Fahad Ehsan

Address: Blk 9 Sengkang Square, #09-01 Singapore 545075

Email: fahade@gmail.com ☎**:** (+65) 9620 4302

CORE COMPETENCIES

Vulnerability Management	Memory Forensics (**FOR526**)	Security Research
Security Consultancy	Development – SQL, C#/C++, Python	Network Security (**CCNA**)
Incident Response (**GCIA**)	Malware Reverse Engineering (**GREM**)	

PROFESSIONAL EXPERIENCE

UBS AG – *Associate Director* ***Singapore (Feb 2012 – Current)***

Security Research and Analytics Jan 2013 – Current

Currently focused on delivering Security Analytics and Big Data Solutions for the firm. I am leading some of the activities around building a global hadoop cluster. These include building the Use Cases, Conceptualizing the workflows and testing the Use Cases. The vision is to deliver a solution, which provides **Search, Analytics, Forensics** and **Visualization** capabilities to the relevant security teams within the bank. This is ongoing project, which will run throughout 2014-15.

During 2013, I successfully delivered a POC for detecting malware, which bypassed firms existing security controls/tools. The POC was focused on detecting malware exploiting **Java/JRE** vulnerabilities. This POC is going to be expanded in 2014 to detect malware, which target weaknesses in HTML, Adobe Flash, PDF, Email etc. The POC was developed on an in-house MS SQL Server based solution, which will be replaced with a **Big Data Analytics** solution in the future.

Vulnerability Management Feb 2012 – Current

I am responsible for the firm's Vulnerability Management toolkit. I am managing a team to deliver comprehensive VM reports across all major platforms I.e. windows, unix, database, networks etc

- Delivered a Scorecard for Windows Workstation and Server Patching, covering over 130k hosts
- Database patch metric covering over 5000 **Sybase** and **Oracle** DB Servers
- Developed an automated **Linux Patch analyzer** for Redhat servers. This info was later used to develop a patch metrics covering over 10k servers.
- Introduced search functionality and various **Business Intelligence** features to the tool.
- **Network device** vulnerability detection for Cisco, Juniper and Infoblox
- Unix configuration related issues added as a scorecard e.g. insecure services enabled, weak passwords etc.

Barclays Capital – *Assistant Vice President* ***Singapore (Aug 2007 – Jan 2012)***

Global Information Security (GIS) Mar 2009 – Jan 2012

As part of the Global Information Security team, I was responsible for overseeing the APAC region.

Achievements:

- Created scorecards measuring **vulnerable software** found on workstations, including Java, Adobe Reader and Flash, Realplayer etc.
- Developed a proposed **Mobile Device Security Standard,** which covers security baseline for all phones, tablet and other mobile devices.
- Prepared responses to queries from regional regulators e.g. responded to **HMKA** (Hong Kong Monitory Authority) questionnaire around RSA hack preparedness and **MAS** (Monitory Authority of Singapore) queries around perimeter security.
- Lead a **recertification exercise**, removing over 40% user admin access on workstations.
- Initiated a global project to detect and remove **unauthorized software** from workstation. Over 20,000 instances of unauthorized software removed. Implemented a block for firefox at the Proxy layer.
- Conducted **Windows 7** and **Firefox** security reviews. These software were being tested for a global roll out as a build.
- Conducted an in-class **Application Security Awareness** Training to developers in Singapore.
- Documented the **GIS Infrastructure Penetration Testing** Process - May 2010
- Developed metrics based on foundstone scan data, showing **vulnerable services** found in Campus, DMZ and OOB networks.

Graduate Program Aug 2007 – Feb 2009

As part of the graduate program I spent 6 months each in IT Production, Application Support and Application Development job roles. These experiences gave me a good understanding of how IT works in Barcap.

Fixed Income .NET / VB Developer: Sep 2008 – Feb 2009

Improved performance of Summit-TMS Reconciler report by 200% in a tight schedule. I quickly identified bottlenecks in existing code and better algorithms to reduce the processing time.

