RuleBreaker: Categorical Correlations as Probabilistic Rules

Nathan Danneman

January 17, 2020

Acknowledgements

Big thanks to:

- BSides Asheville
- Data Machines (www.datamachines.io)
- Uncle Sam

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Outline

1. "Big data" and analytics for cyber defense
2. RuleBreaker: how it works
3. RuleBreaker: security relevance, use cases
4. Next steps, etc.

IF lunch time THEN not too many questions?

nathandanneman [at] datamachines [dot] io