6-19-15

Response from Splunk Inc. to Request for Information for the Federal Cybersecurity R&D Strategic Plan

Splunk appreciates the opportunity to provide input in response to the request for information (RFI) for the Federal Cybersecurity R&D Strategic Plan.

The RFI includes a question about innovative, transformational technologies that have the potential to enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure.

In response to this question, Splunk notes that big data analytics is a transformational technology for cybersecurity. Advanced threats have permanently changed how organizations think about cybersecurity. It is no longer enough to monitor for known threats or to rely solely on security point products that provide a narrow view. Security teams need an infrastructure-wide view of activities in order to identify, understand, and stop attackers.

There are four classes of data that security teams need to leverage for a complete view: network data, endpoint data, threat intelligence, and access/identity data. If any of these data types is missing, there is a higher risk that an attack will go unnoticed. These data types are the building blocks for knowing what is normal and what is not in an organization's environment. Addressing cyber threats requires a big data approach that:

- Will scale to collect tens of terabytes of data per day without normalization at collection time and applies a schema to this data only at search (query) time.
- Can access data anywhere in the environment, including traditional security data sources, personnel time management systems, HR databases, industrial control systems, Hadoop data stores, and custom enterprise applications.
- Delivers fast time-to-answer for continuous monitoring, threat detection, incident response, and forensic analysis.

Big data technologies are already playing an important role in helping government agencies and companies to improve cybersecurity. There are, however, aspects of the big data analytics approach that could be improved through federal R&D. Two examples are:

- Connecting the dots from massive, disparate data sources like networks, endpoints, and business applications to detect cyber threats.
- Detecting advanced threats by analyzing the scope and impact of compromised systems.