

UDAY KUMAR LOKHANDE

✉ udayom@gmail.com

☎ +971 58 860 0185

🌐 linkedin.com/in/udayom

🔗 <http://udayom.blogspot.com>

Summary

With 6+ Years of Total Experience, Uday has been successful in implementing **Policy** and Procedures as per **ISO 27001** standards in various projects, he has also **implemented procedures** based on **PCI DSS and PA DSS** standard and Handled **Internal Auditing** of same.

He has expertly performed **Vulnerability Analysis** and **Penetration Testings** (Web Application, Server, Mobile, all platforms) and he is good in defending the Infrastructure from External Cyber Attacks (*Blue Team Lead*). He can forensically analyze the origin of **Cyber attack** & trace the behavior/malware/unintentional/hacking activity.

Uday has also evaluated risk assessment for business as part of compliance due diligence. He holds **DevOps / DevSecOps** & **Agile Methodology** experience as well, always looking for the scope of Automation in Infrastructure/ process/ IT and he loves open source tools used for **Cyber Forensics, Ethical Hacking**, VAPT activities. Having teaching background Uday can teach, **explain** complex concepts very well to Juniors as well as **senior Management** with ease.

Top Highlights: (Client Facing)

Presenting

Demonstrating

Delivering

Investigating (RCA)

Certificates:

AWS Cloud Practitioner Essentials (Amazon AWS Training & Certifications)

ISO 27001 Lead Auditor (TuV SuD)

PCI DSS Implementation (Qrc)

Certified Ethical Hacking CEH v10 (EC-Council)

Agile Project Management (Udemy)

Diploma in Cyber Law (Asian School of Cyber Law)

Trainings Attended:

Cyber Forensic & Crime Investigation (University Certification)

ITIL Foundation (L & D)

AWS DevOps (Seminar)

DevSecOps (L & D)

Cloud Computing (University Certification)

Linux Lab (University Certification)

**Pursuing:*

AWS Solution Architect - Associate (Amazon AWS)

ToGAF (The Open Group)

CISSP (ISC2)

Experience



Cyber Security Consultant

Apr 2018- Present

Khidmaty Government Services

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. SIEM configuration (AlienVault), Cyber Operations, Reporting, Demonstration. Investigation of the attacks, Fortinet Firewall Rules review (nipper), log and memory based analysis, Forensic evidence finding (SIEM Log and Dump based)

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

IT Security Manager

Jun 2017 - Apr 2018

Finacus Solutions

11 months

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, VAPT, 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.

Major task included the Defining and Implementation of **Information Security** Policies and Procedures. The Automation of business requirements and management, achieved for organization as part of compliance - *Change management, Incident Management, Asset Inventory, Helpdesk, Ticketing, Effort Tracking and Documentation storage Automation*. Administering Azure account for system integration of ticketing system

From **DevSecOps** section, have covered configuration, implementation and Maintenance of various monitoring tool 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!



Cyber Security Analyst

Capgemini

Nov 2014 - Jun 2017

2 years 8 months

>>> Governance Security :

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 and Guidelines for elements governing/ connected to ISO Standards, Analyze **SIEM tools, IDS** and auctioning on alerts

>>> Operational Security:

Involved in **Vulnerability Analysis and Penetration Testing**, worked on tools like *burpsuite, IBM Appscanner, OWASP top 10, wapiti, Paros proxy, Nikto, Nessus, metasploit 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 and extracting footprints for legal purpose to be dealt with Cyber Law team.

>>> DevSecOps:

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, Automation with Jenkins, Ansible, Puppet*

To design business rule-based dashboards in *AppDynamic*. To make dashboards and alerts in AppDynamics based on Business requirement. **AppDynamics** deployment and complete setup

>>> Project Management:

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



Engineer Internship

Asian Associates

Dec 2013 - Nov 2014

1 year

Performed **Vulnerability Analysis and Penetration Testing**, worked on Linux based open source tools like *burpsuite, OWASP, Nikto, wapiti, Paros proxy, Nessus, metasploit 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.

**This is While in Full Time Master Degree Program (Project research and Engineer Internship overlaps)*



Teaching Associate & Practical Lab Assistant

Terna Engineering College

Dec 2012 - Dec 2013

1 year 1 month

Worked as Teaching Associate @ Terna Engineering College, Nerul, Navi Mumbai.

Subjects taught to Engineering Students : **Linux, Cloud Computing, Network Security, Practicals.**

Worked as Practical Lab Assistant where major responsibility emphasis on Security Measures while developing the application in cloud and on-premise infrastructure. (as a part of Masters' first year).

Worked on **Wireshark, tcpdump** tools used to monitor the run-time user traffic for security measures.

Worked on Linux (4 years) tools like telnet, ssh basic concepts that were required for project work to take ahead.

Worked on the multiple **VAPT** (Vulnerability Analysis and Penetration Testing) tools such as **acutinelx, nikto, wapiti, metasploit, nessus** etc to find out vulnerability in website *CVE/CWE* references and possible solution to fix them.

