Sina Manavi

Phone: +601112274183
Email: Manavi.sina@gmail.com
Homepage: linkedin.com/in/sinamanavi/
DOB: 1986
Address: Mont Kiara, Jalan Kiara 5, Mont Kiara,
Kuala Lumpur, Malaysia

Professional Summary

I am Security Manager with over 13 years of experience in Financial and Banking sector, government agencies and SME, based in Malaysia in various fields such as information security management, governance, risk and compliance, Cyber Threat and Vulnerability Management, Threat Intelligence, Penetration Testing, vendor evaluation and management and User Awareness.

Currently I am working as Senior Manager – Technology Risk Governance in AIA Shared Services Group in Malaysia having footprints in more than 18 countries.

Also based on previous experiences (over 10 years) in Vulnerability Assessment and Penetration Testing, Digital Forensics and Incident Handling in my previous roles with other companies, helped me to build the Threat Intelligence for current bank from the scratch which was one of my best achievement during this journey. During this time I used different Threat Hunting tools and Threat Intel service providers and well known EDRs to assist my clients

Working with different industries and multinational countries helped me to gain great experiences building relationship remotely and locally, learn different cultures, how to serve clients and work with people with different language, Timezone.

Work Experience

Senior Manager –- Technology Risk Governance- AIA Shared Service Group – (Feb 2020 Present)

Role	**Senior Manager - Technology Risk Governance- AIA Shared Service Group**
Objective & Achievement	Supporting the Head of Technology Risk Governance to cover 18 countries across the APAC within two main portfolios, managing Cyber Risk and governance program and reporting as well as Information Security Awareness program manager. More details are as follows: • **Build Cyber Risk and Governance Framework** Build and maintain a strong cyber risk and governance framework using top industrial standards and best practices including but not limited to ISO 27001, NIST, COBIT. • **Governance and Risk Reporting:** Oversee key functions of the Information Security Program including Governance Risk & Compliance (GRC) and IT Security, Identity and Access Management (IAM), Third Party Risk Management, Patch and Vulnerability Management, Cloud Security, Security Project initiatives and the overall Security Awareness Program and Report to the GCISO Governing Technology Risk reporting operations, including • **Build Information Security Awareness and Cyber Risk culture:** Build cyber risk atmosphere in the organization and support the GCISO in informed decision making based on the existing security posture and strategy planning as well as budgeting. • **Engaging Stakeholders in Risk Mitigation Planning and Remediation:** Governing an overseeing the cyber risk and work with Business Units to come up with proper mitigation action plan and getting support from the senior management to resolve them in a based-on organization priority and risk appetite Working with IT Security stakeholders and team to optimize the risk posture where is needed.

	• **Developing Information Security Policy and Standards complying with related regulatory compliance and requirements** • **Information Security Awareness:** Define and maintain the Information Security Awareness Program for all Regional Countries as well as Senior Management and stakeholders Defining and develop IS Awareness topics and contents based on the organization risk posture and working with respective team to reduce the human risk factor

Senior Manager –- Group CIMB Bank – (Jun 2016- Jan 2020)

