Devsecops The Tao Of Security Science Rsa Conference

Learn WinUI 3.0
The Best of TaoSecurity Blog, Volume 3
Research Anthology on Artificial Intelligence Applications in Security
The Best of TaoSecurity Blog, Volume 4
Essential COM
ICCWS 2022 17th International Conference on Cyber Warfare and Security
The Tao of Microservices
Vehicle Safety Communications
Enterprise Software Security
Transforming Cybersecurity: Using COBIT 5
Hands-On Meta Learning with Python
DevOps for Developers
Securing Systems
Threat Modeling
Managing the Unmanageable
Data Pipelines with Apache Airflow
Speech Enhancement
An Introduction to Data Science
Interpretable Machine Learning
Artificial Intelligence in Banking
Zero Trust Networks
Healing Love through the Tao

Foundations of Security
Continuous Software Engineering
Reinforcement Learning for Cyber-Physical Systems
Practical Machine Learning with Rust
Extrusion Detection
Logging and Log Management
Big Data Security
Strategic Approaches to Digital Platform Security Assurance
The Practice of Network Security Monitoring
Data Jujitsu
Professional JavaScript
Fundamentals of Computer Security Technology
Introduction to Visual SLAM
The Best of TaoSecurity Blog, Volume 1
Taoist Secrets of Love
Linux and Windows Interoperability Guide
Hands-On Big Data Modeling
The Tao of Network Security Monitoring

PETERSON FRENCH

Learn WinUI 3.0 Simon and Schuster
Explore a diverse set of meta-learning algorithms and techniques to enable human-like cognition for your machine learning models using various Python frameworks Key FeaturesUnderstand the foundations of meta learning algorithmsExplore practical examples to explore various one-

shot learning algorithms with its applications in TensorFlowMaster state of the art meta learning algorithms like MAML, reptile, meta SGDBook Description Meta learning is an exciting research trend in machine learning, which enables a model to understand the learning process. Unlike other ML paradigms, with meta learning you can learn from small datasets faster. Hands-On Meta Learning with Python starts by explaining the fundamentals of meta learning and helps you understand the concept of learning to learn. You will delve into various one-shot learning algorithms, like siamese, prototypical, relation and memory-augmented networks by implementing them in TensorFlow and Keras. As you make your way through the book, you will dive into state-of-the-art meta learning algorithms such as MAML, Reptile, and CAML. You will then explore how to learn quickly with Meta-SGD and discover how you can perform unsupervised learning using meta learning with CACTUs. In the concluding chapters, you will work through recent trends in meta learning such as adversarial meta learning, task agnostic meta learning, and meta imitation learning. By the end of this book, you will be familiar with state-of-the-art meta learning algorithms and able to enable human-like cognition for your machine learning

models. What you will learnUnderstand the basics of meta learning methods, algorithms, and typesBuild voice and face recognition models using a siamese networkLearn the prototypical network along with its variantsBuild relation networks and matching networks from scratchImplement MAML and Reptile algorithms from scratch in PythonWork through imitation learning and adversarial meta learningExplore task agnostic meta learning and deep meta learningWho this book is for Hands-On Meta Learning with Python is for machine learning enthusiasts, AI researchers, and data scientists who want to explore meta learning as an advanced approach for training machine learning models. Working knowledge of machine learning concepts and Python programming is necessary.

The Best of TaoSecurity Blog, Volume 3 Newnes Since 2003, cybersecurity author Richard Bejtlich has been publishing posts on TaoSecurity Blog, a site with 15 million views since 2011. Now, after re-reading over 3,000 stories and approximately one million words, he has selected and republished the very best entries from 17 years of writing, along with commentaries and additional material. In the third volume of the TaoSecurity Blog series, Mr. Bejtlich addresses the evolution of his