Got appreciation from Principal regarding good with documentation and presentations.

Got Bounty from principal for finding miss-configuration in *cyberoam* device in college Infrastructure.

Work from **Cyber Security Forensic Analysis** field, **IPS device, UTM** hardware devices (Cyberoam), **firewalls**, Implemented ISMS policy in theory, IP-tracing, *reputation, spam detection, vulnerability testing, penetration testing, CVE findings*. (White Hat Hacking)

Cloud based Instance customization : To make instance more efficient. (IAAS)

Proof reading logs: *Log file analysis*

VMWare and virtualization technologies.

Router configuration : Implementing / routing paths for efficient routing, making subnets.

Representing graphs in sophisticated graphical format using open source tools/

Interaction + Presentation for clients / Representatives. Vendor finalization for Security stack assets.

**This is While in Full Time Master Degree Program (Project research and Teaching together overlaps)*

Education



University of Mumbai

2012 - 2014

Information Technology, 4

Full Time Education - ME IT Project Title : Security As A Service (Sec-AAS) for A Website.

Semester - I credits Subjects

- > Advance Data Mining with Business Intelligence
- > Data Storage Management and Retrieval
- > Network Design and Management
- > Usability Engineering
- > Software Quality Assurance
- > Lab - I (Course Lab)
- > Lab - II (Elective Lab)

Semester - II credits Subjects

- > Advance Software Architecture
- > Enterprise Security and Risk Management
- > Soft Computing
- > Wireless Ad-Hoc Sensor Network

- > Next Generation Network
- > Lab - III (Course Lab)
- > Lab - IV (Elective Lab)

> Semester III and IV -- Project Stage I and Stage II
 Project - Sec-AAS - Security As A Service for A Website
 (Based on Cloud Computing and Vulnerability Analysis via various open source tools with shell scripting)



Welingkar Institute of Management

2015 - 2017

HPGD - eBusiness, FIRST CLASS

WeSchool PGDM course - Hybrid (eBusiness)
 (This is Part Time Education - While working (in Capgemini) - Lectures Attended during Weekends)



Asian School of Cyber Laws

2017 - 2018

Diploma in Cyber Laws, Cyber/Computer Forensics and Counterterrorism, Diploma

Diploma Study about Indian IT Act 2000, Banker's Book Act, Criminal cases, Computer Forensics related cases, and issues regarding Copyright, patents, trademarks etc.

*(This is Part Time Education - While working - Lectures Attended during Weekends)



University of Mumbai

2008 - 2012

Bachelor of Engineering, Electronics & Telecommunication, A

Full Time Education - L-Lecture, P-Practicals , Hours for Week specified in total, Credits on scale 5

Subjects with all Average credits of 5 Semester VII : (Total Credit 20L, 10P)

- > Mobile Communication Systems
- > Fundamentals of Microwave Engineering
- > Computer Communication Network
- > Discrete Time Signal Processing
- > Data Compression and Encryption (Specialization)
- > Stage I Project

Subjects with all Average credits of 5 Semester VIII : (Total Credit 16L, 8P)

- > Advance Microwave Engineering
- > Optical Fibre Communication
- > Wireless Networks
- > Satellite Communication (Specialization)
- > Stage II project (Interference Analysis of IEEE802.11n)



Parle Tilak Vidyalyaya Associations Sathaye College Dixit

2006 - 2008

Road Vile Parle East Mumbai 400 057

Higher Secondary School, Electrical, Electronics and Communications Engineering, 4
 HSC

10+2 Study Passed with Distinction + Merit 81%



Parle Tilak Vidyalyaya Associations Sathaye College Dixit

1996 - 2006

Road Vile Parle East Mumbai 400 057

Secondary School Certificate, Mathematics and Computer Science, A+
 Pre-High School i.e. SSC And Grade 78%

Skills



Threat & Vulnerability Management • Cyber Operations • Vulnerability Assessment • Cybersecurity • IT Service Management

Certifications

Linux Lab • E-cell, Sardar Patel Institute of Technology

May 2009 - Present

ISO/IEC 27001 LA • TÜV SÜD

Aug 2017 - Present

PCI DSS Implmentation • QRC Consulting & Solutions Pvt. Ltd

Aug 2017 - Present

Qualys Certified Specialist • Qualys

May 2018 - Present

Cloud Computing • E-cell, Sardar Patel Institute of Technology

Jun 2010 - Present

Symantec Endpoint Protection - SEP, ATP, WSS, Email Security • Symantec

Aug 2018 - Present

Agile Project Management And Agile Delivery (Crash Course) • Agile KnowledgeTech

UC-COYMV2YG • Jan 2019 - Present

Cyber Security Law (Crash Course) • Pavan Duggal Associates

UC-9AO4OMUI • Jan 2019 - Present

Certified Ethical Hacker • EC-Council

ECC4518960237 • Feb 2019 - Feb 2022

AWS Cloud Practitioner Essentials • Amazon Web Services (AWS)

Feb 2019 - Present