Network Protection Automation

Recognizing the pretension ways to acquire this books **Network Protection Automation** is additionally useful. You have remained in right site to begin getting this info. acquire the Network Protection Automation associate that we find the money for here and check out the link.

You could buy lead Network Protection Automation or acquire it as soon as feasible. You could quickly download this Network Protection Automation after getting deal. So, taking into account you require the ebook swiftly, you can straight acquire it. Its fittingly very easy and in view of that fats, isnt it? You have to favor to in this atmosphere

Cyber Security: Analytics, Technology and Automation - Martti Lehto 2015-05-30
The book, in addition to the cyber threats and technology, processes cyber security from many sides as a social phenomenon and how the implementation of the cyber security strategy is carried out. The book gives a profound idea of the most spoken phenomenon of this time. The book is suitable for a wide-ranging audience from graduate to professionals/practitioners and researchers. Relevant disciplines for the book are Telecommunications / Network security, Applied mathematics / Data analysis, Mobile systems / Security, Engineering / Security of critical infrastructure and Military science / Security.

Machine Learning for Cyber Physical Systems - Jürgen Beyerer 2016-11-25

The work presents new approaches to Machine Learning for Cyber Physical Systems, experiences and visions. It contains some selected papers from the international Conference ML4CPS – Machine Learning for Cyber Physical Systems, which was held in Karlsruhe, September 29th, 2016. Cyber Physical Systems are characterized by their ability to adapt and to learn: They analyze their environment and, based on observations, they learn patterns, correlations and predictive models. Typical applications are condition monitoring, predictive maintenance, image processing and diagnosis. Machine Learning is the key technology for these developments.

Enterprise Networking, Security, and Automation (Ccnav7) Companion Guide & Labs and Study Guide Value Pack - Allan Johnson 2020-09

Enterprise Networking, Security, and Automation (CCNA v7) Companion Guide is designed as a portable desk reference to use anytime, anywhere to reinforce the material from the Enterprise Networking, Security, and Automation course and organize your time. The book's features help you focus on important concepts to succeed in this course: Chapter Objectives - Review core concepts by answering the focus questions listed at the beginning of each chapter. Key Terms - Refer to the lists of networking vocabulary introduced and highlighted in context in each chapter. Glossary - Consult the comprehensive Glossary with more than 250 terms. Summary of Activities and Labs - Maximize your study time with this complete list of all associated practice exercises at the end of each chapter. Check Your Understanding - Evaluate your readiness with the end-of-chapter questions that match the style of questions you see in the online course quizzes. The answer key explains each answer. How To - Look for this icon to study the steps you need to learn to perform certain tasks. Interactive Activities - Reinforce your understanding of topics with dozens of exercises from the online course identified throughout the book with this icon. Packet Tracer Activities - Explore and visualize networking concepts using Packet Tracer exercises interspersed throughout the chapters and provided in the accompanying Labs & Study Guide book. Videos - Watch the videos embedded within the online course. Hands-on Labs - Work through all the course labs and additional Class Activities that are included in the course and published in the separate Labs & Study Guide. Part of the Cisco Networking Academy Series from Cisco Press, books in this series support and complement the Cisco Networking Academy curriculum.

Cloud Security Automation - Prashant Priyam 2018-03-28

Secure public and private cloud workloads with this comprehensive learning guide. Key Features Take your cloud security functions to the next level by automation Learn to automate your security functions on AWS and OpenStack Practical approach towards securing your workloads efficiently Book Description Security issues are still a major concern for all IT organizations. For many enterprises, the move to cloud computing has raised concerns for security, but when applications are architected with focus on security, cloud platforms can be made just as secure as on-premises platforms. Cloud instances can be kept secure by employing security automation that helps make your data meet your organization's security policy. This book starts with the basics of why cloud security is important and how automation can be the most effective way of controlling cloud security. You will then delve deeper into the AWS cloud environment and its security services by dealing with security functions such as Identity and Access Management and will also learn how these services can be automated. Moving forward, you will come across aspects such as cloud storage and data security, automating cloud deployments, and so on. Then, you'll work with OpenStack security modules and learn how private cloud security functions can be automated for better time- and cost-effectiveness. Toward the end of the book, you will gain an understanding of the security compliance requirements for your Cloud. By the end of this book, you will have hands-on experience of automating your cloud security and governance. What you will learn Define security for public and private cloud services Address the security concerns of your cloud Understand Identity and Access Management Get acquainted with cloud storage and network security Improve and optimize public and private cloud security Automate cloud security Understand the security compliance requirements of your cloud Who this book is for This book is targeted at DevOps Engineers, Security professionals, or any stakeholders responsible for securing cloud workloads. Prior experience with AWS or OpenStack will be an advantage.

