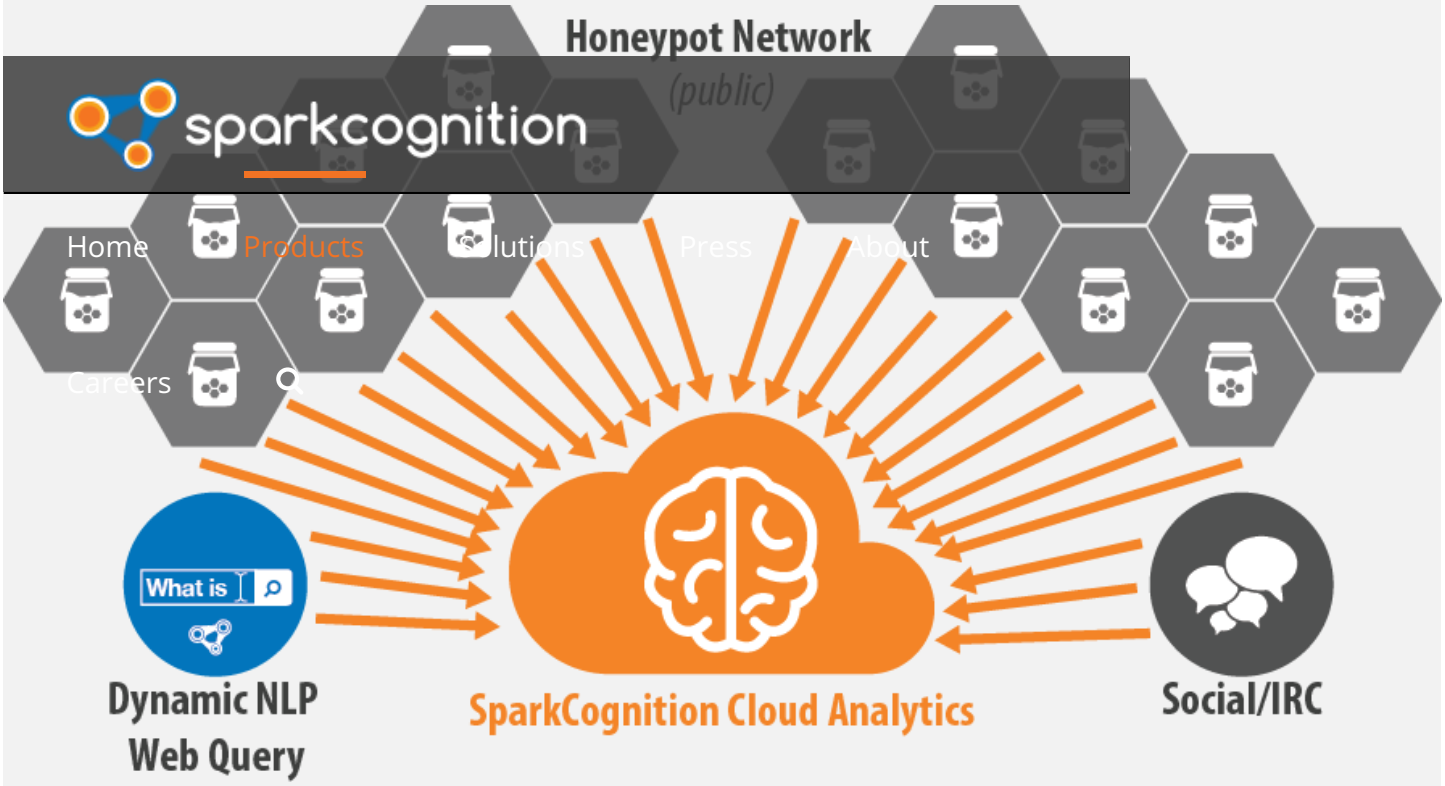
Improves operational efficiencies via predictive analytics

- Helps with capacity planning by anticipating security related volumes
- Free up capacity currently used to serve unwarranted traffic / scan requests

How Do Cognitive Insights Work?

Cognitive Insights works by collecting massive amounts of structured and unstructured data and applying patent-pending machine learning and AI algorithms to find trends,

patterns and anomalies. We call it Automated Signature Construction. And while Cognitive Insights knows about existing signatures that weed out easily identifiable threats, it looks beyond these to threat **behavior** to determine if something out of the ordinary is happening.



