Brennan Lodge
lodge.brennan@gmail.com

Employer and/or affiliations.
Goldman Sachs, Head of Data Science for SIRT

Brennan is a self-proclaimed data nerd. He has been working in the financial industry for the past 10+ years and is striving to save the world with a little help from our machine friends.

He has held cyber security, data scientist, and leadership roles at JP Morgan Chase, the Federal Reserve Bank of New York, Bloomberg, and Goldman Sachs. Brennan holds a masters' degree in Business Analytics from New York University and participates in the data science community with his non-profit pro-bono work at DataKind, and as a co-organizer for the NYU Data Science and Analytics Meetup.

Brennan is also an instructor at the New York Data Science Academy and teaches data science courses in R and Python.

Any significant presentation and educational experience/background.
https://www.kuppingercole.com/sessions/3498

Evaluating cybersecurity defenses with a data science approach
https://conferences.oreilly.com/strata/strata-eu-2019/public/schedule/speaker/334217
https://houseofbeautifulbusiness.com/bio-brennan-lodge

Topic synopsis, Proposed paper title, and a one paragraph description.
Machine Learning Detection as a Service

SOC analysts are under siege to keep pace with the ever-changing threat landscape. The analysts are overworked, burnout and bombarded with the sheer number of alerts that they must carefully investigate. This intense workload can be a true testament against anyone’s patience. We need to empower the Security Operations Center (SOC) analysts with data science implementations to overcome this monotonous work that is leading to career burnout. Security departments should be seeking data-driven approaches for more efficient evaluations on operations. Data Science use cases like detection rule scoring and DGA detection through machine learning are example implementations with immediate value add. With this insight security engineers, management and analysts alike can be empowered to make data driven decisions to tune and lessen the burden on the SOC from investigating fewer false positive related cases.

Reason why this material is innovative or significant or an important tutorial:

Current open source tool for detecting DGAs via machine learning - https://blodgic.com

There is a lot of hype in using AI in cyber security. My presentation will clear the air on a realistic machine learning implementation in an enterprise environment. As a lightning talk alternative, I can demo how to use a machine learning model to detect DGAs (domain generating algorithms)