- Provided second level support for various other applications under TCG.

FX Cash IT - Application Support team: Mar 2008 – Aug 2009

As a support person, I had close interaction with Front and Middle office people. I was able to support high priority users under pressure, and learned management skills. I worked closely with other team members and shared responsibility for SOD and EOD activities.

- Provided first line support to **Devon** and **SACRED** Users, while attending to critical application issues
- Gained valuable knowledge related to FX trading and trading platforms.
- Developed vital **UNIX** skills while managing Devon backend.

GSC DBA First Line Support Aug 2007 – Feb 2008

- Provided first line support for Oracle and MS SQL Server.
- Developed understanding of advanced database feature like replication and data warehousing.

Allegro Manufacturing Pte Ltd. – *System Administrator (Full Time)* ***(Jun 2006 – Jun 2007)***

Allegro Manufacturing is a mid-sized electronics manufacturing company based in Singapore. It provides precision equipment to research labs around the world.

Wholly responsible for handling technical issues involving network, hardware, and operating systems (Windows 2003/2000 Server, Windows XP/9x, Linux). Oversee network connectivity, implementation, integration, and troubleshooting for servers, routers, remote access, storage devices, printers, and scanners.

Key Responsibilities:

- Administer **IBM Lotus Domino Server** and MS Exchange email system to meet all management, employee, and customer needs.
- Direct systems administration of 50+ Windows 9.x/XP/2000/2003 systems utilizing **Active Directory**.
- Manage internal, 100+ node network, successfully integrating 1 Linux and 3 **Windows 2000/2003** servers (connecting Windows 2000/2003 workstations, Windows XP/9x, and printers, and terminals with remote access) through Symantec pcAnywhere and a **VPN firewall**.
- Maintain network security through firewall, **Antivirus console** (Symantec Corp Ed) and spam mail policies.

Allegro Manufacturing Pte Ltd. - *Software Engineer (Part Time)* ***(May 2005 – May 2006)***

Developed strong analytical skills while utilizing software engineering techniques.

Projects Completed:

Procurement Management System - An Online System for managing Purchase Orders and parts inventory. Reduced time taken for processing purchase orders while eliminating paperwork.

Parts Requirement Forecast Process - Designed an application which increased the efficiency of the process by 700%.

Electronic Non-Conformance Requisition System – The system replaced a manual system in August 2005, currently being used by 5 departments. Reduced paperwork and inter-departmental processing.

EDUCATION

National University of Singapore – *Bachelor of Computing* ***Singapore (Aug 2003 - May 2006)***

Coursework: Software Engineering, Information Security, Database Systems, Web Application Development

University College Lahore – *Cambridge GCE A Level* ***Lahore, Pakistan (Sep 2000 - Jun 2002)***

Subjects: Mathematics, Physics, Chemistry and Computing.

CERTIFICATIONS

- Attended the 6-day **SANS FOR526, Memory Forensics In-Depth** course in Oct 2014. Exam Pending.
- Passed **GREM (GIAC Reverse Engineering Malware Certification)** in April 2013 (#3655)
- Passed **GCIA (GIAC Intrusion Analyst Certification)** in Feb 2013 (#9269)
- Passed Certified Professional for **Requirements Engineering** (CPRE - IREB) in Jan 2013
- Passed **GSEC (GIAC Security Essentials Certification)** in Jan 2011. (#30253)
- Passed **CCNA** (CISCO Certified Network Associate) in Mar 2010
- Passed **1Z0-001** (Introduction to Oracle: SQL and PL/SQL) in Mar 2003
- Certificate in **Project Management** by ESI based on PMBOK (Project Management Body of Knowledge)
- Certificate in **Business Analysis** by ESI based on BABOK (Business Analysis Body of Knowledge

GUEST SPEAKER AND TRAINER

BlackHat Asia 2015 Trainer: Detecting Advanced Malware using Volatility and R – Mar 24-25

I will be conducting a 2-day training at the upcoming BlackHat Asia conference. The students will learn how to use opensource tools like Volatility and R to detect malware. The course is designed to help the students build their incident response, memory forensics and malware analysis skills.

