Splunk Search Reference Guide

Big data has incredible business value, and Splunk is the best tool for unlocking that value. Exploring Splunk shows you how to pinpoint answers and find patterns obscured by the flood of machinegenerated data. This book uses an engaging, visual presentation style that quickly familiarizes you with how to use Splunk. You'll move from mastering Splunk basics to creatively solving real-world problems, finding the gems hidden in big data.

A field guide for the unique challenges of data science leadership, filled with transformative insights, personal experiences, and industry examples. In How To Lead in Data Science you will learn: Best practices for leading projects while balancing complex trade-offs Specifying, prioritizing, and planning projects from vague requirements Navigating structural challenges in your organization Working through project failures with positivity and tenacity Growing your team with coaching, mentoring, and advising Crafting technology roadmaps and championing successful projects Driving diversity, inclusion, and belonging within teams Architecting a long-term business strategy and data roadmap as an executive Delivering a data-driven culture and structuring productive data science organizations How to Lead in Data Science is full of techniques for leading data science at every seniority level—from heading up a single project to overseeing a whole company's data strategy. Authors Jike Chong and Yue Cathy Chang share hard-won advice that they've developed building data teams for LinkedIn, Acorns, Yiren Digital, large asset-management firms, Fortune 50 companies, and more. You'll find advice on plotting your long-term career advancement, as well as quick wins you can put into practice right away. Carefully crafted assessments and interview scenarios encourage introspection, reveal personal blind spots, and highlight development areas. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Lead your data science teams and projects to success! To make a consistent, meaningful impact as a data science leader, you must articulate technology roadmaps, plan effective project strategies, support diversity, and create a positive environment for professional growth. This book delivers the wisdom and practical skills you need to thrive as a data science leader at all levels, from team member to the C-suite. About the book How to Lead in Data Science shares unique leadership techniques from high-performance data teams. It's filled with best practices for balancing project trade-offs and producing exceptional results, even when beginning with vague requirements or unclear expectations. You'll find a clearly presented modern leadership framework based on current case studies, with insights reaching all the way to Aristotle and Confucius. As you read, you'll build practical skills to grow and improve your team, your company's data culture, and yourself. What's inside How to coach and mentor team members Navigate an organization's structural challenges Secure commitments from other teams and partners Stay current with the technology landscape Advance your career About the reader For data science practitioners at all levels. About the author Dr. Jike Chong and Yue Cathy Chang build, lead, and grow high-performing data teams across industries in public and private companies, such as Acorns, LinkedIn, large asset-management firms, and Fortune 50 companies. Table of Contents 1 What makes a successful data scientist? PART 1 THE TECH LEAD: CULTIVATING LEADERSHIP 2 Capabilities for leading projects 3 Virtues for leading projects PART 2 THE MANAGER: NURTURING A TEAM 4 Capabilities for leading people 5 Virtues for leading people PART 3 THE DIRECTOR: GOVERNING A FUNCTION 6 Capabilities for leading a function 7 Virtues for leading a function PART 4 THE EXECUTIVE: INSPIRING AN INDUSTRY 8 Capabilities for leading a company 9 Virtues for leading a company PART 5 THE LOOP AND THE FUTURE 10 Landscape, organization, opportunity, and practice 11 Leading in data science and a future outlook

In the spring of 2010, Harvard Business School's graduating class asked HBS professor Clay Christensen to address them—but not on how to apply his principles and thinking to their post-HBS careers. The students wanted to know how to apply his wisdom to their personal lives. He shared with them a set of guidelines that have helped him find meaning in his own life, which led to this now-classic article. Although Christensen's thinking is rooted in his deep religious faith, these are strategies anyone can use. Since 1922, Harvard Business Review has been a leading source of breakthrough ideas in management practice. The Harvard Business Review Classics series now offers you the opportunity to make these seminal pieces a part of your permanent management library. Each highly readable volume contains a groundbreaking idea that continues to shape best practices and inspire countless managers around the world.

If you are a Splunk user and want to enter the wonderful world of Splunk application development, then this book is for you. Some experience with Splunk, writing searches, and designing basic dashboards is expected.

The Mysterious Deaths of Barry and Honey Sherman

The Billionaire Murders

How Will You Measure Your Life? (Harvard Business Review Classics)

Analysis, Visualization and Dashboards

How to Thrive in One of the World's Fastest Growing Careers--While Driving Growth For Your Company

Advanced Splunk

Over the years software systems have evolutionarily become more and more complex. One of the techniques for dealing with this inherent complexity of software systems is dependency injection - a design pattern that allows the removal of hard-coded dependencies and makes it possible to assemble a service by changing dependencies easily, whether at run-time or compile-time. It promotes code reuse and loosely-coupled design which leads to more easily maintainable and flexible code. The guide you are holding in your hands is a primer on using dependency injection with Unity - a lightweight extensible dependency injection container built by the Microsoft patterns & practices team. It covers various styles of dependency injection and also additional capabilities of Unity container, such as object lifetime management, interception, and registration by convention. It also discusses the advanced topics of enhancing Unity with your custom extensions. The guide contains plenty of trade-off discussions and tips and tricks for managing your application cross-cutting concerns and making the most out of both dependency injection and Unity. These are accompanied by a real world example that will help you master the techniques. Keep in mind that Unity can be used in a wide range of application types such as desktop, web, services, and cloud. We encourage you to experiment with the sample code and think beyond the scenarios discussed in the guide. In addition, the guide includes the Tales from the Trenches - a collection of case studies that offer a different perspective through the eyes of developers working on the real world projects and sharing their experiences. These chapters make clear the range of scenarios in which you can use Unity, and also highlight its ease of use and flexibility. Whether you are a seasoned developer or just starting your development journey, we hope this guide will be worth your time studying it. We hope you discover that Unity container adds significant benefits to your applications and helps you to achieve the goals of maintainability, testability, flexibility, and extensibility in your own projects.

