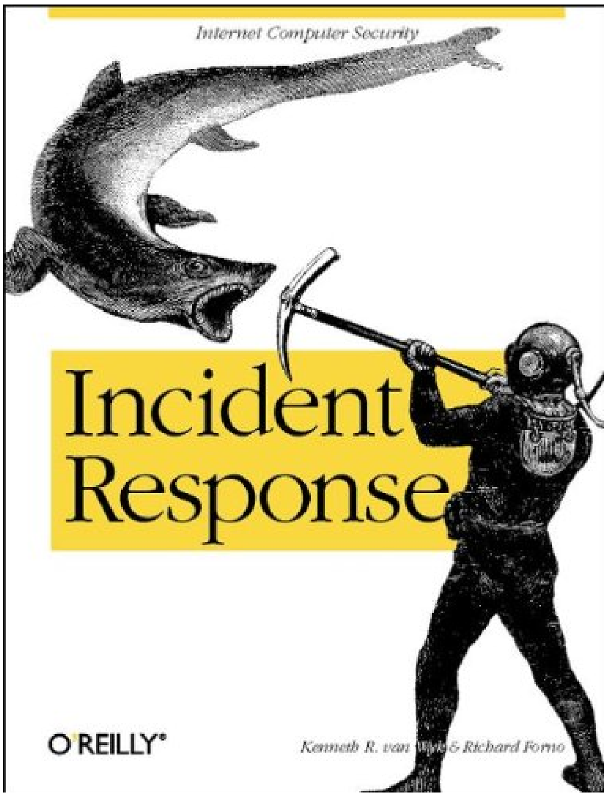
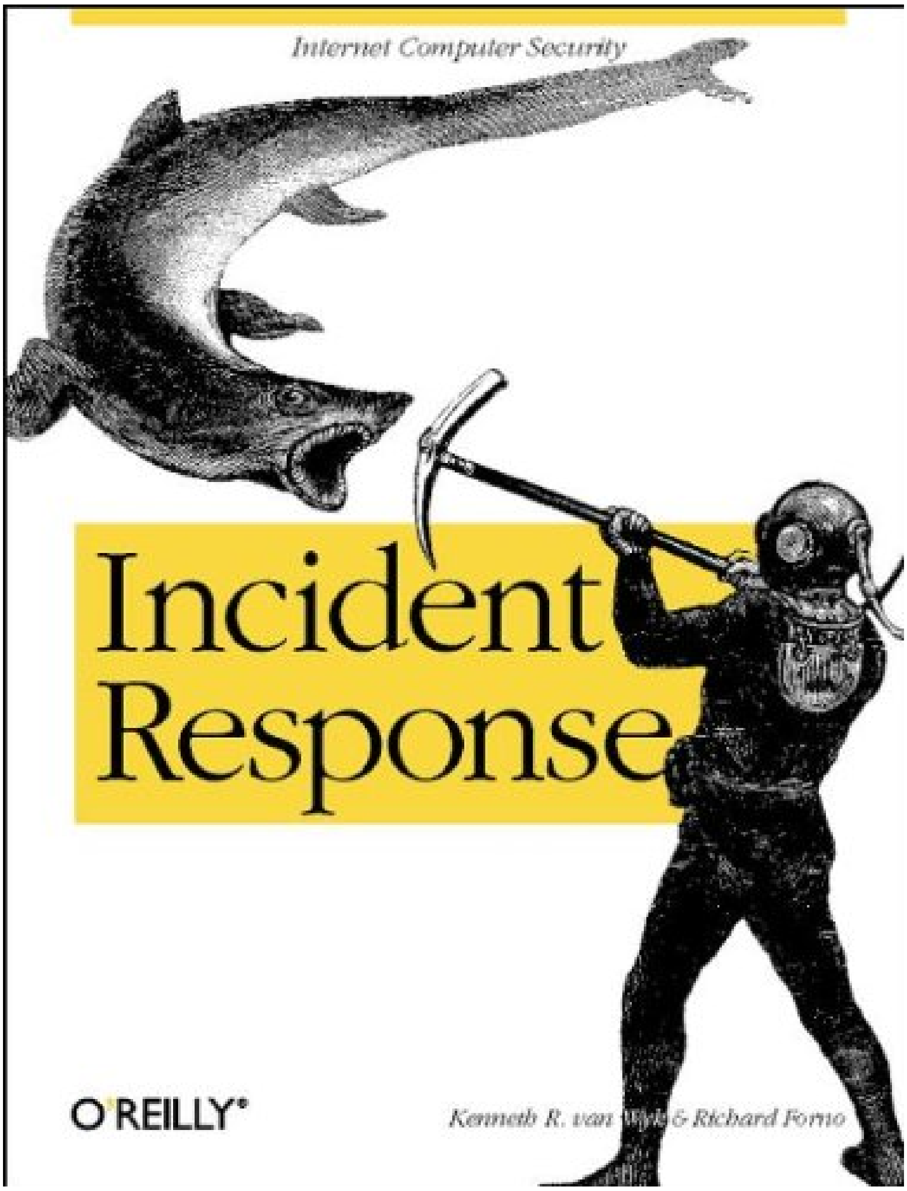
INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO


Internet Computer Security
Incident Response
O'REILLY
Kenneth R. van Wyk & Richard Forno

DOWNLOAD EBOOK : INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO PDF


Internet Computer Security
Incident Response
O'REILLY®
Kenneth R. van Wyk & Richard Forno

INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO PDF

The means to get this publication *Incident Response By Kenneth R. Van Wyk, Richard Forno* is really easy. You may not go for some areas as well as spend the moment to only locate guide Incident Response By Kenneth R. Van Wyk, Richard Forno In fact, you could not always get guide as you want. But below, just by search and locate Incident Response By Kenneth R. Van Wyk, Richard Forno, you can get the lists of the books that you actually anticipate. Often, there are lots of publications that are revealed. Those publications obviously will certainly amaze you as this Incident Response By Kenneth R. Van Wyk, Richard Forno compilation.

Amazon.com Review
Unusually management-oriented for a book from O'Reilly & Associates, Incident Response takes a very high-level look at the tools, techniques, and practices associated with the question of what to do when an intrusion or other attack on information systems has been detected. Systems administrators used to seeing loads of hard-core technical details in O'Reilly books will find this one disappointing, but managers eager for an introduction to incident response with a fair bit of hand-holding and jargon-glossing will put it down happier. On the other hand, even managers will find portions of this book disappointing, as sentences like, "Just about every computer has a 1.44 MB floppy disk drive nowadays" have no place in modern professional literature.

Authors Kenneth van Wyk and Richard Forno do a good job of introducing modes of attack and methods of response to their readers, and take care to explain all potentially unusual terms as they pop up. They also do a good job of explaining the organization and function of the professional, governmental, and ad hoc groups that exist to respond to attacks and disseminate information about them. Much ink is devoted to the considerations managers have to account for as they decide how much money to spend on people, services, and tools associated with incident response. --David Wall

Topics covered: Tools and strategies hackers use to break into systems illegally, and mechanisms and procedures for dealing with such attacks. Emphasis falls on the business considerations associated with incident preparedness and response.

About the Author

Kenneth R. van Wyk is an internationally recognized information security expert and author of the O'Reilly Media books, Incident Response and Secure Coding. In addition to providing consulting and training services through his company, KRvW Associates, LLC, he currently holds numerous positions: as a monthly columnist for on-line security portal, eSecurityPlanet, and a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

Ken has 20+ years experience as an IT Security practitioner in the academic, military, and commercial sectors. He has held senior and executive technologist positions at Tekmark, Para-Protect, Science Applications International Corporation (SAIC), in addition to the U.S. Department of Defense and Carnegie Mellon and Lehigh Universities.

