Internet Security How To Defend Against Attackers On The Web Jones Bartlett Learning Information Systems Security Assurance

This book constitutes the refereed proceedings of the First International Symposium on Mobile Internet Security, MobiSec 2016, held in Taichung, Taiwan, in July 2016. The 15 revised full papers presented were carefully reviewed and selected from 44 submissions. They are closely related to various theories and practical applications in mobility management to highlight the state-of-the-art research.

Print Textbook & Virtual Security Cloud Lab Access: 180-day subscription. Please confirm the ISBNs used in your course with your instructor before placing your order; your institution may use a custom integration or an access portal that requires a different access code. The Second Edition of Internet Security: How to Defend Against Attackers on the Web (formerly titled Security Strategies in Web Applications and Social Networking) provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

The definitive book on UNIX security, this volume covers every aspect of computer security on UNIX machines and the Internet.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Web Applications and Social Networking provides a unique, in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

This collection of papers, articles, and monographs details the ethical landscape as it exists for the distinct areas of Internet and network security, including moral justification of hacker attacks, the ethics behind the freedom of information which contributes to hacking, and the role of the law in policing cyberspace.

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.

Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new

vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

Cybercrimes committed against persons include various crimes like transmission of child-pornography harassment of any one with the use of a computer such as email. The trafficking, distribution, posting and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cybercrimes known today. The worldwide information infrastructure is today increasingly under attack by cyber criminals and terrorists—and the number, cost, and sophistication of the attacks are increasing at alarming rates. The challenge of controlling transnational cyber crime requires a full range of responses, including both voluntary and legally mandated cooperation This book makes an serious attempt to understand the Cyber Crime which involves activities like Credit Card Frauds, unauthorized excess to other’s computer system, Pornography, Software piracy and Cyber stalking etc.

Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You’ll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.

Adopting a multidisciplinary perspective, this book explores the key challenges associated with the proliferation of cyber capabilities. Over the past two decades, a new man-made domain of conflict has materialized. Alongside armed conflict in the domains of land, sea, air, and space, hostilities between different types of political actors are now taking place in cyberspace. This volume addresses the challenges posed by cyberspace hostility from theoretical, political, strategic and legal perspectives. In doing so, and in contrast to current literature, cyber-security is analysed through a multidimensional lens, as opposed to being treated solely as a military or criminal issues, for example. The individual chapters map out the different scholarly and political positions associated with various key aspects of cyber conflict and seek to answer the following questions: do existing theories provide sufficient answers to the current challenges posed by conflict in cyberspace, and, if not, could alternative approaches be developed?; how do states and non-state actors make use of cyber-weapons when pursuing strategic and political aims?; and, how does the advent of conflict in cyberspace challenge our established legal framework? By asking important strategic questions on the theoretical, strategic, ethical and legal implications and challenges of the proliferation of cyber warfare capabilities, the book seeks to stimulate research into an area that has hitherto been neglected. This book will be of much interest to students of cyber-conflict and cyber-warfare, war and conflict studies, international relations, and security studies.

This new Edition of Electronic Commerce is a complete update of the leading graduate level/advanced undergraduate level textbook on the subject. Electronic commerce (EC) describes the manner in which transactions take place over electronic networks, mostly the

Internet. It is the process of electronically buying and selling goods, services, and information. Certain EC applications, such as buying and selling stocks and airline tickets online, are reaching maturity, some even exceeding non-Internet trades. However, EC is not just about buying and selling; it also is about electronically communicating, collaborating, and discovering information. It is about e-learning, e-government, social networks, and much more. EC is having an impact on a significant portion of the world, affecting businesses, professions, trade, and of course, people. The most important developments in EC since 2014 are the continuous phenomenal growth of social networks, especially Facebook , LinkedIn and Instagram, and the trend toward conducting EC with mobile devices. Other major developments are the expansion of EC globally, especially in China where you can find the world's largest EC company. Much attention is lately being given to smart commerce and the use of AI-based analytics and big data to enhance the field. Finally, some emerging EC business models are changing industries (e.g., the shared economy models of Uber and Airbnb). The 2018 (9th) edition, brings forth the latest trends in e-commerce, including smart commerce, social commerce, social collaboration, shared economy, innovations, and mobility.

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.