VMware NSX Automation Fundamentals - Thiago Koga 2018-04-16

Practical Cloud Security - Chris Dotson 2019-03-04

With their rapidly changing architecture and API-driven automation, cloud platforms come with unique security challenges and opportunities. This hands-on book guides you through security best practices for multivendor cloud environments, whether your company plans to move legacy on-premises projects to the cloud or build a new infrastructure from the ground up. Developers, IT architects, and security professionals will learn cloud-specific techniques for securing popular cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM Cloud. Chris Dotson—an IBM senior technical staff member—shows you how to establish data asset management, identity and access management, vulnerability management, network security, and incident response in your cloud environment.

Electric Power Distribution, Automation, Protection, and Control - James A. Momoh 2007-09-07

New methods for automation and intelligent systems applications, new trends in telecommunications, and a recent focus on renewable energy are reshaping the educational landscape of today's power engineer. Providing a modern and practical vehicle to help students navigate this dynamic terrain, Electric Power Distribution, Automation, Protection, and Control infuses new directions in computation, automation, and control into classical topics in electric power distribution. Ideal for a one-semester course for senior undergraduates or first-year graduate students, this text works systematically through basic distribution principles, renewable energy sources, computational tools and techniques, reliability, maintenance, distribution automation, and telecommunications. Numerous examples, problems, and case studies offer practical insight into the concepts and help build a working knowledge of protection schemes, fault analysis and synthesis, reliability analysis, intelligent automation systems, distribution management systems, and distribution system communications. The author details different renewable energy sources and teaches students how to evaluate them in terms of size, cost, and performance. Guided firmly by the author's wealth of industrial and academic experience, your students will learn the tools and techniques used to design, build, and operate future generations of distribution systems with unparalleled efficiency, robustness, and sustainability.

Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation - Suresh Balusamy 2020-10-27

This book constitutes the proceedings of the 4th International Conference on Computational Intelligence, Cyber Security, and Computational Models, ICC3 2019, which was held in Coimbatore, India, in December 2019. The 9 papers presented in this volume were carefully reviewed and selected from 38 submissions. They were organized in topical sections named: computational intelligence; cyber security; and computational models.

Automate Your Network: Introducing the Modern Approach to Enterprise Network Management - John W. Capobianco 2019-03-09

Network automation is one of the hottest topics in Information Technology today. This revolutionary book aims to illustrate the transformative journey towards full enterprise network automation. This book outlines the tools, technologies and processes required to fully automate an enterprise network. Automated network configuration management is more than converting your network configurations to code. The benefits of source control, version control, automated builds, automated testing and automated releases are realized in the world of networking using well established software development practices. The next-generation network administrative toolkit is introduced including Microsoft Team Foundation Server, Microsoft Visual Studio Code, Git, Linux, and the Ansible framework. Not only will these new technologies be covered at length, a new and continuously integrated / continuously delivered pipeline is also introduced. Starting with safe, simple, non-intrusive, non-disruptive information gathering organizations can ease into network automation while building a dynamic library of documentation and on-demand utilities for network operations. Once comfortable with the new ecosystem, administrators can begin making fully automated, orchestrated, and tactical changes to the network. The next evolutionary leap occurs when fully automated network configuration management is implemented. Important information from the network running-configurations is abstracted into data models in a human readable format. Device configurations are dynamically templated creating a scalable, intent-based, source of truth. Much like in the world of software development, full automation of the network using a CI/CD pipeline can be realized. Automated builds, automated testing and automated scheduled releases are orchestrated and executed when changes are approved and checked into the central repository. This book is unlike any on the market today as it includes multiple Ansible playbooks, sample YAML data models and Jinja2 templates for network devices, and a whole new methodology and approach to enterprise network administration and management. The CLI no longer cuts it. Readers should take away from this book a new approach to enterprise network management and administration as well as the full knowledge and understanding of how to use TFS, VS Code, Git, and Ansible to create an automation ecosystem. Readers should have some basic understanding of modern network design, operation, and configuration. No prior programming or software development experience is required. John Capobianco has over 20 years of IT experience and is currently a Technical Advisor for the Canadian House of Commons. A graduate of St. Lawrence College's Computer Programmer Analyst program, John is also a former Professor at St. Lawrence College in the Computer Networking and Technical Support (CNTS) program. John has achieved CCNP, CCDP, CCNA: Data Center, MCITP: EA/SA, CompTIA A+ / Network+, and ITIL Foundation certifications. Having discovered a new way to interface with the network John felt compelled to share this new methodology in hopes of revolutionizing the industry and bringing network automation to the world.

