UDAYKUMAR LOKHANDE

+971-588600185 udayom@gmail.com



**7 years of IT experience, working as Cyber Security Management / DevSecOps Lead**

# Key Skills:

* DevOps / DevSecOps Automation CI/CD Implementation
* Risk Assessment and Management
* Make Policy Procedure for Cyber Security
* Vulnerability Analysis and Penetration Testing
* Project Management
* Ethical Hacking and Cyber Crime Forensic Investigation

# Accomplishments Summary:

* I am working as a Cyber Security Manager for ASGC UAE placed by Khidmaty Government Services
* I have extensively worked on the Governance, risk and compliance, Ethical Hacking, VAPT, Automation and DevOps / DevSecOps workflow Implementation as Lead for 3 years in Capgemini
* I have also worked as Policy and Procedure developer for Security perspective for year in Finacus Solutions

# Certifications:

* AWS Certified Solution Architect – Associate
* AWS Certified Cloud Practitioner
* Certified Ethical Hacker v10
* Agile Methodology and Project Management
* Diploma in Cyber Law
* PCI DSS Qualified Implementer
* ISO 27001 Lead Auditor

# Employment History:

* **1 Years:** April 2018 till Date, **ASGC** via Khidmaty Govt. Services, UAE
* **1 Years:** June 2017 to March 2018, **Finacus Solutions** Pvt Ltd, India
* **3 Years:** November 2014 to June 2017, **Capgemini**, India
* **1 Years:** November 2013 to October 2014, **Asian Associates**, Mumbai, India

# Educational Qualifications:

* 2012-2014, M.Eng. (IT) from University of Mumbai, CGPA - 8.49
* 2008-2012, B.Eng. (Electronics and telecommunications) from University of Mumbai, 67%

# Projects in reverse chronology:

April 2018 till date:

* Client: ASGC, UAE
* Role: **Cyber Security Manager**
* Responsibilities: Lead reporting to CIO for Cyber Security domain with the responsibilities of
  + Vulnerability Analysis
  + Penetration Testing
  + Risk Assessment
  + Governance, Risk, Compliance
  + Automation
* Description:

Operational and Governance related tasks that relates to Security for Client ASGC, Dubai. Major task includes the Defining and Implementation of Information Security Policies and Procedures as per ISO27001 Standards.

The Automation of Management Reports, Analyze the vulnerabilities found in infrastructure by Vulnerability Analysis and Penetration Testing (Manual + Automated), Threat Remediation, highlight risk to management, risk assessment, vendor management, security checks for vendor, hardening checks on the Oracle Linux operating system, schedule Antivirus scans and highlight the Major vulnerability to IT Infra team, schedule patch management, Ensure compliance of the policies on the servers, Manage and Administer IT security and Forensic tools such as LanSweeper, QualysGuard, Symantec Endpoint protection, ATP, ETP, EDR, MS Office 365 Admin, Azure Portal Admin, Cloud Server Management Activities like New Provisioning server, Migrate, Destroy server etc.

Perform VAPT on in-house Applications using OpenVAS. Manage AWS cloud EC2 instance, SIEM configuration (AlienVault), Reporting, Demonstration. Investigation of the attacks, Fortinet Firewall Rules review (nipper), log and memory-based analysis, Forensic evidence gathering.

Technical Policy defining and Implementation in Symantec Endpoint Protection, Data Leakage Protection (DLP), Email+Cloud Security, Email Threat Protection (FireEye, Microsoft, Mimecast), Web Isolation etc.

June 2017 To March 2018:

* Client: Multiple Banks across India and Latin America (Paraguay)
* Role: **Cyber Security Manager** (CISO)
* Responsibilities: Lead reporting to Board of Directors for Cyber Security domain with the responsibilities of
  + Vulnerability Analysis
  + Penetration Testing
  + Risk Assessment
  + Governance, Risk, Compliance
  + Automation
* Description:

Automation with Security Compliance checks, Policy procedures defining, ISO/IEC 27001, PCI-DSS implementation, Process Management, Incident Management, Change management, Automation of operational tasks, Internal Security Auditing, Continuous Development and Automation with open-source tools (DevOps), Complete Financial Domain, Payment gateway interface Audit as per PCI DSS Compliance, Process Auditing. Reporting ROC (Report on Compliance), ROV (Report on Validation), Performing ASV Scans as part of PCI DSS Implementation.

