

Contact

ravi.dhungel@gmail.com

www.linkedin.com/in/ravidhungel

(LinkedIn)

www.nepalilad.blogspot.com

(Personal)

Top Skills

Multiagents

Documentation

Fundraising

Languages

English (Full Professional)

Nepali

Certifications

Design Control Requirements

Learning GDPR

Certificate CVSS 4.0

GDPR

Google Cybersecurity Specialization

Honors-Awards

Graduate Assistantship

Publications

Software Quality Challenges Ahead

Engineering Cyber Resilient
Organizations for Insider Threats

Create Travel-tech Products In
Nepal

Addressing security complexities for
the Internet of Things

Ensure cybersecurity for biomedical
device

Ravi Dhungel

Medical Device Cybersecurity Engineer | Author| EB2-NIW |
Mentoring Mental Health & Cyber | Cyber Conference Speaker |
Google L7 SD Local Guide | Born & Raised in Himalayas, Nepal |
High Altitude Hiking/Climbing

San Diego, California, United States

Summary

Expertise on technology management, medical cyber security, and site reliability engineering. Solid foundation on the principles of security, distributed systems, and software engineering supporting large scale distributed systems in telecom, software, biomedical, university, healthcare, and the military. I double majored in computer science and geographic information science from graduate school at Southern Illinois University, Carbondale. A former major of Nepalese Army and a military fellow at Nanjing university of science and technology, a recipient of a self-petitioned National Interest Waiver (NIW) green card. (<1% of green card recipients with a master's degree) and a naturalized US citizen. I taught cyber warfare in Nepalese Army Command and staff College and was a UN military peacekeeper in ONUB mission in Burundi.

I mentor on (medical) cyber security, Nepal, computer science, immigration, mental health, high altitude hiking, and higher education. I am interested in global affairs and south-Asia politics and hiking in the Himalayas. I have published more than twenty articles and whitepapers in cyber security, privacy and digital transformation and a book, The Hope (available in Amazon) - <https://tinyurl.com/2aw948np>

My industry experience coupled with a graduate degree in computer science & Advanced Computer Security from Stanford University and (ongoing) embedded system engineering certificate from UCSD:

- ▶ FDA Design Controls - FDA 21 CFR Part 820.30 for Cybersecurity.
- ▶ Security Risk Management and cybersecurity risk assessment
- ▶ Security Assessment of unresolved anomalies and defects
- ▶ Third party software and libraries
- ▶ Security Architecture Views and security controls

- ▶ Enforcing FDA cyber-security postmarket/premarket guidance's for biomedical devices.
- ▶ Corrective Action and Preventive Action (CAPA)
- ▶ Cyber security frameworks (CIS Top 20, NIST, ISO 2700/27001, Kill Chain, Diamond etc)
- ▶ Threat Modeling (DFD, STRIDE, Attack tree, OWASP, Kill Chain, PASTA)
- ▶ Automated and manual Code review - static scanning
- ▶ Vulnerability Scanning tools
- ▶ Product security engineering (Threat modeling, static/dynamic scanning, vulnerability & pentest)
- ▶ V&V plan - security functional testing and non-functional testing,
- ▶ Exploratory and Penetration Testing
- ▶ Develop Key Security/Risk Indicators (KS/RI) and security metrics.
- ▶ Security Incidence response & complaint Investigations and Root Cause Analysis
- ▶ Privacy, Audit and Compliance (PCI, SOX, HIPAA,HITECH,FDA,GDPR, DOD STIG)

Experience

BD

Lead/Staff Medical Device CyberSecurity Engineer

2022 - Present (3 years)

San Diego, California, United States

- Spearhead initiatives to enhance **Trust, Cyber Risk Management, and Safety** across the Infusion Platforms.
- Lead cybersecurity projects aligned with business objectives, collaborating with cross-functional teams including **R&D, Regulatory, Marketing, HF Engineering and Operations**.
- Conduct and drive **design and architecture reviews** focused on software defects, anomalies, and vulnerabilities.
- Develop security architectures diagrams, threat modeling and secure CICD.
- Manage cyber security Verification and Validation - static and dynamic scanning, SBOM management, penetration testing across the total product life cycle.
- Secure coding, cybersecurity metrics and trends.
- Provide support for internal and external regulatory audits