Master the art of getting the maximum out of your machine data using Splunk About This Book A practical and comprehensive guide to the advanced functions of Splunk,, including the new features of Splunk 6.3 Develop and manage your own Splunk apps for greater insight from your machine data Full coverage of high-level Splunk techniques including advanced searches, manipulations, and visualization Who This Book Is For This book is for Splunk developers looking to learn advanced strategies to deal with big data from an enterprise architectural perspective. It is expected that readers have a basic understanding and knowledge of using Splunk Enterprise. What You Will Learn Find out how to develop and manage apps in Splunk Work with important search commands to perform data analytics on uploaded data Create visualizations in Splunk Explore tweaking Splunk Integrate Splunk with any pre-existing application to perform data crunching efficiently and in real time Make your big data speak with analytics and visualizations using Splunk Use SDK and Enterprise integration with tools such as R and Tableau In Detail Master the power of Splunk and learn the advanced strategies to get the most out of your machine data with this practical advanced guide. Make sense of the hidden data of your organization – the insight of your servers, devices, logs, traffic and clouds. Advanced Splunk shows you how. Dive deep into Splunk to find the most efficient solution to your data problems. Create the robust Splunk solutions you need to make informed decisions in big data machine analytics. From visualizations to enterprise integration, this well-organized high level guide has everything you need for Splunk mastery. Start with a complete overview of all the new features and advantages of the latest version of Splunk and the Splunk Environment. Go hands on with uploading data, search commands for basic and advanced analytics, advanced visualization techniques, and dashboard customizing. Discover how to tweak Splunk to your needs, and get a complete on Enterprise Integration of Splunk with various analytics and visualization tools. Finally, discover how to set up and use all the new features of the latest version of Splunk. Style and approach This book follows a step by step approach. Every new concept is built on top of its previous chapter, and it is full of examples and practical scenarios to help the reader experiment as they read.

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.

Transform machine-generated data into valuable business insights using the powers of Splunk Key Features Explore the all-new machine learning toolkit in Splunk 7.x Tackle any problems related to searching and analyzing your data with Splunk Get the latest information and business insights on Splunk 7.x Book Description Splunk makes it easy for you to take control of your data and drive your business with the cutting edge of operational intelligence and business analytics. Through this Learning Path, you'll implement new services and utilize them to quickly and efficiently process machine-generated big data. You'll begin with an introduction to the new features, improvements, and offerings of Splunk 7. You'll learn to efficiently use wildcards and modify your search to make it faster. You'll learn how to enhance your applications by using XML dashboards and configuring and extending Splunk. You'll also find step-by-step demonstrations that'll walk you through building an operational intelligence application. As you progress, you'll explore data models and pivots to extend your intelligence capabilities. By the end of this Learning Path, you'll have the skills and confidence to implement various Splunk services in your projects. This Learning Path includes content from the following Packt products: Implementing Splunk 7 - Third Edition by James Miller Splunk Operational Intelligence Cookbook - Third Edition by Paul R Johnson, Josh Diakun, et al What you will learn Master the new offerings in Splunk: Splunk Cloud and the Machine Learning Toolkit Create efficient and effective searches Master the use of Splunk tables, charts, and graph enhancements Use Splunk data models and pivots with faster data model acceleration Master all aspects of Splunk XML dashboards with hands-on applications Apply ML algorithms for forecasting and anomaly detection Integrate advanced JavaScript charts and leverage Splunk's API Who this book is for This Learning Path is for data analysts, business analysts, and IT administrators who want to leverage the Splunk enterprise platform as a valuable operational intelligence tool. Existing Splunk users who want to upgrade and get up and running with Splunk 7.x will also find this book useful. Some knowledge of Splunk services will help you get the most out of this Learning Path.

Prepare for the User, Power User, and Enterprise Admin Certifications

Offense versus defense in real-time computer conflict

Splunk Certified Study Guide

How to Lead in Data Science

The Customer Success Professional's Handbook

Writing Technical Documentation in a Product Development Group

NATIONAL BESTSELLER A top journalist crosses the yellow tape to investigate a shocking high-society crime. Billionaires, philanthropists, socialites . . . victims. Barry and Honey Sherman appeared to lead charmed lives. But the world was shocked in late 2017 when their bodies were found in a bizarre tableau in their elegant Toronto home. First described as murder-suicide — belts looped around their necks, they were found seated beside their basement swimming pool — police later ruled it a staged, targeted double murder. Nothing about the case made sense to friends of the founder of one of the world's largest generic pharmaceutical firms and his wife, a powerhouse in Canada's charity world. Together, their wealth has been estimated at well over $4.7 billion. There was another side to the story. A strategic genius who built a large generic drug company — Apotex Inc. — Barry Sherman was a self-described workaholic, renowned risk-taker, and disruptor during his fifty-year career. Regarded as a generous friend by many, Sherman was also feared by others. He was criticized for stifling academic freedom and using the courts to win at all costs. Upset with building issues at his mansion, he sued and recouped millions from tradespeople. At the time of his death, Sherman had just won a decades-old legal case involving four cousins who wanted 20 percent of his fortune. Toronto Star investigative journalist Kevin Donovan chronicles the unsettling story from the beginning, interviewing family members, friends, and colleagues, and sheds new light on the Shermans' lives and the disturbing double murder. Deeply researched and authoritative, The Billionaire Murders is a compulsively readable tale of a strange and perplexing crime.

Big Data Analytics Using Splunk is a hands-on book showing how to process and derive business value from big data in real time. Examples in the book draw from social media sources such as Twitter (tweets) and Foursquare (check-ins). You also learn to draw from machine data, enabling you to analyze, say, web server log files and patterns of user access in real time, as the access is occurring. Gone are the days when you need be caught out by shifting public opinion or sudden changes in customer behavior. Splunk's easy to use engine helps you recognize and react in real time, as events are occurring. Splunk is a powerful, yet simple analytical tool fast gaining traction in the fields of big data and operational intelligence. Using Splunk, you can monitor data in real time, or mine your data after the fact. Splunk's stunning visualizations aid in locating the needle of value in a haystack of a data. Geolocation support spreads your data across a map, allowing you to drill down to geographic areas of interest. Alerts can run in the background and trigger to warn you of shifts or events as they are taking place. With Splunk you can immediately recognize and react to changing trends and shifting public opinion as expressed through social media, and to new patterns of eCommerce and customer behavior. The ability to immediately recognize and react to changing trends provides a tremendous advantage in today's fast-paced world of Internet business. Big Data Analytics Using Splunk opens the door to an exciting world of real-time operational intelligence. Built around hands-on projects Shows how to mine social media Opens the door to real-time operational intelligence

A hands-on book showing how to process and derive business value from big data in real time. Examples in the book draw from social media sources such as Twitter (tweets) and Foursquare (check-ins). You also learn to draw from machine data, enabling you to analyze web server log files and patterns of user access in real time, as the access is occurring.