Ken also served a two-year elected position as a member of the Steering Committee, and a one-year elected position as the Chairman of the Steering Committee, for the Forum of Incident Response and Security Teams (FIRST) organization. At the Software Engineering Institute of Carnegie Mellon University, Ken was one of the founders of the Computer Emergency Response Team (CERT®). He holds an engineering degree from Lehigh University and is a frequent speaker at technical conferences, and has presented papers and speeches for CSI, ISF, USENIX, FIRST, AusCERT, and others. Ken is also a CERT® Certified Computer Security Incident Handler.

Richard Forno is a recognized security professional and coauthor of The Art of Information Warfare. He has held high-profile security positions at major companies and government organizations; he helped establish the first incident response team for the United States House of Representatives and provided advisory support to offices of the Department of Defense on information warfare. He is the cofounder of G2-Forward, a prominent information analysis and distribution service supporting the military intelligence and law enforcement communities. In 1998, he became the chief security officer for Network Solutions (the InterNIC), the company responsible for developing and operating the Internet Shared Registry System.

INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO PDF

Incident Response By Kenneth R. Van Wyk, Richard Forno. Eventually, you will certainly uncover a new journey as well as expertise by investing more money. But when? Do you assume that you should acquire those all demands when having significantly cash? Why don't you aim to obtain something basic initially? That's something that will lead you to recognize even more regarding the globe, experience, some places, history, home entertainment, and also much more? It is your own time to proceed reviewing behavior. Among the publications you can enjoy now is Incident Response By Kenneth R. Van Wyk, Richard Forno right here.

If you obtain the published book *Incident Response By Kenneth R. Van Wyk, Richard Forno* in on the internet book store, you might likewise find the exact same issue. So, you should move shop to store Incident Response By Kenneth R. Van Wyk, Richard Forno and also search for the offered there. However, it will not take place right here. Guide Incident Response By Kenneth R. Van Wyk, Richard Forno that we will certainly provide right here is the soft file idea. This is exactly what make you can easily discover as well as get this Incident Response By Kenneth R. Van Wyk, Richard Forno by reading this site. We provide you Incident Response By Kenneth R. Van Wyk, Richard Forno the most effective item, always as well as consistently.

Never ever question with our deal, since we will always give exactly what you require. As such as this updated book Incident Response By Kenneth R. Van Wyk, Richard Forno, you may not locate in the other location. But below, it's quite easy. Merely click and download and install, you can have the Incident Response By Kenneth R. Van Wyk, Richard Forno When convenience will relieve your life, why should take the difficult one? You could purchase the soft file of the book Incident Response By Kenneth R. Van Wyk, Richard Forno here and be participant people. Besides this book Incident Response By Kenneth R. Van Wyk, Richard Forno, you can additionally discover hundreds listings of the books from many resources, compilations, publishers, and authors in worldwide.

INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO PDF

Seventy percent of businesses reported security breaches in 2000, and the rate is on the rise. Is your organization ready to respond to such an incident head-on? Will you be able to tell whether an incident is an attack or a glitch in the system? Do you know how to assess the possible damage from an incident? Incident Response shows you how to answer questions like these and create a plan for exactly what to do before, during, and after an incident.The authors of Incident Response draw on years of experience developing and taking part in incident response teams at the highest levels of government and business. They guide you through both the technical and administrative details of effective incident response planning as they describe:

- What incident response is, and the problems of distinguishing real risk from perceived risk
- The different types of incident response teams, and advantages and disadvantages of each
- Planning and establishing an incident response team
- State of the Hack® information about different types of attacks
- Recommendations and details about available tools for incident response teams
- Resources available to incident response teams

Whatever your organization's size or purpose, Incident Response shows how to put in place an incident-response process that's as planned, efficient, and businesslike as any other IT operation in a mature organization. Incidents happen, and being able to respond to them effectively makes good business sense.