- Ensure adherence to cybersecurity standards with **ISO 13485, IEC 62304, HIPAA, FDA, and AAMI/FDA cybersecurity guidance**.
- Maintain Requirement Traceability Matrix (RTM)** for cybersecurity requirements and cyber labeling.
- Support cyber 510(k) clearance for new and sustaining products in Infusion Platforms.
- Drive improvements in ** Cyber Quality Assurance**, including Quality Plans, CAPA processes, and audit readiness.
- Lead **Design Assurance* efforts, including design controls, Design History File (DHF) management, traceability, and risk management.
- Manage **Vulnerability Management** processes in accordance with FDA's pre-market and post-market cybersecurity guidance.
- Promote excellence in secure software development methodologies.
- Ensure compliance with **Federal Regulations** including HIPAA, GDPR, FDA 21 CFR 820.30, STIG, and FIPS 140-2.
- Apply industry standards such as **FDA guidance, NIST CSF, NIST RM, AAMI TIR57/97/SWE96, IEC 81001-5-1, and UL 2900**.
- Promote Coordinated Vulnerability Disclosure - cyber labeling and white papers.
- Implement symmetric/asymmetric encryption, homomorphic encryption, PKI, TPM, secure boot, and network security protocols.

Health-ISAC
Member
January 2023 - Present (2 years 11 months)

<https://www.medicsec.com/hp/>
Managing Editor (Medical Cybersecurity)
2024 - Present (1 year)
San Diego, California, United States

Develop comprehensive cyber security portal for medical device cyber security practitioners. It includes:
Regulatory compliance directives
SOP/SWI to develop resilient cyber security programs
FDA compliances
Templates for the deliverable required for 510K submission.
Emerging technologies and security of medical devices that includes AI.

IBM, The Rising Nepal, KU Computer Club, NepalArmy , Planetrisk, LinkedIn et. al.

Freelance Writer - More than 20 articles and white paper published in technology

March 2000 - Present (25 years 9 months)

Nepal, US

Freelance contributor on National security, border management, Cyber security , immigration

Articles published on The Rising Nepal, The Kathmandu Post, The Himalayan Times

White Paper and articles contributed to IBM, PlanetRisk, linkedin etc

UC San Diego Health

Principal Cyber Security Engineer

2019 - August 2022 (3 years)

San Diego County, California, United States

- Enabling digital health focusing on privacy and data security by design at UCSD medical center.
- Strategy, governance and data framework for digital health transformation and PHI data.
- Advising and supporting world class medical researchers on PHI security and privacy.
- CyberSecurity- Engineering, Operations , Product and Cloud (AWS, Azure, GCP, yourcloud)
- Biomedical and product security engineering
- Threat modeling , static/dynamic scanning, vulnerability , pentest management and security review
- Major Engineering Projects:
 - Microsoft Security and Compliance Center
 - Endpoint/Email data loss prevention system
 - CASB/DLP
 - SSDLC -Static scanning
- Incidents response, forensics and investigations
- Development of SOP/WI for Incidence Response and Investigations

Perspecta

Cyber Security Architect

June 2019 - October 2019 (5 months)

Greater San Diego Area

ServiceNow

Senior Cybersecurity Engineer

May 2018 - May 2019 (1 year 1 month)

Greater San Diego Area

- /~Lead Proof-Of-Concepts (POC) and security projects with cross functional teams - product, HR, finance, legal etc
- /~Work with legal teams to refresh security policies on Employee Privacy Statement, Acceptable Use Policy (AUP).
- /~Cloud Security-Azure (security center, key vault, information protection, DDOS protection, application
- /~ Improve vulnerability, risk, and incident management processes.
- /~ Secure applications, infrastructure, cloud and end point security.
- /~ Develop and automate dashboard for KPI and security metrics
- /~ Lead Data loss and protection initiatives - CASB, DLP, Email Security etc.
- /~ Tools(Linux, Bash, Golang, OpenSSL,nmap,Tcpdump)
- /~ Support end point solutions (AV,Tanium,DLP)
- /~ Develop DLP policies for compliance (PCI, FINRA, PII, HIPAA)
- /~ SME of Email security (Proofpoint) - firewall, authentication, spam detection, virus protection, TAP (Targeted Attack Protection)
- /~ Training and Knowledge transfer (SOP, KB articles, Architectural diagrams, Metrics)

Dexcom

Cybersecurity | Principal Cloud and Product Security Engineer

2017 - 2018 (1 year)

Greater San Diego Area

- /~ Lead Cybersecurity Initiatives - Strategy, Framework, Engineering, Compliance, and Operation.
- /~ Identify security gaps, controls and remediate vulnerability.
- /~ Lead vulnerability management program (OpenVAS, Qualys)
- /~ Threat Modeling of application, infrastructure security.
- /~ Lead Security Root Cause Analysis (RCA) & Incidence Response
- /~ Security engineering principles: Confidentiality, Integrity, Availability & Safety.
- /~ Develop resilient end to end frictionless security controls for health data pipelines.
- /~ Develop Key Cyber Security Indicators(KCSI) and metrics to measure cyber-security deliverables.
- /~ Demonstrable Compliance enforced as a code.
- /~ Support Quality, External/Internal security compliance requirements.
- /~ Documentation- Standard Operating Procedures(SOP), WI - Work Instruction
- /~ Security services- Research & Development (ThreatIntel, Agents/ML,)

- /~ Mentoring, awareness, and training
- /~ Liaison with Legal counsel on regulatory compliance, policies, data governance and security incidence response.

