Jason Sherman, CSSLP, GPCA, Logical Software Solutions
jsherman@logicalsoftware.co

EDUCATION & TRAINING

- BS, Software Engineering [Summa Cum Laude], Colorado Technical University, May 2006
- AAS, Criminal Justice, Community College of the Air Force, November 2003
- AAS, Electronic Systems Technology, Community College of the Air Force, August 1995
- Self-directed projects and online courses spanning all popular languages and technologies

CERTIFICATIONS

- $(ISC)^2$ CSSLP, 389654, Oct 2014
- $(ISC)^2$ CISSP, 389654, Mar 2012
- Google Cloud Professional – Architect, 2020

QUALIFICATION HIGHLIGHTS

Secure software development life-cycle, Node / Javascript, Java, Python, shell, NiFi, Redis, Elasticsearch, postgres. mentor

TECHNICAL SKILLS & EXPERTISE

Systems:	Linux (OpenSUSE, CentOS, Debian, RHEL), Windows
Languages:	Java, Python, C++ 99/11, javascript
Software:	Intellij, JBoss, GlassFish, Tomcat, VMWare workstation and ESXi

Logical Software Solutions, LLC **09/2016 – Present**
Owner

- **Technologies**: Java 6/7/8, AWS/AC2SP, NiFi, Security Onion, Squert, Sguil, Spark, Hadoop
- **BzzyBoard, 03/2020 – Present**
  - Envisioned, designing, and developing hyper-local social, family oriented, social app
  - Designed for Google firebase and Google Cloud with full CI/CD pipelines
- **Iron EagleX, 06/2019 – 05/2020**
  - Porting security tracking application to AC2SP, the Army cloud implementation
  - Provided analysis on feasibility of implementing prior contractor's application in cloud
- **D4C Global, 05/2017 – 04/2018**
  - Partnered to design and implement custom intrusion detection systems to identify nefarious activity on high net worth clients' home networks
  - Provided weekly summaries and monthly reports with actionable intelligence
  - Implemented software to automate mundane analytic tasks, such as IP correlation
- **DARPA, 09/2016 – 05/2017**
  - Worked with data scientists to developed pseudo random number detector using five of Dr. Donald Knuth's algorithms (frequency, serial, gap, poker, run)
  - Developed with latest Java streaming and functional programming techniques
  - Runs on multi-billion row tables with minimum resource requirements (5B rows / 3 min)
- **Zapata Technologies, 09/2016 – 05/2017**
  - Consulted and developed for NiFi projects to ingest data from legacy systems
  - Developed custom NiFi processors to parse streaming data (NiFi 1.0+)
  - Developed simple REST server to allow testing of NiFi flows

Mantech International **05/2019 – Present**
Software Engineer, Sr. Principal

- **Technologies**: Javascript, Vue/Vuetify, Python 2/3, Java, NiFi, Postgres, Redis
- Lead engineer, managing four engineers across three projects and two distant locations
  - My combination of technical and soft skills have developed a team recognized by our customer's and company's leadership as high performing and highly motivated
- Envisioned, designed, developed, and maintain the CyberLab application
  - Helps manage deployed assets, and provides error, state, and processing information
  - Created grok developer application to easily integrate unique logs into NiFi flow
- Ported outdated logfile processing to NiFi using custom, modified, and built in processors
  - Developed several custom NiFi processors and integrated into flows of 100GBs daily
  - My initial flow design reduced overloaded daily processing from 24+ hours to 3 hours
- Refactored and implemented unit tests for already built custom python tools
- Supports network and system engineers in t/s issues related to new technology implementation

Invictus International Consulting, LLC **09/2017 – 05/2019**
Web Developer

- **Technologies**: ES6, AngularJS, Vue/Vuex, D3, Karma, Jasmine, Selenium, ElasticSearch
- Technical lead for development of Business Intelligence Engine
    - Researched viability and capability of using Vue/Vuex for analytic engine redesign
    - Led software architecture design and implementation, championed consistent testing, performed code reviews, provided feedback and guidance to junior engineers
- Developed and maintained UI tools and features for Business Logic Data Warehouse
    - Refactored major components to improve maintainability and ease of modification
    - Championed and incorporated Selenium/Protractor automated tests
    - Improved graph display to include pivot chart and element highlighting
    - provided bug fixes back to original OSS authors of angular-json-tree module

CACI (L-3 NSS/Data Tactics Corporation) **08/2015 – 08/2016**
Sr. Software Engineer

- **Technologies**: Java 6/7/8, Spark, NiFi, Accumulo, Hadoop, TDF
- Developed and maintained analytics systems for DARPA that enabled detection and mitigation of advanced network security threats
- Developed single point of entry script to enabled end-to-end run of complex analytic algorithms
- Developed and maintained ingest capabilities for the Tactical Cloud Reference Architecture
- Developed custom NiFi processors to parse streaming data (NiFi 0.2 / 0.3)
- Used TDF/Jblocks classification API to verify format and adherence to marking standards

