

# ALBERT JOHN "A.J." WRIGHT

---

7344 Toxaway Drive, Knoxville, TN 37909 – Mobile: 865-388-9951 – Email: [ajw@ajw.io](mailto:ajw@ajw.io)

## EXPERIENCE

- Jewelry Television, Technical Operations**  
*UNIX Staff Architect*  
Responsible for designing, implementing, operating, maintaining, and securing networking, hosts, and infrastructure to support highly-available, reliable, business-critical services.

**2014 – Present**

  - Support software engineers in secure development of UNIX- and Linux-based services.
  - Design and deploy Puppet-based configuration management system to maintain ideal service platforms.
  - Deploy and maintain enterprise-class cloud-based dynamic retail web services based on Oracle Commerce/ATG that includes custom content management and automated failover between multiple cities.
  - Partially responsible for ongoing compliance with PCI Data Security Standard (PCI-DSS)
  - Implemented GPU-based image manipulation and machine learning platform
  - Designed and implemented data science and collection platform
- University of Tennessee, University-Wide System**  
*Chief Technology Officer and Chief Information Security Officer*  
Responsible for leading the Information Security efforts and selected active and preferred technologies for the University.

**2009 – 2014**

  - Lead development of long-term research administration software strategy
  - Lead deployment of Banner Student Information System web portal
  - Lead development of new University-wide IT risk management process based on NIST Special Publication 800 series.
  - Lead development of Technical Review Board for selecting technology strategy based on technical, business, and customer feedback
  - Lead IT industry and legal compliance and risk management for HIPAA Security Rule, PCI Data Security Standard (PCI-DSS), etc.
  - Acted as Security Officer under HIPAA security rule for Knoxville Campus
- University of Tennessee, University-Wide System**  
*IT Security Assessment Team Lead*  
Responsible for leading team of analysts performing full-spectrum (physical, network, host, etc.) security assessments of local and state-wide systems.

**2007 – 2009**

  - Worked with executive staff to create university IT Security policies and best practices.
  - Lead team that performed first self-assessment of Office of Information Technology
  - Developed software to automate, store, and correlate network vulnerability scan information
  - Lead development of university-wide enterprise identity management office
  - Developed HIPAA compliance plan for management of desktop workstations in Audiology and Speech Pathology Department
- University of Tennessee, Knoxville**  
*Senior Security Analyst*  
Analyst responsible for leading day-to-day operations of the security group at the Knoxville campus. Part of team responsible for full-spectrum (physical, network, host, etc.) security assessments both local and state-wide, forensics, as well as university security policies.

**2005 – 2007**

- Implemented ArcSight Enterprise Security Manager software for analyzing and correlating firewall, and IDS/IPS logs.
- Implemented web-based interface to Nessus security scanner for use by user community, including system for supplementing scanner findings with language understandable by non-technical audiences.
- Lead development of workflow for security event response
- Implemented customized web applications for statistic analysis of network baselines

- **University of Tennessee, Knoxville**

1999 - 2005

*System Programmer/Analyst and IT Administrator*

Part of team responsible for administration and troubleshooting of the university's central UNIX (Solaris, Linux, AIX, IRIX) servers, with focus on web servers and high-availability SMTP, DNS/DHCP, database, and computation clusters. Partial responsibility for forensic analysis on team-maintained systems.

- Co-authored first UNIX/Linux security policy with Information Security Office.
- Implemented automated Linux system installation that performs system hardening, application configuration, and firewall setup for SMTP and Oracle cluster systems.
- Designed and implemented multi-tiered redundant SMTP server infrastructure with virus-scanning, spam-scoring, and distributed denial-of-service defense using a local real-time black-hole list to share data across servers and platforms.
- Implemented automated Solaris system hardening scripts that meet or exceed industry and university standards.
- Wrote policy briefs on enterprise storage and Linux system hardening using analysis from Typhon III, Nessus, and other tools.
- Presented papers and tutorials on Sendmail configuration, Solaris system hardening, and SMTP server defense.
- Member of IT Faculty Advisory board

- **Pellissippi State Technical Community College**

1994 – 1999

*Computer Technician and System Administrator*

Part of team responsible for maintaining the college's 400+ microcomputer lab systems as well as multi-campus and multi-protocol computer network. Sole responsibility for management of the college's Sun and UNIX servers. Create and maintain in-shop system, script, and application software for UNIX, MS-DOS, Macintosh and VMS systems in C/C++ and appropriate script or batch languages.