Design, implement, and publish custom Splunk applications by following best practices About This Book This is the most up-to-date guide on the market and will help you finish your tasks faster, easier, and more efficiently. Highly practical guide that addresses common and not-so-common pain points in Splunk. Want to explore shortcuts to perform tasks more efficiently with Splunk? This is the book for you! Who This Book Is For This book is for administrators, developers, and search ninjas who have been using Splunk for some time. A comprehensive coverage makes this book great for Splunk veterans and newbies alike. What You Will Learn Use Splunk effectively to gather, analyze, and report on operational data throughout your environment Expedite your reporting, and be empowered to present data in a meaningful way Create robust searches, reports, and charts using Splunk Modularize your programs for better reusability. Build your own Splunk apps and learn why they are important Learn how to integrate with enterprise systems Summarize data for longer term trending, reporting, and analysis In Detail This book will give you an edge over others through insights that will help you in day-to-day instances. When you're working with data from various sources in Splunk and performing analysis on this data, it can be a bit tricky. With this book, you will learn the best practices of working with Splunk. You'll learn about tools and techniques that will ease your life with Splunk, and will ultimately save you time. In some cases, it will adjust your thinking of what Splunk is, and what it can and cannot do. To start with, you'll get to know the best practices to get data into Splunk, analyze data, and package apps for distribution. Next, you'll discover the best practices in logging, operations, knowledge management, searching, and reporting. To finish off, we will teach you how to troubleshoot Splunk searches, as well as deployment, testing, and development with Splunk. Style and approach If you're stuck or want to find a better way to work with Splunk environment, this book will come handy. This easy-to-follow, insightful book contains step-by-step instructions and examples and scenarios that you will connect to.

Demystify machine data by leveraging datasets, building reports, and sharing powerful insights, 3rd Edition

Exploring Splunk

The Product Is Docs

Logging and Log Management

Big Data Analytics in Cybersecurity

Uncanny Valley

Use this practical guide to the Splunk operational data intelligence platform to search, visualize, and analyze petabyte-scale, unstructured machine data. Get to the heart of the platform and use the Search Processing Language (SPL) tool to query the platform to find the answers you need. With more than 140 commands, SPL gives you the power to ask any question of machine data. However, many users (both newbies and experienced users) find the language difficult to grasp and complex. This book takes you through the basics of SPL using plenty of hands-on examples and emphasizes the most impactful SPL commands (such as eval, stats, and timechart). You will understand the most efficient ways to query Splunk (such as learning the drawbacks of subsearches and join, and why it makes sense to use tstats). You will be introduced to lesser-known commands that can be very useful, such as using the command rex to extract fields and erex to generate regular expressions automatically. In addition, you will learn how to create basic visualizations (such as charts and tables) and use prescriptive guidance on search optimization. For those ready to take it to the next level, the author introduces advanced commands such as predict, kmeans, and cluster. What You Will Learn Use real-world scenarios (such as analyzing a web access log) to search, group, correlate, and create reports using SPL commands Enhance your search results using lookups and create new lookup tables using SPL commands Extract fields from your search results Compare data from multiple time frames in one chart (such as comparing your current day application performance to the average of the past 30 days) Analyze the performance of your search using Job Inspector and identify execution costs of various components of your search Who This Book Is For Application developers, architects, DevOps engineers, application support engineers, network operations center analysts, security operations center (SOC) analysts, and cyber security professionals who use Splunk to search and analyze their machine data

Build next-generation Artificial Intelligence systems with Java Key Features Implement AI techniques to build smart applications using Deeplearning4j Perform big data analytics to derive quality insights using Spark MLlib Create self-learning systems using neural networks, NLP, and reinforcement learning Book Description In this age of big data, companies have larger amount of consumer data than ever before, far more than what the current technologies can ever hope to keep up with. However, Artificial Intelligence closes the gap by moving past human limitations in order to analyze data. With the help of Artificial Intelligence for big data, you will learn to use Machine Learning algorithms such as k-means, SVM, RBF, and regression to perform advanced data analysis. You will understand the current status of Machine and Deep Learning techniques to work on Genetic and Neuro-Fuzzy algorithms. In addition, you will explore how to develop Artificial Intelligence algorithms to learn from data, why they are necessary, and how they can help solve real-world problems. By the end of this book, you'll have learned how to implement various Artificial Intelligence algorithms for your big data systems and integrate them into your product offerings such as reinforcement learning, natural language processing, image recognition, genetic algorithms, and fuzzy logic systems. What you will learn Manage Artificial Intelligence techniques for big data with Java Build smart systems to analyze data for enhanced customer experience Learn to use Artificial Intelligence frameworks for big data Understand complex problems with algorithms and Neuro-Fuzzy systems Design stratagems to leverage data using Machine Learning process Apply Deep Learning techniques to prepare data for modeling Construct models that learn from data using open source tools Analyze big data problems using scalable Machine Learning algorithms Who this book is for This book is for you if you are a data scientist, big data professional, or novice who has basic knowledge of big data and wish to get proficiency in Artificial Intelligence techniques for big data. Some competence in mathematics is an added advantage in the field of elementary linear algebra and calculus.

This book is for those Splunk developers who want to learn advanced strategies to deal with big data from an enterprise architectural perspective. You need to have good working knowledge of Splunk.

