Proofpoint Messaging Security Gateway Appliances

Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure "how to"

solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, Threat Hunting in the Cloud is also an indispensable guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy. An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device

level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

"Jaap's Practical Guide to Exchange Server 2010 draws upon all that experience to deliver an easy-to-use guide to this latest platform, full of useful examples and top tips for SysAdmins, both new and experienced"--Resource description page.

Cloud Security and Privacy

InfoWorld

Ransomware

The Independent Guide to IBM-standard Personal Computing

Software Defined Networks

Software Defined Networks: A Comprehensive Approach, Second Edition provides in-depth coverage of the technologies collectively known as Software Defined Networking (SDN). The book shows how to explain to business decision-makers the benefits and risks in shifting parts of a network to the SDN model, when to integrate SDN technologies in a network, and how to develop or acquire SDN applications. In addition, the book emphasizes the parts of the technology that encourage opening up the network, providing treatment for alternative approaches to SDN that expand the definition of SDN as networking vendors adopt traits of SDN to their existing solutions. Since the first edition was published, the SDN market has matured, and is being gradually integrated and morphed into something more compatible with mainstream networking vendors. This book reflects these changes, with coverage of the OpenDaylight controller and its support for multiple southbound protocols, the Inclusion of NETCONF in discussions on controllers and devices, expanded coverage of NFV, and updated coverage of the latest approved version (1.5.1) of the OpenFlow specification. Contains expanded coverage of controllers Includes a new chapter on NETCONF and SDN Presents expanded coverage of SDN in optical networks Provides support materials for use in computer networking courses
IBM DFSMS and the IBM DS8000 added functionality to provide elements of serverless data movement, and for IBM z/OS® to communicate with a

storage cloud. The function is known as Transparent Cloud Tiering and is composed of the following key elements: A gateway in the DS8000, which allows the movement of data to and from Object Storage by using a network connection, with the option to encrypt data in the Cloud. DFSMShsm enhancements to support Migrate and Recall functions to and from the Object Storage. Other commands were enhanced to monitor and report on the new functionality. DFSMShsm uses the Web Enablement toolkit for z/OS to create and access the metadata for specific clouds, containers, and objects. DFSMSdss enhancements to provide some basic backup and restore functions to and from the cloud. The IBM TS7700 can also be set up to act as if it were cloud storage from the DS8000 perspective. This IBM Redbooks publication is divided into the following parts: Part 1 provides you with an introduction to clouds. Part 2 shows you how we set up the Transparent Cloud Tiering in a controlled laboratory and how the new functions work. We provide points to consider to help you set up your storage cloud and integrate it into your operational environment. Part 3 shows you how we used the new functionality to communicate with the cloud and to send data and retrieve data from it.. This edition applies to DS8900F Release 9.2 and covers more recent features of TCT such as multi-cloud connections. along with additional advice for high availabilty cloud connectivity and DFSMShsm improvements.

InfoWorld is targeted to Senior IT professionals. Content is segmented into Channels and Topic Centers. InfoWorld also celebrates people, companies, and projects.

AWS Certified Security Study Guide

Adversarial Tradecraft in Cybersecurity

Machine Learning Forensics for Law Enforcement, Security, and Intelligence

Network World

PC Mag

If you create, manage, operate, or configure systems running in the cloud, you're a cloud engineer--even if you work as a system administrator, software developer, data scientist, or site reliability engineer. With this book, professionals from around the world provide valuable insight into today's cloud engineering role. These concise articles explore the entire cloud computing experience, including fundamentals, architecture, and migration. You'll delve into security and compliance, operations and reliability, and software development. And examine networking, organizational culture, and more. You're sure to find 1, 2, or 97 things that inspire you to dig deeper and expand your own career. "Three Keys to Making the Right Multicloud Decisions," Brendan O'Leary "Serverless Bad Practices," Manases Jesus Galindo Bello "Failing a Cloud Migration," Lee Atchison "Treat Your Cloud Environment as If It Were On Premises," Iyana Garry "What Is Toil, and Why Are SREs Obsessed with It?", Zachary Nickens "Lean QA: The QA Evolving in the DevOps World," Theresa Neate "How

Economies of Scale Work in the Cloud," Jon Moore "The Cloud Is Not About the Cloud," Ken Corless "Data Gravity: The Importance of Data Management in the Cloud," Geoff Hughes "Even in the Cloud, the Network Is the Foundation," David Murray "Cloud Engineering Is About Culture, Not Containers," Holly Cummins

