https://linkedin.com/in/karthikmalla

KARTHIK MALLA

E: me@karthikmalla.com
M: 0451 123 299

ADDRESS
16/164 Culloden Rd.,
Marsfield, NSW 2122

ABOUT ME

A professional Security Consultant & Full Stack Security Integration Developer with more than 9 years of industrial experience. I have strong coding skills in multiple languages and worked with the most recent security tools to protect corporate environment with high-end cyber security techniques that can challenge complex modern cyber-attacks.

My experience lies in Security Incidents & Event Management, Threat Hunting, Investigating, PCI compliance, Splunk, Splunk Enterprise Security (ES) and DLP etc.

VISA STATUS

Permanent Resident – Skilled Migration Visa (No restrictions and no sponsorship required)

KEY DELIVERABLES

- As a single resource I installed & configured complete DLP solution in on-premises servers of Suncorp Group and wrote DLP policies for Web, Email & Endpoint using Symantec DLP.
- Integrated Symantec DLP logs with Splunk and created dashboards to categorise DLP incidents based on anomaly and improved the DLP policies.
- Able to deliver complete DLP setup, writing banking level policies & Splunk integration for Suncorp Group in just 4 months contract as a single resourse.
- At Qantas, I discovered an actual SQL Injection that was leaking sensitive data and had not been blocked by WAF.
- At Qantas, I detected a vulnerability that lets attackers to reset Qantas staff “active directory” accounts without providing any previous password or answering security questions.

- At Qantas, I wrote Splunk use-cases to design dashboards, raise alerts and generate reports.
- At Mash Marketing, I was pivotal in setting up their website. Ensured the network was more secured and performed pen-testing where I found and reporting numerous potential vulnerabilities.
- At Queensland Supreme Court project, I was able to complete the project within the given tight project deadlines.

EDUCATION

- Bachelor of Engineering – Computer Science (Anna University, India)
- Microsoft Visual C# .NET Certification (A Grade) from NIIT
- XML and ADO.NET Certification (A Grade) Certification from NIIT
- Obfuscation (Code & Web Security) Certification from VIT University
- Web Services & Tools Certification from Arunai Engineering College
- Cisco Routing Basics from Cisco Academy

SKILLS

- **Languages & Frameworks**
  C | C++ | C# | Visual Basics | Microsoft.NET | PHP | Perl | Python | Ruby | Rails | Shell | ABAP | Java | HTML | JavaScript | CSS | jQuery | Angular JS | VBScript | SSH | jSON | XML | AJAX | Solidity

- **Application Program Interfaces**
  Web API | jSON | XML | ReST | Soap

- **Databases & Indexers**
  Oracle | MySQL | SQL Server | PostgreSQL | MS Access | MongoDB | Sphinx | Solr | Elastic Search | LDAP

- **Security Incidents and Event Management**
  Splunk | Splunk Enterprise Security (ES) | ArcSight

- **Network Firewalls**
  Palo Alto | Trend Micro | Juniper | Sophos Firewall | McAfee | Checkpoint | F5

- **Web Application Firewalls**
  Akamai | Imperva | AWS WAF | Cloudflare | F5

- **Endpoint Security**
  Crowdstrike | Trend Micro Security Suite | Sophos Endpoint Security | McAfee | Kaspersky Total Security | Symantec Endpoint

- **Identity Access Management (IAM)**
  Microsoft Active Directory | Microsoft Azure | PAM | FIM | MIM | Open ID | RSA Tokens

- **Information Rights Management (IRM)**
  Microsoft Active Directory | Microsoft Azure

- **PCI Compliance Monitoring**
  Qualys Monitoring | Metasploit

- **DevOps Automation**
  Docker | Puppet | Chef

- **Cryptography & Data Security**
  a. **Encryptions** – RSA, Key Pairs
  b. **Hashing** – MD5, SHA
  c. Proxies – Squid, Nginx, Websense
  d. Virtual Private Network
  e. **Network Encryption** – SSL, TLS
  f. Disk Encryptions – Bitlocker, AWS Disk Encryption

- **Endpoint File Audit**
  Windows Security Audits | Linux AuditD

- **Authorisation & Access Management, Anomalies and Alerting**
  Brute-Forcing | Account Lockouts | Account Creation | Account Modification | Privileged Group Modification | Domain Admins Modifications | Staff Login to unauthorised workstations

- **Data Loss Prevention**
  McAfee ePO | Symantec Enforce Server

- **Remote Access and Remove Access Events Monitor**

- **DNS Monitor**
  InfoBlox | MX ToolBox

- **Threat Hunting**

- **Penetration Testing**

MetaSploit	SQLMap	Wireshark	SSL Testing	Manual PenTesting	Cookie Strength Testing
BeEF	nMap	Dmitry	Session Management	OWASPZap	

Senior Security Engineer	Insurance Australia Group	Oct 2017 – Present

- Developing Splunk Enterprise Security use-cases.
- Writing Splunk correlation searches and improving existing Splunk ES correlation searches to align with the business model and reduce the number of false-positives.
- Tuning the Splunk SIEM incidents.
- Installing ServiceNow app for Splunk.
- Integrating Splunk incidents to ServiceNow SecOps.