Major Responsibility included all the Operational and Governance related tasks that relates to Security for Finacus Solutions Pvt. Ltd. which deals with its various clients (100+) as Reputed Banks spread across India.  
The Automation of business requirements and management, covered Change management, Incident Management, Asset Inventory, Helpdesk, Ticketing, Effort Tracking and Documentation storage Automation. Administering Azure cloud account for system integration of ticketing system and maintenance of cloud virtual machine instance for integration.

From DevSecOps section, have covered configuration, implementation and Maintenance of various monitoring tool for project such as Nagios, Baretail, OpenNMS, Graylog, RanCID. Automated Email/SMS Triggering from monitoring tool if critical alert arrives as per business requirement. Configuring and Administration of Manage Engine PIM Tool Password Manager Pro, WatchGuard Firewall Rules, Implementing Trend Micro Anti-Virus, Involvement of banking domain requires more emphasize on PCI-DSS compliance which talks about internal and external Auditing reports. Jenkins Automation for day to day jobs as well as code deployment on Linux servers via Shell Scripts developed and implemented.  
  
Following Agile Way of Methodology with Sprint Framework and DevSecOps Practice to achieve Automation with End to End Project workflow Integration including Automated Security Check Components!

November 2014 To June 2017:

* Client: Royal Mail Group, UK
* Role: **Cyber Security Analyst & DevSecOps**
* Responsibilities: Lead in Security Team for VAPT and DevOps team for Automation, Major aspects includes:
  + Vulnerability Analysis
  + Penetration Testing
  + Risk Assessment
  + Automation (CI/CD)
* Description:

Manage Audits, Compliance check along with certifications for various standards such as ISO 27001:2013 and PCI DSS. Multi-operational experience in Networking Operations, Systems Administration, Security and Audit & Support of Heterogeneous IT Infrastructure and BCP/DR. Handling Incident Management. Formulating, Reviewing, Upgrading, Developing Policy, Procedures & Guidelines for elements governing/ connected to ISO Standards, Analyze SIEM tools, IDS and Action on Alerts.

Involved in Vulnerability Analysis and Penetration Testing, worked on tools like burpsuite, IBM Appscanner, OWASP top 10, wapiti, Paros proxy, Nikto, Nessus, metasploite etc. IPS and DDOS mitigation device reports analysis firewall rule dump and analysis, proxy logs, user administration, OSSEC, SIEM tool monitoring and configuration, ITIL Tool - Service now. Cyber Forensics and Analysis using tools like The Sleuth Kit, Autopsy, Rekall, DumpIT, Volatility, log2timeline and most of the tools from Kali Linux OS. Handled SOC activities in which Analysis of complete trail of activities of user based on the logs, Forensic report creation (Narrative based) & extracting footprints for legal purpose to be dealt with Legal team.

Digital Transformation of Project: Worked on Multiple open source tools like Nagios, Munin, graphite, Jenkins, Apache, ldap, mongodb, maven, Exim, ELK stack, graylog, graphite, redis-cache, memcache, exim, Linux shell scripting, Doker with Kubernates cluster, Ansible, Puppet. To design business rule-based dashboards in AppDynamic. To make dashboards and alerts in AppDynamics based on Business requirement. AppDynamics deployment, Management, Designing, Dashboard, all setup.

Experience on Atlassian tools like JIRA, Confluence, stash, bitbucket. Studied ITIL Fv4 & worked on Kanban boards for project progress tracking. Project management experience for deployment, schedule.  
Good at Incident, change management, onshore & offshore interaction & Documentation handling, following Agile methodology, Scrum Meetings.

November 2013 To October 2014:

* Client: Multiple FINTECH Companies
* Role: **SOC Lead (Intern)**
* Responsibilities: Analyst in Security Team for VAPT and Monitoring including Automation tool Implementations.
* Description:

Performed Vulnerability Analysis and Penetration Testing, worked on Linux based open source tools like burpsuite, OWASP, Nikto, wapiti, Paros proxy, Nessus, metasploite etc. Implemented and Administered IPS and Performed DDOS mitigation device reports analysis, Forensic Analysis on attack trace, proxy logs, user administration. Complete SOC level Monitoring setup including Nagios, OSSEC, SIEM tool monitoring and configuration.Tweaking in existing scripts/IT Tools for performance boosting and Automating of the tasks performed (While Pursuing Full Time Masters also worked as 1 Year Asst. Prof including this role)