Microservices is an architectural style in which large, complex software applications are composed of one or more smaller services. Each of these microservices focuses on completing one task that represents a small business capability. These microservices can be developed in any programming language. They communicate with each other using language-neutral protocols, such as Representational State Transfer (REST), or messaging applications, such as IBM® MQ Light. This IBM Redbooks® publication gives a broad understanding of this increasingly popular architectural style, and provides some real-life examples of how you can develop applications using the microservices approach with IBM BluemixTM. The source code for all of these sample scenarios can be found on GitHub (https://github.com/). The book also presents some case studies from IBM products. We explain the architectural decisions made, our experiences, and lessons learned when redesigning these products using the microservices approach. Information technology (IT) professionals interested in learning about microservices and how to develop or redesign an application in Bluemix using microservices can benefit from this book.

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help

you make better buying decisions and get more from technology.
Leading with IT
Defending Against Digital Extortion
Challenges in the IoT and Smart Environments
Lessons from Singapore's First CIO
Blocking Spam & Spyware For Dummies

This is the first book to present a full, socio-technical-legal picture on the security practices of cyber criminals, based on confidential police sources related to some of the world's most serious and organized criminals.

This book brings a high level of fluidity to analytics and addresses recent trends, innovative ideas, challenges and cognitive computing solutions in big data and the Internet of Things (IoT). It explores domain knowledge, data science reasoning and cognitive methods in the context of the IoT, extending current data science approaches by incorporating insights from experts as well as a notion of artificial intelligence, and performing inferences on the knowledge The book provides a comprehensive overview of the constituent paradigms underlying cognitive computing methods, which illustrate the increased focus on big data in IoT problems as they evolve. It includes novel, in-depth fundamental research contributions from a methodological/application in data science accomplishing sustainable solution for the future perspective. Mainly focusing on the design of the best cognitive embedded data science

technologies to process and analyze the large amount of data collected through the IoT, and aid better decision making, the book discusses adapting decision-making approaches under cognitive computing paradigms to demonstrate how the proposed procedures as well as big data and IoT problems can be handled in practice. This book is a valuable resource for scientists, professionals, researchers, and academicians dealing with the new challenges and advances in the specific areas of cognitive computing and data science approaches.

There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch each potential vulnerability or address each new attack one-by-one is a bit like emptying the Atlantic with paper cup.If you're a network administrator, the pressure is on you to defend your systems from attack. But short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems? Where do you start?Using the steps laid out by professional security analysts and consultants to identify and assess risks, Network Security Assessment offers an efficient testing model that an administrator can adopt, refine, and reuse to create proactive defensive strategies to protect their systems from the threats that are out there, as well as those still being developed.This thorough and insightful guide covers offensive technologies by grouping and analyzing them at a higher

level--from both an offensive and defensive standpoint--helping administrators design and deploy networks that are immune to offensive exploits, tools, and scripts. Network administrators who need to develop and implement a security assessment program will find everything they're looking for--a proven, expert-tested methodology on which to base their own comprehensive program--in this time-saving new book.

Exchange 2010

PC Magazine

Network Security Assessment

How to Keep What's Good, Fix What's Wrong, and Unlock Great Performance

97 Things Every Cloud Engineer Should Know

A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In Click Here to Kill Everybody, renowned expert and best-selling author Bruce Schneier

examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical, political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

Get prepared for the AWS Certified Security Specialty certification with this excellent resource By earning the AWS Certified Security Specialty certification, IT professionals can gain valuable recognition as cloud security experts. The AWS Certified Security Study Guide: Specialty (SCS-C01) Exam helps cloud security practitioners prepare for success on the certification exam. It's also an excellent reference for professionals, covering security best practices and the implementation of security features for clients or employers. Architects and engineers with knowledge of cloud computing architectures will find significant value in this book, which offers guidance on primary security threats and defense principles. Amazon Web Services security controls and tools are explained through real-world scenarios. These examples demonstrate how professionals can design, build, and operate secure cloud environments that run modern applications. The study guide serves as a primary source for those who are ready to apply their skills and seek certification. It addresses how cybersecurity can be improved using the AWS cloud and its native security services. Readers will benefit from detailed coverage of AWS Certified Security Specialty Exam topics. Covers all AWS

Certified Security Specialty exam topics Explains AWS cybersecurity techniques and incident response Covers logging and monitoring using the Amazon cloud Examines infrastructure security Describes access management and data protection With a single study resource, you can learn how to enhance security through the automation, troubleshooting, and development integration capabilities available with cloud computing. You will also discover services and tools to develop security plans that work in sync with cloud adoption.