Role	**Senior Manager –Regional IT Security Strategy Planning and Reporting**
Objective & Achievement	• **Security Posture Assessment and IT Security Blueprint and Roadmap:** Developing Security Risk and Gap Assessment using International Standards and Benchmarks and prioritizing countries initiatives to meet the Business Goal and Strategy (Vision & Mission) and complying with regulatory requirement locally and regionally. Variation of standards and frameworks including but not limited CIS CSC, CSF NIST, COBIT and ISO 27k1 series have been leveraged based on the entity and business units as well as regional countries maturity level as well as existing budget to enhance the strategy planning and roadmap. • **Budgeting for Regional Countries:** Based on Security Posture assessment and IT Security blueprint and roadmap defining the security projects and budget and monitoring the budget utilization to ensure that resources have been used utilized efficiently. • **Governance and Oversight for Regional Countries:** Governing regional countries based on the defined Group IT Security Policy, Standards and SOPs including VAPT Finding Remediation Tracking, Security Patch Deployment state, Security Projects and Initiatives, SOC an Incident Management, IT Security Audits and Remediation, Threat Intelligence, and based on the gaps, identifying the challenges and risk and advising how to improve the current state. The process and performance have been improved tremendously and using the risk approach, helped to close the gap and mitigate the risk more efficiently. • **Review, Develop and Implement Group IT Security Strategy, Policy, Standards Procedures** • **Vulnerability and Threat Monitoring** Managing Regional Countries vulnerability and patch management and oversighting on countries compliance state and work with stakeholders to deploy the patches and remediate the vulnerabilities to mitigate the cyber risk and compliance issues. Define metrics and SLA and priority planning to expedite the remediation planning • **Establishing Threat Intelligence:** Threat Intelligence process and foundation have been defined as one of the main tasks during my early days at CIMB. Different technologies and process have been defined and implemented to cover cyber (external) and internal threats to protect the CIMB and customer interests such as Cyber and Financial Fraud, Credential leakage, social media and other regular phishing and scamming campaigns, monitoring and responding to potential data leakage, and monitoring attack campaign and other relevant threat monitoring and advise different teams how to mitigate the risk and take required action to patch, block and/or any required workaround. Also building Cyber Threat Intelligence awareness culture and briefing senior manager on requirement basis is one of other achievements during my presents in CIMB. Defining Threat Intelligence process and Framework and build the foundation requirement as well as enhancing the current maturity level based on the defined roadmap. • **Reporting directly to Group Head of IT Security** On a monthly basis, regional countries are compiled and report to the senior management by highlighting the existing Gap and risks and providing required action plan and/or solution to meet the requirements.

Senior Manager, EC-Council (Jun 2016-Dec 2017)

- As a Contract project at CIMB Bank (Regional IT Security)

- **Security Evangelist and Information Security Consultant in KAAPAGAM TECHNOLOGIES and Kaapagam Academy (March 2015-April 2016)**
    - Security Posture Assessments and helping clients in digital transformation to the next maturity level.

- Providing Vulnerability Assessment and Penetration Testing, Code Review, Infrastructure Architecture Review for different government agencies and enterprise companies from Network to Web and Mobile applications. Some (but not all) of the projects have been listed in the bellow table.
- Developing and Managing Vulnerability and Threat Monitoring end to end for clients using Nessus, Nexpose and Qualys.
- Content development of the training materials as well Industry Trainer in Kaapagam Academy as a sister company for Kaapagam Technologies, such as Android Application Penetration Testing, Network Penetration Testing, and Web Application Penetration testing
- Invited Speaker Note in Many Universities and Government Agencies.

Hereby, some of the Project details have been listed. Due to Company policy, it is not possible to name all clients or more details.

Project Name	**Web Hosting (Web and Network Infrastructure Penetration Testing)**
Client	The client is one of the top Internet Service Providers focusing on DNS, Digital brand management and many more services, which is established more than a decade ago and having offices in Singapore, Taiwan, and Malaysia. Sina Handled penetration testing and vulnerability assessment as well as proposing patch management techniques to enhance and improve the client infrastructure security.
Responsibility	o Working directly with the Business Owner and Senior Managers o Security Posture and Maturity Assessment. o Vulnerability assessment and penetration testing o Risk Assessment and Remediation o Advisory and Information Security Transformation. o Security awareness training sessions for respective development teams

Project Name	**Network Infrastructure, Web Application and Payment Application Penetration Testing**
Client	The client is one of the leading film exhibitor Cinema located in Malaysia, and other APAC countries. Sina was involved with Network (Wireless/LAN) Security Assessment and penetration Testing, Firewall Penetration Testing as well as web application penetration testing. In addition, the payment gateways have been manually analyzed via the PCI DSS standard. The objective of the project was to pinpoint the security flaws by Network and application assessment
Responsibility	o Vulnerability assessment and penetration testing Wireless and Network Infrastructures, Web application and the payment gateways. o Network Design Segmentation and Hardening (LAN and Wireless). o Helping the client to understand the risk and remediation advisory.