Network Programmability and Automation - Khaled Abuelenain 2020

Introduction to Python Network Automation - Brendan Choi 2021-05-23

Learn and implement network automation within the Enterprise network using Python 3. This introductory book will be your guide to building an integrated virtual networking lab to begin your Network Automation journey and master the basics of Python Network Automation. The book features a review of the practical Python network automation scripting skills and tips learned from the production network, so you can safely test and practice in a lab environment first, various Python modules such as paramiko and netmiko, pandas, re, and much more. You'll also develop essential skills such as Python scripting, regular expressions, Linux and Windows administration, VMware virtualization, and Cisco networking from the comfort of your laptop/PC with no actual networking hardware. Finally, you will learn to write a fully automated and working Cisco IOS XE upgrade application using Python. Introduction to Python Network Automation uses a canonical order, where you begin at the bottom and by the time you have completed this book, you will at least reach the intermediate level of Python coding for enterprise networking automation using native Python tools. What You'll Learn Build a proper GNS3-based networking lab for Python network automation needs. Write the basics of Python codes in both the Windows and Linux environments. Control network devices using telnet, SSH, and SNMP protocols using Python codes. Understand virtualization and how to use VMware workstation Examine virtualization and how to use VMware Workstation Pro Develop a working Cisco IOS upgrade application Who This Book Is For IT Engineers and developers, network managers and students, who would like to learn network automation using Python.

Industrial Cybersecurity - Pascal Ackerman 2017-10-18

Your one-step guide to understanding industrial cyber security, its control systems, and its operations. About This Book Learn about endpoint protection such as anti-malware implementation, updating, monitoring, and sanitizing user workloads and mobile devices Filled with practical examples to help you secure critical infrastructure systems efficiently A step-by-step guide that will teach you the techniques and methodologies of building robust infrastructure systems Who This Book Is For If you are a security professional and want to ensure a robust environment for critical infrastructure systems, this book is for you. IT professionals interested in getting into the cyber security domain or who are looking at gaining industrial cyber security certifications will also find this book useful. What You Will Learn Understand industrial cybersecurity, its control systems and operations Design security-oriented architectures, network segmentation, and security support services Configure event monitoring systems, anti-malware applications, and endpoint security Gain knowledge of ICS risks, threat detection, and access management Learn about patch management and life cycle management Secure your industrial control systems from design through retirement In Detail With industries expanding, cyber attacks have increased significantly. Understanding your control system's vulnerabilities and learning techniques to defend critical infrastructure systems from cyber threats is increasingly important. With the help of real-world use cases, this book will teach you the methodologies and security measures necessary to protect critical infrastructure systems and will get you up to speed with identifying unique challenges.Industrial cybersecurity begins by introducing Industrial Control System (ICS) technology, including ICS architectures, communication media, and protocols. This is followed by a presentation on ICS (in) security. After presenting an ICS-related attack scenario, securing of the ICS is discussed, including topics such as network segmentation, defense-in-depth strategies, and protective solutions. Along with practical examples for protecting industrial control systems, this book details security assessments, risk management, and security program development. It also covers essential cybersecurity aspects, such as threat detection and access management. Topics related to endpoint hardening such as monitoring, updating, and anti-malware implementations are also discussed. Style and approach A step-by-step guide to implement Industrial Cyber Security effectively.

Mastering Python for Networking and Security - Jose Manuel Ortega 2021-01-04

Tackle security and networking issues using Python libraries such as Nmap, requests, asyncio, and scapy Key FeaturesEnhance your Python programming skills in securing systems and executing networking tasksExplore Python scripts to debug and secure complex networksLearn to avoid common cyber events with modern Python scriptingBook Description It's now more apparent than ever that security is a critical aspect of IT infrastructure, and that devastating data breaches can occur from simple network line hacks. As shown in this book, combining the latest version of Python with an increased focus on network security can help you to level up your defenses against cyber attacks and cyber threats. Python is being used for increasingly advanced tasks, with the latest update introducing new libraries and packages featured in the Python 3.7.4 recommended version. Moreover, most scripts are compatible with the latest versions of Python and can also be executed in a virtual environment. This book will guide you through using these updated packages to build a secure network with the help of Python scripting. You'll cover a range of topics, from building a network to the procedures you need to follow to secure it. Starting by exploring different packages and libraries, you'll learn about various ways to build a network and connect with the Tor network through Python scripting. You will also learn how to assess a network's vulnerabilities using Python security scripting. Later, you'll learn how to achieve endpoint protection by leveraging Python packages, along with writing forensic scripts. By the end of this Python book, you'll be able to use Python to build secure apps using cryptography and steganography techniques. What you will learnCreate scripts in Python to automate security and pentesting tasksExplore Python programming tools that are used in network security processesAutomate tasks such as analyzing and extracting information from serversUnderstand how to detect server vulnerabilities and analyze security modulesDiscover ways to connect to and get information from the Tor networkFocus on how to extract information with Python forensics toolsWho this book is for This Python network security book is for network engineers, system administrators, or any security professional looking to overcome networking and security challenges. You will also find this book useful if you're a programmer with prior experience in Python. A basic understanding of general programming structures and the Python programming language is required before getting started.