Enhance Windows security and protect your systems and servers from various cyber attacks Key Features Protect your device using a zero-trust approach and advanced security techniques Implement efficient security measures using Microsoft Intune, Configuration Manager, and Azure solutions Understand how to create cyber-threat defense solutions effectively Book Description Are you looking for effective ways to protect Windows-based systems from being compromised by unauthorized users? Mastering Windows Security and Hardening is a detailed guide that helps you gain expertise when implementing efficient security measures and creating robust defense solutions. We will begin with an introduction to Windows security fundamentals, baselining, and the importance of building a baseline for an organization. As you advance, you will learn how to effectively secure and harden your Windows-based system, protect identities, and even manage access. In the concluding chapters, the book will take you through testing, monitoring, and security operations. In addition to this, you'll be equipped with the tools you need to ensure compliance and continuous monitoring through security operations. By the end of this book, you'll have developed a full understanding of the processes and tools involved in securing and hardening your Windows environment. What you will learn Understand baselining and learn the best

practices for building a baseline Get to grips with identity management and access management on Windows-based systems Delve into the device administration and remote management of Windows-based systems Explore security tips to harden your Windows server and keep clients secure Audit, assess, and test to ensure controls are successfully applied and enforced Monitor and report activities to stay on top of vulnerabilities Who this book is for This book is for system administrators, cybersecurity and technology professionals, solutions architects, or anyone interested in learning how to secure their Windows-based systems. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.

A Comprehensive Approach

Microservices from Theory to Practice: Creating Applications in IBM Bluemix Using the Microservices Approach

Frameworks, Tools and Applications

An Enterprise Perspective on Risks and Compliance

Threat Hunting in the Cloud

Explore the insights of a world-leading CIO as he expounds on the challenges faced by technology executives and how to overcome them As the pace of change in business continues to rapidly accelerate, Chief Information Officers and Chief Technology Officers are often left with accountability for future-proofing their organizations. Renowned professor, executive, and author Alex Siow shows you how you can meet that challenge while managing the information overload that often accompanies these positions. In Leading with IT: Lessons from Singapore's

First CIO, the author uses his expansive and impressive experience in academia and industry to lead you down a path to achieving success as a CIO or CTO. Filled with practical tips, case studies, and personal insights, the book discusses: The management of legacy information and telecommunications technology The information overload often suffered by technology executives How to motivate and mentor a workforce How to manage change effectively The fostering of innovation The future of money, work, and artificial intelligence Perfect for CIOs, CTOs, and the executives, managers, and employees who work with and for them, Leading with IT delivers an engaging and insightful exploration of what it takes to achieve astounding results at the intersection of technology and business.

Increasingly, crimes and fraud are digital in nature, occurring at breakneck speed and encompassing large volumes of data. To combat this unlawful activity, knowledge about the use of machine learning technology and software is critical. Machine Learning Forensics for Law Enforcement, Security, and Intelligence integrates an assortment of deductive

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Campus Technology

Results

Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks

Cognitive Computing for Big Data Systems Over IoT

Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the

various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

Master cutting-edge techniques and countermeasures to protect your organization from live hackers. Learn how to harness cyber deception in your operations to gain an edge over the competition. Key Features Gain an advantage against live hackers in a competition or real computing environment Understand advanced red team and blue team techniques with code examples Learn to battle in short-term memory, whether remaining unseen (red teams) or monitoring an attacker's traffic (blue teams) Book Description Little has been written about what to do when live hackers are on your system and running amok. Even experienced hackers tend to choke up when they realize the network defender has caught them and is zoning in on their implants in real time. This book will provide tips and tricks all along the kill chain of an attack, showing where hackers can have the upper hand in a live conflict and how defenders can outsmart them in this adversarial game of computer cat and mouse. This book contains two subsections in each chapter, specifically focusing on the offensive and defensive teams. It begins by introducing you to adversarial operations and principles of computer conflict where you will explore the core principles of deception, humanity, economy, and more about human-on-human conflicts. Additionally, you will understand everything from planning to setting up

