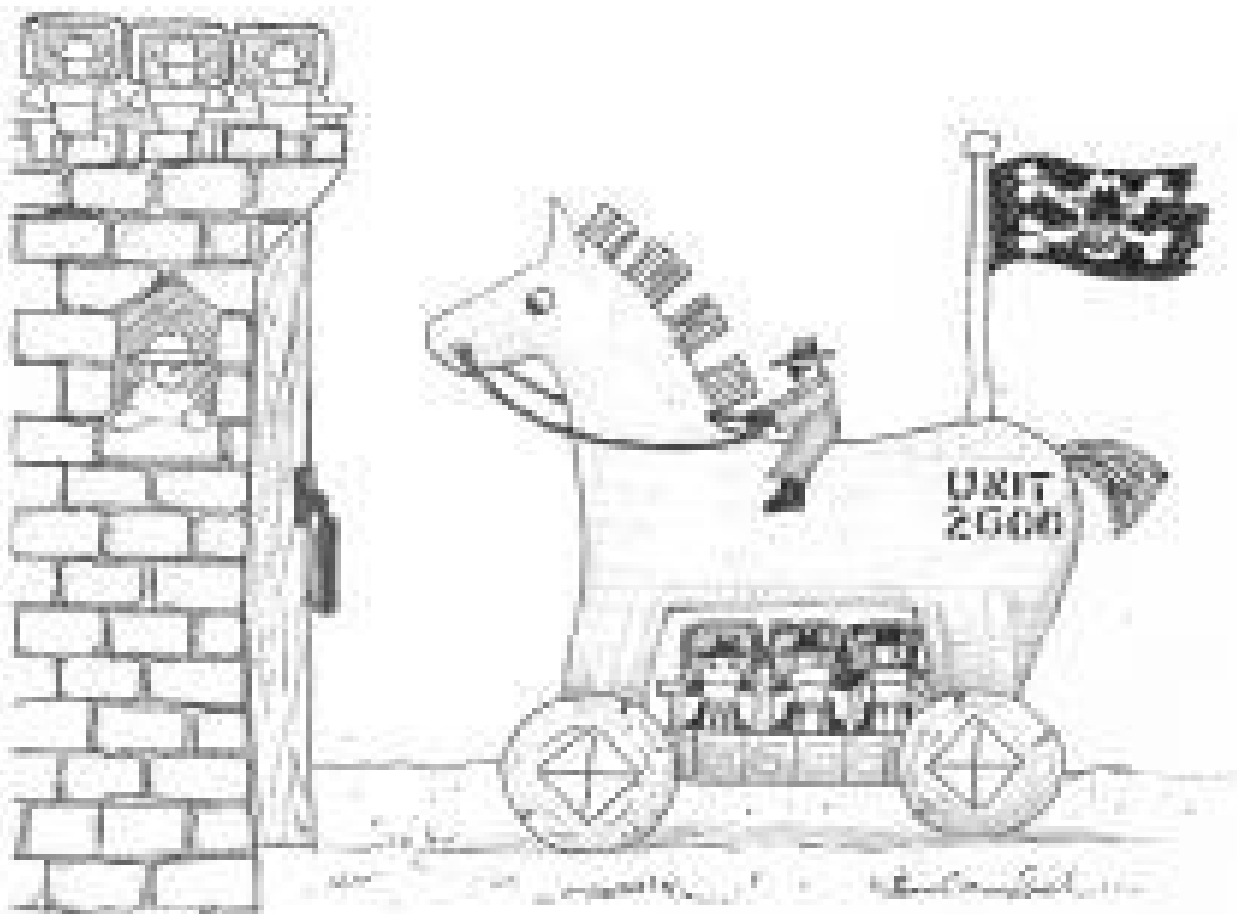


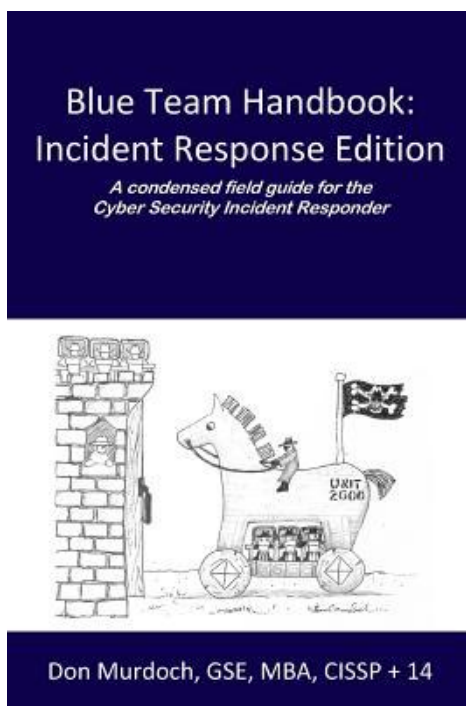
Blue Team Handbook: Incident Response Edition

*A condensed field guide for the
Cyber Security Incident Responder*



Don Murdoch, GSE, MBA, CISSP + 14

* Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder. *



Books Details

Author : Don Murdoch Pages : 164 pages Publisher : CreateSpace Independent Publishing Platform Language : eng ISBN-10 : 1500734756 ISBN-13 : 9781500734756

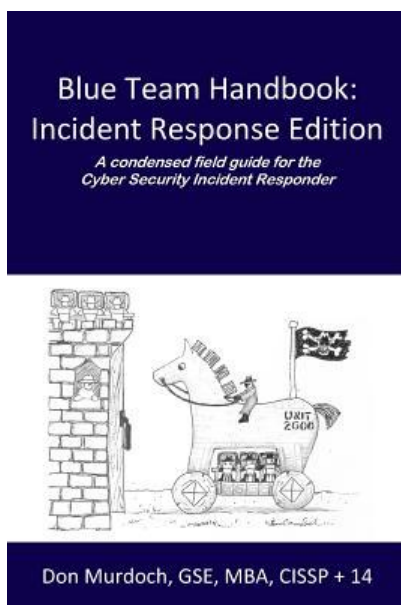
Books Descriptions

The Blue Team Handbook is a "zero fluff" reference guide for cyber security incident responders, security engineers, and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format. Main topics include the incident response process, how attackers work, common tools for incident response, a methodology for network analysis, common indicators of compromise, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, packet headers, and numerous other quick reference topics. The book is designed specifically to share "real life experience," so it is peppered with practical techniques from the authors'

extensive career in handling incidents. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way.



You Can Get This Books By Click Link/Button In Below .



/

<https://www.worldbookcollection.com/?book=1500734756>