Jibran Ilyas

DIRECTOR

PROFESSIONAL EXPERIENCE

STROZ FRIEDBERG, LLC
Director, Incident Response, July 2015 to Present
Assistant Director, Incident Response, August 2014 to July 2015
Chicago, IL

- Assist in development of incident response methodologies and threat intelligence initiatives. Serve as investigative lead for high profile data breaches.
- Uses real time experience to benefit organizations with proactive risk assessments to minimize vulnerability to breaches.
- Lead the development of Threat Hunting capabilities, mainly the hunt for Advanced Persistent Threats (APT) and Point of Sale (POS) adversaries.

HALOCK Security Labs
Incident Response and Forensics Lead
Chicago, IL

June 2013 – August 2014

Team Lead for Crises Management and Investigations for data breach incidents. Plan Malware Threat Assessments for principal clients and devise strategies to combat the modern day threats via innovative Malware Kill Chain Strategies and Incident Response Plans.

- Conduct Advanced Malware Threat Assessments to test organizations Prevention, Detection and Response Controls for incidents.
- Conduct Malware Risk Assessments for organizations to come up with a holistic Malware Defense Strategy.
- Advisor for Incident Response Plans, First Responder Training and Threat Intelligence.

PAKISTAN TEHREEK-E-INSAF
Overseas Volunteer Coordinator for Election Campaign/Mobile Apps Lead
Pakistan
March 2013 – May 2013

Led the team of 3000 overseas volunteers for the Election Campaign in Pakistan and led the iPhone and Android Mobile Apps project.

150 North Wacker Drive, Chicago, IL 60606

jilyas@strozfriedberg.com | T: 630.730.8537 | strozfriedberg.com

Jibran Ilyas

DIRECTOR

- As a member of Social Media Core Team, created content for Facebook and Twitter Accounts.
- Development of Anti-Rigging website and other Election Day activities.

TRUSTWAVE
Senior Security Consultant
Chicago, IL
June 2007 – March 2013

Led the investigations on high-profile and publicly disclosed data breaches across the world. Speaker at Several Global Conference and researcher for published security advisories.

- Designed and delivered Forensic Training to Federal Law Enforcement agencies in USA and Canada.
- Conducted research in Memory Analysis and presented a talk at DEFCON Skytalks on the subject.
- Deep knowledge of Security Threats in the Commercial, Education, and Government environments.
- Knowledge of Incident response methodology and forensic tools such as EnCase, FTK, SIFT, F-Response, Volatility, Memoryze, lot2timeline, Sleuth Kit.
- Worked on new forensic methodology using Open Source Forensic Tools.
- Speaker at BlackHat, DEF CON, SecTor, SOURCE Barcelona.
- Featured by security publications including Dark Reading, Infoworld, Threatpost, IT World and Search Security.
- Established relationships with all major card brands, PCI Security Standards Council, Processing Banks, and Federal Law Enforcement agencies.
- Member of United States Secret Service Electronic Crimes Task Force (USSS ECTF).
- Assisted Federal Law Enforcement agencies in intelligence & suspect profiling.

AMBIRONTRUSTWAVE
Network Security Engineer, Manager Security Services
Chicago, IL

150 North Wacker Drive, Chicago, IL 60606

jilyas@strozfriedberg.com | T: 630.730.8537 | strozfriedberg.com

Jibran Ilyas

DIRECTOR

February 2006 – June 2007

Provided Security Architecture advice to Fortune 500 clients and managed their security operations from Firewall configurations, Intrusion Detection Systems and Log Monitoring.

- Vulnerability Assessment and design Security Architectures for clients.
- Manage and build client Intrusion Detection Systems and Internal Vulnerability Scanners.

CLARK CONSULTING
IT Infrastructure & Security Engineer
Chicago, IL
July 2004 – February 2006

Performed audit on the infrastructure of the data centers and offices to make them SEC compliant. Configured daily backups and drafter disaster recovery plan & technology policy to ensure confidentiality, integrity and availability of the network. Configured Nagios on Linus to monitor the hosts; configured Snort as a network IDS; installed a Syslog server to centralize logging.