security mindset, influenced by current events and advice from his so-called set of "wise people." He talks about why speed is not the key to John Boyd's OODA loop, and why security strategies designed for and by the "security 1%" may be irrelevant at best, or harmful at worst, for the remaining "99%". His history section explores the origins of the terms threat hunting and indicators of compromise, and reveals who really created the quote "there are two types of companies." His chapter on law highlights traps that might catch security teams, with advice to chief information security officers.This volume contains some of Mr. Bejtlich's favorite posts, such as Marcus Ranum's answer to what happens when security teams confront professionals, or how the Internet continues to function despite constant challenges, or reactions to comments by Dan Geer, Bruce Schneier, Marty Roesch, and other security leaders. Mr. Bejtlich has written new commentaries to accompany each post, some of which would qualify as blog entries in their own right. Read how the security industry, defensive methodologies, and strategies to improve national security have evolved in this new book, written by one of the authors who has seen it all and survived to blog about it.

Research Anthology on Artificial Intelligence Applications in Security

CRC Press
Nowadays it is impossible to imagine a business without technology as most industries are becoming "smarter" and more tech-driven, ranging from small individual tech initiatives to complete business models with intertwined supply chains and "platform"-based business models. New ways of working, such as agile and DevOps, have been introduced, leading to new risks. These risks come in the form of new challenges for teams working together in a distributed manner, privacy concerns, human autonomy, and cybersecurity concerns. Technology is now integrated into the business discipline and is here to stay leading to the need for a thorough understanding of how to address these risks and all the potential problems that could arise. With the advent of organized crime, such as hacks and denial-of-service attacks, all kinds of malicious actors are infiltrating the digital society in new and unique ways. Systems with poor design, implementation, and configurations are easily taken advantage of. When it comes to integrating business and technology, there needs to be approaches for assuring security against risks that can threaten both businesses and their digital platforms. Strategic Approaches to Digital Platform Security Assurance

offers comprehensive design science research approaches to extensively examine risks in digital platforms and offer pragmatic solutions to these concerns and challenges. This book addresses significant problems when transforming an organization embracing API-based platform models, the use of DevOps teams, and issues in technological architectures. Each section will examine the status quo for business technologies, the current challenges, and core success factors and approaches that have been used. This book is ideal for security analysts, software engineers, computer engineers, executives, managers, IT consultants, business professionals, researchers, academicians, and students who want to gain insight and deeper knowledge of security in digital platforms and gain insight into the most important success factors and approaches utilized by businesses.

The Best of TaoSecurity Blog, Volume 4 Simon and Schuster

A beginner's guide to building Windows applications with WinUI for UWP and desktop applications Key FeaturesCreate modern Windows 10 applications and gain access to UI controls that were previously limited to UWP applicationsDiscover how to modernize your existing Win32 apps with a modern Windows 10 UILearn to

embed a single page application (SPA) in a WinUI application with a web framework like BlazorBook Description WinUI 3.0 takes a whole new approach to delivering Windows UI components and controls, and is able to deliver the same features on more than one version of Windows 10. Learn WinUI 3.0 is a comprehensive introduction to WinUI and Windows apps for anyone who is new to WinUI, Universal Windows Platform (UWP), and XAML applications. The book begins by helping you get to grips with the latest features in WinUI and shows you how XAML is used in UI development. You'll then set up a new Visual Studio environment and learn how to create a new UWP project. Next, you'll find out how to incorporate the Model-View-ViewModel (MVVM) pattern in a WinUI project and develop unit tests for ViewModel commands. Moving on, you'll cover the Windows Template Studio (WTS) new project wizard and WinUI libraries in a step-by-step way. As you advance, you'll discover how to leverage the Fluent Design system to create beautiful WinUI applications. You'll also explore the contents and capabilities of the Windows Community Toolkit and learn to create a new UWP user control. Toward the end, the book will teach you how to build, debug, unit test, deploy, and monitor apps in production. By

the end of this book, you'll have learned how to build WinUI applications from scratch and modernize existing WPF and WinForms applications using WinUI controls. What you will learnGet up and running with WinUI and discover how it fits into the landscape of Project Reunion and Windows UI developmentBuild new Windows apps quickly with robust templatesDevelop testable and maintainable apps using the MVVM patternModernize WPF and WinForms applications with WinUI and XAML IslandsDiscover how to build apps that can target Windows and leverage the power of the webInstall the XAML Controls Gallery sample app and explore available WinUI controlsWho this book is for This book is for anyone who wants to develop Windows applications with a modern user experience (UX). If you are familiar with UWP and WPF and are looking to enhance your knowledge of Windows development and modernize existing apps, you will find this book useful. Hands-on experience with C# and .NET is expected but no prior knowledge of WinUI is required.