Occupational Outlook Handbook - United States. Bureau of Labor Statistics 1976

Enterprise Networking, Security, and Automation Companion Guide (Ccnav7) - Cisco Networking Academy 2020-06-12

Enterprise Networking, Security, and Automation (CCNA v7) Companion Guide is designed as a portable desk reference to use anytime, anywhere to reinforce the material from the Enterprise Networking, Security, and Automation course and organize your time. The book's features help you focus on important concepts to succeed in this course: Chapter Objectives - Review core concepts by answering the focus questions listed at the beginning of each chapter. Key Terms - Refer to the lists of networking vocabulary introduced and highlighted in context in each chapter. Glossary - Consult the comprehensive Glossary with more than 250 terms. Summary of Activities and Labs - Maximize your study time with this complete list of all associated practice exercises at the end of each chapter. Check Your Understanding - Evaluate your readiness with the end-of-chapter questions that match the style of questions you see in the online course quizzes. The answer key explains each answer. How To - Look for this icon to study the steps you need to learn to perform certain tasks. Interactive Activities - Reinforce your understanding of topics with dozens of exercises from the online course identified throughout the book with this icon. Packet Tracer Activities - Explore and visualize networking concepts using Packet Tracer exercises interspersed throughout the chapters and provided in the accompanying Labs & Study Guide book. Videos - Watch the videos embedded within the online course. Hands-on Labs - Work through all the course labs and additional Class Activities that are included in the course and published in the separate Labs & Study Guide. Part of the Cisco Networking Academy Series from Cisco Press, books in this series support and complement the Cisco Networking Academy curriculum.

Emerging Automation Techniques for the Future Internet - Boucadair, Mohamed 2018-10-12

Automation techniques are meant to facilitate the delivery of flexible, agile, customized connectivity services regardless of the nature of the networking environment. New architectures combine advanced forwarding and routing schemes, mobility features, and customer-adapted resource facilities used for operation and delivery of services. Emerging Automation Techniques for the Future Internet is a collection of innovative research on the methods and applications of new architectures for the planning, dynamic delivery, and operation of services. While highlighting topics including policy enforcement, self-architectures, and automated networks, this book is ideally designed for engineers, IT consultants, professionals, researchers, academicians, and students seeking current research on techniques and structures used to enhance experience and services rendered.

Practical Security Automation and Testing - Tony Hsiang-Chih Hsu 2019-02-04

Your one stop guide to automating infrastructure security using DevOps and DevSecOps Key FeaturesSecure and automate techniques to protect web, mobile or cloud servicesAutomate secure code inspection in C++, Java, Python, and JavaScriptIntegrate security testing with automation frameworks like fuzz, BDD, Selenium and Robot FrameworkBook Description Security automation is the automatic handling of software security assessments tasks. This book helps you to build your security automation framework to scan for vulnerabilities without human intervention. This book will teach you to adopt security automation techniques to continuously improve your entire software development and security testing. You will learn to use open source tools and techniques to integrate security testing tools directly into your CI/CD framework. With this book, you will see how to implement security inspection at every layer, such as secure code inspection, fuzz testing, Rest API, privacy, infrastructure security, and web UI testing. With the help of practical examples, this book will teach you to implement the combination of automation and Security in DevOps. You will learn about the integration of security testing results for an overall security status for projects. By the end of this book, you will be confident implementing automation security in all layers of your software development stages and will be able to build your own in-house security automation platform throughout your mobile and cloud releases. What you will learnAutomate secure code inspection with open source tools and effective secure code scanning suggestionsApply security testing tools and automation frameworks to identify security vulnerabilities in web, mobile and cloud servicesIntegrate security testing tools such as OWASP ZAP, NMAP, SSLyze, SQLMap, and OpenSCAPImplement automation testing techniques with Selenium, JMeter, Robot Framework, Gauntlt, BDD, DDT, and Python unittestExecute security testing of a Rest API Implement web application security with open source tools and script templates for CI/CD integrationIntegrate various types of security testing tool results from a single project into one dashboardWho this book is for The book is for software developers, architects, testers and QA engineers who are looking to leverage automated security testing techniques.