Uncover hidden patterns of data and respond withcountermeasures Security professionals need all the tools at their disposal toincrease their visibility in order to prevent security breaches andattacks. This careful guide explores two of the most powerful data analysis and visualization. You'll soon understand how toharness and wield data, from collection and storage to managementand analysis as well as visualization and presentation. Using ahands-on approach with real-world examples, this book shows you howto gather feedback, measure the effectiveness of your securitymethods, and make better decisions. Everything in this book will have practical application forinformation security professionals. Helps IT and security professionals understand and use data, sothey can thwart attacks and understand and visualizevulnerabilities in their networks Includes more than a dozen real-world examples and hands-onexercises that demonstrate how to analyze security data andintelligence and translate that information into visualizationsthat make plain how to prevent attacks Covers topics such as how to acquire and prepare security data,use simple statistical methods to detect malware, predict roguebehavior, correlate security events, and more Written by a team of well-known experts in the field ofsecurity and data analysis Lock down your networks, prevent hacks, and thwart malware byimproving visibility into the environment, all through the power ofdata and Security Using Data Analysis, Visualization, andDashboards.

Splunk Best Practices

Splunk Primer and the Search Processing Language

Gain business data insights from operational intelligence

Artificial Intelligence for Big Data

Introduction to IBM Common Data Provider for z Systems

Splunk: Enterprise Operational Intelligence Delivered

This guide follows a Splunk software engineering team on a journey to build solutions with partners, focusing on the real world use cases to showcase various technologies of the Splunk Developer Platform. Like a documentary, it captures our story from envisioning and user experience prototyping to development, packaging and multiple production deployments. It includes the diverse perspectives of developers and testers, administrators and product owners, security experts and release engineers. As on any real journey, we make mistakes, have arguments, and change our minds along the way. So in addition to showing you how best to do things, we highlight the pitfalls and issues that we encounter, and the solutions we find. The key element of this guidance, of course, is the code. We've made the code repos open, and recommend you study the source code of the reference apps and the associated tests. In fact, you can see and replay the code in motion, as it was developed. We encourage you to reuse and learn from it.

Transform machine data into powerful analytical intelligence using Splunk Key Features Analyze and visualize machine data to step into the world of Splunk! Leverage the exceptional analysis and visualization capabilities to make informed decisions for your business This easy-to-follow, practical book can be used by anyone - even if you have never managed data before Book Description Splunk is a search, reporting, and analytics software platform for machine data, which has an ever-growing market adoption rate. More organizations than ever are adopting Splunk to make informed decisions in areas such as IT operations, information security, and the Internet of Things. The first two chapters of the book will get you started with a simple Splunk installation and set up of a sample machine data generator, called Eventgen. After this, you will learn to create various reports, dashboards, and alerts. You will also explore Splunk's Pivot functionality to model data for business users. You will then have the opportunity to test-drive Splunk's powerful HTTP Event Collector. After covering the core Splunk functionality, you'll be provided with some real-world best practices for using Splunk, and information on how to build upon what you've learned in this book. Throughout the book, there will be additional comments and best practice recommendations from a member of the SplunkTrust Community, called "Tips from the Fez". What you will learn Install and configure Splunk for personal use Store event data in Splunk indexes, classify events into sources, and add data fields Learn essential Splunk Search Processing Language commands and best practices Create powerful real-time or user-input dashboards Be proactive by implementing alerts and scheduled reports Tips from the Fez: best practices using Splunk features and add-ons Understand security and deployment considerations for taking Splunk to an organizational level Who this book is for This book is for the beginners who want to get well versed in the services offered by Splunk 7. If you want to be a data/business analyst or want to be a system administrator, this book is what you want. No prior knowledge of Splunk is required.

Over 70 practical recipes to gain operational data intelligence with Splunk Enterprise About This Book This is the most up-to-date book on Splunk 6.3 and teaches you how to tackle real-world operational intelligence scenarios efficiently Get business insights using machine data using this easy-to-follow guide Search, monitor, and analyze your operational data skillfully using this recipe-based, practical guide Who This Book Is For This book is intended for users of all levels who are looking to leverage the Splunk Enterprise platform as a valuable operational intelligence tool. The recipes provided in this book will appeal to individuals from all facets of business, IT, security, product, marketing, and many more! Also, existing users of Splunk who want to upgrade and get up and running with Splunk 6.3 will find this book invaluable. What You Will Learn Use Splunk to gather, analyze, and report on data Create dashboards and visualizations that make data meaningful Build an operational intelligence application with extensive features and functionality Enrich operational data with lookups and workflows Model and accelerate data and perform pivot-based reporting Build real-time, scripted, and other intelligence-driven alerts Summarize data for longer term trending, reporting, and analysis Integrate advanced JavaScript charts and leverage Splunk's API In Detail Splunk makes it easy for you to take control of your data, and with Splunk Operational Cookbook, you can be confident that you are taking advantage of the Big Data revolution and driving your business with the cutting edge of operational intelligence and business analytics. With more than 70 recipes that demonstrate all of Splunk's features, not only will you find quick solutions to common problems, but you'll also learn a wide range of strategies and uncover new ideas that will make you rethink what operational intelligence means to you and your organization. You'll discover recipes on data processing, searching and reporting, dashboards, and visualizations to make data shareable, communicable, and most importantly meaningful. You'll also find step-by-step demonstrations that walk you through building an operational intelligence application containing vital features essential to understanding data and to help you successfully integrate a data-driven way of thinking in your organization. Throughout the book, you'll dive deeper into Splunk, explore data models and pivots to extend your intelligence capabilities, and perform advanced searching to explore your data in even more sophisticated ways. Splunk is changing the business landscape, so make sure you're taking advantage of it. Style and approach Splunk is an excellent platform that allows you to make sense of machine data with ease. The adoption of Splunk has been huge and everyone who has gone beyond installing Splunk wants to know how to make most of it. This book will not only teach you how to use Splunk in real-world scenarios to get business insights, but will also get existing Splunk users up to date with the latest Splunk 6.3 release.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Search Reference Guide