Security Strategies in Web Applications and Social NetworkingJones & Bartlett Learning

Security Strategies in Web Applications and Social Networking provides a unique, in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications. The Jones & Bartlett Learning: Information Systems Security & Assurance Series delivers fundamental IT security principles packed with real-world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information Systems Security programs. Authored by Certified Information Systems Security Professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of today and tomorrow.

The Second Edition of Security Strategies in Web Applications and Social Networking provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully

secure Web-enabled applications.

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, What Every Engineer Should Know About Cyber Security and Digital Forensics is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

Cyberspace is a ubiquitous realm interconnecting every aspect of modern society, enabled by broadband networks and wireless signals around us, existing within local area networks in our schools, hospitals and businesses, and within the massive grids that power most countries. Securing cyberspace to ensure the continuation of growing economies and to protect a nation’s way of life is a major concern for governments around the globe. This book contains papers presented at the NATO Advanced Research Workshop (ARW) entitled Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework, held in Ohrid, the Former Yugoslav Republic of Macedonia (FYROM), in June 2013. The workshop aimed to develop a governing policy framework for nation states to enhance the cyber security of critical infrastructure. The 12 papers included herein cover a wide range of topics from web security and end-user training, to effective implementation of national cyber security policies and defensive countermeasures. The book will be of interest to cyber security professionals, practitioners, policy-makers, and to all those for whom cyber security is a critical and an important aspect of their work.

Here's the book you need to prepare for exam 1D0-410, CIW Foundations. This study guide provides: In-depth coverage of official exam objective groups Hundreds of challenging review questions, in the book and on the CD Leading-edge exam preparation software, including a testing engine and electronic flashcards Authoritative coverage of all exam topics, including: Networking fundamentals OSI reference model TCP/IP protocol suite HTML basics and web page authoring tools Multimedia and active web content Risk assessment and security E-commerce fundamentals Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Cyber Security – Essential principles to secure your organisation takes you

through the fundamentals of cyber security, the principles that underpin it, vulnerabilities and threats, and how to defend against attacks.

Most computer systems that interface with the internet today presume that users will adopt additional security measures to protect themselves against phishing and malware attacks, and are capable of configuring software to obtain optimal security. This assumption is worrying, as prior work has repeatedly shown that not all computer users face similar levels of risk, and at-risk users may not have the resources or know-how to adopt obtain optimal levels of security. The first part of this thesis conducts an empirical analysis of the HTTPS configuration of over 4 million websites in order to assess the security posture of the ecosystem, as well as the factors that influence operators' security decisions. We show that while most websites have secure configurations, this is largely due to major cloud providers that supply secure defaults. Individually configured servers are more often insecure than not. We show that both server software defaults and online configuration recommendations are frequently insecure, and conclude with lessons for improving the HTTPS ecosystem. Among these, is the recommendation that server software should provide optimal security by default, thereby removing the burden of achieving optimal security from users. As technologies to defend against phishing and malware (e.g., two factor authentication or security keys) often impose an additional financial and usability cost on users, a key question is who should adopt these heightened protections. The second part of the thesis uses computational and survey methods to construct data-driven tools that identify at risk users for (1) malware, with a special focus on ransomware, and (2) for e-mail based phishing and malware. We measure over 287 phishing and malware attacks against Gmail users to identify the factors place a user at heightened risk of attack. Secondly, we present a machine learning model that draws on detailed web browsing behavior to predict users at risk of malware infection the following month; lastly, we develop and administer a survey to a representative sample of the U.S. population to first, provide a representative estimate of the prevalence of ransomware attacks within the general population, and second, to develop a proof-of-concept self-assessment of future ransomware risk.

This handbook introduces the basic principles and fundamentals of cyber security towards establishing an understanding of how to protect computers from hackers and adversaries. The highly informative subject matter of this handbook, includes various concepts, models, and terminologies along with examples and illustrations to demonstrate substantial technical details of the field. It motivates the readers to exercise better protection and defense mechanisms to deal with attackers and mitigate the situation. This handbook also outlines some of the exciting areas of future research where the existing approaches can be implemented. Exponential increase in the use of computers as a means of storing and retrieving security-intensive information, requires placement of adequate security measures to safeguard the entire computing and

communication scenario. With the advent of Internet and its underlying technologies, information security aspects are becoming a prime concern towards protecting the networks and the cyber ecosystem from variety of threats, which is illustrated in this handbook. This handbook primarily targets professionals in security, privacy and trust to use and improve the reliability of businesses in a distributed manner, as well as computer scientists and software developers, who are seeking to carry out research and develop software in information and cyber security. Researchers and advanced-level students in computer science will also benefit from this reference.

