bayes

Sensitivity and specificity
https://en.wikipedia.org/wiki/Sensitivity_and_specificity

Qsf – a small fast accurate spam filter
https://acampbell.uk/wp/2019/04/11/a-small-fast-accurate-spam-filter/

Quick Spam Filter
http://www.ivarch.com/programs/qsf/

spam-filter
https://github.com/topics/spam-filter

heuristics

Artificial intelligence
https://en.wikipedia.org/wiki/Artificial_intelligence

Machine learning
https://en.wikipedia.org/wiki/Machine_learning

Training dataset
https://en.wikipedia.org/wiki/Training,_validation,_and_test_sets#Training_dataset

Deep learning
https://en.wikipedia.org/wiki/Deep_learning

Artificial neural network
https://en.wikipedia.org/wiki/Artificial_neural_network

Neural Networks
https://www.ibm.com/cloud/learn/neural-networks

Basic Concepts of Neural Network
http://sciencious.com/basic-concepts-of-neural-network/

Neural Network
https://www.investopedia.com/terms/n/neuralnetwork.asp

Simple Neural Network from Scratch
https://medium.com/swlh/simple-neural-network-from-scratch-130b175eb1e6 –> LAB

Artificial neural network model to predict transport parameters of reactive solutes from basic soil properties☆
https://www.sciencedirect.com/science/article/abs/pii/S0269749119312631

Exploring Weight Agnostic Neural Networks
https://ai.googleblog.com/2019/08/exploring-weight-agnostic-neural.html

products

counterflow-ai / dragonfly-mle
https://github.com/counterflow-ai/dragonfly-mle

research

ANDREW FAST
https://resources.sei.cmu.edu/library/author.cfm?authorid=512133

ERIC LEBLOND
https://resources.sei.cmu.edu/library/author.cfm?authorid=449885

Using Triangulation to Evaluate Machine Learning Models
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=539582

VILHELM GUSTAVSSON, Machine Learning for a Network-based Intrusion Detection System
PDF - FULLTEXT01.pdf

Improving quality control by early prediction of manufacturing outcomes
https://dl.acm.org/doi/10.1145/2487575.2488192 –> Baseman et al. SIGKDD Workshop 2016

Prediction of wind pressure coefficients on building surfaces using Artificial Neural Networks
https://www.researchgate.net/figure/Artificial-neural-network-architecture-ANN-i-h-1-h-2-h-n-o_fig1_321259051

honey

Honeypot
https://www.honeynet.org/category/honeypot/

Chapter 5 - Honeypotting
https://www.sciencedirect.com/science/article/pii/B9781597493055000050

honey products

LaBrea: “Sticky” Honeypot and IDS
http://labrea.sourceforge.net/labrea-info.html

Best Honeypots for Detecting Network Threats
https://securitytrails.com/blog/top-20-honeypots

Open Source Honeypots That Detect Threats For Free
https://www.smokescreen.io/practical-honeypots-a-list-of-open-source-deception-tools-that-detect-threats-for-free

Open Source Honeypots: Learning with Honeyd
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=92ad63dd-a90f-4375-9015-ca74b19d1faa

Honeyd: The open source honeypot
https://www.infoworld.com/article/2624595/honeyd--the-open-source-honeypot.html

OWASP Honeypot
https://owasp.org/www-project-honeypot/

OWASP Honeypot: open source software for creating honeypot and honeynet
https://securityonline.info/owasp-honeypot/

hardinfra

5 Tools to Scan a Linux Server for Malware and Rootkits
https://www.tecmint.com/scan-linux-for-malware-and-rootkits/

staffan / unblacklist
https://git.shangtai.net/staffan/unblacklist

ids

Network intrusion detection system
https://patents.google.com/patent/US20100251370A1/en

Using decoys by a data loss prevention system to protect against unscripted activity
https://patents.google.com/patent/US8549643B1/en

things to assist in packet analysis
https://github.com/noahdavids/packet-analysis/blob/master/README.md

Taxonomy and Survey of Collaborative Intrusion Detection
https://dl.acm.org/doi/10.1145/2716260

Snort 2 DCE/RPC Preprocessor Buffer Overflow
https://www.rapid7.com/db/modules/exploit/multi/ids/snort_dce_rpc

community rules

Snort Rule for the Bluekeep Module in Metasploit
https://medium.com/@alexandrevvo/snort-rule-for-the-bluekeep-module-in-metasploit-17613066915d

span / port-mirror

RSPAN and 2950 switches
https://community.cisco.com/t5/other-network-architecture/rspan-and-2950-switches/td-p/353667

Configuring Local SPAN, RSPAN, and ERSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.pdf

Configuring SPAN and RSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swspan.pdf

Understanding SPAN,RSPAN,and ERSPAN
https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951

Configuring Local SPAN, RSPAN, and ERSPAN
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.pdf

videos

USENIX Enigma 2016 - The Golden Age of Bulk Surveillance
https://www.youtube.com/watch?v=zqnKdGnzoh0

USENIX Enigma 2017 — StreamAlert: A Serverless, Real-time Intrusion Detection Engine
https://www.youtube.com/watch?v=QVtzMy_tNcQ

USENIX Enigma 2018 - Some Thoughts on Deep Learning and Infosec
https://www.youtube.com/watch?v=i76E6tvey_M

USENIX Enigma 2017 — Classifiers under Attack
https://www.youtube.com/watch?v=XYJamxDROOs