Technologies stacks / Processes

- # Security Ecosystems (IPS/IDS/End points, Netflow, SIEM)
- # Google/AWS Cloud Platform (Cloud Security Engineering and hardening)
- # Product/Infrastructure Security review
- # Threat Modeling and attack surface hardening
- # Compliances - FDA ,SEC,HIPAA,PCI,GDPR,HITECH
- # Frameworks - NIST 800-XX,ISO/IEC 27001, UL
- # FDA post/pre market cybersecurity guidelines
- #API security
- #AWS SDK, Goolge SDK, Bash,Golang,C
- ISO/IEC 30111:2013: ISO/IEC 29147:2014: NH-ISAC,CSF;AAMI TIR57, IEC 80001

Information Security, Intuit

Cybersecurity | Senior Information Security Engineer

February 2016 - October 2017 (1 year 9 months)

Greater San Diego Area

Security reference architecture, processes and cyber risk assessments
Strategic and operational support for security controls, guidelines and best practices

End-to-End Security Engineering, Secure Design, Deployment & Patterns
(AWS / Gcloud).

Tools and Automation (security metadata, compliance assessments, auditing - RESTful API)

Secure SDLC, Agile Development Practices, DevSecOps Engineering Practices

Threat Intelligence Platforms Engineering (SIEM/IPS/EndPoints/IDS/AV)
- Splunk, Tanium, Fireeye, SourceFire, Lancope

Standard Operating Procedures & Architecture Documentation

Root Cause Analysis (All Stacks)/ Incidence Response Plan / Processes

Risks Management - Threat Modeling, Attack Vectors, Resource Enumeration, Risk Grading

Identify security vulnerabilities , risks, and implement mitigation plans.

Evaluate security tools and services, in an individual and/or project leadership role.

Influence security policy & security initiatives across a large organization.

Compliance, Security Controls and Governance Support (NIST/PCI/SOX etc)

Forensics Infrastructures - Processes and Operations, Reverse Engineering

Security Science, Research & Development

Mentoring and Knowledge Sharing

University of San Diego
Linux Systems Architect
February 2015 - April 2016 (1 year 3 months)
Greater San Diego Area

Enterprise Linux System Architect for Academic and Research Platforms
Subject Matter Expert (SME) of High Performance Computing (HPC) and Linux
Infrastructures
Advise CIO/Directors /Professors on Internet of Things, Big Data , Research
computing and Security
Lead project, deliver milestones, motivate team members and take ownership
Mentor and knowledge transfer (Design Documents, Operating
Procedures ,Training etc)
Identify business necessity, process disruptions, align technology and
decrease cost

MAJOR ACCOMPLISHMENTS:

- * Principal Engineer to Lead, design and deploy First High Performance Cluster (HPC) - SABER
(RHEL, TORQUE/MOAB, DNS, DHCP,XCAT, MPI)
(project management, design, deployment and operation)
Completed the project months before the deadline.
- * Developed enterprise technical documentation(>100 pages)
- * Designed provisioning (PXE/DHCP/TFTP) infrastructures to deploy bare metal linux nodes.
- * Install and configure analytic software (Matlab, Maple, Mathematica, SPSS etc) on Linux nodes
- * Provide Linux/Unix support to faculty members that includes provisioning of operating systems, deploying applications, monitoring applications and developing disaster management policies.
- * Authored Tools and Automation (MPI/C/Python/Bash)
- * Monitoring / Alarms

- * Manage , deploy and support production - VM's/applications on Vsphere with DRS/HA
- * Root Cause Analysis (RCA)
- * Performance Engineering (Network , Load Balancers, Operating Systems, Applications,JVM)
- * Taught Linux101
- * Secure Design , Application , Infrastructure and Network Security

<http://www.helpnepalearthquakevictims.social>

Architect & Co-Founder - >Uniting Together To Help Nepal
May 2015 - August 2015 (4 months)

US--->Nepal

#This is smart humanitarian programming at Everest, Nepal
#Lets compete for this programming
#Written By : ravi.dhungel@gmail.com
Truly open source (Version 1.1) – Please distribute this code. Copy- left Policy

WHILE TRUE

Do

For crisis-Happening in Nepal

Do

Echo "HELP NEPAL"

lynx <http://www.helpnepalearthquakevictims.social>

For help in food shelter water first-aid medicine ...