Adversarial Tradecraft in Cybersecurity

A Memoir

A Distributed Real-Time Search and Analytics Engine

The Parent Search

Dependency Injection with Unity

Make your Splunk certification easier with this exam study guide that covers the User, Power User, and Enterprise Admin certifications. This book is divided into three parts. The first part focuses on the Splunk User and Power User certifications starting with how to install Splunk, Splunk Processing Language (SPL), field extraction, field aliases and macros, and Splunk tags. You will be able to make your own data model and prepare an advanced dashboard in Splunk. In the second part, you will explore the Splunk Admin certification. There will be in-depth coverage of Splunk licenses and user role management, and how to configure Splunk forwarders, indexer clustering, and the security policy of Splunk. You'll also explore advanced data input options in Splunk as well as .conf file merging logic, btool, various attributes, stanza types, editing advanced data inputs through the .conf file, and various other types of .conf file in Splunk. The concluding part covers the advanced topics of the Splunk Admin certification. You will also learn to troubleshoot Splunk and to manage existing Splunk infrastructure. You will understand how to configure search head, multi-site indexer clustering, and search peers besides exploring how to troubleshoot Splunk Enterprise using the monitoring console and matrix.log. This part will also include search issues and configuration issues. You will learn to deploy an app through a deployment server on your client's instance, create a server class, and carry out load balancing, socks proxy, and indexer discovery. By the end of the Splunk Certified Study Guide, you will have learned how to manage resources in Splunk and how to use REST API services for Splunk. This section also explains how to set up Splunk Enterprise on the AWS platform and some of the best practices to make them work efficiently together. The book offers multiple choice question tests for each part that will help you better prepare for the exam. What You Will Learn Study to pass the Splunk User, Power User, and Admin certificate exams Implement and manage Splunk multi-site clustering Design, implement, and manage a complex Splunk Enterprise solution Master the roles of Splunk Admin and troubleshooting Configure Splunk using AWS Who This Book Is For People looking to pass the User, Power User, and Enterprise Admin exams. It is also useful for Splunk administrators and support engineers for managing an existing deployment.

It's time to redefine the CEO success story. Meet eight iconoclastic leaders who helmed firms where returns on average outperformed the S&P 500 by more than 20 times.

Whether you need full-text search or real-time analytics of structured data—or both—the Elasticsearch distributed search engine is an ideal way to put your data to work. This practical guide not only shows you how to search, analyze, and explore data with Elasticsearch, but also helps you deal with the complexities of human language, geolocation, and relationships. If you're a newcomer to both search and distributed systems, you'll quickly learn how to integrate Elasticsearch into your application. More experienced users will pick up lots of advanced techniques. Throughout the book, you'll follow a problem-based approach to learn why, when, and how to use Elasticsearch features. Understand how Elasticsearch interprets data in your documents Index and query your data to take advantage of search concepts such as relevance and word proximity Handle human language through the effective use of analyzers and queries Summarize and group data to show overall trends, with aggregations and analytics Use geo-points and geo-shapes—Elasticsearch's approaches to geolocation Model your data to take advantage of Elasticsearch's horizontal scalability Learn how to configure and monitor your cluster in production

A NEW YORK TIMES BESTSELLER. ONE OF THE NEW YORK TIMES'S 10 BEST BOOKS OF 2020. Named one of the Best Books of 2020 by The Washington Post, NPR, the Los Angeles Times, ELLE, Esquire, Parade, Teen Vogue, The Times (UK), Fortune, Glamour, Town & Country, Apartment Therapy, Good Housekeeping, Electric Literature, Self, The Week (UK) and BookPage. One of Amazon's Best 100 Books of 2020. A New York Times Book Review Editors' Choice and a January 2020 IndieNext Pick. "A definitive document of a world in transition: I won't be alone in returning to it for clarity and consolation for many years to come." --Jia Tolentino, author of Trick Mirror: Reflections on Self-Delusion The prescient, page-turning account of a journey in Silicon Valley: a defining memoir of our digital age In her mid-twenties, at the height of tech industry idealism, Anna Wiener—stuck, broke, and looking for meaning in her work, like any good millennial--left a job in book publishing for the promise of the new digital economy. She moved from New York to San Francisco, where she landed at a big-data startup in the heart of the Silicon Valley bubble: a world of surreal extravagance, dubious success, and fresh-faced entrepreneurs hell-bent on domination, glory, and, of course, progress. Anna arrived amidst a massive cultural shift, as the tech industry rapidly transformed into a locus of wealth and power rivaling Wall Street. But amid the company ski vacations and in-office speakeasies, boyish camaraderie and ride-or-die corporate fealty, a new Silicon Valley began to emerge: one in far over its head, one that enriched itself at the expense of the idyllic future it claimed to be building. Part coming-of-age-story, part portrait of an already-bygone era, Anna Wiener's memoir is a rare first-person glimpse into high-flying, reckless startup culture at a time of unchecked ambition, unregulated surveillance, wild fortune, and accelerating political power. With wit, candor, and heart, Anna deftly charts the tech industry's shift from self-appointed world savior to democracy-endangering liability, alongside a personal narrative of aspiration, ambivalence, and disillusionment. Unsparing and incisive, Uncanny Valley is a cautionary tale, and a revelatory interrogation of a world reckoning with consequences its unwitting designers are only beginning to understand.