BACnet - H. Michael Newman 2013-08-05
This new book, by the original developer of the BACnet standards, explains how BACnet's protocols manage all basic building functions in a seamless, integrated way. BACnet is a data communication protocol for building automation and control systems, developed within ASHRAE in cooperation with ANSI and the ISO. This book explains how BACnet works with all major control systems--including those made by Honeywell, Siemens, and Johnson Controls--to manage everything from heating to ventilation to lighting to fire control and alarm systems. BACnet is used today throughout the world for commercial and institutional buildings with complex mechanical and electrical systems. Contractors, architects, building systems engineers, and facilities managers must all be cognizant of BACnet and its applications. With a real 'seat at the table,' you'll find it easier to understand the intent and use of each of the data sharing techniques, controller requirements, and opportunities for interoperability between different manufacturers' controllers and systems. Highlights include: * A review of the history of

BACnet and its essential features, including the object model, data links, network technologies, and BACnet system configurations; * Comprehensive coverage of services including object access, file access, remote device management, and BACnet-2012's new alarm and event capabilities; * Insight into future directions for BACnet, including wireless networking, network security, the use of IPv6, extensions for lifts and escalators, and a new set of BACnet Web Services; * Extensive reference appendices for all objects and services; and * Acronyms and abbreviations

Practical Electrical Network Automation and Communication Systems - Cobus Strauss 2003-10-07

In the past automation of the power network was a very specialized area but recently due to deregulation and privatization the area has become of a great importance because companies require more information and communication to minimize costs, reduce workforce and minimize errors in order to make a profit. * Covers engineering requirements and business implications of this cutting-edge and ever-evolving field * Provides a unique insight into a fast-emerging and growing market that has become and will continue to evolve into one of leading communication technologies * Written in a practical manner to help readers handle the transformation from the old analog environment to the modern digital communications-based one

Zero Trust Networks - Evan Gilman 2017-06-19

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That’s an all-too-familiar scenario today. With this practical book, you’ll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they’re internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you’ll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

Threat Modeling - Izar Tarandach 2020-11-13 Threat modeling is one of the most essential--and most misunderstood--parts of the development lifecycle. Whether you're a security practitioner or a member of a development team, this book will help you gain a better understanding of how you can apply core threat modeling concepts to your practice to protect your systems against threats. Contrary to popular belief, threat modeling doesn't require advanced security knowledge to initiate or a Herculean effort to sustain. But it is critical for spotting and addressing potential concerns in a cost-effective way before the code's written--and before it's too late to find a solution. Authors Izar Tarandach and Matthew Coles walk you through various ways to approach and execute threat modeling in your organization. Explore fundamental properties and mechanisms for securing data and system functionality Understand the relationship between security, privacy, and safety Identify key characteristics for assessing system security Get an in-depth review of popular and specialized techniques for modeling and analyzing your systems View the future of threat modeling and Agile development methodologies, including DevOps automation Find answers to frequently asked questions, including how to avoid common threat modeling pitfalls

Programming and Automating Cisco Networks - Ryan Tischer 2016-09-09

Improve operations and agility in any data center, campus, LAN, or WAN Today, the best way to stay in control of your network is to address devices programmatically and automate network interactions. In this book, Cisco experts Ryan Tischer and Jason Gooley show you how to do just that. You'll learn how to use programmability and automation to solve business problems, reduce costs, promote agility and innovation, handle accelerating complexity, and add value in any data center, campus, LAN, or WAN. The authors show you how to create production solutions that run on or interact with Nexus NX-OS-based switches, Cisco ACI, Campus, and WAN technologies.You'll learn how to use advanced Cisco tools together with industry-standard languages and platforms, including Python, JSON, and Linux. The authors demonstrate how to support dynamic application environments, tighten links between apps and infrastructure, and make DevOps work better. This book will be an indispensable resource for network and cloud designers, architects, DevOps engineers, security specialists, and every professional who wants to build or operate high-efficiency networks. Drive more value through programmability and automation, freeing resources for high-value innovation Move beyond error-prone, box-by-box network management Bridge management gaps arising from current operational models Write NX-OS software to run on, access, or extend your Nexus switch Master Cisco's powerful on-box automation and operation tools Manage complex WANs with NetConf/Yang, ConfD, and Cisco SDN Controller Interact with and enhance Cisco Application Centric Infrastructure (ACI) Build self-service catalogs to accelerate application delivery Find resources for deepening your expertise in network automation

