

Gordon MacKay

Senior Software Consultant

Quandary Peak Research

205 S Broadway, Suite 300

Los Angeles, CA 90012

Phone: 210.942.4244

Email: gordon@quandarypeak.com

PROFESSIONAL ACCOMPLISHMENTS

- Investigated, searched over 1.2TB of Wireless technology code and identified key infringing software related to patent litigation case.
- Granted three software patents related to cyber-security scanning, correlating and management (US 9667643, US 9667642, and US08938531).
- Architected, designed and lead team in emergence of multi-tenant vulnerability management solution now handling millions of scans per week.
- Presented and evangelized cyber-security technology solutions at many conferences including RSA, ISC2 Security Congress, ISSA International Conference, Many USA BSides Conferences.
- Expert in software with 25+ years of experience as an engineer and programmer.
- Currently serves as a software intellectual property and Due Diligence consultant focusing on software patents & trade secrets, software development best-practices, and digital copyright/code theft.

CAREER EXPERIENCE

- **Senior Software Consultant**

July 2021 – present

Quandary Peak Research, Los Angeles, CA

Bringing my computer science, software architecture and strong source code implementation knowledge to bear, in serving Quandary Peak clients such as investors, private equity firms, and companies pursuing mergers, acquisitions, IP Litigation and more.

- Researching patents and related technologies as part of investigating patent infringement cases.
- Searching through millions of lines of software and finding source code related to patent claims.
- Assisting in writing expert testimonial reports related to patent infringement cases.
- Evaluating software architectures of various products and assessing overall characteristics, strengths and weaknesses.
- Analyzing source code to opine on various software characteristics such as scalability, interoperability, security and extensibility.
- Employing suite of tools to programmatically detect and inventory the presence of open-source software and potential exposure to problematic open-source licenses and security vulnerabilities.
- Interfacing with Private Equity, VC, and other clients, as well as executives/technical team from target companies.

- Documenting and conveying technical findings to clients in the form of formal reports and/or executive briefings.

- **Executive Vice President and Chief Technology Officer**

Jan 2010 – Apr 2021

Digital Defense, Inc., San Antonio, TX

Spearhead, develop and maintain DDI's technology roadmap by teaming up with others – cross functional DDI teams, 3rd party technology partners, and most of all, with DDI clients. Oversee, manage, encourage, help DDI's Technology team in emerging and delivering valuable integration solutions between frontline vulnerability management platform and other IT and security technologies.

- Successfully managed, guided, mentored and acted as player/coach with multiple technology teams, including feature development, vulnerability research, and quality assurance team by steering operational efficiency.
- Served as Agile Product Owner for the DDI Technology Integrations team, helping define the team's stories, prioritizing the team's backlog, interfacing with DDI Product Management and the Executive team to ensure effective prioritization of integrations on the roadmap.
- Interfaced and socialized with DDI clients and prospects to understand and negotiate requirements for integrations between DDI's vulnerability management platform, and IT/security solutions thereby helping clients reduce operations spend by 20%.
- Spearheaded vulnerability management gamification idea within the Frontline VM platform which enabled Digital Defense to anonymously compare client risk scored and influenced entire ecosystem to minimize security risk.
- Developed, interacted and worked with legal team, and ultimately attained 3 patents for DDI's vulnerability scanning and management technology.
- Worked side-by-side and contributed to DDI's Marketing arm by serving as key spokesperson for DDI's solutions. Presented on security related topics at many security conferences, including RSA security, ISC2 Security Congress, ISSA International Conference, Many USA BSides Conferences, while highlighting across media and security articles including, Forbes, Fox Business News, CIO review, SoftPedia, and IT World Canada and leading DDI blog website www.digitaldefense.com.

- **Vice President, Platform Development**

Jan 2006 – Jan 2010

Digital Defense, Inc., San Antonio, TX

Partnered, managed, guided and mentored large team of developers to develop security features for frontline vulnerability management platform as well as engaged with clients and internal stakeholders to consolidate feature requirements, set priorities and meet expectations.

