YEONG LEE WEI

evandrix@gmail.com

EDUCATION

2008 - 2012	Imperial College London	Computing (MEng) - 1st Class Honours FYP: Python unit test generation
2004 - 2005	Anderson Junior College (AJC) Singapore	GCE A-Level: Mathematics A, Further Mathematics A, Chemistry A, Physics A, Mathematics 'S' Paper Distinction, Physics 'S' Paper Distinction
2000 - 2003	The Chinese High School Singapore	GCE O-Level: Chinese A, Mathematics A, Additional Mathematics A, Biology A, Chemistry A, Physics A, Geography A

ACADEMIC HONOURS AND AWARDS

2017-2021	FEYE/Mandiant Flare-On Finisher
2021	Cellebrite 2021 CTF Magnet Virtual Summit 2021 CTF Tenable CTF

2020	Winner:
	• Magnet Virtual Summit 2020 CTF
	• SANS Grid NetWars (ICS Summit APAC)
	• SANS DISC-SANS ICS NetWars
	• SANS Cyber Defense NetWars Tournament Live Online
	• SANS Core NetWars Tournament Live Online
	• SANS Pen Test Hackfest & Cyber Ranges Summit
	    o Global Cyber Ranges Competition
	    o Core NetWars Tournament
	• SANS DFIR NetWars Tournament Live Online

2019	SANS Core NetWars Tournament of Champions Participant
2019	SANS Core NetWars Champion
2018	MINDEF Defence Technology Prize (R&D) - Intelligence Analytics Team
2018	SANS DFIR NetWars Champion
2018	SANS SEC555: SIEM with Tactical Analytics Capstone Winner
2018	SANS Cyber Defense NetWars Winner
2018	DSO Special Recognition Award
2017	PANW LabyREnth Finisher
2017	SANS DFIR NetWars Winner - Lethal Forensicator
2010	Gloucester Research Prize - top 10 in 2nd year Computing
2009	BCS YPG Student Contest Judges Choice Award and 1st runner-up
2008	Morgan Stanley Bank Award - top 10 in 1st year Computing
2006	SAT II: Chemistry(790), Math Level II(800), Physics(800)
2005	SAT I: Critical Reading(550), Math(800), Writing(690)
2005	21st National Software Competition (IT Algorithm Category) - 2nd runner-up

Feb 2021 - Present	**Senior Malware Analyst at Ensign InfoSecurity, Singapore** • Teach@Ensign - conducted internal training

Mar 2019 - Feb 2021 (seconded)	• Automated Malware Triage System (AMTS)
	  o Malware Database
	  o Malware Zoo

Aug 2012 - Feb 2021	**Senior Member of Technical Staff at DSO National Laboratories, Singapore**
	• <u>Cybersecurity Analytics</u>
	  o Network + Endpoints in Enterprise Environment
	  o ArtifactVerifier (SWI-Prolog)
	  o Adversary Emulation
	  o Visualization
	• <u>Social Media Analytics</u>
	  o Data Collection
	  o Natural Language Processing (NLP)
	    ■ Information Retrieval/Extraction
	    ■ Sentiment Analysis
	    ■ Entity Resolution
	  o Visualization
	  o Mobile Application Reverse Engineering

Jan 2012 - Present	**System Administrator at Calvary Pandan B-P Church, Singapore** • https://calvarypandan.sg • https://signup.calvarypandan.sg
Aug 2015 - Aug 2017	**Information Security Partner at Starbucks, US** • Bug Bounty program participant
Apr 2011 - Sep 2011	**Software Developer at LShift, UK** http://evandrix.github.io/slidy-ppt • Freedom from Torture's Project Daylight - QA • "High street bank" project • Eurotunnel CIFFCO website • Trac plugins - Burndown Chart + Email Digest • "Mobile content provider" project - NLP • Chartered Insurance Institute - C# tool
Sep 2010 - Jun 2011	**Undergraduate Teaching Assistant at Imperial College London, UK** • for first year Computing students
Jul 2010 - Sep 2010	**Intern at EnterpriseIT, Defence Science & Technology Agency (DSTA), Singapore** • eWorkplace: eMeetings Java EE Web Application
Jul 2008 - Sep 2008	**Intern at Business Objects (SAP Asia Pacific), Singapore** • Data Mining & Technical Support (Global)
Jan 2008 - Jun 2008	**Intern at Simulation and Modelling, DSTA, Singapore** • Google Map Tiles Recognition (C#) • Microsoft Flight Simulator X tooling • offline deployment of Mapping application

PROFESSIONAL DEVELOPMENT

30 Sep-01 Oct 2021	SAS'21 - Kaspersky Reverse Engineering Malware the Hard Way
07 May-08 Nov 2021	Kaspersky Targeted Malware Reverse Engineering
15-17 Nov 2020	HITB - Software Deobfuscation Techniques
12-17,22-23 Mar 2018	SANS SEC555: SIEM with Tactical Analytics
04-14 Dec 2017	Cyberbit EDR Analyst training
11-15 Apr 2016	Darknet & Cryptocurrency - iTrust@SUTD and TNO
29 Mar-01 Apr 2016	BHAsia16 - Hunting Malware across the Enterprise
20-24 Mar 2016	SANS FOR578: Cyber Threat Intelligence
07-08 Dec 2015	Nanyang ENC Advanced Ethical Hacking for Active Network Security
23 Jun 2015	Cyber Defence Workshop - iTrust@SUTD
10 Apr 2015	Splunk Hands On Technical Workshop
16-21 Mar 2015	SANS SEC511: Continuous Monitoring and Security Operations
27 Nov 2014	DSO Secure Software System Development Process
01-02 Sep 2014	NTU-EEE Cybersecurity Workshop
27-28 Feb 2014	SMU Living Analytics: Analyzing High-Dimensional Behavioral and Other Data from Dynamic Network Environments
04-06 Jun 2013	ISS World Europe

SKILLS AND ACHIEVEMENTS

Languages:	Fluent English Shell (Zsh), Python, Javascript, Competitive C++, Java, PowerShell, PHP
Platforms:	Desktop (Windows/Linux/MacOSX) + Mobile (iOS/Android)
Leadership:	Executive committee member in AJC Computer Club
Publications:	"Troll detection by domain-adapting sentiment analysis", Fusion 2015
Miscellaneous:	ACM Professional Member (2013) Holder of an international driving license

REFERENCES

Available upon request