Do you know what is hacking? Do you want to learn about cyber security? Are you unaware of mistakes made in cybersecutity? This book is for you!!! This book teaches cyber security, how to defend themselves and defend against cyber-attacks. This book covers the latest security threats and defense strategies. Cyber security starts with the basics that organizations need to know to maintain a secure posture against outside threat and design a robust cybersecurity program. It takes you into the mindset of a Threat Actor to help you better understand the motivation and the steps of performing an actual attack - the Cybersecurity kill chain. This book also focuses on defense strategies to enhance the security of a system. You will also discover in-depth tools, including Azure Sentinel, to ensure there are security controls in each network layer, and how to carry out the recovery process of a compromised system. What you will learn The importance of hacking. Use cyber security kill chain to understand the attack strategy Common cyber attacks Benefits of cyber security. Utilize the latest defense tools, including Azure Sentinel and Zero Trust Network strategy Identify different types of cyber-attacks, such as SQL injection, malware and social engineering threats such as phishing emails Weigh the pros and cons of popular cybersecurity strategies of the past two decades Implement and then measure the outcome of a cybersecurity strategy Get an in-depth understanding of the security and hacking. Understand how to consistently monitor security and implement a vulnerability management strategy for on-premises and hybrid cloud Learn demand of cyber security. This open access book provides an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those problems. Who this book is for ? For the IT professional venturing into the IT security domain, IT pen testers, security consultants, or those looking to perform ethical hacking. Prior knowledge of penetration testing is beneficial issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies. WHAT ARE YOU WAITING FOR!!!! ORDER YOUR COPY NOW.....

A plethora of real - life case studies illustrate how to secure computer networks and provide examples on how to avoid being attacked.

The Internet of Things describes a world in which smart technologies enable objects with a network to communicate with each other and interface with humans effortlessly.

This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability. Security Solutions for Hyperconnectivity and the Internet of Things offers insights from cutting-edge research about the strategies and techniques that can be implemented to protect against cyber-attacks. Calling for revolutionary protection strategies to reassess security, this book is an essential resource for programmers, engineers, business professionals, researchers, and advanced students in relevant fields.

Connecting your home network to the internet. Physical security and insurance. Data protection.

In recent years, computer programming, or coding, has become a core competency for all kinds of skilled workers, opening the door to a variety of jobs. Among these are jobs in internet security, which is a field that has grown in importance as more people work, shop, and play online. This essential guide introduces readers to the types of jobs available in this field both now and in the future, and the industries these jobs serve. It also discusses common security threats, new technologies to address them, and critical resources for getting involved.

Global change and advancing technology have transformed the government sector with the use of information and communication technology to improve service delivery. The use of such technologies in electronic and mobile government services raises issues relating to security, privacy, and data protection. Security Frameworks in Contemporary Electronic Government is a pivotal reference source that provides vital research on the application of special security requirements in electronic government transactions. While highlighting topics such as digital environments, public service delivery, and cybercrime, this publication explores the difficulties and challenges faced in implementing e-government technologies, as well as the different aspects of security in e-government. This book is ideally designed for policymakers, software developers, IT specialists, government officials, academicians, researchers, and students seeking current research on secure environments in electronic and mobile government.

Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization; cryptography; system intrusion; UNIX and Linux security; Internet security, intranet security; LAN security; wireless network security; cellular network security, RFID security, and more. This compilation of 13 chapters is tightly focused and ideally suited as an essential desk reference in this high-growth subject area. Chapters contributed by leaders in the field covering foundational and practical aspects of system and network security, providing a new level of technical expertise not found elsewhere Comprehensive and updated coverage of the subject area allows the reader to put current technologies to work Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Cyber threats can evolve with almost unimaginable speed and serious consequences for the nation's security. The Government needs to put in place - as it has not yet done - mechanisms, people, education, skills, thinking and policies which take into account both the opportunities and the vulnerabilities which cyberspace presents. Evidence received by the Committee

