1. Record Nr. UNINA9910463800203321

Autore	Nathans David
Titolo	Designing and building a security operations center / / David Nathans ; designer, Matthew Limbert
Pubbl/distr/stampa	Waltham, Massachusetts : , : Syngress, , 2015 ©2015
ISBN	0-12-801096-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (281 p.)
Disciplina	005.8
Soggetti	Computer security Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Title Page; Copyright Page; Contents; Author Biography; Technical Editor Biography; Foreword; Acknowledgments; Chapter 1 - Efficient operations; Defining an operations center; Purpose of the operations center; Emergency operations center; Mission operations center; Threat operations center; Network operations center; Let us build a SOC!; Technology phase; Organizational phase; Policy phase; Operational phase; Intelligence phase; Plan your SOC; Logs; Event; Alerts; False positive; True positive; False negative; True negative; Incidents; Problems; Define your requirements; Summary Chapter 2 - Identify your customersInternal versus external customers; Human resources; Legal; Audit; Engineering/R&D; IT; External customers; Customer objectives; Service level agreements; Build and document your use cases; Use case: unauthorized modification of user accounts; Stakeholders: compliance and audit departments; Use case: disabled user account reactivated; Stakeholders: HR and IT; Use case: any IDS event that scores over a severity of 7; Use case: AV failure; Stakeholders: desktop support team, IT server management teams; Use case: security device outage Stakeholders: security and ITUse case rule summary; Use case: top vulnerabilities detected in the network; Stakeholders: security, IT, audit, and management; Use case reporting summary; Expectations; Chapter 3 - Infrastructure; Organizational infrastructure > operations

infrastructure > support infrastructure; Organizational security infrastructure; Perimeter defenses; Network defense; Host defenses; Application defenses; Data defense; Policies and procedures; Security architecture; SIEM/log management; Operation center infrastructure; Ticketing systems; Building the ticket system; Subject Parsed values from eventsTime ticket created; User\group\queue; Source (SIEM, email, phone); Category; Status; Reason codes; Acknowledgment/ticket feedback; Workflow and automation; Portal interface; Mobile devices; Support infrastructure; Physical; Private SOC network; Video walls; Video projectors; Labs; Chapter 4 - Organizational structure; Different reporting lines; Legal; CISO; CIO; Compliance; SOC organization; Engineering; Security architecture; Security monitoring and analysis; Responsibility; Authority; Fulfilling needs; Chapter 5 - Your most valuable resource is your people Operational securityCulture; Personality; Core skill sets; Analysts; Security analyst-job description; Security engineering; Security operations engineer-job description; Security architect; Security architect-job description; SOC team lead; SOC team lead-job description; SOC management; SOC manager-job description; SOC games; Special projects; Do not forget your people; Chapter 6 - Daily operations; Problem and change event communications; Master station logs; Shift turn overs; Daily operations calls; Critical bridges; IR; Detection; Confirmation; Analysis; Containment; Recovery; Review Communication plan

Sommario/riassunto

Do you know what weapons are used to protect against cyber warfare and what tools to use to minimize their impact? How can you gather intelligence that will allow you to configure your system to ward off attacks? Online security and privacy issues are becoming more and more significant every day, with many instances of companies and governments mishandling (or deliberately misusing) personal and financial data. Organizations need to be committed to defending their own assets and their customers' information. Designing and Building a Security Operations Center will show you how to develop t