George M Jones

<gmj@port111.com>, 540-272-7468
https://www.linkedin.com/in/georgemjones/

Summary

My **professional objective** is to apply my experience in cloud computing, data engineering, data analysis, software development, machine learning and security to build, deploy and operate reliable systems that serve the needs of people.

Recent Problem Solving:

Threat Feed Acquisition and Ingest While at AWS, I was listening to a presentation at the USENIX Security Symposium, and realized that a threat feed being described would be useful for protecting ourselves and our customers. I talked to the presenter after the talk, stayed in touch, obtained access to the feed and wrote an automatd ETL process to load it nightly. It has helped detect infected systems.
Splunk Application Development Redjack was tasked with developing and deploying solutions to a restrictive customer environment. I created a process for packaging required functionality as a Python PEX file inside a custom Splunk search application. We can now deliver solutions and are leveraging this to meet specific customer requirements.
Large Scale Spark ETL Redjack network sensors currently generate over 5 terabytes of data per day for our largest customer. This data can be used to answer ad-hoc operational and security questions, but the volume makes that impossible using traditional tools on even the largest instance types. To address this problem I drove an evaluation of Databricks Spark on Azure, developed two iterations of an ETL process, prototyped analytic queries, and brought analysts up to speed on the platform. As a result, we are now able to answer ad-hoc queries for our customer across large volumes of data.

Experience includes **cloud platforms** (AWS, Azure, Google Cloud, VMWare, Docker), **data/database engineering** (Databricks/Spark, SQL, ETL, Redshift, Athena, BigQuery, Hadoop) **data analysis tools** (Jupyter, Zeppelin, Pandas, Splunk) **analytic development**, **software development** (Python, shell, Scala, Rust, Perl, C, Go, git, others), **open source software development and project coordination** (Router Audit Tool [WS03]), **standards development** (IETF,RFC3871 [Jon04] [Jon03]), **conference chair** (FloCon 2013 [GJ13], 2014 [GJ14]). **research** [JS14], **training development and delivery** (Network profiling [JW12]), **product evaluations**, **operational network security support** (router security, flow analysis, tooling, firewalls)
Positions have included *Senior Cyber Research Engineer*, Expanse (6/2020-present) *Data Scientist*, RedJack (6/2017-6/2020), *Senior Security Engineer*, Amazon AWS (1/2016-6/2017), *Senior Network Security Engineer*, AOL *Verizon (11/2014-12/2015), /Senior MTS*, CERT Carnegie-Mellon University, (2/2011-11/2014), *Lead Information Systems Engineer*, MITRE (3/2003-1/2011), *Network Security Engineer*, UUNET, *Information Security Architect*, BankOne, *Internet Applications Architect*, CompuServe.
Education BS, Computer and Information Science, The Ohio State University. Graduate work in Computer and Information Science, The Ohio State University. Online courses in Machine Learning.
Clearance and Certifications Active TS (10/2018), GIAC GSEC (12/2018)

Selected Publications and Citations

References

[GJ13] Program Chair George Jones. Flocon. In *"FloCon 2013"*, Pittsburgh, PA, USA, 2013. CERT. `https://resources.sei.cmu.edu/news-events/events/flocon/past-conferences.cfm`, Accessed: 2020-02-06.

[GJ14] Program Chair George Jones. Flocon. In *"FloCon 2014"*, Pittsburgh, PA, USA, 2014. CERT. `https://resources.sei.cmu.edu/news-events/events/flocon/past-conferences.cfm`, Accessed: 2020-02-06.

[Jon03] George Jones. Knobs, Levers, Dials and Switches: Now and Then (please sir, may I have some more ?). In *Proceedings of NANOG 29*. NANOG, October 2003. `http://port111.com/george/pubs/2003-Jones-NANOG.pdf`, Accessed: 2014-07-29.

[Jon04] G. Jones. Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure. RFC 3871 (Informational), September 2004. `http://www.ietf.org/rfc/rfc3871.txt`, Accessed: 2013-04-06.

[JS14] George Jones and John Stogoski. ALTernatives to Signatures (ALTS). In *CERT/CC Whitepaper*. CERT, April 2014. `http://port111.com/george/pubs/2014-Jones-Stogoski-ALTS.pdf`, Accessed: 2014-07-29.

[JW12] George Jones and Austin Whisnant. Network Profiling with SiLK. In *FloCon 2012 Proceedings*, Pittsburgh, PA, USA, 2012. CERT. `http://port111.com/george/pubs/2012-Jones-Whisnant-FloCon.pdf`, Accessed: 2014-07-29.

[WS03] Joshua L Wright and John N Stewart. *Securing Cisco routers*. SANS Institute, 2003. `http://www.amazon.com/Securing-Cisco-Routers-Step-Step/dp/0972427333`.