Wild World - Peter S. Rush 2017-08-31

Set against the backdrop of the Vietnam War and the protest era of the early 1970s, WILD WORLD is a gripping novel of a power, corruption, injustice, courage, and hope¿and one tenacious young man whose determination to overturn the system holds unexpected consequences for his own life.Steve Logan wants to make the world better. Weeks before his graduation from Brown University, he meets a reform-minded cop from New York City who convinces Steve that to change the system, he has to get involved. Fueled by a strong sense of moral justice, Steve joins the Providence Police Department. Though he¿s eager to make a difference, fighting the establishment is overwhelming. His education makes him an outsider, and his honesty makes him a threat to the corrupt cops who use the badge for money and power. At home, his college friends think he¿s a traitor, and even Roxy, the med student he loves, has begun to pull away. But Steve isn¿t going to give up. He devises a dangerous plan to radically shake up the system and take his enemies down . . . unless they take him out first.

Electricity Supply Systems of the Future - Nikos Hatziargyriou 2020-07-20

This book offers a vision of the future of electricity supply systems and CIGRE’s views on the know-how that will be needed to manage the transition toward them. A variety of factors are driving a transition of electricity supply systems to new supply models, in particular the increasing use of renewable sources, environmental factors and developments in ICT technologies. These factors suggest that there are two possible models for power network development, and that those models are not necessarily exclusive: 1. An increasing importance of large networks for bulk transmission capable of interconnecting load regions and large centralized renewable generation resources, including offshore and of providing more interconnections between the various countries and energy markets. 2. An emergence of clusters of small, largely self-contained distribution networks, which include decentralized local generation, energy storage and active customer participation, intelligently managed so that they operate as active networks providing local active and reactive support. The electricity supply systems of the future will likely include a combination of the above two models, since additional bulk connections and active distribution networks are needed in order to reach ambitious environmental, economic and security-reliability targets. This concise yet comprehensive reference resource on technological developments for future electrical systems has been written and reviewed by experts and the Chairs of the sixteen Study Committees that form the Technical Council of CIGRE.

Network Security Auditing - Chris Jackson 2010-06-02

This complete new guide to auditing network security is an indispensable resource for security, network, and IT professionals, and for the consultants and technology partners who serve them. Cisco network security expert Chris Jackson begins with a thorough overview of the auditing process, including coverage of the latest regulations, compliance issues, and industry best practices. The author then demonstrates how to segment security architectures into domains and measure security effectiveness through a comprehensive systems approach. Network Security Auditing thoroughly covers the use of both commercial and open source tools to assist in auditing and validating security policy assumptions. The book also introduces leading IT governance frameworks such as COBIT, ITIL, and ISO 17799/27001, explaining their values, usages, and effective integrations with Cisco security products.

Computational Intelligence, Cyber Security and Computational Models - G. Sai Sundara Krishnan 2013-11-26

This book contains cutting-edge research material presented by researchers, engineers, developers, and practitioners from academia and industry at the International Conference on Computational Intelligence, Cyber Security and Computational Models (ICC3) organized by PSG College of Technology, Coimbatore, India during December 19–21, 2013. The materials in the book include theory and applications to provide design, analysis, and modeling of the key areas. The book will be useful material for students, researchers, professionals, as well academicians in understanding current research trends and findings and future scope of research in computational intelligence, cyber security, and computational models.

Industrial Network Security - David J. Teumim 2010

Whether we talk about process control systems that run chemical plants, supervisory control and data acquisition systems for utilities, or factory automation systems for discrete manufacturing, the backbone critical infrastructure consists of these industrial networks and is dependent on their continued operation. This introduces managers, engineers, technicians, and operators on how to keep industrial networks secure amid rising threats from hackers, disgruntled employees, and even cyberterrorists.

Network-on-Chip Security and Privacy - Prabhat Mishra 2021-06-04

This book provides comprehensive coverage of Network-on-Chip (NoC) security vulnerabilities and state-of-the-art countermeasures, with contributions from System-on-Chip (SoC) designers, academic researchers and hardware security experts. Readers will gain a clear understanding of the existing security solutions for on-chip communication architectures and how they can be utilized effectively to design secure and trustworthy systems.

