Product Matrix For 2017 Fortinet

Navigating Cybersecurity Leadership Challenges with Insights from Pioneers
Understanding and Managing Risks and the Internet of Things
Emerging Trends in ICT Security
Mastering FortiOS
24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I
15th International Conference, DIMVA 2018, Saclay, France, June 28–29, 2018, Proceedings
Controlling the Human Element of Security
15th International Conference on Information Technology
The Art of Deception
Industrial Network Security
Forward Resilience
Computer Security – ESORICS 2019
Security Information and Event Management (SIEM) Implementation
Understanding the Process of Creative Genius
The Practice of Network Security Monitoring
Sustainable Innovation, Disruption, and Change
Microsoft Azure Sentinel
4th International Conference, ICISSP 2018, Funchal - Madeira, Portugal, January 22-24, 2018, Revised Selected Papers
Know Your Network
Network and System Security
Microsoft Azure Security Center
Zero Days, Thousands of Nights
Understanding Incident Detection and Response
Functionality and Applications in Human Health
RIoT Control
The Definitive Guide to Attacking the Internet of Things
Trends and Advances in Information Systems and Technologies
Managing the Mail
Food Bioactives
Detection of Intrusions and Malware, and Vulnerability Assessment
Infrastructure security with Red Team and Blue Team tactics
Principles of SAN Design
12th EAI International Conference, AFRICOMM 2020, Ebène City, Mauritius, December 2-4, 2020, Proceedings
CISO COMPASS
Proceedings of FICR-TEAS 2020
Network Security Assessment
Internet Regulation, Social Media Use, and Online Civic Engagement
Building a Practical Information Security Program
A Brain-Friendly Guide

Product Matrix For 2017 Fortinet

Downloaded from blog.gmercyu.edu ***by guest***

PHILLIPS MCCONNELL

Navigating Cybersecurity Leadership Challenges with Insights from Pioneers Springer Nature
As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering
Understanding and Managing Risks and the Internet of Things Springer
This valuable volume addresses the growing consumer demand for novel functional food products and for high-value, nutritionally rich products by focusing on the sources and applications of bioactives from food. The chapters in the book describe functional properties and discuss applications of the selected food ingredients obtained from various sources, including culinary banana, phalsa, pseudocereals, roselle calyces, asparagus, and more. Several chapters address the resurgence of interest in pseudocereals due to their excellent nutritional and biological values, gluten-free composition, and the presence of some health-promoting compounds. The book also looks at utilizing industrial byproducts for making functional and nutraceutical ingredients. The chapters on prebiotics and probiotics highlight different functional properties, and a chapter on food allergens discusses advancements in detection and management in the food manufacturing industries.
Emerging Trends in ICT Security UTM Security with FortinetMastering FortiOS Storage Area Networks provide highly reliable, high-performance connectivity between hosts and storage devices. This allows storage resource sharing, improving asset utilization, and enabling solutions such as high availability, disaster recovery, information lifecycle management, and utility computing. These solutions provide a high return on investment, resulting in an accelerating SAN adoption rate in all IT markets.This book provides an overview of SAN protocols and technologies, and practical guidance on SAN design, implementation, and management topics. Some future SAN trends and technologies are discussed, but the focus is on designing SANs with current, real-world products such as Fibre Channel switches and routers.Principles of SAN Design offers a "one stop shop" for SAN design knowledge. Why wait?

Read the definitive work on SAN design today!

Mastering FortiOS Syngress

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I "O'Reilly Media, Inc."

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

15th International Conference, DIMVA 2018, Saclay, France, June 28–29, 2018, Proceedings Morgan Kaufmann
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.
Controlling the Human Element of Security Syngress
This book constitutes the thoroughly refereed proceedings of the 11th International Conference on Security for Information Technology and Communications, SecITC 2018, held in Bucharest, Romania, in November 2018. The 35 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 70 submissions. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.
15th International Conference on Information Technology Springer
This volume presents a collection of peer-reviewed, scientific articles from the 15th International Conference on Information Technology – New Generations, held at Las Vegas. The collection addresses critical areas of Machine Learning, Networking and Wireless Communications, Cybersecurity, Data Mining, Software Engineering, High Performance Computing Architectures, Computer Vision, Health, Bioinformatics, and Education.
The Art of Deception Center for Transatlantic Relations Sais
Todd Fitzgerald, co-author of the ground-breaking (ISC)2 CISO Leadership: Essential Principles for Success, Information Security Governance Simplified: From the Boardroom to the Keyboard, co-author for the E-C Council CISO Body of Knowledge, and contributor to many others including Official (ISC)2 Guide to the CISSP CBK, COBIT 5 for Information Security, and ISACA CSX Cybersecurity Fundamental Certification, is back with this new book incorporating practical experience in leading, building, and sustaining an information security/cybersecurity program. CISO COMPASS includes personal, pragmatic perspectives and lessons learned of over 75 award-winning CISOs, security leaders, professional association leaders, and cybersecurity standard setters who