Big Data Analytics Using Splunk

The Outsiders

The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management

Elasticsearch: The Definitive Guide

Web Style Guide, 4th Edition

Complete guide to automating Big Data solutions using Artificial Intelligence techniques

Handbook of Digital Forensics and Investigation builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to Digital Evidence and Computer Crime. This unique collection details how to conduct digital investigations in both criminal and civil contexts, and how to locate and utilize digital evidence on computers, networks, and embedded systems. Specifically, the Investigative Methodology section of the Handbook provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery, and Intrusion Investigation. The Technology section is extended and updated to reflect the state of the art in each area of specialization. The main areas of focus in the Technology section are forensic analysis of Windows, Unix, Macintosh, and embedded systems (including cellular telephones and other mobile devices), and investigations involving networks (including enterprise environments and mobile telecommunications technology). This handbook is an essential technical reference and on-the-job guide that IT professionals, forensic practitioners, law enforcement, and attorneys will rely on when confronted with computer related crime and digital evidence of any kind. *Provides methodologies proven in practice for conducting digital investigations of all kinds *Demonstrates how to locate and interpret a wide variety of digital evidence, and how it can be useful in investigations *Presents tools in the context of the investigative process, including EnCase, FTK, ProDiscover, foremost, XACT, Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms *Case examples in every chapter give readers a practical understanding of the technical, logistical, and legal challenges that arise in real investigations

The definitive "Customer Success Manager How-To-Guide" for the CSM profession from Gainsight, who brought you the market-leading Customer Success The Customer Success Manager has become a critical asset to organizations across the business landscape. As the subscription model has spread from the cloud and SaaS to more sectors of the economy, that pivotal role will only grow in importance. That's because if you want to compete and thrive in this new environment, you need to put the customer at the center of your strategy. You need to recognize you're no longer selling just a product. You're selling an outcome. Customer Success Managers (CSM) are committed to capturing and delivering those outcomes by listening to their customers, understanding their needs, and adapting products and services to drive success. Although several existing resources address the customer success imperative, there is no authoritative instruction manual for the CSM profession—until now. The Customer Success Professional's Handbook is the definitive reference book for CSMs and similar roles in the field. This practical, first-of-its-kind manual fills a significant gap in professional customer success literature, providing the knowledge every CSM needs to succeed—from the practitioner level all the way to senior leadership. The authors—acknowledged experts in building, training, and managing Customer Success teams—offer real-world guidance and practical advice for aspiring and experienced CSMs alike. The handbook is written by practioners for practioners. An indispensable resource for front-line Customer Success Managers, this much-needed book: Demonstrates how to build, implement, and manage a Customer Success team Helps new CSMs develop their skills and proficiency to be more employable and grow in their careers Provides clear guidance for managers on how to hire a stellar CSM Presents practical tactics needed to drive revenue growth during renewal, expansion, and customer advocacy opportunities Explains proven methods and strategies for mentoring CSMs throughout their careers Offers valuable insights from Gainsight, the Customer Success Company, and the broader customer success community with more than a dozen of the industry's most respected leaders contributing their perspectives Currently, with over 70,000 open positions, Customer Success Manager in one of the fastest-growing jobs in the world. The Customer Success Professional's Handbook: How to Thrive in One of the World's Fastest Growing Careers—While Driving Growth For Your Company will prove to be your go-to manual throughout every stage of your CSM career.

This book provides a broad perspective about the essential aspects of creating technical documentation in today's product development world. It is a book of opinions and guidance, collected as short essays. You can read selectively about subjects that interest you, or you can read the entire collection in any order you like. Information development is a multidimensional discipline, and it is easy to theorize. We have written this book from our direct experience, using the concrete insights and practices we apply to our work every day.If you work as an information developer, a manager in a documentation team, or in another part of product development that collaborates with a doc team, there is information in this book for you. Perhaps you are a technical writer in a small, high-growth company that is figuring out its processes. Perhaps you are an information-development manager in a large enterprise company with an expanding product line and an ever more complex matrix of cross-functional dependencies. You might work at a medium-sized company where your management is asking you to do more with fewer people, and you want some additional perspective that will help you find a leaner and more effective way to deliver what your business demands. Or you might work outside the technical documentation world, in another part of product development, and are wondering how to collaborate most effectively with the documentation team.The purpose of The Product is Docs is to provoke discussion, shine light on some murky areas, and--we hope--inspire our colleagues to consider their processes and assumptions with new eyes.All proceeds from the sale of The Product is Docs will go to charity.

Learn what it takes to succeed in the the most in-demand tech job Harvard Business Review calls it the sexiest tech job of the 21st century. Data scientists are in demand, and this unique book shows you exactly what employers want and the skill set that separates the quality data scientist from other talented IT professionals. Data science involves extracting, creating, and processing data to turn it into business value. With over 15 years of big data, predictive modeling, and business analytics experience, author Vincent Granville is no stranger to data science. In this one-of-a-kind guide, he provides insight into the essential data science skills, such as statistics and visualization techniques, and covers everything from analytical recipes and data

science tricks to common job interview questions, sample resumes, and source code. The applications are endless and varied: automatically detecting spam and plagiarism, optimizing bid prices in keyword advertising, identifying new molecules to fight cancer, assessing the risk of meteorite impact. Complete with case studies, this book is a must, whether you're looking to become a data scientist or to hire one. Explains the finer points of data science, the required skills, and how to acquire them, including analytical recipes, standard rules, source code, and a dictionary of terms Shows what companies are looking for and how the growing importance of big data has increased the demand for data scientists Features job interview questions, sample resumes, salary surveys, and examples of job ads Case studies explore how data science is used on Wall Street, in botnet detection, for online advertising, and in many other business-critical situations Developing Analytic Talent: Becoming a Data Scientist is essential reading for those aspiring to this hot career choice and for employers seeking the best candidates.

OSSEC Host-Based Intrusion Detection Guide

Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources

Ten Strategies of a World-Class Cybersecurity Operations Center

Practical Splunk Search Processing Language

Splunk Developer Guide

Handbook of Digital Forensics and Investigation

Learn to effectively use, configure, deploy and extend Splunk and implement its powerful capabilities.