Pragmatik IO Solutions, LLC **04/2015 – 07/2016**
VP Engineering / Technical Lead

- **Technologies**: Python, Docker, Ansible, Taiga, Software defined networks
- Led geographically separated team of 10 software and hardware engineers to develop disruptive network monitoring defense system; Created harmony and focus of purpose within team
- Solidified ambiguous requirements into demonstration alpha product for investors

Anavation LLC **04/2015 – 08/2015**
Software Engineer

- **Technologies**: Java 6/7, Python, Accumulo, Hadoop, TDF, JBlocks
- Developed API to convert incoming messages into trusted data format (TDF) XML
- Used Jblocks classification API to verify format and adherence to marking standards

Data Tactics Corporation **07/2010 – 04/2015**
Sr Software Engineer

- **Technologies**: Java 6/7, Python, Accumulo, Hadoop, Storm, NiFi, ActiveMQ, Jboss, custom built wireshark/tshark, Linux, Javascript
- Developed, Evangelized and implemented secure development practices using industry standard tools and techniques; Atlassian toolset, static and dynamic analysis, TDD, scrum, sprint reviews
- Redesigned/refactored natural language processing module for cutting edge big data solutions for commercial, USG, and DoD; cleaned up code, sped up, and added significant testing
- Provided professional services to a partner company for time critical ground up design and engineering of new advertising tracking system
- Principal architect for document ingest system of Defense Cross Domain Analytic Capability II (DCAC-II) based on very fluid customer requirements
- Integrated enterprise security labeling system with another project by porting capabilities to Storm, NiFi, and their custom ingest solution; provided additional support as needed

- Developed python wrapper to automate ingest of etherpeek formatted network captures
    - Built custom wireshark to enable multithreading and other performance enhancements
    - Script supports entire set of tshark display filters and protocol fields
- Wrote behavior driven development tests for Ruby on Rails ExUmbra project

Mantech International **07/2009 – 06/2010**
Cyber Counterintelligence Analyst / Forensic Engineer/Software Tester

- **Technologies**: Nessus, NetWitness, EnCase
- Developed honeypot operation to enhance enterprise security for national level agency
- Performed intrusion investigations, vulnerability assessments, computer forensics, and penetration testing using Nessus, NetWitness, EnCase, and custom Linux and Windows tools
- Developed portable process in Python to integrate automated software testing on hardware with virtual machine provisioning system. Doubled test coverage and enabled testing on arbitrary Windows OSes
- Developed fully automated virtual machine guest OS update process
- Tested and analyzed software faults and provided critical information to kernel development team

United States Air Force **01/2002 – 07/2009**
Special Agent, Air Force Office of Special Investigations
Computer Crimes Investigator
AFOSI Liaison to the National Cyber Investigative Joint Task Force

- **Technologies**: EnCase, iLook, Logicube, shell scripting, wireshark, Palantir, Analysts Notebook, Honeypots, custom network monitoring tools and equipment
- Led 10 person cyber investigations team; acting Branch Chief during 6 month deployment of leadership; responsible for all Air Force cyber assets in 18 state region of eastern United States
- Briefed senior-level executives at DoD, FBI, CIA, HQ USAF, AFOSI and other agencies on status of complex national security operations and investigations being run through the NCIJTF
- Led Threat Focus Cell team of 40 senior and technical personnel from USG and DOD, developed novel network operations concept against APT actors
- Deployed to Iraq from March-September 2004 as EDET 2409 Superintendent at Tallil AB

United States Air Force **09/1989 – 01/2002**
Ground Radio Maintenance Technician

- Led multiple tactical communications teams, ranging in size from 4 to 10 personnel
- Routinely improved mission capable rates with minimum cost to unit
- President of squadron Top IV; led fund drives, community service, and squadron activities
- Volunteered for deployment taskings within and outside of career field
- Fully qualified on dozens of communications systems, small and large

Personal Projects

- **Technologies**: Python, C++, Kafka, Storm
- Continuous education through self-directed projects and online courses
- Developed C++ based sudoku solver problem as learning tool for new C++ 11/14 standards; exploring unit testing, multithreading, and concurrency in C++
- Developed Python based stock analysis program using open source libraries and custom code
- Designed and developed “Logic Solver” application in C++/MFC as own personal learning tool with custom grid engine designed to be adaptable to various puzzle types
- Built 5 node Kafka/Storm cluster using VMWare virtual machines with process management to enable high availability

MEMBERSHIPS & AFFILIATIONS
Member, ISC2 since March 2012 (CSSLP / CISSP)

AWARDS

- Meritorious Service Medal, Air Force Commendation Medal (3 oak leaf clusters), Joint Service Achievement Medal, Air Force Achievement Medal
- Awarded 33d Field Investigations Squadron/2d Field Investigations Squadron Team of the Quarter on 3 separate occasions; 2 of them back to back
- 375th AES Non-Commissioned Officer of the Quarter for 2nd quarter of 2000
- 1st CC Squadron, Group, and HQ USAFE/DO NCO of the quarter for 2nd quarter of 1998