Predictive Threat Intelli

Cognitive Insights doesn't just look at your logs. It aggregates threat intelligence from the web and data from our own Cognitive Security Repository to constantly identify emerging types of attacks. Patent-pending "Cognitive Fingerprinting" machine-learning algorithms learn from this curated data. Starting from this vast base of knowledge, Cognitive Insights analyzes activity from your

When the Shellshock bash shell vulnerability manifested in HTTP request data coming in to SparkCognition's Cognitive Security Repository, heuristics identified these inbound requests to be malicious. Once the HTTP request was tagged appropriately, the sequence of characters used to execute arbitrary executables was catalogued and developed into a

logs to identify never before seen threats, and predict future attack trends for your assets.

signature.

Automated Research, Prioritization, and Remediation

Once threats are identified, they are automatically researched using a variety of techniques to reduce false positives. Each researched threat is also given a score to help your security analysts prioritize their efforts. Then, defensive strategies to protect against these threats are generated and delivered in the form of immediately applicable Linux security configuration, including web server policies, remote login policies and more. As attacks unfold on the open internet, additional insights are developed and used to constantly adapt and improve policies and rules.

In-Context, Conversational Advisory via IBM's Watson

SparkCognition has trained Watson on a large corpus of security content and relevant product data, transforming Watson into an intelligent advisor that draws from trusted literature to protect customers against diverse threats. Your security analysts simply query Watson using natural language and Watson provides – not a set of results – but an **answer**. Our capabilities combined with IBM Watson yield a perpetually evolving and learning, virtual security expert within your virtual machines, your physical servers and cloud instances. Better yet, Watson will never find a new job or get hit by a bus. The knowledge acquired stays within your company forever.

We do Hybrid Clouds!

SparkSecure can be delivered as a cloud service or an on-premise application

PRODUCTS

SparkPredict™

SparkSecure™

MindFabric™

SOLUTIONS

Oil and Gas

Utilities

Information Technology

RECENT POSTS

SparkCognition Announced as the Only US-Based Winner of the 2015 Nokia Open Innovation Challenge

Forecasters.org/Foresight

Can Cognitive Computing Solve Cyber Security Challenges?

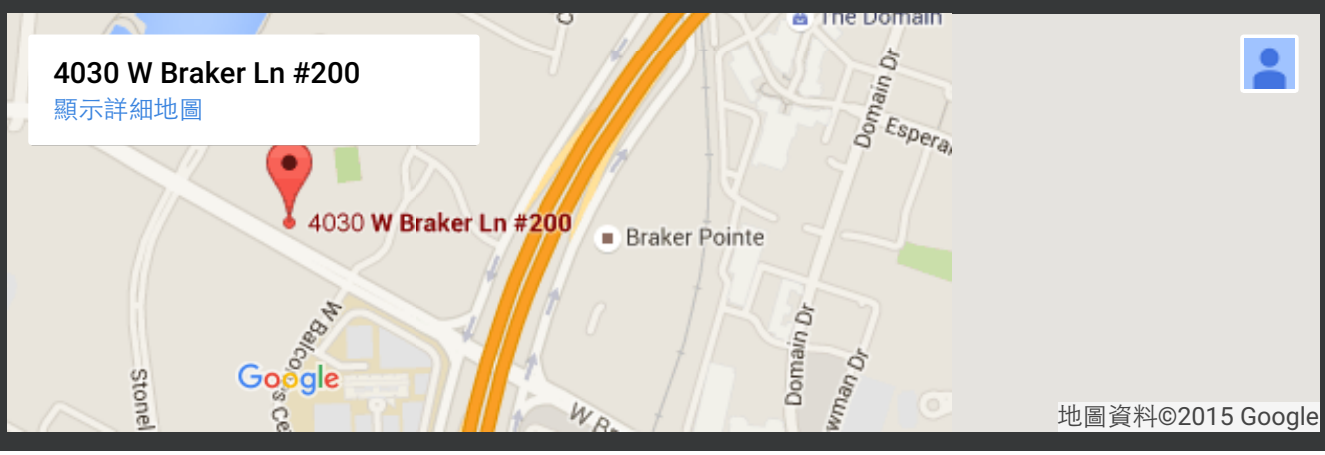
A case for machine inspection

The gloves are off in the US-China Cyberwar

RECENT TWEETS

Holiday party twice the size of last year. Twice as much to be thankful for! https://t.co/cEwZk2si7y
5 days ago

Let Sympathy Lead to Action (https://t.co/eIsF4CsPJs)
6 days ago



4030 W. Braker Lane
Suite 200
Austin, Texas, 78759
Email: info@sparkcognition.com
Web: www.sparkcognition.com