Network Science Models for Data Analytics Automation - Xin W. Chen 2022-02-21

This book explains network science and its applications in data analytics for critical infrastructures, engineered systems, and knowledge acquisition. Each chapter describes step-by-step processes of how network science enables and automates data analytics through examples. The book not only dissects modeling techniques and analytical results but also explores the intrinsic development of these models and analyses. This unique approach bridges the gap between theory and practice and channels' managerial and problem-solving skills. Engineers, researchers, and managers would benefit from the extensive theoretical background and practical examples discussed in this book. Advanced undergraduate students and graduate students in mathematics, statistics, engineering, business, public health, and social science may use this book as a one-semester textbook or a reference book. Readers who are more interested in applications may skip Chapter 1 and peruse through the rest of the book with ease.

Network Programmability and Automation - Jason Edelman 2018-02-02

Like sysadmins before them, network engineers are finding that they cannot do their work manually anymore. As the field faces new protocols, technologies, delivery models, and a pressing need for businesses to be more agile and flexible, network automation is becoming essential. This practical guide shows network engineers how to use a range of technologies and tools—including Linux, Python, JSON, and XML—to automate their systems through code. Network programming and automation will help you simplify tasks involved in configuring, managing, and operating network equipment, topologies, services, and connectivity. Through the course of the book, you'll learn the basic skills and tools you need to make this critical transition. This book covers: Python programming basics: data types, conditionals, loops, functions, classes, and modules Linux fundamentals to provide the foundation you need on your network automation journey Data formats and models: JSON, XML, YAML, and YANG for networking Jinja templating and its applicability for creating network device configurations The role of application programming interfaces (APIs) in network automation Source control with Git to manage code changes during the automation process How Ansible, Salt, and StackStorm open source automation tools can be used to automate network devices Key tools and technologies required for a Continuous Integration (CI) pipeline in network operations

Control and Automation of Electrical Power Distribution Systems - James Northcote-Green 2017-12-19

Implementing the automation of electric distribution networks, from simple remote control to the application of software-based decision tools, requires many considerations, such as assessing costs, selecting the control infrastructure type and automation level, deciding on the ambition level, and justifying the solution through a business case. Control and Automation of Electric Power Distribution Systems addresses all of these issues to aid you in resolving automation problems and improving the management of your distribution network. Bringing together automation concepts as they apply to utility distribution systems, this volume presents the theoretical and practical details of a control and automation solution for the entire distribution system of substations and feeders. The fundamentals of this solution include depth of control, boundaries of control responsibility, stages of automation, automation intensity levels, and automated device preparedness. To meet specific performance goals, the authors discuss distribution planning, performance calculations, and protection to facilitate the selection of the primary device, associated secondary control, and fault indicators. The book also provides two case studies that illustrate the business case for distribution automation (DA) and methods for calculating benefits, including the assessment of crew time savings. As utilities strive for better economies, DA, along with other tools described in this volume, help to achieve improved management of the distribution network. Using Control and Automation of Electric Power Distribution Systems, you can embark on the automation solution best suited for your needs.

Protective Relays - A. R. van. C. Warrington 2012-12-06

1. Purpose of Protective Relays and Relaying. Causes of Faults. Definitions. Functions of Protective Relays. Application to a Power System.- 2. Relay Design and Construction. Characteristics. Choice of Measuring Units. Construction of Measuring Units. Construction of Timing Units. Details of Design. Cases. Panel Mounting. Operation Indicators. Finishes.- 3. The Main Characteristics of Protective Relays. Phase and Amplitude Comparators. Relay Characteristics. General Equation for Characteristics. Inversion Chart. Resonance. Appendix.- 4. Overcurrent Protection. Time-Current Characteristics. App.

Pro Google Kubernetes Engine - Navin Sabharwal 2020-11-08

Discover methodologies and best practices for getting started with Google Kubernetes Engine (GKE). This book helps you understand how GKE provides a fully managed environment to deploy and operate containerized applications on Google Cloud infrastructure. You will see how Kubernetes makes it easier for users to manage clusters and the container ecosystem. And you will get detailed guidance on deploying and managing applications, handling administration of container clusters, managing policies, and monitoring cluster resources. You will learn how to operate the GKE environment through the GUI-based Google Cloud console and the "gcloud" command line interface. The book starts with an introduction to GKE and associated services. The authors provide hands-on examples to set up Container Registry and GKE Cluster, and you will follow through an application deployment on GKE. Later chapters focus on securing your GCP GKE environment, GKE monitoring and dashboarding, and CI/CD automation. All of the code presented in the book is provided in the form of scripts, which allow you to try out the examples and extend them in interesting ways. What You Will Learn Understand the main container services in GCP (Google Container Registry, Google Kubernetes Engine, Kubernetes Engine, Management Services) Perform hands-on steps to deploy, secure, scale, monitor, and automate your containerized environment Deploy a sample microservices application on GKE Deploy monitoring for your GKE environment Use DevOps automation in the CI/CD pipeline and integrate it with GKE Who This Book Is For Architects, developers, and DevOps engineers who want to learn Google Kubernetes Engine