Do

Echo <http://lnkd.in/bDKgqqD>

Echo "PLEASE ACT – HELP NEPAL"

Done

Done

Done

For Thanks To Ericsson, Sprint, Microsoft , Google, T –Mobile,Facebook

Do

Echo “ \$ Thanks - Thanks for your self-less service “
done

Ericsson

System Reliability Engineer II

November 2013 - February 2015 (1 year 4 months)
Overland Park, KS

System Reliability Engineer for Data Mobility National Platforms
(DNS,BMI,OAP,DEG)

* Thirty Three Data Centers (>4000 Physical Servers and Load Balancers (F5))

* Five Major Platforms that includes DNS

* Nation's Highest Tier engineer for Tier I Telecommunication Service Providers (55+ million users)

Lead/participate for Application, Network, OS,DNS -Root Cause Analysis Troubleshoot and mitigate DDOS (DNS, Applications)

IP Packet Analysis(Tcpdump, Wireshark)

System , Applications and Security upgrades & patches

Installed , Configured and Managed RedHat in IBM Blades; Sun OS; HP Blades;Viprion F5;NAS

Load Balancing -GTM/LTM (Virtuals, Pools , Monitors, irules) on bigip/viprions F5

Project Management (sales engineers, design engineers, platform leads)

Authoring Internal System Tools and Automation

* Automating Continuous Integration (Scripts, Alarms, Patches,Updates)

* Authored Internal Dashboard (Bash, Python, PHP)

* Authored Internal Tools (Bash, C, PHP, Python)

* Authored File , String and Log manipulation Tools (Python, Awk,bash,C)

* Authored scripts to report operational Analytic for managers and higher executives

* Author scripts for Performance Engineering (Process, Network and System)

Authored / Revise Standard Operating Procedures (SOP)

Mentoring and Training

*Aced IP Essentials Certifications Exam of Ericsson within first 100 days of employment.

CafePress Inc.

Linux/Hadoop System Engineer

May 2013 - November 2013 (7 months)

Louisville, Kentucky Area

Production Linux/Hadoop Engineer for www.cafepress.com

Design, Deploy and Operate Apache Hadoop Clusters in Staging and Production

Deploy VM's using Cobbler/Xen Virtualization (>1000 Servers - VM/PM)

Troubleshoot JVM and Heap Memory on Java applications/ memory leaks on clusters

Deploy and provision OS using Chef / PXE/DHCP/TFTP

Provision/Manage nodes on Amazon EC2 and two data centers.

Monitoring / Alerting (Graphite, Elastic Search , Nagios)

Infrastructure Upgrades/ Capacity Planning (Hardware, Memory etc)

Support QE, DBA, Developers and Tier I specialists

Troubleshoot (Cisco UCS, HP, Dell, EMC ISILON)

Problem, Incident and Change Management

Data Center and Vendor Management

Mentoring and Training

Documentation

Computerized Assessments & Learning

Linux System Administrator

January 2013 - May 2013 (5 months)

System & Network Engineering

Infrastructure Management, Integration and Automation

Monitoring and Virtualization

Incident, Problem and Change Management

Support Development, QA and Production

Collaborate with Ops Engineers, Developers, QA's , and Project managers

Documentation and Troubleshooting

Southern Illinois University Carbondale

System Administrator (Graduate Assistant)

January 2011 - December 2012 (2 years)

Carbondale, IL

Manage System Softwares and Services in EGIS, AGIS labs.

Maintain Scientific Computing Framework

Technical Documentation and Inventory Management

Systems Support for more than 200 students and faculties.

Configure, update , and install system / applications patches.

Lab instructor Introduction to GIS - Summer of 2012

Nepalese Army

Lead System and Security Engineer - Army Major

May 2002 - November 2010 (8 years 7 months)

Kathmandu, Nepal

System Engineering Manager/ Lead System Engineer (Major)

Cyber-warfare Instructor - Army Command College

Subject Matter Expert (SME) of System Engineering, Information Security and Cyber-warfare

Lead system engineering team by communicating job expectations; disciplining and motivating the platoon

Lead project by coordinating resources within military departments, DOD and vendors

Design Disaster Recovery and back-up procedures

Develop Information Technology Strategies (C4ISR)

Accomplished financial objectives by forecasting requirements

Maintains professional expertise by attending national workshops; reviewing professional publications; bench-marking state-of-the-art practices; participating in professional societies.

Directly commanded >100 IT experts that includes junior engineers and Officers.

Research and Development Engineer - Highly classified Actionable Intelligence Technologies****

Education

UC San Diego

Professional Certificate., Embedded System Engineering · (September 2023 - July 2026)

Stanford University

Professional Certificate, Advanced Computer Security

Southern Illinois University, Carbondale

Master of Science - MS, Computer Science

Southern Illinois University, Carbondale

Master's Degree (Double Major), Geography and Environmental Resources and Computer Science.

Nanjing University of Science and Technology
Diploma in Computer Engineering, Computer Engineering