Corporate Cybersecurity: Identifying Risks and the Bug Bounty Program

John Jackson

<table>
<thead>
<tr>
<th>Format</th>
<th>ISBN</th>
<th>Date</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Book</td>
<td>978-1-119-78254-4</td>
<td>October 2021</td>
<td>$88.00</td>
</tr>
<tr>
<td>Hardcover</td>
<td>978-1-119-78252-0</td>
<td>October 2021</td>
<td>$110.00</td>
</tr>
<tr>
<td>O-Book</td>
<td>978-1-119-78256-8</td>
<td>November 2021</td>
<td>Available on Wiley Online Library</td>
</tr>
</tbody>
</table>

DESCRIPTION

CORPORATE CYBERSECURITY

An insider’s guide showing companies how to spot and remedy vulnerabilities in their security programs

A bug bounty program is offered by organizations for people to receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. *Corporate Cybersecurity* gives cyber and application security engineers (who may have little or no experience with a bounty program) a hands-on guide for creating or managing an effective bug bounty program. Written by a cyber security expert, the book is filled with the information, guidelines, and tools that engineers can adopt to sharpen their skills and become knowledgeable in researching, configuring, and managing bug bounty programs.

This book addresses the technical aspect of tooling and managing a bug bounty program and discusses common issues that engineers may run into on a daily basis. The author includes information on the often-overlooked communication and follow-through approaches of effective management. *Corporate Cybersecurity* provides a much-needed resource on how companies identify and solve weaknesses in their security program. This important book:

- Contains a much-needed guide aimed at cyber and application security engineers
- Presents a unique defensive guide for understanding and resolving security vulnerabilities
- Encourages research, configuring, and managing programs from the corporate perspective
• Topics covered include bug bounty overview; program set-up; vulnerability reports and disclosure; development and application
  Security Collaboration; understanding safe harbor and SLA

Written for professionals working in the application and cyber security arena, Corporate Cybersecurity offers a comprehensive
resource for building and maintaining an effective bug bounty program.

ABOUT THE AUTHOR

John Jackson is a Cyber Security Professional, Hacker, and the founder of the Hacking Group: Sakura Samurai. He is skilled
in the art of configuring, managing, and utilizing Application Security Tools and programs, and an effective leader in the Cyber
Security space. His unique perspective as both an Engineer and a Security Researcher provides hands-on experience towards
configuring programs in a way that both organizations and researchers can benefit.

SERIES

IEEE Press

To purchase this product, please visit https://www.wiley.com/en-us/9781119782544