1. Record Nr. UNINA9910300637303321

Autore	Donaldson Scott E.
Titolo	Enterprise Cybersecurity : How to Build a Successful Cyberdefense Program Against Advanced Threats / / by Scott Donaldson, Stanley Siegel, Chris K. Williams, Abdul Aslam
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2015
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (508 p.)
Collana	Expert's Voice in Cybersecurity
Disciplina	004
Soggetti	Data protection Data encryption (Computer science) Security Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Contents at a Glance; Contents; Foreword; About the Authors; Acknowledgments ; Introduction; Part I: The Cybersecurity Challenge ; Chapter 1: Defining the Cybersecurity Challenge; The Cyberattacks of Today; The Sony Pictures Entertainment Breach of 2014; Advanced Persistent Threats; Waves of Malware; Types of Cyberattackers; Commodity Threats; Hacktivists; Organized Crime ; Espionage ; Cyberwar ; The Types of Cyberattacks; Confidentiality: Steal Data; Integrity: Modify Data (Steal Money); Availability: Deny Access; The Steps of a Cyberintrusion; Attack Trees and Attack Graphs Lockheed Martin Kill Chain Mandiant Attack Life Cycle; Enterprise Cybersecurity Attack Sequence; Why Cyberintrusions Succeed; The Explosion in Connectivity; Consolidation of Enterprise IT; Defeat of Preventive Controls; Failure of Detective Controls; Compliance over Capability; The Gap in Cybersecurity Effectiveness; A New Cybersecurity Mindset; An Effective Enterprise Cybersecurity Program; Chapter 2: Meeting the Cybersecurity Challenge; Cybersecurity Frameworks; The Cybersecurity Process; Cybersecurity Challenges; The Risk Management Process Considering Vulnerabilities, Threats, and Risks Risk Analysis and Mitigation; Cybersecurity Controls; Cybersecurity Capabilities;

Cybersecurity and Enterprise IT; Emplacing Cyberdefenses ; H ow Cyberdefenses Interconnect; An Enterprise Cybersecurity Architecture; Part II: A New Enterprise Cybersecurity Architecture ; Chapter 3: Enterprise Cybersecurity Architecture; Systems Administration; S ystems Administration: Goal and Objectives ; Systems Administration: Threat Vectors ; Systems Administration: Capabilities; Network Security; Network Security: Goal and Objectives
Network Security: Threat Vectors Network Security: Capabilities ; Application Security; Application Security: Goal and Objectives ; Application Security: Threat Vectors ; Application Security: Capabilities ; Endpoint, Server, and Device Security; Endpoint, Server, and Device Security: Goal and Objectives ; Endpoint, Server, and Device Security: Threat Vectors ; Endpoint, Server, and Device Security: Capabilities ; Identity, Authentication, and Access Management; Identity, Authentication, and Access Management: Goal and Objectives
Identity, Authentication, and Access Management: Threat Vectors
Identity, Authentication, and Access Management: Capabilities; Data Protection and Cryptography; Data Protection and Cryptography: Goal and Objectives ; Data Protection and Cryptography: Threat Vectors ; Data Protection and Cryptography: Capabilities ; Monitoring, Vulnerability, and Patch Management; Monitoring, Vulnerability, and Patch Management: Goal and Objectives ; Monitoring, Vulnerability, and Patch Management: Threat Vectors; Monitoring, Vulnerability, and Patch Management: Capabilities
High Availability, Disaster Recovery, and Physical Protection

Sommario/riassunto

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise’s computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization’s people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.