- Sales Rank: #1816797 in Books
- Brand: Brand: O'Reilly Media
- Published on: 2001-08-11
- Original language: English
- Number of items: 1
- Dimensions: 9.19" h x .61" w x 7.00" l,
- Binding: Paperback
- 240 pages

Features

- Used Book in Good Condition

Amazon.com Review
Unusually management-oriented for a book from O'Reilly & Associates, Incident Response takes a very high-level look at the tools, techniques, and practices associated with the question of what to do when an intrusion or other attack on information systems has been detected. Systems administrators used to seeing loads of hard-core technical details in O'Reilly books will find this one disappointing, but managers eager for an introduction to incident response with a fair bit of hand-holding and jargon-glossing will put it down happier. On the other hand, even managers will find portions of this book disappointing, as sentences like, "Just about every computer has a 1.44 MB floppy disk drive nowadays" have no place in modern professional literature.

Authors Kenneth van Wyk and Richard Forno do a good job of introducing modes of attack and methods of response to their readers, and take care to explain all potentially unusual terms as they pop up. They also do a good job of explaining the organization and function of the professional, governmental, and ad hoc groups that exist to respond to attacks and disseminate information about them. Much ink is devoted to the considerations managers have to account for as they decide how much money to spend on people, services, and tools associated with incident response. --David Wall

Topics covered: Tools and strategies hackers use to break into systems illegally, and mechanisms and procedures for dealing with such attacks. Emphasis falls on the business considerations associated with incident preparedness and response.

About the Author

Kenneth R. van Wyk is an internationally recognized information security expert and author of the O'Reilly Media books, Incident Response and Secure Coding. In addition to providing consulting and training services through his company, KRvW Associates, LLC, he currently holds numerous positions: as a monthly columnist for on-line security portal, eSecurityPlanet, and a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

Ken has 20+ years experience as an IT Security practitioner in the academic, military, and commercial sectors. He has held senior and executive technologist positions at Tekmark, Para-Protect, Science Applications International Corporation (SAIC), in addition to the U.S. Department of Defense and Carnegie Mellon and Lehigh Universities.

Ken also served a two-year elected position as a member of the Steering Committee, and a one-year elected position as the Chairman of the Steering Committee, for the Forum of Incident Response and Security Teams (FIRST) organization. At the Software Engineering Institute of Carnegie Mellon University, Ken was one of the founders of the Computer Emergency Response Team (CERT®). He holds an engineering degree from Lehigh University and is a frequent speaker at technical conferences, and has presented papers and speeches for CSI, ISF, USENIX, FIRST, AusCERT, and others. Ken is also a CERT® Certified Computer Security Incident Handler.

Richard Forno is a recognized security professional and coauthor of The Art of Information Warfare. He has held high-profile security positions at major companies and government organizations; he helped establish the first incident response team for the United States House of Representatives and provided advisory support to offices of the Department of Defense on information warfare. He is the cofounder of G2-Forward, a prominent information analysis and distribution service supporting the military intelligence and law enforcement communities. In 1998, he became the chief security officer for Network Solutions (the InterNIC), the company responsible for developing and operating the Internet Shared Registry System.

Most helpful customer reviews

3 of 3 people found the following review helpful.
Good for organizing IR team
By Anton
At only 200 or so pages, the Incident Response is too brief to qualify as the Bible of Incident Response, but it certainly comes close. This excellent manual by two renowned security experts describes the administrative measures needed to create, train, maintain and operate an information incident response team. It also sheds light on sniffers, intrusion detection systems, vulnerability scanners, computer forensics utilities and other

"tools of the trade" for the emergency response professional.

Co-author Kenneth R. van Wyk helped found CERT/CC, chaired the FIRST organization and helped launch the first commercial incident response team in the US. His collaborator, Richard Forno, established the first computer incident response team for the US House of Representatives, served as Chief Security Officer for the domain registry Network Solutions and has written a book on information warfare.

Together, they have produced a book that will be most useful to large companies -- since smaller ones just cannot afford a dedicated internal emergency team. However, they also discuss the considerations of choosing an outside team (public or commercial), which will definitely help smaller companies, as will the simple steps for handling incidents before the response team flies in. The team lifetime is outlined in a clear and concise manner: planning, reporting, staffing, training, developing procedures and testing them in real life. Additionally, van Wyk and Forno explain the logical steps to take in case of a penetration and they have optimized these steps for deployment under pressure.