infrastructure and tooling that both sides should have in place. Throughout this book, you will learn how to gain an advantage over opponents by disappearing from what they can detect. You will further understand how to blend in, uncover other actors' motivations and means, and learn to tamper with them to hinder their ability to detect your presence. Finally, you will learn how to gain an advantage through advanced research and thoughtfully concluding an operation. By the end of this book, you will have achieved a solid understanding of cyberattacks from both an attacker's and a defender's perspective. What you will learn Understand how to implement process injection and how to detect it Turn the tables on the offense with active defense Disappear on the defender's system, by tampering with defensive sensors Upskill in using deception with your backdoors and countermeasures including honeypots Kick someone else from a computer you are on and gain the upper hand Adopt a language agnostic approach to become familiar with techniques that can be applied to both the red and blue teams Prepare yourself for real-time cybersecurity conflict by using some of the best techniques currently in the industry Who this book is for Pentesters to red teamers, security operations center analysts to incident responders, attackers, defenders, general hackers, advanced computer users, and security engineers should gain a lot from this book. This book will also be beneficial to those getting into purple teaming or adversarial simulations, as it

includes processes for gaining an advantage over the other team. Basic knowledge of Python programming, Go programming, Bash, PowerShell, and systems administration is desirable. Furthermore, knowledge of incident response and Linux is beneficial. Prior exposure to cybersecurity, penetration testing, and ethical hacking basics is desirable.

The biggest online threat to businesses and consumers today is ransomware, a category of malware that can encrypt your computer files until you pay a ransom to unlock them. With this practical book, you'll learn how easily ransomware infects your system and what steps you can take to stop the attack before it sets foot in the network. Security experts Allan Liska and Timothy Gallo explain how the success of these attacks has spawned not only several variants of ransomware, but also a litany of ever-changing ways they're delivered to targets. You'll learn pragmatic methods for responding quickly to a ransomware attack, as well as how to protect yourself from becoming infected in the first place. Learn how ransomware enters your system and encrypts your files Understand why ransomware use has grown, especially in recent years Examine the organizations behind ransomware and the victims they target Learn how wannabe hackers use Ransomware as a Service (RaaS) to launch campaigns Understand how ransom is paid—and the pros and cons of paying Use methods to protect your organization's workstations and servers

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World
IoT Security
Specialty (SCS-C01) Exam
IBM DS8000 Transparent Cloud Tiering (DS8000 Release 9.2)
Know Your Network

Every company has a personality. Does yours help or hinder your results? Does it make you fit for growth? Find out by taking the quiz that's helped 50,000 people better understand their organizations at OrgDNA.com and to learn more about Organizational DNA. Just as you can understand an individual's personality, so too can you understand a company's type—what makes it tick, what's good and bad about it. Results explains why some organizations bob and weave and roll with the punches to consistently deliver on commitments and produce great results, while others can't leave their corner of the ring without tripping on their own shoelaces. Gary Neilson and Bruce Pasternack help you identify which of the seven company types you work for—and how to keep what's good and fix what's wrong. You'll feel the shock of recognition ("That's me, that's my company") as you find out whether your organization is: • Passive-Aggressive ("everyone agrees, smiles, and nods, but nothing changes"): entrenched underground resistance makes getting anything done like trying to nail Jell-O to the wall

• Fits-and-Starts ("let 1,000 flowers bloom"): filled with smart people pulling in different directions • Outgrown ("the good old days meet a brave new world"): reacts slowly to market developments, since it's too hard to run new ideas up the flagpole • Overmanaged ("we're from corporate and we're here to help"): more reporting than working, as managers check on their subordinates' work so they can in turn report to their bosses • Just-in-Time ("succeeding, but by the skin of our teeth"): can turn on a dime and create real breakthroughs but also tends to burn out its best and brightest • Military Precision ("flying in formation"): executes brilliant strategies but usually does not deal well with events not in the playbook • Resilient ("as good as it gets"): flexible, forward-looking, and fun; bounces back when it hits a bump in the road and never, ever rests on its laurels For anyone who's ever said, "Wow, that's a great idea, but it'll never happen here" or "Whew, we pulled it off again, but I'm tired of all this sprinting," Results provides robust, practical ideas for becoming and remaining a resilient business. Also available as an eBook From the Hardcover edition.

Mastering Windows Security and Hardening

Offense versus defense in real-time computer conflict

Advances in Authentication

A Practical Approach

A Practitioners' Guide to Security, Ethics and Criminal Threats