Project Name	**Security Posture and Penetration Testing (Network Infrastructure, Web Application, SAP)**
Client	The client is one of the most well-known international Food company operates globally in many countries (e.g. Australia, Singapore…etc.), and many more, including stores in Malaysia. This Project covers different security consultation aspect from the security posture of Firewall policy, wireless and LAN Security, to Network, SAP, and web application penetration testing. Sina was responsible to conduct the Security Posture to analyze firewall policy, wireless/LAN network Security and segmentations. In addition, deep network penetration testing has been conducted through the Call Center, Data Center, IT department, Finance and Marketing department. Web application penetration testing has been conducted on both Malaysia and Singapore web sites. And finally, SAP penetration testing has been conducted on Finance and Production systems successfully.
Responsibility	o Wireless and LAN Network Security Posture. o Firewall Policy Analysis. o Network application security assessment for all four platforms (Windows, Linux, and Mac) o Web application penetration testing o Risk Assessment and Management. o Helping the client to review the Security Policies, Infrastructure, at the Headquarter as well as Branches. o Vendor evaluation to help the client to choose the best Data Leakage solution and vendor based on the client budget and requirement. o Vendor and third-party vendor risk management.

- **Penetration Tester and Security Trainer in Condition Zebra (Jan 2014 – Jan 2015)**
  As a security consultant and penetration testing served clients in cyber security audit, security posture assessment, helping to develop SOPs and Policies, and performing penetration testing on different Web and Mobile application penetration testing, SAP penetration testing, payment gateways and network penetration testing. The list of the clients cannot be disclosed due to company policy.
  Sina has also provided Security training such as Network penetration testing, Web and Mobile application penetration testing, secure coding, Incident handling and Digital Forensics investigation for different clients such as Tenega National Malaysia (TNB), Telecom companies, Universities, MEPS.
- **Part Time Trainer in EC-Council Academy Malaysia, (Jan 2014 to Nov 2014):**
  Sina has provided different courses and workshops in EC Council Academy Malaysia as a part time trainer.
- **Mobile Security Ethical Hacking- Keeping Your Secret Safe, as a Freelancer**
  The course covered about BYOD Security, Android OS Fundamental Security Architecture and Application Analysis, Rooting Android, File and Network Monitoring, Android Auditing, Forensics Investigation of Android Phones, and Android Malware Analysis. Kuala Lumpur, Malaysia, 9-10 Sep.
- **Instructor of Tutorials and Workshops in University Putra Malaysia:**
  Sina has conducted short courses and practical workshops have been conducted in University Putra Malaysia for Security students and Security Research Lab members with network security, Network forensics, advance SQL Injection, understanding of Honeynet and Honeypot systems, session management techniques and secure implementation of techniques on web application systems.

- **Chairman in Conference:**
  - Co-Chairperson in Cloud Security's Session in the "International IEEE conference on Cyber Security, Cyber warfare and Digital Forensics (Cybersec 2012)", Kuala Lumpur, Malaysia June 26-28, 2012.
  - Internship for Tim Pierson, in Hacker Halted Asia Pacific 2012, for Cloud and virtualization Security's session in EC-Council Kuala Lumpur, Malaysia, 19-22 November, 2012.
- **Application Security Consultant IRSA SHABAKEH, Rasht, Iran (2007-2011):**
  - Application Penetration Testing (Web and Thick Client Applications).

  Designing the Application Security Architecture, leading the Application development team with secure coding standards, performing vulnerability assessment and penetration testing before launching the application and helping the application development team to remediate the vulnerabilities and software bugs.
- **Teacher Assistant and Tutor in Azad University, Lahijan, Iran (2008-2010):**
  - Teacher Assistant for C/C++.
  - Tutor of Visual Basic. Net for junior students.
  - Teacher Assistant in Database Lab (MS.SQL Server 2008 and T-SQL).

Public Speaking:

- "The Cyber Security Teams' Role Post COVID-19: Key Lessons Learned and Next Steps" Webinar, Featured Speaker. 8th Sep 2020
- "**Threat Intelligence and Defense in Depth**", SecureConf 2019, Kuala Lumpur Malaysia, 13th July 2019.
- SQLSaturday "Introducing SQL Server Security Features, GDPR – Data Security and Protection" Microsoft Malaysia, 13th Jan 2018.
- "**Cyber Crime as a Service and Quick Win Strategies**" OWASP Malaysia at Microsoft, 18th July 2017
- OWASP Day 2016:" IoT **Security and Defense Against Ransomware**" 17th Nov 2016
- Enterprise Security Today:" Cyber **Attacks on Government Critical Infrastructure**" Tenaga Nasional Berhad, 18th Aug 2016
- Cyber Security Awareness Talk: "**Next generation of Cyber Threats**" Japatan Perkhidamatan Awan (JPA) Malaysia, (Driving Public Service Transformation), 18th Dec 2015
- OWASP MEETUP Q3, "**Mobile Application Security Threads and Vulnerabilities**" University Kuala Lumpur, 14 Sep 2015.
- Job Fair 2014, "**The Realities of Today's Cyber Security Landscape**", University Tenaga National (UNITEN), 5 Dec 2014.
- Malaysian Investment Development Authority (MIDA) "**Top User Weakness in Cyber Environment - User Awareness**", 17 December 2014

