

**Kenneth R. van Wyk**  
7716 Effingham Square  
Alexandria, Virginia 22315-5917 USA  
[Ken@KRvW.com](mailto:Ken@KRvW.com)  
+1 703 782 4388

## **Summary**

Mr. Van Wyk is a career security technologist as well as a CERT® Certified Computer Security Incident Handler, specializing in Incident Response, Network Security, and Software Security in production business environments of many of the largest companies in the world. He is a published author of two O'Reilly & Associates books, one of the founders of the Carnegie Mellon CERT/CC, and a frequently invited lecturer on a wide range of security technology topics.

## **Work Experience**

### **2003 to Present – KRvW Associates, LLC, Principal Consultant (Active DoD SECRET clearance, with SSBI in progress for TOP SECRET)**

Responsibilities include:

- *Consulting services*, including: Incident Response planning and emergency operational support; Intrusion monitoring systems design, review, and deployment planning; IT Security process and design reviews; IT Security technology decision support; and Firewall/Secure Network Design and Review
- *Training services*, including ½ day through 2 ½ day seminars on Incident Response, Secure Coding Practices, and Threat Awareness

### **2006 to Present – Member of the Board of Directors, FIRST.org, Inc., and Steering Committee member, FIRST (an elected, 2-year position)**

Responsibilities include:

- Setting of strategic direction for this non-profit professional organization
- Budget planning and oversight
- Oversight and membership liaison with various member activities, from technical colloquia to annual conference

### **2004 to Present – Carnegie Mellon University Software Engineering Institute, Visiting Scientist (part-time)**

Responsibilities include:

- Instructor for various CERT/CC courses
- Consultant to CERT/CC

### **2004 to Present – eSecurityPlanet (Jupiter Media), Columnist**

Responsible for writing monthly opinion columns for eSecurityPlanet's on-line IT Security portal (<http://www.eSecurityPlanet.com>).

### **2005 to 2006 – Cigital, Inc., Director (part-time), Cigital Labs**

Responsibilities included:

- Overall direction and oversight of Cigital Labs' research projects
- Defining a research vision and agenda for Cigital Labs

- Business development of research projects among Cigital's customers and research collaboration organizations

**2002 to 2003 – TGS Solutions, Technology Risk Management, Technology Director**

Responsibilities included:

- Technical oversight of all work product within Technology Risk Management practice, software tool development and utilization, architectures, etc.
- Project leader on all incident response and litigation support work
- Final quality assurance authority on all client deliverable products
- Spokesperson for TRM practice at conferences, with media, etc.
- On-going pre- and post-sales technical consultation on key client accounts

**1998 to 2002 – Para-Protect, Inc., Corporate Vice President, CTO and Co-Founder**

Responsibilities included:

- Technical oversight of all work product, software tool development and utilization, architectures, etc.
- Project leader on numerous incident response and other client engagements
- Final quality assurance authority on all client deliverable products
- Company spokesperson at conferences, with media, etc.
- On-going pre- and post-sales technical consultation on key client accounts
- Supervised company's research and development staff and projects
- Held seat on Board of Directors to provide company with strategic guidance

**1995 to 1998 – Science Applications International Corporation, Technical Director and Deputy Division Manager (DoD Cleared to TOP SECRET)**

Responsibilities included:

- Senior technical project leader on various client engagements, ranging from incident response operations through in-depth client security assessments
- Supervised incident response staff and operations
- Wrote and presented briefings on information security at numerous conferences and symposia

**1993 to 1995 – U.S. Department of Defense, Operations Chief, GS-14 (DoD Cleared to TS/SCI(SI/TK/G) SSBI)**

Responsibilities included:

- Supervised and lead all 24x7 incident response operations for DoD-wide incident response team
- Participated in the development and execution of the DoD's first internal penetration testing program
- Presented security threat briefings to senior DoD civilian and military executive management, as well as at dozens of conferences

**1989 to 1993 – Carnegie Mellon University CERT/CC, Technical Coordinator (DoD Cleared to SECRET)**

Responsibilities included:

- Technical lead on incident response operations, including interfacing with and providing first level of support to affected client organizations

- Tracked and analyzed software product security vulnerabilities as reported by client organizations
- Assisted product vendor community in validating and correcting reported security vulnerabilities in their products

### **1985 to 1989 – Lehigh University, Senior Technical Consultant**

Responsibilities included:

- Provided technical support to faculty, staff, and graduate researchers on the use of the University's mainframe computing facilities
- Developed and taught computer training seminars for the entire campus community
- Developed software for connecting from campus PCs to campus mainframe computers via the voice/data network

### **Publications and Related Experience**

- 2007, Adapting Penetration Testing for Software Development Purposes, <http://BuildSecurityIn.US-CERT.Gov>, (a Dept. of Homeland Security portal on Software Assurance).
- 2006-present, Elected to Steering Committee for the Forum of Incident Response and Security Teams (FIRST).
- 2005, Training and Awareness, Build Security In, <http://BuildSecurityIn.US-CERT.Gov>.
- 2005, Bridging the Gap Between Software Development and Information Security, Kenneth R. van Wyk and Gary McGraw. IEEE Security & Privacy, September/October 2005.
- 2004-present, Founded, moderate, and host the SC-L Secure Coding Internet mailing list discussion forum.
- 2006-2007, Re-elected to serve on Steering Committee for the Forum of Incident Response and Security Teams (FIRST).
- 2004-present, CERT® Certified Computer Security Incident Handler.
- 2004, Admitted as an Adjunct Faculty Member of The Round Table Group. RTG provides consultation and expert testimony services. See <http://www.roundtablegroup.com> for more details.
- 2003, Co-author of O'Reilly and Associates book, *Secure Coding: Principles and Practices*, ISBN 0-59600-242-4, <http://www.securecoding.org>.
- 2001, Co-author of O'Reilly and Associates book, *Incident Response*, ISBN 0-59600-130-4, <http://www.incidentresponse.com>.
- 2001, Co-author "Corporate Risk Management" chapter of *Data Security and Privacy Law: Combating Cyberthreats* by Kevin P. Cronin and Ronald N. Weikers, Thomson West, ISBN 0-314-10372-4, <http://www.westgroup.com>.
- 1995-1997, Elected to and served on FIRST Steering Committee, including 1 year as the group's Chairperson
- 1988-1994, Founded and moderated the VIRUS-L/comp.virus Internet discussion forum on computer viruses
- Frequently invited speaker at numerous conferences and symposia on such topics as incident response, intrusion detection, security threats, security tools, etc.

### **Education**

Lehigh University, Bachelor of Science in Mechanical Engineering, 1987

Completed additional significant graduate coursework at both Lehigh and Carnegie Mellon Universities in Computer Science and Software Engineering