- Served, managed and mentored a large team of software developers, vulnerability researchers, and QA team members in the development, delivery and ongoing maintenance of DDI's products.

- Spearheaded deployment of key DDI frontline features, including application-level encryption of cloud data, requiring expert familiarity with symmetric and asymmetric encryption.
- Oversaw maintenance and execution of relational data architecture model for all vulnerability management software features.
- Developed security features for SaaS based Frontline platform by directing DDI development organization

- **Principal, Software Architect**

Nov 2002 – Jan 2006

Digital Defense, Inc., San Antonio, TX

Led a team of 4 engineers in architecting, designing and deploying the company's multi-tenant SaaS-based patented in-house vulnerability management platform. Acted as team's primary data architect, as well primed the Java based business logic layer.

- **Senior Software Engineer and Team Lead**

Jan 1996 – Nov 2002

Alcatel USA, Plano, TX

Led team of engineers designing and implementing internal in-memory database for Alcatel VoIP Softswitch product.

Worked on Call Processing and platform features for Alcatel/DSC switching group. Included design and implementation for call processing features involving SS7 protocols as well as call-state software design. Worked on features such as Local Number Portability, Calling Card features, and more.

EDUCATION

- **Bachelor's of Electrical Engineering, Computer Engineering Option.**

May 1992

CERTIFICATIONS

- **CISSP (Certified Information Systems Security Professional)**

LITIGATION CONSULTING

- **Provisur Technologies, Inc. v. Weber, Inc.**

Jan 2022 – Present

- Case Number: 5:21-cv-06113
- Filed in: Western District of Missouri
- Filing date: 09/21/2021
- Searched source code for multiple versions to identify software related to patent claims. Printed significant findings to PDF. Interacted with attorney team to share critical findings.

- **Flypsi, Inc. v. Dialpad, Inc.** **Jan 2022 – Present**

 - Case Number: 6:21-cv-00642
 - Filed in: Western District of Texas
 - Filing date: 06/21/2021
 - Inventoried source code for 17 million lines of code, identifying software architecture employed and major software technologies used.
 - Searched through millions of lines of code identifying source code that maps to infringement contentions and patent claims. Utilized tools such as Understand, as well as Linux file utilities such as grep and find.

- **Roche Diabetes Care, Inc. v. Insulet Corp.** **Jan 2022 – Present**

 - Case Number: 1:20-cv-00825
 - Filed in: District of Delaware
 - Filing date: 06/17/2020
 - Examined software design specifications and mapped these to Insulet's source code in order to assist in responses to infringement.
 - Searched through source code to identify areas mapping to patent claims and infringement charts.
 - Assisted in writing Insulet's expert report.

- **Wirtgen America, Inc v. Caterpillar Inc.** **Dec 2021 – Present**

 - Case Number: 1:17-cv-00770
 - Filed in: District of Delaware
 - Filing date: 06/16/2017
 - Participated in meeting sessions with team of attorneys to strategize on doctrine of equivalence infringement approaches.
 - Searched through 5 million lines of code and found software related to patent claims. Extensive use of tools such as Understand, Linux grep and other tools.

- **IPCom GmbH v. AT&T Mobility LLC., et al** **July 2021 - Present**

 - Case Number: 2:20-cv-00322
 - Filed in: Eastern District of Texas
 - Filing date: 10/01/2020
 - Researched Telecom Wireless standards related to selected patents within case scope.
 - Searched through 1.2 TB of software code in order to find software directly related to patent claims. Extensive use of tools such as Understand, Linux grep and other tools.
 - Assisted in writing expert testimonial report related to the findings I identified for multiple Wireless Base-Stations.

PATENTS

- **U.S. 9667643**

Apparatus, system, and method for correlating security vulnerabilities from multiple independent vulnerability assessment methods. (Granted).

- **U.S. 9667642**

Apparatus, system, and method for reconciling network discovered hosts across time. (Granted).

- **U.S. 8938531B1**

Apparatus, system and method for multi-context event streaming network vulnerability scan. (Granted).