Industrial Network Security - Eric D. Knapp 2014-12-09

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems

Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

Fieldbus and Networking in Process Automation - Sunit Kumar Sen 2017-12-19

Fieldbuses, particularly wireless fieldbuses, offer a multitude of benefits to process control and automation. Fieldbuses replace point-to-point technology with digital communication networks, offering increased data availability and easier configurability and interoperability. Fieldbus and Networking in Process Automation discusses the newest fieldbuses on the market today, detailing their utilities, components and configurations, wiring and installation methods, commissioning, and safety aspects under hostile environmental conditions. This clear and concise text: Considers the advantages and shortcomings of the most sought after fieldbuses, including HART, Foundation Fieldbus, and Profibus Presents an overview of data communication, networking, cabling, surge protection systems, and device connection techniques Provides comprehensive coverage of intrinsic safety essential to the process control, automation, and chemical industries Describes different wireless standards and their coexistence issues, as well as wireless sensor networks Examines the latest offerings in the wireless networking arena, such as WHART and ISA100.11a Offering a snapshot of the current state of the art, Fieldbus and Networking in Process Automation not only addresses aspects of integration, interoperability, operation, and automation pertaining to fieldbuses, but also encourages readers to explore potential applications in any given industrial environment.

Network Automation Made Easy - Ivo Pinto 2021-11-24

As networks grow ever more complex, network professionals are seeking to automate processes for configuration, management, testing, deployment, and operation. Using automation, they aim to lower expenses, improve productivity, reduce human error, shorten time to market, and improve agility. In Network Automation Made Easy, expert practitioner Ivo Pinto presents all the concepts and techniques you'll need to move your entire physical and virtual infrastructure towards greater automation, and maximize the value it delivers. Writing for experienced professionals, Ivo Pinto reviews today's leading use cases for automation, compares leading tools, and presents a deep dive into using the open source Ansible engine to automate common tasks. You'll find everything you need: from practical code snippets to real-world case studies to a complete methodology for planning strategy. Coverage includes: Exploring modern use cases for network automation, and comparing today's most widely used automation tools Capturing essential data for use in network automation, using standard formats such as JSON, XML, and YAML Getting more value from the data your network can capture Installing Ansible and mastering its building blocks, including plays, tasks, modules, variables, conditionals, loops, and roles Performing common networking tasks with Ansible playbooks: managing files, devices, VMs, cloud constructs, APIs, and more Discovering how Ansible can be used to automate even the largest global network architectures Using NetDevOps to transform your approach to automation Creating a new NetDevOps pipeline, step by step Building a network automation strategy from the ground up, reflecting enterprise lessons

Computers at Risk - National Research Council 1990-02-01

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

Guide to Computer Network Security - Joseph Migga Kizza 2020-06-03

This timely textbook presents a comprehensive guide to the core topics in cybersecurity, covering issues of security that extend beyond traditional computer networks to the ubiquitous mobile communications and online social networks that have become part of our daily lives. In the context of our growing dependence on an ever-changing digital ecosystem, this book stresses the importance of security awareness, whether in our homes, our businesses, or our public spaces. This fully updated new edition features new material on the security issues raised by blockchain technology, and its use in logistics, digital ledgers, payments systems, and digital contracts. Topics and features: Explores the full range of security risks and vulnerabilities in all connected digital systems Inspires debate over future developments and improvements necessary to enhance the security of personal, public, and private enterprise systems Raises thought-provoking questions regarding legislative, legal, social, technical, and ethical challenges, such as the tension between privacy and security Describes the fundamentals of traditional computer network security, and common threats to security Reviews the current landscape of tools, algorithms, and professional best practices in use to maintain security of digital systems Discusses the security issues introduced by the latest generation of network technologies, including mobile systems, cloud computing, and blockchain Presents exercises of varying levels of difficulty at the end of each chapter, and concludes with a diverse selection of practical projects Offers supplementary material for students and instructors at an associated website, including slides, additional projects, and syllabus suggestions This important textbook/reference is an invaluable resource for students of computer science, engineering, and information management, as well as for practitioners working in data- and information-intensive industries.

Industrial Automation and Control System Security Principles - Ronald L. Krutz 2016-07

Network Protection & Automation Guide - 2002