

Resume of Jack Whitsitt | sintixerr@gmail.com | 703-409-9366 | Washington, DC

SUMMARY

Top Secret cleared, [SABSA Business Security Architecture Certified](#), National Critical Infrastructure (CIP) Cyber Security SME, Enterprise Information Security Architect, Data Correlation and Analysis Specialist, and experienced conference speaker.

Desire opportunities to support organizations in enabling business through security and in developing new paradigms of enterprise security which overcome past deficiencies.

Currently customizing SABSA business security architecture methodology to help manage the process of “securing” the Critical Cyber Infrastructure of the U.S. Transportation Systems Sector.

EMPLOYMENT AND WORK HISTORY

- 09/08 - Present | KCG on contract at TSA (Transportation Security Administration)

National Critical Infrastructure Protection Cyber Security SME: Subject Matter Expert for Cyber Security of National Critical Infrastructure in the Transportation Sector per the [National Infrastructure Protection Plan \(NIPP\)](#). Support TSA as the Sector Specific Agency (SSA) responsible for facilitating improved security and cooperation across the transportation and postal sectors (including private industry, public, state, local, and tribal stakeholders).

Responsibilities include development of sector strategic security plan and framework, sector business security architectural methodology, and risk model implementation. Also work on sector education and outreach, internal business case development, disaster recovery and COOP planning.

- 09/06 - 09/08 | KCG on contract at TSA (Transportation Security Administration)

Senior Enterprise Information Security Architect: Used [MEGA](#) and other tools to design the governance, artifacts, and models required in a robust policy and risk-driven NIST 800-series and FEA-compliant architecture. Focus on data-centric security and business drivers in order to account for the fundamentally de-perimeterized nature of business IT requirements and to allow for better synthesis of knowledge from data through layered information-sharing architectures. Contributed to the additional development of TSA security policy and system security reviews.

- 07/06 - 09/06 | Lockheed Martin on contract at FBI ESOC

Lead Analyst: Brought ArcSight correlation and SOC CONOPS experience to the FBI’s internal SOC team. Worked with ArcSight administrator, ESOC lead, and other team members to develop ArcSight rules, channels, and analysis methodology which continued to be used after my departure.

- *10/03 - 07/06 | NetSec, MCI, Verizon Business (through acquisitions)*

SOC Security Analytics and Correlation Architect: Conceptually designed and implemented NetSec's multi-layered correlation and analysis methodologies and tool-sets. Designed security statistical correlation modules based on MCI's fraud detection engine to integrate with any data source (including ArcSight). The modules were designed to mitigate SEM scaling issues and to augment Verizon's "Network Intelligence" efforts by correlating endpoint monitoring (via the Security Operations Center) with internet backbone data. Developed visualization methodology and integrated business visual analytics tool allowing analysis to explore up to 7 million IDS events on screen at once. Techniques were shared with and ultimately used by ArcSight in developing their Interactive Discovery tool.

Computer Security Incident Response Center (CSIRC) Lead: Managed operational client relationship and the SOC's role as a large federal government agency's top-level incident response coordinator.

Senior TAC Security Engineer: Worked as senior technical engineer to support marketing, sales, and executive staff in supporting existing large client relationships, landing additional clients, and defining future technical and operational SOC strategy. Also provided long-term trending and analysis support to customers and assisted shift analysts on escalated issues.

Senior SOC IDS Analyst: Monitored the networks of several of the largest global businesses and US federal agencies for potential intrusions and questionable traffic. Was recognized as the leading analyst in this area at the time and was shortly moved to a more senior role in the organization.

- *2003-2005 independent Open Source Development*

<http://baitnswitch.sourceforge.net> : Wrote the Snort IDS extension "Bait And Switch Honeypot System" to redirect identified "hostile" traffic from a production server to a honeypot with the same IP address. Bait and Switch has generated numerous academic papers, been used multiple production networks, utilized in thesis level research work, been the subject of a SANS certification paper, and has subsequently been partially re-implemented as a Bleeding-Snort project.

- *10/98 - 10/03 Perot Systems*

Various network specialist and IT support roles in Florida, Chicago, and Indiana: Clients supported included AT&T, USG, National Car Rental, MCI, Parsons Engineering, Knology, internal project offices, and others. In addition to technical responsibilities, I received training and experience in formal (PMI) project management as technical lead for a number of clients.

SPEAKING ENGAGEMENTS

- *DHS Security Conference in Baltimore, MD 2007 and 2008:*
 - **Policy Driven Information Security Architecture at TSA**
- *DoD/JTF-GNO's Joint Information Assurance Tech Exchange 2005:*
 - **“Data visualization, asset management, and risk scoring for network security”**
- *Recon reverse-engineering conference in Montreal 2005:*
 - **“Creating and Using a Visual Security Analysis System”**
- *Northeastern University's ACM Speaker Series 2005:*
 - **“Massive Data Visualization for the purposes of monitoring IDS”**
- *U.S. Department of Housing and Urban Development 2005:*
 - **“Optimizing IT Security at HUD: IDS Monitoring”**
- *Rubicon Security Conference 2003 (Co-presenter):*
 - **“Aggressive Honeypots”**: New paradigms of honeypot and IDS combinations. Working code available.

VOLUNTEER

Chairman of the Board | Art Outlet | Arlington, VA (2007/2008)

Art Outlet is a 501c(3) non-profit corporation located in Arlington, VA dedicated to supporting and bringing art to the local Arlington community and the greater Washington, DC area.

TECHNOLOGY USED IN THE PAST (Not exhaustive)

- **SEM / SIM:** ArcSight, NeuSecure, Custom correlation tools
- **Enterprise Architecture:** MEGA tool, SABSA methodology, FEA Framework
- **IDS / IPS / HIDS / NIDS:** ISS, Enterasys Dragon, NFR, Sourcefire, MacAfee (Intrushield), Cisco , Intrusion, Snort
- **Scripting and Programming:** C, Bash Shell Scripting, Python, PHP
- **Vulnerability Scanning:** Nessus
- **Services:** Postfix, Apache, IIS, MySQL, Oracle, others
- **Firewalls:** Checkpoint, Cisco Pix, iptables
- **Ticketing:** Remedy
- **Visualization:** Advizor Solutions' “Advizor” visualization tool
- **Server Platforms:** Linux (various flavors), Windows 2000, Windows NT
- **Protocols:** TCP/IP (OS, network, and packet analysis), Custom developed TCP/IP extensions
- **Honeypots / Honeynets:** various flavors