1126-68-211 **Ben Greco*** (bgreco@soteria.io), Soteria, LLC, P.O. Box 22572, Charleston, SC 29403, and
Nel Abdiel (nabdiel@soteria.io), Soteria, LLC, P.O. Box 22572, Charleston, SC 29403.
Products, Challenges, and Solutions Related to Data Analytics in Cyber Security Consulting.

Soteria is a cyber security consulting company based in Charleston, SC. We seek to leverage large-scale data analytics and machine learning to create value through automating tasks typically done by expensive security consultants. Our solutions include multiple security software products that work alone or in tandem with veteran consultants by augmenting their knowledge with automatic recognition and analysis of security events and indicators. Due to the complex nature of cyber security, effective event recognition and diagnosis has many challenges. Chief among these are high false positive rates, setting proper thresholds to detect malicious events, processing large amounts of data in near real time, and storing and accessing data in a massively scalable way while still allowing for full text search. We will discuss several ways we address these analytics challenges to provide value to clients. (Received January 16, 2017)