Security Analyst	Suncorp Group	Jun 2017 – Oct 2017

- Installing, configuring and managing Symantec Enforce Console Three Tier Platform and writing policies for data loss prevention that supports Windows 7 Embedded in Thin Client Wyse Terminals.
- Upgrading bluecoat proxies to SG400-30
- Upgrading Blue Coat Content Analysis CAS to S400-A3
- Upgrading Blue Coat Malware Analysis to MAA-S500-10
- Reviewing and updating firewall policies of F5.
- Setting up Splunk add-ons, on-boarding logs and creating dashboards and generating Splunk reports.
- Monitoring DLP and Firewall policy behaviour in Splunk.
- Creating Splunk dashboard for Application Security Management (ASM/WAF).
- Creating Splunk dashboard for Blue Coat traffic & bandwidth of internal staff.
- Testing network compliance using Splunk logs.

Security Engineer	Mash Marketing	Jan 2017 – Jun 2017

- Improving the company Security Posture.
- Reviewing the ruby on rails code and updating the large-scale application to the latest version of ruby & latest version of rails with thousands of lines of hand written code.
- Performing database migrations and adding encryptions & hashing to the sensitive data wherever required.
- Writing use-cases for Splunk to create dashboards, generate reports and generate alerts. Investigating events and performing drilldown searches to identify the origin.
- Performing penetration testing and improving the WAF rules wherever required.

Security Analyst	Qantas Airways	Sep 2016 – Jan 2017

- On a daily-basis, I did review the incidents in Splunk Enterprise Security and look through dashboards & run search queries to investigate it.
- Designed & developed Splunk use-cases to create alerts for detecting anomaly & vulnerabilities in IAM. IRM, DSS, DLP, PCI Compliance, Malware, Firewalls, DNS, Proxies, etc.
- Migrating logs, dashboards and search strings from ArcSight to Splunk.
- Designed Splunk dashboards to visually identify the treats and WAF activities to identify the potential & actual treats that are not blocked by WAF.
- Monitored logs from 9000 servers hosted in AWS, IBM, TCS, Fujitsu & other data centres and work on Windows, RHEL, Solaris, Mainframe, AIX, etc.

Security Engineer	Mash Marketing	Jan 2016 – Aug 2016

- On a daily-basis, I did review the incidents in McAfee ePO dashboard & AWS WAF and respond to the incidents.
- Created AWS instances with security groups, disk encryptions, IAM, installing patches, backing up, snapshotting.
- Setup cloudfront, AWS WAF, replicating data across multiple availabilities zones, monitoring EC2 performance & usage.
- Installed McAfee ePO and did setup DLP rules and application access rules for the client workstations.
- Created auto scaling groups for the AWS instances.
- Configured VPN connection with proxy servers.
- Installing Splunk and Splunk Enterprise Security App for SIEM and compliance monitoring.
- Developing Splunk use-cases for PCI continuous monitoring.
- Performed Penetration Testing.

Security Integration Dev	Onion Blue	Sep 2015 – Jan 2016

- Configured network as per PCI Compliance Regulations Checklist.
- Designed the application as per the standards of OWASP.
- Connected the ReSTful API to call Sphinx using encryption.
- Deployed the AWS instances for this project.
- Configured firewall and IAM rules for the AWS instances.

Security Integration Dev	Queensland Supreme Court	Jan 2015 – Sep 2015

- Designed the application as per the standards of OWASP.
- Deployed the AWS instances for this project.
- Configured the WAF and McAfee tools in the instance.
- Create Splunk to detect security breaches, analytics.
- Assembled IAM roles within the web application for access management.
- Built ReST API for external access of the application.
- Configured the web server and mail server with SSL certificates.

- Monitoring events in ArcSight for identity access management, web application firewall and improving WAF & firewall rules.

Blockchain Developer	Purchase Bitcoin	Jul 2014 – Jan 2015

- Initially developing apps for Bitcoin Blockchain to sign plain text message into Bitcoin Blockchain.
- Created API to generate wallets.
- Created apps & API to sign transactions.
- Created API to sign plain text with the public key and decrypting it using private key.
- Created API to check the blockchain for transaction history, confirmations, balance, etc.
- Worked on data encryption, key pairs, distributed ledgers, etc.
- Later connected it to Ethereum using Solidity (in 2016 soon Ethereum arrived in market).
- Configured the network as per PCI compliance regulations checklist.
- Developed a payment gateway for bitcoin.

Security Integration Dev	Expedia (EAN)	Dec 2013 – Jul 2014

- Designed Web Application as per PCI Compliance Regulations for Web Application.
- Created Web Application as per OWASP.
- Deployed the dedicated cloud server for this project.
- Configured IAM for this web application.
- Created encryptions for REST API for EAN XML & JSON API.
- Built up WAF and cloudflare, configured firewall rules, web server, SSL, mail servers, etc.
- Configured ArcSight to monitor server workloads, network traffic, applications usage, Endpoint events, anti-malware events, firewall events, identity access management, etc.

PATENTS

1. Remote Accounts Suspension – USPTO 2011
2. Unique Password Generation with/without hashing – USPTO 2011
3. URL Session parser for cross language scripting – USPTO 2011
4. HID bypassing for spam prevention – USPTO 2011
5. Email public reference code for spam prevention – USPTO 2011

EMPLOYMENT REFERENCES

Will be provided later on request