Industry Practice Expo Invited Talk

Cyber Security - How Visual Analytics Unlock Insight

Raffael Marty
Pixlcloud
raffy@raffy.ch

ABSTRACT

In the Cyber Security domain, we have been collecting 'big data' for almost two decades. The volume and variety of our data is extremely large, but understanding and capturing the semantics of the data is even more of a challenge. Finding the needle in the proverbial haystack has been attempted from many different angles. In this talk we will have a look at what approaches have been explored, what has worked, and what has not. We will see that there is still a large amount of work to be done and data mining is going to play a central role. We'll try to motivate that in order to successfully find bad guys, we will have to embrace a solution that not only leverages clever data mining, but employs the right mix between human computer interfaces, data mining, and scalable data platforms.

Traditionally, cyber security has been having its challenges with data mining. We are different. We will explore how to adopt data mining algorithms to the security domain. Some approaches like predictive analytics are extremely hard, if not impossible. How would you predict the next cyber attack? Others need to be tailored to the security domain to make them work.

Visualization and visual analytics seem to be extremely promising to solve cyber security issues. Situational awareness, large-scale data exploration, knowledge capture, and forensic investigations are four top use-cases we will discuss. Visualization alone, however, does not solve security problems. We need algorithms that support the visualizations. For example to reduce the amount of data so an analyst can deal with it, in both volume and semantics.

Categories and Subject Descriptors

H.2.8 [Database Management]: Data Mining.

General Terms

Algorithms, Performance

Keywords

Cyber Security, Data Visualization.

Bio

Raffael Marty is one of the world's most recognized authorities on security data analytics. The author of Applied Security Visualization and creator of the open source DAVIX analytics platform, Raffy, is the founder and CEO of PixlCloud, a next-generation data visualization application for big data. With a track record at companies including IBM Research and ArcSight, Raffy is thoroughly familiar with established practices and emerging trends in data analytics. He has served as Chief Security Strategist with Splunk and was a co-founder of Loggly, a cloud-based log management solution. For more than 12 years, Raffy has helped Fortune 500 companies defend themselves against sophisticated adversaries and has trained organizations around the world in the art of data visualization for security. Practicing zen has become an important part of Raffy's life.

KDD'13, August 11–14, 2013, Chicago, Illinois, USA.
ACM 978-1-4503-2174-7/13/08.