suggested that in the event of a sustained cyber attack the ability of the Armed Forces to operate effectively could be fatally compromised due to their dependence on information and communication technology. The Committee has asked the Government to set out details of the contingency plans it has in place should such an attack occur. If it has none, it should say so - and urgently create some. The Committee was impressed by aspects of the co-operation and joint working between the MoD and private sector contractors. It welcomed the Government's commitment to foster a vibrant and innovative cyber security sector in the UK including a distinct role for the MoD to deliver military capabilities both to confront high-end threats and to provide a potential offensive capability. The opportunity created by cyber tools and techniques to enhance the military capabilities of our Armed Forces is clear. The MoD needs to explore this thoroughly. For this reason, the Committee supports the use of National Cyber Security Programme funding to develop these capabilities, but also wish to be assured that the MoD will maintain its investment in existing defence intelligence services which provide a vital UK cross-government capability

Market research guide to the wireless access and cellular telecommunications industry ?????? ?? ?????????????? a tool for strategic planning, competitive intelligence, employment searches or financial research. Contains trends, statistical tables, and an industry glossary. Also provides profiles of 350 leading wireless, Wi-Fi, RFID and cellular industry firms - includes addresses, phone numbers, executive names.

Attain true cyber security amidst ever–evolving threats using a holistic approach to defense Advanced Cyber Security is a practical guide to protecting your organization from cyber attacks using advanced active counter measures. Predict and guard against cyber attacks before they occur, by implementing cutting–edge static and dynamic active defense operations based on attack profile intelligence. This book walks you through the tools, techniques, and strategies that keep your organization?s information secure, providing tips and tricks, as well as warning about common pitfalls. Case studies demonstrate the latest in attack intelligence profiling, active defense through social media, email operations, crowd sourcing, and cross–disciplinary data science applications, giving you insight into how these tools are being applied most effectively by companies around the world. A discussion about the future of cyber security proposes future defense models and provides an insightful look at what?s coming down the pipeline. Cyber–threats are a top priority for businesses and governments and, as the threats change and develop, the need for effective countermeasures will only increase. This book helps you get out in front of the threat with a robust defense strategy, utilizing the newest, most effective methods in the field today. Locate your system?s vulnerabilities Build an effective defense against attacks Navigate the new security ecosystem Explore emerging cyber defense technology Effective cyber defense requires a holistic approach. Attacks can come from any quarter, and are becoming increasingly sophisticated, leaving traditional countermeasures wholly inadequate and reactive approaches insufficient. Defense–as–usual is now simply damage control. Advanced Cyber Security shows you what true cyber security now requires, and gives you clear guidance toward effective implementation.

In our hyper-connected digital world, cybercrime prevails as a major threat to online security and safety. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. The Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance combines the most recent developments in data protection and information communication technology (ICT) law with research surrounding current criminal behaviors in the digital sphere. Bridging research and practical application, this comprehensive reference source is ideally designed for use by investigators, computer forensics practitioners, and experts in ICT law, as well as academicians in the fields of information security and

criminal science.

Plunkett's InfoTech Industry Almanac presents a complete analysis of the technology business, including the convergence of hardware, software, entertainment and telecommunications. This market research tool includes our analysis of the major trends affecting the industry, from the rebound of the global PC and server market, to consumer and enterprise software, to super computers, open systems such as Linux, web services and network equipment. In addition, we provide major statistical tables covering the industry, from computer sector revenues to broadband subscribers to semiconductor industry production. No other source provides this book's easy-to-understand comparisons of growth, expenditures, technologies, imports/exports, corporations, research and other vital subjects. The corporate profile section provides in-depth, one-page profiles on each of the top 500 InfoTech companies. We have used our massive databases to provide you with unique, objective analysis of the largest and most exciting companies in: Computer Hardware, Computer Software, Internet Services, E-Commerce, Networking, Semiconductors, Memory, Storage, Information Management and Data Processing. We've been working harder than ever to gather data on all the latest trends in information technology. Our research effort includes an exhaustive study of new technologies and discussions with experts at dozens of innovative tech companies. Purchasers of the printed book or PDF version may receive a free CD-ROM database of the corporate profiles, enabling export of vital corporate data for mail merge and other uses.

The book discussess the categories of infrastucture that require protection. The issues associated with each, and the responsibilities of the public and private sector in securing this infrastructure.

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.