Demystify Big Data and discover how to bring operational intelligence to your data to revolutionize your work About This Book Get maximum use out of your data with Splunk's exceptional analysis and visualization capabilities Analyze and understand your operational data skillfully using this end-to-end course Full coverage of high-level Splunk techniques such as advanced searches, manipulations, and visualization Who This Book Is For This course is for software developers who wish to use Splunk for operational intelligence to make sense of their machine data. The content in this course will appeal to individuals from all facets of business, IT, security, product, marketing, and many more What You Will Learn Install and configure the latest version of Splunk. Use Splunk to gather, analyze, and report data Create Dashboards and Visualizations that make data meaningful Model and accelerate data and perform pivot-based reporting Integrate advanced JavaScript charts and leverage Splunk's APIs Develop and Manage apps in Splunk Integrate Splunk with R and Tableau using SDKs In Detail Splunk is an extremely powerful tool for searching, exploring, and visualizing data of all types. Splunk is becoming increasingly popular, as more and more businesses, both large and small, discover its ease and usefulness. Analysts, managers, students, and others can quickly learn how to use the data from their systems, networks, web traffic, and social media to make attractive and informative reports. This course will teach everything right from installing and configuring Splunk. The first module is for anyone who wants to manage data with Splunk. You'll start with very basics of Splunk— installing Splunk— before then moving on to searching machine data with Splunk. You will gather data from different sources, isolate them by indexes, classify them into source types, and tag them with the essential fields. With more than 70 recipes on hand in the second module that demonstrate all of Splunk's features, not only will you find quick solutions to common problems, but you'll also learn a wide range of strategies and uncover new ideas that will make you rethink what operational intelligence means to you and your organization. Dive deep into Splunk to find the most efficient solution to your data problems in the third module. Create the robust Splunk solutions you need to make informed decisions in big data machine analytics. From visualizations to enterprise integration, this well-organized high level guide has everything you need for Splunk mastery. This learning path combines some of the best that Packt has to offer into one complete, curated package. It includes content from the following Packt products: Splunk Essentials - Second Edition Splunk Operational Intelligence Cookbook - Second Edition Advanced Splunk Style and approach Packed with several step by step tutorials and a wide range of techniques to take advantage of Splunk and its wide range of capabilities to deliver operational intelligence within your enterprise

IBM Common Data Provider for z Systems collects, filters, and formats IT operational data in near real-time and provides that data to target analytics solutions. IBM Common Data Provider for z Systems enables authorized IT operations teams using a single web-based interface to specify the IT operational data to be gathered and how it needs to be handled. This data is provided to both on- and off-platform analytic solutions, in a consistent, consumable format for analysis. This Redpaper discusses the value of IBM Common Data Provider for z Systems, provides a high-level reference architecture for IBM Common Data Provider for z Systems, and introduces key components of the architecture. It shows how IBM Common Data Provider for z Systems provides operational data to various analytic solutions. The publication provides high-level integration guidance, preferred practices, tips on planning for IBM Common Data Provider for z Systems, and example integration scenarios.

Learn the A to Z of building excellent Splunk applications with the latest techniques using this comprehensive guide About This Book This is the most up-to-date book on Splunk 6.3 for developers Get ahead of being just a Splunk user and start creating custom Splunk applications as per your needs Your one-stop-solution to Splunk application development Who This Book Is For This book is for those who have some familiarity with Splunk and now want to learn how to develop an efficient Splunk application. Previous experience with Splunk, writing searches, and designing basic dashboards is expected. What You Will Learn Implement a Modular Input and a custom D3 data visualization Create a directory structure and set view permissions Create a search view and a dashboard view using advanced XML modules Enhance your application using eventtypes, tags, and macros Package a Splunk application using best practices Publish a Splunk application to the Splunk community In Detail Splunk provides a platform that allows you to search data stored on a machine, analyze it, and visualize the analyzed data to make informed decisions. The adoption of Splunk in enterprises is huge, and it has a wide range of customers right from Adobe to Dominos. Using the Splunk platform as a user is one thing, but customizing this platform and creating applications specific to your needs takes more than basic knowledge of the platform. This book will dive into developing Splunk applications that cater to your needs of making sense of data and will let you visualize this data with the help of stunning dashboards. This book includes everything on developing a full-fledged Splunk application right from designing to implementing to publishing. We will design the fundamentals to build a Splunk application and then move on to creating one. During the course of the book, we will cover application data, objects, permissions, and more. After this, we will show you how to enhance the application, including branding, workflows, and enriched data. Views, dashboards, and web frameworks are also covered. This book will showcase everything new in the latest version of Splunk including the latest data models, alert actions, XML forms, various dashboard enhancements, and visualization options (with D3). Finally, we take a look at the latest Splunk cloud applications, advanced integrations, and development as per the latest release. Style and approach This book is an easy-to-follow guide with lots of tips and tricks to help you master all the concepts necessary to develop and deploy your Splunk applications.

Splunk 7.x Quick Start Guide

Eight Unconventional CEOs and Their Radically Rational Blueprint for Success

Splunk Developer's Guide

Data-Driven Security

Splunk Operational Intelligence Cookbook

Improving Your Splunk Skills

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis. This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers. Comprehensive coverage of log management including analysis, visualization, reporting and more Includes information on different uses for logs -- from system operations to regulatory compliance Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

A classic reference book on user interface design and graphic design for web sites, updated to reflect a rapidly changing market Consistently praised as the best volume on classic elements of web site design, Web Style Guide has sold many thousands of copies and has been published around the world. This new revised edition confirms Web Style Guide as the go-to authority in a rapidly changing market. As web designers move from building sites from scratch to using content management and aggregation tools, the book's focus shifts away from code samples and toward best practices, especially those involving mobile experience, social media, and accessibility. An ideal reference for web site designers in corporations, government, nonprofit organizations, and academic institutions, the book explains established design principles and covers all aspects of web design—from planning to production to maintenance. The guide also shows how these principles apply in web design projects whose primary concerns are information design, interface design, and efficient search and navigation.

This document is intended to facilitate the deployment of the Splunk Enterprise Solutions using IBM All Flash Array systems for the Hot and Warm tiers, and IBM Elastic Storage System for the Cold and Frozen tiers. This document provides the reference architecture and configuration guidelines for the IBM Storage systems. The information in this document is distributed on an "as is" basis without any warranty that is either expressed or implied. Support assistance for the use of this material is limited to situations where IBM Storage Systems are supported, entitled and where the issues are specific to a blueprint implementation.