Essential COM

Springer Science & Business Media

Software developers need to worry about security as never before. They need clear guidance on safe coding practices, and that’s exactly what this book delivers. The book does not delve

deep into theory, or rant about the politics of security. Instead, it clearly and simply lays out the most common threats that programmers need to defend against. It then shows programmers how to make their defense. The book takes a broad focus, ranging over SQL injection, worms and buffer overflows, password security, and more. It sets programmers on the path towards successfully defending against the entire gamut of security threats that they might face.

ICCWS 2022 17th International Conference on Cyber Warfare and Security Walter de Gruyter GmbH & Co KG Explore machine learning in Rust and learn about the intricacies of creating machine learning applications. This book begins by covering the important concepts of machine learning such as supervised, unsupervised, and reinforcement learning, and the basics of Rust. Further, you'll dive into the more specific fields of machine learning, such as computer vision and natural language processing, and look at the Rust libraries that help create applications for those domains. We will also look at how to deploy these applications either on site or over the cloud. After reading Practical Machine Learning with Rust, you will have a solid understanding of creating high computation libraries using Rust. Armed with

the knowledge of this amazing language, you will be able to create applications that are more performant, memory safe, and less resource heavy. What You Will Learn Write machine learning algorithms in RustUse Rust libraries for different tasks in machine learningCreate concise Rust packages for your machine learning applicationsImplement NLP and computer vision in RustDeploy your code in the cloud and on bare metal servers Who This Book Is For Machine learning engineers and software engineers interested in building machine learning applications in Rust.

The Tao of Microservices John Wiley & Sons
Internet attack on computer systems is pervasive. It can take from less than a minute to as much as eight hours for an unprotected machine connected to the Internet to be completely compromised. It is the information security architect's job to prevent attacks by securing computer systems. This book describes both the process and the practice of as

Vehicle Safety Communications Apress
STRENGTHEN SOFTWARE SECURITY BY HELPING DEVELOPERS AND SECURITY EXPERTS WORK TOGETHER Traditional approaches to securing software are inadequate. The solution: Bring software engineering

and network security teams together in a new, holistic approach to protecting the entire enterprise. Now, four highly respected security experts explain why this “confluence” is so crucial, and show how to implement it in your organization. Writing for all software and security practitioners and leaders, they show how software can play a vital, active role in protecting your organization. You’ll learn how to construct software that actively safeguards sensitive data and business processes and contributes to intrusion detection/response in sophisticated new ways. The authors cover the entire development lifecycle, including project inception, design, implementation, testing, deployment, operation, and maintenance. They also provide a full chapter of advice specifically for Chief Information Security Officers and other enterprise security executives. Whatever your software security responsibilities, Enterprise Software Security delivers indispensable big-picture guidance–and specific, high-value recommendations you can apply right now. COVERAGE INCLUDES: • Overcoming common obstacles to collaboration between developers and IT security professionals • Helping programmers design, write, deploy, and operate more secure software • Helping network security engineers use

application output more effectively • Organizing a software security team before you've even created requirements • Avoiding the unmanageable complexity and inherent flaws of layered security • Implementing positive software design practices and identifying security defects in existing designs • Teaming to improve code reviews, clarify attack scenarios associated with vulnerable code, and validate positive compliance • Moving beyond pentesting toward more comprehensive security testing • Integrating your new application with your existing security infrastructure • "Ruggedizing" DevOps by adding infosec to the relationship between development and operations • Protecting application security during maintenance

Enterprise Software Security IGI Global Offering a distinctive approach, this book will teach readers not only how to use COM but how to think in COM. COM can greatly improve the efficiency of applications, but COM fluency is a difficult task. The book is a top resource for developers who need to make the transition from superficial understanding to deep knowledge.

