

# ALEX SULSKY

(917) 913 6586 ♦ alex.sulsky@gmail.com

2727 Revere st, Houston, TX, 77098

## BRIEF

---

Information security architect with experience building, protecting and automating resilient distributed systems.

## EXPERIENCE

---

### DigitalCrafts

September, 2017 - January, 2017

*Student*

*Houston, TX*

Accelerated School for Software Engineering - Full Stack Immersive Program

- Introduced to application development using popular JavaScript and Python frameworks - NodeJS, JQuery, React, Express, Flask, Tornado, etc
- Working with databases - Postgresql and Firebase
- DevOps with AWS, Heroku, Dokku and git
- Built and deployed web applications using the above tools

### Macquarie Bank Ltd.

May, 2015 - April, 2017

*Engineer*

*Houston, TX*

- Built and supported private and public cloud web-application delivery systems around F5 LTM load balancing proxies.
- Secured access to public applications using F5 APM and Palo Alto firewalls.
- Built out monitoring and reporting using Splunk and other off-the shelf systems - e.g. SiteScope
- Built a web app to report on F5 LTM configuration and status using F5's iconcontrol api
- Worked with internal researchers to contain possible threats and discovered zero-day exploits via custom rule sets on McAfee Intrushield IPS and F5's ASM Web Application Firewall.

### Texas Children's Hospital

October, 2011 - May, 2015

*Data Security Architect*

*Houston, TX*

- Developed security standards, advised leadership and technical staff on security risks and best practices.
- Served on the "Architectural Review Committee" to approve the design of proposed IT systems, create technical standards and advise policy.
- Built an application delivery system around F5's BIG-IP technologies using Global and Local Traffic Managers.
- Set up a centralized multi-factor authentication system for websites with a mix of F5's Access Policy Manager (APM) and RSA's Adaptive Authentication.
- Single Sign On (SSO) to third party applications through F5's SAML-capable authentication federating proxy - APM.
- Protected web applications through F5's Applications Security Manager - a web application firewall, SourceFire NGIPS - IPS
- Built a DDOS mitigation scheme through a combination of ISP peering via BGP and Arbor's Pravail APS - a DDOS protection suite.
- Developed baseline security configurations for common OS's and applications on NIST and CIS Benchmarks.

- Set up Symantec's Control & Compliance Suite (CCS) to audit system compliance to configuration standards.
- Setup a meaningful risk assessment and reporting practice through the integration of Symantec's CCS with Symantec's Data Leak Protection, Endpoint Protection, and Rapid 7's Nexpose vulnerability scan results.
- Ran popular security tools including Checkpoint and Cisco firewalls, BlueCoat forward proxies, Rapid 7's and and RADIUS AAA servers.

### **Texas Children's Hospital**

*Enterprise Systems Engineer - Contract*

May, 2011 - October, 2011

*Houston, TX*

- Worked on improving Microsoft Active Directory Services, PKI, and Microsoft Exchange systems.
- Integrated Wifi authentication with Active Directory through RADIUS & 802.1x capable APs
- Automated common administrative tasks through VBscript and PowerShell scripts.

### **Alvarez & Marsal**

*System Engineer*

February, 2007 - November, 2010

*New York, NY*

- Created detailed continuity and disaster recovery plans, for messaging, DNS and web services.
- Minimized disaster recovery times by integrating VMWare's Site Recovery Manager with EMC Clariion snapshot and mirroring services.
- Managed encryption tools: PGP, Bitlocker, EFS, and Safend.
- Built data center storage systems for Exchange, VMWare, file share, and backup around EMC Clariion
- Built branch office storage systems around FreeNAS, and HP StorageWorks.

### **Katzenbach Partners LLC**

*Systems & Networking Lead*

December, 2002 - September, 2006

*New York, NY*

- Designed a highly available, multi-office WAN through dedicated inter-office frame relay links, backed by IPSec VPNs over the Internet.
- Designed a multi-homed data center by way of BGP-peering with two ISPs
- Built a multi-site WLAN around Cisco APs and Active Directory-based authentication.
- Automated desktop deployment using Microsoft's Remote Installation Server and distributed filesystem storage.
- Led two Active Directory and Exchange upgrades, and worked with consultants to build an Exchange-integrated Avaya VoIP system.
- Secured systems, firewalls, and networking equipment using NSA, NIST, and vendor guidelines.
- Managed SonicWall/NetStructure, and Cisco firewalls.
- Set up detailed network monitoring by displaying WMI, WBEM, SNMP counters and alerts in a WhatsUp Gold console.

### **Comtex**

*Desktop, Server Support*

1997 - 2001

*New York, NY*