



## Evaluating cybersecurity defenses with a data science approach

**Brennan Lodge**

*Data Scientist, Goldman Sachs, United States.*

### Abstract:

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.

### Biography:

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.



### Publication of speakers:

1. Murphy, Sean & Lodge, G.M. & Brennan, M.A.. (2010). Tropical grasses capture winter rainfall. Proceedings of the 25th Annual Conference of the Grassland Society of NSW. 137-140.
2. Tennant, D & Hall, David. (2001). Improving water use of annual crops and pastures - Limitations and opportunities in Western Australia. Australian Journal of Agricultural Research. 52. 171-182. 10.1071/AR00005.
3. Culvenor, R. & Boschma, Suzanne. (2005). Evaluation of phalaris (*Phalaris aquatica* L.) germplasm for persistence under grazing on the North-West Slopes, New South Wales. Crop and Pasture Science. 56. 731-741. 10.1071/AR04300.
4. Dolling, Perry. (2001). Water use and drainage under phalaris, annual pasture, and crops on a duplex soil in Western Australia. Crop and Pasture Science. 52. 305-316. 10.1071/AR99167.

[International Conference on Ethicalhacking and Cybersecurity | May 21, 2020 | London, UK](#)

**Citation:** Brennan Lodge; Evaluating cybersecurity defenses with a data science approach; Cyber Security 2020; May 21, 2020; London, UK