Learn how to architect, implement, and administer a complex Splunk Enterprise environment and extract valuable insights from business data. Key Features Understand the various components of Splunk and how they work together to provide a powerful Big Data analytics solution. Collect and index data from a wide variety of common machine data sources Design searches, reports, and dashboard visualizations to provide business data insights Book Description Splunk is a leading platform and solution for collecting, searching, and extracting value from ever increasing amounts of big data - and big data is eating the world! This book covers all the crucial Splunk topics and gives you the information and examples to get the immediate job done. You will find enough insights to support further research and use Splunk to suit any business environment or situation. Splunk 7.x Quick Start Guide gives you a thorough understanding of how Splunk works. You will learn about all the critical tasks for architecting, implementing, administering, and utilizing Splunk Enterprise to collect, store, retrieve, format, analyze, and visualize machine data. You will find step-by-step examples based on real-world experience and practical use cases that are applicable to all Splunk environments. There is a careful balance between adequate coverage of all the critical topics with short but relevant deep-dives into the configuration options and steps to carry out the day-to-day tasks that matter. By the end of the book, you will be a confident and proficient Splunk architect and administrator. What you will learn Design and implement a complex Splunk Enterprise solution Configure your Splunk environment to get machine data in and indexed Build searches to get and format data for analysis and visualization Build reports, dashboards, and alerts to deliver critical insights Create knowledge objects to enhance the value of your data Install Splunk apps to provide focused views into key technologies Monitor, troubleshoot, and manage your Splunk environment Who this book is for This book is intended for experienced IT personnel who are just getting started working with Splunk and want to quickly become proficient with its usage. Data analysts who need to leverage Splunk to extract critical business insights from application logs and other machine data sources will also benefit from this book.

Building Splunk Solutions

Implementing Splunk - Big Data Reporting and Development for Operational Intelligence

Developing Analytic Talent

Splunk 7 Essentials, Third Edition

Foundations of User Experience Design

A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome

Big data is presenting challenges to cybersecurity. For an example, the Internet of Things (IoT) will reportedly soon generate a staggering 400 zettabytes (ZB) of data a year. Self-driving cars are predicted to churn out 4000 GB of data per hour of driving. Big data analytics, as an emerging analytical technology, offers the capability to collect, store, process, and visualize these vast amounts of data. Big Data Analytics in Cybersecurity examines security challenges surrounding big data and provides actionable insights that can be used to improve the current practices of network operators and administrators. Applying big data analytics in cybersecurity is critical. By exploiting data from the networks and computers, analysts can discover useful network information from data. Decision makers can make more informative decisions by using this analysis, including what actions need to be performed, and improvement recommendations to policies, guidelines, procedures, tools, and other aspects of the network processes. Bringing together experts from academia, government laboratories, and industry, the book provides insight to both new and more experienced security professionals, as well as data analytics professionals who have varying levels of cybersecurity expertise. It covers a wide range of topics in cybersecurity, which include: Network forensics Threat analysis Vulnerability assessment Visualization Cyber training. In addition, emerging security domains such as the IoT, cloud computing, fog computing, mobile computing, and cyber-social networks are examined. The book first focuses on how big data analytics can be used in different aspects of cybersecurity including network forensics, root-cause analysis, and security training. Next it discusses big data challenges and solutions in such emerging cybersecurity domains as fog computing, IoT, and mobile app security. The book concludes by presenting the tools and datasets for future cybersecurity research.

This book is the definitive guide on the OSSEC Host-based Intrusion Detection system and frankly, to really use OSSEC you are going to need a definitive guide. Documentation has been available since the start of the OSSEC project but, due to time constraints, no formal book has been created to outline the various features and functions of the OSSEC product. This has left very important and powerful features of the product undocumented...until now! The book you are holding will show you how to install and configure OSSEC on the operating system of your choice and provide detailed examples to help prevent and mitigate attacks on your systems. -- Stephen Northcutt OSSEC determines if a host has been compromised in this manner by taking the equivalent of a picture of the host machine in its original, unaltered state. This "picture" captures the most relevant information about that machine's configuration. OSSEC saves this "picture" and then constantly compares it to the current state of that machine to identify anything that may have changed from the original configuration. Now, many of these changes are necessary, harmless, and authorized, such as a system administrator installing a new software upgrade, patch, or application. But, then there are the not-so-harmless changes, like the installation of a rootkit, trojan horse, or virus. Differentiating between the harmless and the not-so-harmless changes determines whether the system administrator or security professional is managing a secure, efficient network or a compromised network which might be funneling credit card numbers out to phishing gangs or storing massive amounts of pornography creating significant liability for that organization. Separating the wheat from the chaff is by no means an easy task. Hence the need for this book. The book is co-authored by Daniel Cid, who is the founder and lead developer of the freely available OSSEC host-based IDS. As such, readers can be certain they are reading the most accurate, timely, and insightful information on OSSEC. * Nominee for Best Book Bejtlich read in 2008! * http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html • Get Started with OSSEC Get an overview of the features of OSSEC including commonly used terminology, pre-install preparation, and deployment considerations. • Follow Steb-by-Step Installation Instructions Walk through the installation process for the "local , “agent , and "server" install types on some of the most popular operating systems available. • Master Configuration Learn the basic configuration options for your install type and learn how to monitor log files, receive remote messages, configure email notification, and configure alert levels. • Work With Rules Extract key information from logs using decoders and how you can leverage rules to alert you of strange occurrences on your network. • Understand System Integrity Check and Rootkit Detection Monitor binary executable files, system configuration files, and the Microsoft Windows registry. • Configure Active Response Configure the active response actions you want and bind the actions to specific rules and sequence of events. • Use the OSSEC Web User Interface Install, configure, and use the community-developed, open source web interface available for OSSEC. • Play in the OSSEC VMware Environment Sandbox • Dig Deep into Data Log Mining Take the “high art of log analysis to the next level by breaking the dependence on the lists of strings or patterns to look for in the logs.

IBM Storage Solutions for Splunk Enterprise

Leverage the operational intelligence capabilities of Splunk to unlock new hidden business insights

Becoming a Data Scientist

Mastering Splunk