- Setup log centralization with NTP-synchronized time stamps.
- Wrote multi-protocol packet analysis tool before TCP-Dump was available.
- Wrote software to maintain ideal software state in student labs.

## SKILLS

- **Leadership:** written and oral communications, experienced public speaker, business process analysis, critical thinking, problem solving, crisis management, ITIL, and systems-analysis skills
- **Languages and Tools:** Puppet, Ansible, Perl, Python, C, C++, Bash Shell Scripting, SQL, HTML,  $\text{\LaTeX}$ , git, Kubernetes, Java, Rust, ZFS, Docker
- **Operating Systems:** Linux (Red Hat- and Debian-based systems), Solaris, Apple MacOS X, CISCO IOS, and Microsoft Windows
- **Applications and Services:** Apache, Sendmail, Postgres, Oracle, SSH, TCPDump suite
- **Platform Providers:** Amazon Web Services, Rackspace Platform, and VMware vSphere Hypervisor

- **Security:** NIST IT Risk Management (Special Publication 800 series), hardware and software firewalls, host-based intrusion detection systems, forensic compromise analysis
- **Networking:** in-depth knowledge of TCP/IP network protocol suite and packet analysis, Ethernet switches and routers, F5 load balancers

## EDUCATION

- *University of Tennessee, Knoxville*
  - Master of Business Administration (2010)
  - Master of Science in Computer Science (2007)
    - \* Member of CS honor society *Upsilon Pi Epsilon*
  - Bachelor of Science in Computer Science (2004)
- *Pellissippi State Technical Community College*
  - Associate of Arts in Computer Science Technology 1999
  - Associate of Applied Science in Computer Science Technology 1997

## WORKSHOPS AND CONFERENCES

- SANS Network Security 2013, as an attendee (2013)
- Microsoft TechEd, as an attendee (2010)
- University of Tennessee SCUBA Diving Course, as an assistant instructor (2010)
- EDUCAUSE Annual Conference, as an attendee (2009)
- SANS WhatWorks in Log Management Summit, as a speaker (2009)
- Gartner Identity and Access Management Summit, as an attendee (2008)
- SANS WhatWorks in Mobile Encryption Summit, as a speaker (2007)
- SANS WhatWorks in Log Management Summit, as a speaker (2007)
- SANS Log Management Summit, as a speaker (2006)
- Tennessee Higher Education IT Symposium, as a presenter (2006)
- East Tennessee CyberSecurity Summit, as a host and speaker (2005, 2006)
- SANSFIRE Conference, as an attendee (2005)
- Tennessee Statewide Security Workshop, as a presenter (2005)
- Oracle Application Server Administration, as a student (2004)
- Internet2 IPv6, as an attendee (2003)
- Storage Area Network (SAN) Management, as a student (2002)

## ACHIEVEMENTS

- ITIL Foundation in IT Service Management (2014)
- NAUI Assistant SCUBA Instructor Certification (2013)
- NAUI Master SCUBA Diver Certification (2012)
- NAUI Advanced & Nitrox SCUBA Diver Certification (2009)

- NAUI SCUBA Diver Certification (2009)
- Certified Information Systems Security Professional (CISSP #303142, 2008)
- GIAC Securing Oracle Certification (GSOC #0036, 2007)
- GIAC Certified Intrusion Analyst (GCIA #0961, 2005)
- GIAC Cutting-Edge Hacker Techniques (GHTQ #0061, 2005)
- THAWTE Web of Trust Notary (2004)
- SunService Certified Solaris System Administrator (1995)
- A+ Certified Service Technician (1995)
- FBLA State-wide Computer Concepts Competition Winner (1992)
- Earned Eagle Scout Rank, Boy Scouts of America (1991)