Transforming Cybersecurity: Using COBIT 5 Prentice Hall Professional Since 2003, cybersecurity author Richard Bejtlich has

been writing posts on TaoSecurity Blog, a site with 15 million views since 2011. Now, after re-reading over 3,000 posts and approximately one million words, he has selected and republished the very best entries from 17 years of writing. In the first volume of the TaoSecurity Blog series, Bejtlich addresses milestones, philosophy and strategy, risk, and advice. He has written new commentaries to accompany each post, some of which would qualify as blog entries in their own right. Read how the security industry, defensive methodologies, and strategies to improve career opportunities have evolved in this new book, written by one of the authors who has seen it all and survived to blog about it.

Hands-On Meta Learning with Python
Lulu.com

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have

untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts,

computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

DevOps for Developers
Apress
“Mantle and Lichty have assembled a guide that will help you hire, motivate, and mentor a software development team that functions at the highest level. Their rules of thumb and coaching advice are great blueprints for new and experienced software engineering managers alike.” —Tom Conrad, CTO, Pandora “I wish I’d had this material available years ago. I see lots and lots of ‘meat’ in here that I’ll use over and over again as I try to become a better manager. The writing style is right on, and I love the personal anecdotes.” —Steve Johnson, VP, Custom Solutions, DigitalFish All too often, software development is deemed unmanageable. The news is filled with stories of projects that have run catastrophically over schedule and budget. Although adding some formal discipline to the development process has improved the situation, it has by no means solved the problem. How can it be, with so much time and money spent to get software development under control, that it remains so unmanageable? In Managing the Unmanageable: Rules,

Tools, and Insights for Managing Software People and Teams , Mickey W. Mantle and Ron Lichty answer that persistent question with a simple observation: You first must make programmers and software teams manageable. That is, you need to begin by understanding your people—how to hire them, motivate them, and lead them to develop and deliver great products. Drawing on their combined seventy years of software development and management experience, and highlighting the insights and wisdom of other successful managers, Mantle and Lichty provide the guidance you need to manage people and teams in order to deliver software successfully. Whether you are new to software management, or have already been working in that role, you will appreciate the real-world knowledge and practical tools packed into this guide.

Securing Systems

Springer Nature

This book offers a systematic and comprehensive introduction to the visual simultaneous localization and mapping (vSLAM) technology, which is a fundamental and essential component for many applications in robotics, wearable devices, and autonomous driving vehicles. The book starts from very basic mathematic background knowledge such as 3D rigid body

geometry, the pinhole camera projection model, and nonlinear optimization techniques, before introducing readers to traditional computer vision topics like feature matching, optical flow, and bundle adjustment. The book employs a light writing style, instead of the rigorous yet dry approach that is common in academic literature. In addition, it includes a wealth of executable source code with increasing difficulty to help readers understand and use the practical techniques. The book can be used as a textbook for senior undergraduate or graduate students, or as reference material for researchers and engineers in related areas.

Threat Modeling
Pearson Education
The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn

effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security. Managing the

Unmanageable Packt Publishing Ltd
In these highly competitive times and with so many technological advancements, it is impossible for any industry to remain isolated and untouched by innovations. In this era of digital economy, the banking sector cannot exist and operate without the various digital tools offered by the ever new innovations happening in the field of Artificial Intelligence (AI) and its sub-set technologies. New technologies have enabled incredible progression in the finance industry. Artificial Intelligence (AI) and Machine Learning (ML) have provided the investors and customers with more innovative tools, new types of financial products and a new potential for growth.According to Cathy Bessant (the Chief Operations and Technology Officer, Bank of America), AI is not just a technology discussion. It is also a discussion about data and how it is used and protected. She says, "In a world focused on using AI in new ways, we're focused on using it wisely and responsibly."