Information Security Management Skills

- Information Security Blueprint and roadmap and performing maturity assessment regularly
- IT Security Governance, Risk and Compliance
- Threat Intelligence
- Threat and Vulnerability Management
- Leading the business governance and strategic oversight of information security
- Budgeting and Project Management
- Third Party Evaluation and Risk Management, Performance Review
- Leading Incident Handling, Disaster Recovery and Business Continuity and Cyber Resilience
- Leading Purple Team activities, threat modelling and Hunting
- Analyze key metrics (KPI, KRI) to performance Measurement
- Security Operation Center (SOC) Management
- Vulnerability Management and Penetration Testing
- Leadership and Team Building
- User Awareness & Training
- C-Suite Reporting

Security Standard, Framework Knowledge, Compliance and Regulations (APAC):

- Having Knowledge of RMIT, NIST 800 –X series, ISO 27001, 27002, PCI-DSS, CIS CSC Top 20, OWASP
- Bank Negara Malaysia (BNM) - Malaysia
- MAS- Monetary Authority Singapore - Singapore
- SEC- Security and Exchanges Commission

Technical Skills

- Threat Intelligence Platforms
- Penetration Testing Tools, Technologies, and Methods
- Malware Analysis and Threat Analysis
- Computer forensic tools, technologies, and methods
- Systems and application architectures

- Source Code Review

Online Course Completion and Certifications:

Certified Foundations of Purple Teaming – AttackIQ Aug 2020
Certified Data Privacy Solutions Engineer (CDPSE) – ISACA – Certificate Number: 2002754
Certified Information Systems Security Professional (CISSP): Cybrary, Certificate Number: C-06cb2696e-5517b2, 2017
Certified Information Security Manager (CISM): Cybrary, Certificate Number: C-06cb2696e-3295b3, 2018
Intro to Splunk Enterprise: Cybrary, Certificate Number:C-06cb2696e07951d09a, 2018
COBIT 5: Cybrary, Certificate Number: C-06cb2696e-c3485cda, 2019
Data-Driven Network Security Essentials: LinkedIn, 2018
CHFI v8: Computer Hacking Forensic Investigator Course from EC-Council, 2014.
CEH v8: Certified Ethical Hacking course from EC-Council, 2013.
Designing SQL Server 2005 in Cybertech Institute, 2008.
Developing & Implementing Windows-based Application with Visual C#. Net in Cybertech Institute, 2008.

Membership:

1- OWASP Malaysia Chapter
2- ISACA Malaysia Chapter

Publication:

Book:

KAAPAGAM ACADEMY (Under Company Copyright)

- Android Application Vulnerability Assessment and Penetration Testing
- Network Vulnerability Assessment and Penetration Testing
- Web Application Vulnerability Assessment and Penetration Testing

Technical Reviewer Board Packetpub Publication:

- Kali Linux Wireless Penetration Testing Essentials

Journal:

- **Reviewer Member** of "International Journal of Cyber-Security and Digital Forensics (IJCSDF)", since 2012 to present. (Hong Kong).
- Reviewer member of "International Journal of New Computer Architectures and Their Applications (IJNCAA)", since 2013 to present. (Hong Kong).

Conferences:

- Many IEEE Conferences around in Malaysia and other Countries, detail information is available on demand.

Education:

M.Sc. in Computer Science, University Putra Malaysia, in the field of Security in Computing, 2012-2015.
  - Thesis Topic: "Thesis Topic: "Live Forensics Investigation Framework for Raspberry Pi "

B.Sc. In Software Engineering, Azad University, Lahijan, Iran, 2005-2010.
  - Thesis Topic: "Attack Analysis and detection by investigating the server Logs"

Language

English: Fluent
Persian: Native Speaker
Malay: Moderate