1. Record Nr. UNINA9910300743803321

| | |
|---|---|
| Autore | Thompson Eric C. |
| Titolo | Cybersecurity Incident Response / : How to Contain, Eradicate, and Recover from Incidents / / by Eric C. Thompson |
| Pubbl/distr/stampa | Berkeley, CA : , : Apress : , : Imprint : Apress, , 2018 |
| ISBN | 9781484238707<br>1484238702 |
| Edizione | [1st ed. 2018.] |
| Descrizione fisica | 1 online resource (184 pages) |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Security |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references. |
| Nota di contenuto | Chapter 1: The Significance of Incident Response -- Chapter 2: Necessary Prerequisites -- Chapter 3: Incident Response Frameworks -- Chapter 4: Leadership, Teams, and Culture -- Chapter 5: The Incident Response Strategy -- Chapter 6: Cyber Risks and the Attack Lifecycle -- Chapter 7: Detection and Identification of Events -- Chapter 8: Containment -- Chapter 9: Eradication, Recovery, and Post-Incident Review -- Chapter 10: Continuous Monitoring of Incident Response Program -- Chapter 11: Incident Response Story -- Chapter 12: This Is a Full-Time Job -- Appendix A: NIST CSF. |
| Sommario/riassunto | Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support. Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each phase of incident response are explored in the book. |

Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You'll Learn: Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team.