Overall, Incident Response is a great book to own if you are an information security professional or an IT professional wearing the "security hat." It is also extremely useful if you are a manager tasked with creating a response team, because it can serve as a summary of special knowledge developed in the area.

7 of 8 people found the following review helpful.

Good management level introduction to incident response

By Ben Rothke

Anyone who has flown on a commercial airliner knows well of the pre- flight safety briefings. From the water floatation safety cushions to the oxygen masks, it's the cabin crew's duty to ensure that every passenger is briefed. Why is this safety briefing so vital? Because when a passenger is gasping for air at 39,000 feet, it is unlikely that they will get a response when they press the flight attendant call button.

In many ways, computer incident response is akin to airplane safety; you need to know what to expect when the inevitable occurs. If an organization attempts to manage things ex post facto -- whether it is a depressurization at cruise level or a hack attack - their response will invariably fail. As such, the need for IT-based incident response strategy is crucial.

Why is incident response a necessity? According to data from the Computer Security Institute (and backed-up by many other security surveys), more than 70% of businesses reported security breaches in the year 2000. While 70% may have answered the survey affirmatively, the reality is that every business on the planet has security breaches. It's simply a matter of how effectively they handle the incident. System and network hacks are to be expected; how well they are handled, and how the damage is mitigated is up to the organizations and their respective incident response teams.

Although I used the airline example, the authors of Incident Response compare it to fire fighting. Incident response is akin to firefighting in that it involves the coordination of various disciplines, namely: prevention, planning, detection, analysis, containment, investigation, eradication, and post-incident analysis.

The difference between a fire and incident response is that whereas a fire can be extinguished with perhaps one or two of the controls just mentioned, effective incident response requires that all eight of the controls be effectively carried out. Another difference between firefighting and incident response is that humanity has thousands of years of experience in putting out fires. Computer security, however, has only been around for a few decades. From an incident response perspective, the CERT/CC (Computer Emergency Response Team Coordination Center) is only 13 years old. The fact that Smokey the Bear is older than information security and incident response should be humbling to those in technology.

The problem within many elements of corporate information technology is that they don't understand the intricacies involved with incident response. With that, Incident Response provides a non-technical introduction to the rudiments of setting up an incident response team. Many technology managers don't know the difference between Certs candy and the CERT organization. For those managers, this book will be a good start toward teaching them how to deal with the inevitable.

Overall, Incident Response is a thorough introduction to incident response. The authors go into detail about defining what an incident is and analyzing its various components to show how a multi-disciplinary approach is required to rectify the situation. Those of us in technology easily understand the need for incident response; unfortunately, many IT managers think that incident response can be handled in a much more informal and unofficial way. Such an erroneous management attitude will only lead to many undetected security incidents.

Although Forno and Van Wyk give a good overview of incident response, the topic is far too broad to be thoroughly covered in this monograph alone. For those who need a deeper and more technical look at incident response and its associated field of computer forensics, the following books will likely be beneficial:

- Incident Response: A Strategic Guide to Handling System and Network Security Breaches by Russell Shumway & Gene Schultz, New Riders Publishing 2002; ISBN: 1578702569 2002
- Incident Response: Investigating Computer Crime by Chris Prosise & Kevin Mandia, McGraw-Hill Professional Publishing 2001; ISBN: 0072131829
- Computer Forensics -- Incident Response Essentials by Warren Kruse & Jay Heiser, Addison-Wesley 2001, ISBN: 0201707195.

1 of 2 people found the following review helpful.

Very helpful - management oriented, not techno-geeky

By Gina Reynolds

The book is a great introduction to incident handling, and is appropriate for both systems folks as well as their managers. This is not the heaviest security book in the world and that's because it doesn't get bogged down in the nitty-gritty technology stuff of computer security. (If you want a hand-holding how-to-do-it book, there are others better suited.)

