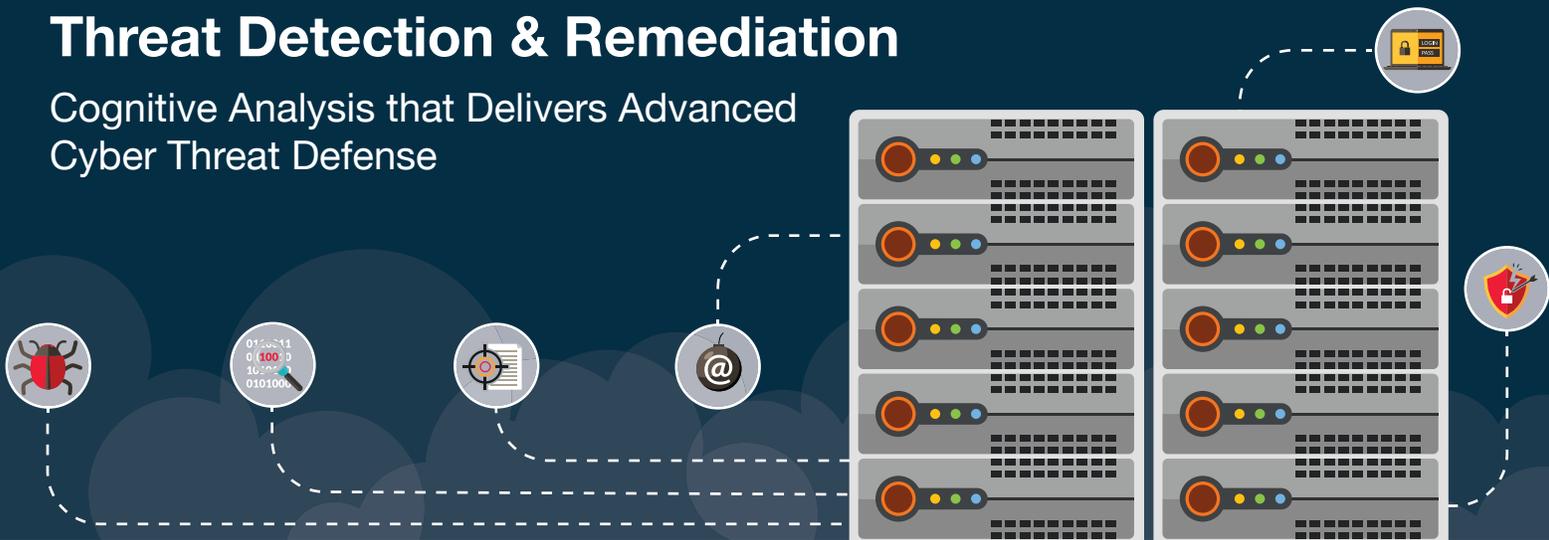# sparksecure

# Threat Detection & Remediation

Cognitive Analysis that Delivers Advanced
Cyber Threat Defense

SparkSecure is world's first cognitive security analytics solution capable of adding a cognitive layer to traditional security solutions. This increases the operational efficiency and knowledge retention of your security analyst team. SparkSecure does much of what a human security analyst can do, but at machine speed and Big Data scale.

### Machine Learning Anti-Virus
Signature Free file analysis method analyzes the DNA of every file to identify potential malicious intentions
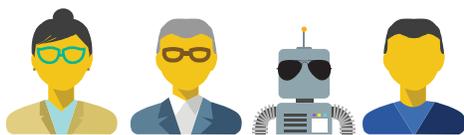
### Bot Detection
Advanced algorithms identify unlabeled bots capable of hogging bandwidth and exploiting vulnerabilities

### Data Querying
Hadoop back-end capable of searching through Petabytes of data in a matter of seconds

## Drawing Insights From Big Data

SparkSecure brings big data and global trends to your door by collecting information from Honeypots around the world. These Honeypot systems, acting much like the canary in a coal mine, sit on the web and analyze the ways in which new attacks try to compromise existing information systems. SparkSecure then ingests these new threat vectors and continuously learns and adapts to catch abnormal activities, malicious traffic, and attacks seeking to exploit a system.

## Predictive Threat Intelligence

SparkSecure identifies emerging attacks the same way a human would, using a suite of advanced machine-learning pipelines. These algorithms look at log data, such as firewall or web logs, and aggregate threat intelligence from the web, view the DNA of downloaded files, and analyze user behaviors to find compromise within a system. Best of all, SparkCognition's patent-pending "Cognitive Fingerprinting" algorithms remember these patterns and adapt to this curated data.

## Automated Research, Prioritization, & Remediation

Threats are automatically researched using a variety of techniques to reduce false positives. Each researched threat is given a score to help your security analysts prioritize their efforts. To further help, SparkSecure also contains the largest security corpus ever ingested into IBM Watson. Analysts can use in-context advisory tools to easily view additional information from malware encyclopedias, policy manuals, and knowledge bases to remediate every threat.