RSA Conference APAC 2014 – July 22-23
I was a guest Speaker at RSA Conference APAC in July 2014 presenting 'Memory Forensics and Security Analytics: Detecting Unknown Malware'. This was based on my personal research over the course of 8 months.

Guest Speaker at Other Conferences:
Defcamp 2014, Bucharest : Nov 28-29
DeepSec IDSC 2014, Vienna : Nov 20-21
ISACA Ireland GRC 2.0 2014, Dublin : Oct 3
SEC-T 2014, Stockholm : Sep 18-19
ISACA Malaysia - GRC Conference 2014 : Jun 25-26
BlueSpace CyberSecurity Conference Malaysia 2014 – Feb 18-20

As a CyberSecurity Expert, I have given several internal talks while working with UBS AG and Barclays Capital throughout my career. Some of the topics, which I recently presented, are **Evolution of Malware** (Apr 2014), **Malware Reverse Engineering basics** (June 2013), **Personal Security** (2011) and **Application Security 101** (2010).

VOLUNTEERING AND AWARDS

UBS Global Employee Volunteering Award – Team Category – Nov 2014 - CampVision
I was recently awarded the UBS Global Employee Volunteering Award, for my part in mentoring underprivileged youth in Singapore to inspire them and uplift their self-esteem. This was a 6-month program during run by UBS in collaboration with Campvision Charity.

UBS APAC Innovation Award – Apr 2014:
I received the award for Innovation for my contributions to the Vulnerability Management Project. This is regional award granted to individuals who continue to innovate and provide sustainable solutions for the firm.

Singapore Food from the Heart Charity - 2012-2013
As part of the UBS Volunteering team, I frequently spent time with charity to prepare food bags for the needy.

Barclays Chairman Awards (£1,000 Awarded) – Mar 2011
I initiated and coordinated Singapore wide (6 offices) charity fund for Pakistan Flood Victims collecting over SGD$22,000. I was shortlisted for the Barclays Global Chairman Award and awarded a further £**1,000** to be given out to my charity.

SKILLS

- Excellent written and verbal communication skills.
- Ability to handle heavy workload in an efficient manner.
- Able to interact and work successfully with others so to achieve goals through teamwork.
- *Platforms:* Windows XP/7/2003/2008, Linux, Unix, DOS
- *Languages:* SQL/PLSQL, C/C++, Java , .NET, Perl, VB/VBA, Python

EXTRA CURRICULAR ACTIVITIES

- **Represented UBS at a NUS Student Meet and Greet Event – Sep 2013**
  The students from National University of Singapore were introduced to the various UBS recruitment opportunities.
- **Volunteered for the Singapore Food from the Heart Charity - 2012-2013**
  As part of the UBS Volunteering team, I frequently spent time with charity to prepare food packets for the needy.
- **Represented Barclays Capital at Recruitment Event – Sep 2011**
  Graduate Recruitment event held at Nanyang Technology University Singapore.
- **Haiti Earthquake volunteer - 2010**
  Collected SGD$800 as a volunteer for this campaign
- **Barcap, Cricket Team - 2009/2010**
  Member of the cricket team Singapore.
- **Sports Day for Special Children - 2009**
  Successfully organized a sports day for children with disabilities.
- **School of Computing, Hockey Team**
  Won Silver Medal in Inter Varsity Games 2004/2005.
- **Member of NUS PAK.**
  Organized a University wide fund raising drive for South Asian Earthquake victims (Oct 2005). Donation collected valued approximately S$15,000.
- **Represented NUS Cricket Team in 2005**

LANGUAGES

Fluent in English, Urdu, Hindi, Punjabi

REFERENCES

References can be provided on request.