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

Revel Solutions LLC *RevelSec*   October 2018 - Present

Sr. Security Engineer   *Houston, TX*

- Redesigned delivery and protection of a Fortune 500's main retail sites around the F5 BigIP stack - Advanced WAF(ASM), DNS and LTM

- Redesigned Vulnerability Management program for a Fortune 500 retailer around Rapid7's InsightVM. 1000+ sites, automated asset collections and classification with custom code written in Python.

- Built Proof-of-Concepts/labs for prospective clients around F5's ASM, APM, LTM, DNS

- Migration of Fortune 10 Energy co. from Cisco ESA to Office 365 ATP for email protection

- Final escalation point for existing clients with their F5 issues

Independent Contractor   June 2017 - October 2018

- F5 LTM, GTM, APM and ASM migration for a large healthcare provider in Texas.

- Firewall & IPS log consolidation for SIEM consumption for a financial institution in Connecticut.

- IPS upgrade for a financial institution in Connecticut.

Macquarie Bank Ltd.   May, 2015 - April, 2017

Network Security Engineer - Contract   *Houston, TX*

- Built out and supported private and public cloud web-application and email delivery systems based on F5 LTM GTM load balancing proxies.

- Last level of support for F5 load balancers, F5's APM network access control suite.

- 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 iControl API.

- Maintained, operated and expanded McAfee Intrushield IPS & Aruba Clearpass.

Texas Children's Hospital   October, 2011 - May, 2015

Data Security Architect   *Houston, TX*

- Protected business-critical web applications with F5's Applications Security Manager. Set up ASM to detect and block OWASP's top 10 application layer attacks as well as, DOS, DDOS, bot-nets and brute forcing attempts.

- Responsible for developing applications, systems & network security solutions from concept to implementation.

- 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.

- Set up F5's APM SAML-capable proxy to allow SSO with third-party applications.

- Built a DDOS mitigation scheme by peering with multiple ISPs and incorporating Arbor's Pravail APS.

- Developed baseline security configurations for MS Windows 7, Linux & AIX systems along with popular applications like MS Office, Internet Explorer & Firefox applications on NIST and CIS Benchmarks.

- Set up Symantec's Control & Compliance Suite to audit system compliance to configuration standards.

- Rolled out Symantec's Endpoint Protection, PGP to encrypt email, hard drives and removable media.

- Ran popular security tools including Checkpoint and Cisco firewalls, BlueCoat forward proxies, Rapid 7's and and RADIUS servers.

- Set up phishing campaigns using Rapid 7's Metasploit.

Texas Children's Hospital   May, 2011 - October, 2011
Enterprise Systems Engineer - Contract   *Houston, TX*

- Deployed, upgraded and improved Microsoft Active Directory Services, PKI, and Microsoft Exchange systems.

- Set up Wifi Network Access Control via Active Directory through NPS RADIUS & 802.1x capable APs.

- Automated common administrative tasks through VBscript, PowerShell Python scripts.

Alvarez & Marsal   February, 2007 - November, 2010
Systems Engineer   *New York, NY*

- Lead for MS Active Directory and MS Exchange.

- Created detailed continuity and disaster recovery plans for messaging, DNS and web services.

- Managed encryption tools: PGP, Bitlocker, EFS, and SafEnd.

Katzenbach Partners LLC   December, 2002 - September, 2006
Systems & Networking Lead   *New York, NY*

- Designed a highly available, multi-office WAN through dedicated inter-office frame relay links, backed by IPSec VPNs over the Internet.

- Deployed hosting data centers and new office sites including all data, management and storage networks.

- Led all Network, Security, MS Active Directory & Exchange-related work.

- 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 $802.1x + Radius$.

- Automated desktop deployment using Microsoft's Remote Installation Server and distributed filesystem storage.

- Secured systems, firewalls, and networking equipment using NSA, NIST, and vendor guidelines.

- Deployed and managed Cisco PIX/ASA firewalls

- Deployed AnyConnect based VPN.

- Migrated from 3M /Motorola/Intel network to Cisco switches and routers.

- Set up detailed network monitoring.

Comtex   1997 - 2001
Desktop, Server Support   *New York, NY*

· Maintained WindowsNT & Novel servers
· Wrote user logon and usage reporting shell scripts

CERTIFICATIONS

MS Certified Azure Security Engineer MCID 6310169

Red Hat Delivery Specialist - Automation II #40333102

F5 Certified BIG-IP Administrator 50000080912

Palo Alto Accredited Configuration Engineer PAN6

CISSP #394506 (2011 - 2018)

EDUCATION

Digital Crafts   September, 2017 - January, 2018
Student   *Houston, TX*

Accelerated School for Software Engineering - Full Stack Immersive Program

- Introduced to application development using popular JavaScript and Python frameworks such as NodeJS, jQuery, React, Express, Flask, Tornado.

- Worked with Postgresql and Firebase databases.

- DevOps with AWS, Heroku, Dokku and Git.

- Built and deployed web applications using the above tools.

- GitHub: https://github.com/xanlex/

Brooklyn College, CUNY   *June 2001*
B.S. in Computer Science (Incomplete)