Rare for a technology book, they take a management approach instead of a purely technical one, and thus probably means they have a wider target audience that will benefit from it. Also, the book isn't Unix- or Windows- based, what they talk about is handy for any computing platform for any size company.

However it does do a great job of introducing you to incident response - why it's needed and what options you have for it. They are correct that it is a process not a solution.

The tools section is a good overview and introduction - by no means complete - and the authors even say that it's not all-incompassing. I guess we all know how fast software changes, and that it's impossible to cover everything.

See all 8 customer reviews...

INCIDENT RESPONSE BY KENNETH R. VAN WYK, RICHARD FORNO PDF

By clicking the link that we offer, you can take the book **Incident Response By Kenneth R. Van Wyk, Richard Forno** completely. Attach to net, download, as well as conserve to your device. What else to ask? Checking out can be so very easy when you have the soft documents of this Incident Response By Kenneth R. Van Wyk, Richard Forno in your gadget. You could additionally duplicate the data Incident Response By Kenneth R. Van Wyk, Richard Forno to your office computer or at home as well as in your laptop computer. Merely discuss this great news to others. Recommend them to see this page and get their looked for publications Incident Response By Kenneth R. Van Wyk, Richard Forno.

Amazon.com Review
Unusually management-oriented for a book from O'Reilly & Associates, Incident Response takes a very high-level look at the tools, techniques, and practices associated with the question of what to do when an intrusion or other attack on information systems has been detected. Systems administrators used to seeing loads of hard-core technical details in O'Reilly books will find this one disappointing, but managers eager for an introduction to incident response with a fair bit of hand-holding and jargon-glossing will put it down happier. On the other hand, even managers will find portions of this book disappointing, as sentences like, "Just about every computer has a 1.44 MB floppy disk drive nowadays" have no place in modern professional literature.

Authors Kenneth van Wyk and Richard Forno do a good job of introducing modes of attack and methods of response to their readers, and take care to explain all potentially unusual terms as they pop up. They also do a good job of explaining the organization and function of the professional, governmental, and ad hoc groups that exist to respond to attacks and disseminate information about them. Much ink is devoted to the considerations managers have to account for as they decide how much money to spend on people, services, and tools associated with incident response. --David Wall

Topics covered: Tools and strategies hackers use to break into systems illegally, and mechanisms and procedures for dealing with such attacks. Emphasis falls on the business considerations associated with incident preparedness and response.

About the Author

Kenneth R. van Wyk is an internationally recognized information security expert and author of the O'Reilly Media books, Incident Response and Secure Coding. In addition to providing consulting and training services through his company, KRvW Associates, LLC, he currently holds numerous positions: as a monthly columnist for on-line security portal, eSecurityPlanet, and a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

Ken has 20+ years experience as an IT Security practitioner in the academic, military, and commercial sectors. He has held senior and executive technologist positions at Tekmark, Para-Protect, Science Applications International Corporation (SAIC), in addition to the U.S. Department of Defense and Carnegie Mellon and Lehigh Universities.

Ken also served a two-year elected position as a member of the Steering Committee, and a one-year elected position as the Chairman of the Steering Committee, for the Forum of Incident Response and Security Teams (FIRST) organization. At the Software Engineering Institute of Carnegie Mellon University, Ken was one of the founders of the Computer Emergency Response Team (CERT®). He holds an engineering degree from Lehigh University and is a frequent speaker at technical conferences, and has presented papers and speeches for CSI, ISF, USENIX, FIRST, AusCERT, and others. Ken is also a CERT® Certified Computer Security Incident Handler.

Richard Forno is a recognized security professional and coauthor of The Art of Information Warfare. He has held high-profile security positions at major companies and government organizations; he helped establish the first incident response team for the United States House of Representatives and provided advisory support to offices of the Department of Defense on information warfare. He is the cofounder of G2-Forward, a prominent information analysis and distribution service supporting the military intelligence and law enforcement communities. In 1998, he became the chief security officer for Network Solutions (the InterNIC), the company responsible for developing and operating the Internet Shared Registry System.