Raffael Marty

Applied Security Visualization

Use Visualization to Secure Your Network Against the Toughest, Best-Hidden Threats

As networks become ever more complex, securing them becomes more and more difficult. The solution is visualization. Using today's state-of-the-art data visualization techniques, you can gain a far deeper understanding of what's happening on your network right now. You can uncover hidden patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures that are far more likely to succeed than conventional methods.

In *Applied Security Visualization*, leading network security visualization expert Raffael Marty introduces all the concepts, techniques, and tools you need to use visualization on your network. You'll learn how to identify and utilize the right data sources, then transform your data into visuals that reveal what you really need to know. Next, Marty shows how to use visualization to perform broad network security analyses, assess specific threats, and even improve business compliance.

He concludes with an introduction to a broad set of visualization tools. The book's CD also includes DAVIX, a compilation of freely available tools for security visualization.

YOU'LL LEARN HOW TO:

- Intimately understand the data sources that are essential for effective visualization
- Choose the most appropriate graphs and techniques for your IT data
- Transform complex data into crystal-clear visual representations
- Iterate your graphs to deliver even better insight for taking action
- Assess threats to your network perimeter, as well as threats imposed by insiders
- Use visualization to manage risks and compliance mandates more successfully
- Visually audit both the technical and organizational aspects of information and network security
- Compare and master today's most useful tools for security visualization
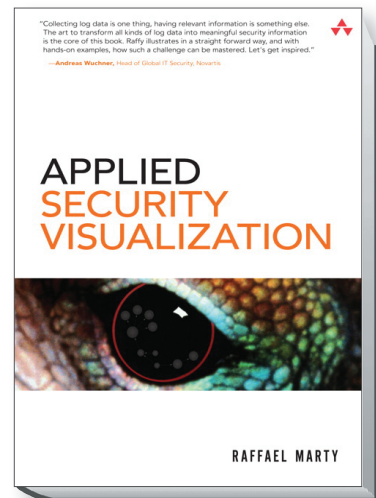
AVAILABLE
- BOOK/CD: 9780321510105
- SAFARI ONLINE **Safari** Books Online
- E-BOOK: 0321564308
- MOBI: 0321564324
- SONY: 0321564316

About the Author

RAFFAEL MARTY is chief security strategist and senior product manager for Splunk, the leading provider of large-scale, high-speed indexing and search technology for IT infrastructures. As customer advocate and guardian, he focuses on using his skills in data visualization, log management, intrusion detection, and compliance. An active participant on industry standards committees such as CEE (Common Event Expression) and OVAL (Open Vulnerability and Assessment Language), Marty created the Thor and AfterGlow automation tools, and founded the security visualization portal secviz.org. Before joining Splunk, he managed the solutions team at ArcSight, served as IT security consultant for PriceWaterhouseCoopers, and was a member of the IBM Research Global Security Analysis Lab.

Table of Contents

Addison-Wesley