- Management of Exchange 2003 servers with Anti Virus/Anti Spam Filters.
- Network Security Management / Infrastructure Support / Disaster Recovery Planning
- Cisco PIX and IDS Management along with security auditing of systems.
- Cisco VOIP Management (Call Manager and Unity Servers).

MORGAN STANLEY DEAN WITTER
IT Intern Coordinator
Chicago, IL
December 2002 – July 2004

Provided technology support for Morgan Stanley's two Loop offices. Designed and maintained Chicago Complex website which integrated the data from two Loop offices and Oakbrook Branch. Also interviewed and hired interns for two quarters for Loop offices.

- Provided software and technical support to the senior financial advisors and other managers.
- Write technical manuals for new technologies and software.

150 North Wacker Drive, Chicago, IL 60606

jilyas@strozfriedberg.com | T: 630.730.8537 | strozfriedberg.com

Jibran Ilyas

DIRECTOR

HOMETECH COMPUTER SOLUTIONS
Network Engineer – Part Time Consulting
Chicago, IL
July 2003 – February 2005

Created a guide to combat the spyware problem which included custom registry scripts and a custom toolkit.

- Plan growth of business by introducing cutting edge services and keeping positive relationships with clients and prospects.

EDUCATION

NORTHWESTERN UNIVERSITY
Masters in Information Technology (Class of 2009)
- Focus on Infotech Management
- Courses taught by McCormick and Kellogg Schools Faculty

DEPAUL UNIVERSTIY
Bachelors of Science in Networks Technology (Class of 2005)
- Focus on Network Security

TRAINING

CERTIFICATIONS

Qualified Security Assessor, (QSA)

Cisco Certified Network Associate, (CCNA)

Security + (CompTIA)

Network Security (IPD)

PUBLICATIONS

Co-Author of Trustwave's Global Security Reports from 2011 to 2013

Co-Author of Malware Freakshow (BlackHat Whitepaper)

Lead Researcher on Visa Data Security Alert on Memory Dumper Malware

150 North Wacker Drive, Chicago, IL 60606

jilyas@strozfriedberg.com | T: 630.730.8537 | strozfriedberg.com

Jibran Ilyas

DIRECTOR

Researcher on Evolution of POS Malware

LECTURES AND PRESENTATIONS

Speaker at Department of Homeland Security “Technical Threat Intelligence Exchange” 2015

Speaker at University of Chicago, Tech Talk “Anatomy of a Data Breach, a view from the Trenches” 2014

Speaker at CAMPIT Enterprise Risk / Security Management 2013 (Malware Risk Assessment)

Speaker at HITEC Hospitality Technology Show 2013 (Security Hospitality PII)

Speaker at Cyber Secure Pakistan 2013 (Forensics Case File)

Presenter at Chase/MasterCard Merchant Seminar (Trustwave Global Security Report)

Co-presented at Microsoft’s Digital Crimes Consortium 2011 (POS Forensic Investigations)

Trainer at United States Secret Service (Incident Response and Digital Forensics)

Presented at HITEC World Largest Hospitality Technology Show (Hospitality Attacks and Malware)

Speaker at SecTor and DEF CON 2011 (Malware Freakshow 3)

Speaker at SOURCE Barcelona (BlackHats don’t always win)

Speaker at BlackHat, SecTor and DEF CON 2010 (Malware Freakshow 2)

Speaker at DEF CON 2009 (Malware Freakshow)

AWARDS

Recipient of a four-year, full tuition scholarship to DePaul University. Winner of a TV show “Who wants to win a Scholarship”

150 North Wacker Drive, Chicago, IL 60606

jilyas@strozfriedberg.com | T: 630.730.8537 | strozfriedberg.com