Data Pipelines with Apache Airflow Addison-Wesley Professional
Go beyond TaoSecurity Blog with this new volume from author Richard Bejtlich.In the first three volumes of the series, Mr. Bejtlich selected and republished the very best entries from 18 years of writing and

over 18 million blog views, along with commentaries and additional material. In this title, Mr. Bejtlich collects material that has not been published elsewhere, including articles that are no longer available or are stored in assorted digital or physical archives.Volume 4 offers early white papers that Mr. Bejtlich wrote as a network defender, either for technical or policy audiences. It features posts from other blogs or news outlets, as well as some of his written testimony from eleven Congressional hearings. For the first time, Mr. Bejtlich publishes documents that he wrote as part of his abandoned war studies PhD program. This last batch of content was only available to his advisor, Dr. Thomas Rid, and his review committee at King's College London.Read how the security industry, defensive methodologies, and strategies to improve national security have evolved in this new book, written by one of the authors who has seen it all and survived to blog about it.

Speech Enhancement

Addison-Wesley Professional

Provides an up-to-date, in-depth look at the current research, design, and implementation of cooperative vehicle safety communication protocols and technology Improving traffic safety has been a top concern for transportation agencies around the

world and the focus of heavy research and development efforts sponsored by both governments and private industries. Cooperative vehicle systems—which use sensors and wireless technologies to reduce traffic accidents—can play a major role in making the world's roads safer. Vehicle Safety Communications: Protocols, Security, and Privacy describes fundamental issues in cooperative vehicle safety and recent advances in technologies for enabling cooperative vehicle safety. It gives an overview of traditional vehicle safety issues, the evolution of vehicle safety technologies, and the need for cooperative systems where vehicles work together to reduce the number of crashes or mitigate damage when crashes become unavoidable. Authored by two top industry professionals, the book: Summarizes the history and current status of 5.9 GHz Dedicated Short Range Communications (DSRC) technology and standardization, discussing key issues in applying DSRC to support cooperative vehicle safety Features an in-depth overview of on-board equipment (OBE) and roadside equipment (RSE) by describing sample designs to illustrate the key issues and potential solutions Takes on security and privacy protection requirements and challenges, including how to design privacy-

preserving digital certificate management systems and how to evict misbehaving vehicles Includes coverage of vehicle-to-infrastructure (V2I) communications like intersection collision avoidance applications and vehicle-to-vehicle (V2V) communications like extended electronic brake lights and intersection movement assist Vehicle Safety Communications is ideal for anyone working in the areas of—or studying—cooperative vehicle safety and vehicle communications.

An Introduction to Data Science SAGE Publications

"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an

accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the

NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Interpretable Machine Learning Apress

Network security is not simply about building impenetrable walls—determined attackers will

eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: –Determine where to deploy NSM platforms, and size them for the monitored networks –Deploy stand-alone or distributed NSM installations –Use command line and graphical packet analysis tools, and NSM consoles –Interpret network evidence from server-side and client-side intrusions –Integrate threat intelligence into NSM software to identify sophisticated adversaries There’s no foolproof way to keep attackers out of your network. But when they get in, you’ll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Artificial Intelligence in Banking "O'Reilly

Media, Inc."
A new edition of the bestseller • The first book to reveal in the West the Taoist techniques that enable women to cultivate and enhance their sexual energy • Reveals Taoist secrets for shortening menstruation, reducing cramps, and compressing more chi into the ovaries for greater sexual power • Teaches the practice of total body orgasm For thousands of years the sexual principles and techniques presented here were taught by Taoist masters in secret only to a small number of people (sworn to silence), in the royal courts and esoteric circles of China. This is the first book to make this ancient knowledge available to the West. The foundation of healing love is the cultivation, transformation, and circulation of sexual energy, known as jing. Jing energy is creative, generative energy that is vital for the development of chi (vital life-force energy) and shen (spiritual energy), which enables higher practices of spiritual development. Jing is produced in the sexual organs, and it is energy women lose continually through menstruation and child bearing. Mantak Chia teaches powerful techniques developed by Taoist masters for the conservation of jing and how it is used to revitalize women's physical, mental, and spiritual well-being. Among the many benefits conferred by these practices are a

reduction in the discomfort caused by menstruation and the ability to attain full-body orgasm.

Related with Devsecops The Tao Of Security Science Rsa Conference:
• Valora A Tu Madre Una Historia Para Reflexionar : click here