have fought the tough battle. Todd has also, for the first time, adapted the McKinsey 7S framework (strategy, structure, systems, shared values, staff, skills and style) for organizational effectiveness to the practice of leading cybersecurity to structure the content to ensure comprehensive coverage by the CISO and security leaders to key issues impacting the delivery of the cybersecurity strategy and demonstrate to the Board of Directors due diligence. The insights will assist the security leader to create programs appreciated and supported by the organization, capable of industry/ peer award-winning recognition, enhance cybersecurity maturity, gain confidence by senior management, and avoid pitfalls. The book is a comprehensive, soup-to-nuts book enabling security leaders to effectively protect information assets and build award-winning programs by covering topics such as developing cybersecurity strategy, emerging trends and technologies, cybersecurity organization structure and reporting models, leveraging current incidents, security control frameworks, risk management, laws and regulations, data protection and privacy, meaningful policies and procedures, multi-generational workforce team dynamics, soft skills, and communicating with the Board of Directors and executive management. The book is valuable to current and future security leaders as a valuable resource and an integral part of any college program for information/ cybersecurity.

Industrial Network Security Springer This book presents high-quality, peer-reviewed papers from the FICR International Conference on Rising Threats in Expert Applications and Solutions 2020, held at IIS University Jaipur, Rajasthan, India, on January 17–19, 2020. Featuring innovative ideas from researchers, academics, industry professionals and students, the book covers a variety of topics, including expert applications and artificial intelligence/machine learning; advanced web technologies, like IoT, big data, and cloud computing in expert applications; information and cybersecurity threats and solutions; multimedia applications in forensics, security and intelligence; advances in app development; management practices for expert applications; and social and ethical aspects of expert applications in applied sciences.

Forward Resilience "O'Reilly Media, Inc." This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming

initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.

Computer Security – ESORICS 2019
Elsevier
Around the world, SCADA (supervisory control and data acquisition) systems and other real-time process control networks run mission-critical infrastructure--everything from the power grid to water treatment, chemical manufacturing to transportation. These networks are at increasing risk due to the move from proprietary systems to more standard platforms and protocols and the interconnection to other networks. Because there has been limited attention paid to security, these systems are seen as largely unsecured and very vulnerable to attack. This book addresses currently undocumented security issues affecting SCADA systems and overall critical infrastructure protection. The respective co-authors are among the leading experts in the world capable of addressing these related-but-independent concerns of SCADA security. Headline-making threats and countermeasures like malware, sidejacking, biometric applications, emergency communications, security awareness llanning, personnel & workplace preparedness and bomb threat planning will be addressed in detail in this one of a kind book-of-books dealing with the threats to critical infrastructure protection. They collectivly have over a century of expertise in their respective fields of infrastructure protection. Included among the contributing authors are Paul Henry, VP of Technology Evangelism, Secure Computing, Chet Hosmer, CEO and Chief Scientist at Wetstone Technologies, Phil Drake, Telecommunications Director, The Charlotte Observer, Patrice Bourgeois, Tenable Network Security, Sean Lowther, President, Stealth Awareness and Jim Windle, Bomb Squad Commander, CMPD. * Internationally known experts provide a detailed discussion of the complexities of SCADA security and its impact on critical infrastructure * Highly technical chapters on the latest vulnerabilities to SCADA and critical infrastructure and countermeasures * Bonus chapters on security awareness training, bomb threat planning, emergency communications, employee safety and much more * Companion Website featuring video interviews with subject matter experts offer a "sit-down" with the leaders in the field

Security Information and Event Management (SIEM) Implementation
Springer
As recently as five years ago, securing a network meant putting in a firewall, intrusion detection system, and installing antivirus software on the desktop. Unfortunately, attackers have grown more nimble and effective, meaning that

traditional security programs are no longer effective. Today's effective cyber security programs take these best practices and overlay them with intelligence. Adding cyber threat intelligence can help security teams uncover events not detected by traditional security platforms and correlate seemingly disparate events across the network. Properly-implemented intelligence also makes the life of the security practitioner easier by helping him more effectively prioritize and respond to security incidents. The problem with current efforts is that many security practitioners don't know how to properly implement an intelligence-led program, or are afraid that it is out of their budget. Building an Intelligence-Led Security Program is the first book to show how to implement an intelligence-led program in your enterprise on any budget. It will show you how to implement a security information a security information and event management system, collect and analyze logs, and how to practice real cyber threat intelligence. You'll learn how to understand your network in-depth so that you can protect it in the best possible way. Provides a roadmap and direction on how to build an intelligence-led information security program to protect your company. Learn how to understand your network through logs and client monitoring, so you can effectively evaluate threat intelligence. Learn how to use popular tools such as BIND, SNORT, squid, STIX, TAXII, CyBox, and splunk to conduct network intelligence.

Understanding the Process of Creative Genius No Starch Press

Implement a robust SIEM system Effectively manage the security information and events produced by your network with help from this authoritative guide. Written by IT security experts, Security Information and Event Management (SIEM) Implementation shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You'll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource. Assess your organization's business models, threat models, and regulatory compliance requirements Determine the necessary SIEM components for small- and medium-size businesses Understand SIEM anatomy—source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring Develop an effective incident response program Use the inherent capabilities of your SIEM system for business intelligence Develop filters and correlated event rules to reduce false-positive alerts Implement AlienVault's Open Source Security Information Management (OSSIM) Deploy the Cisco Monitoring Analysis and Response System (MARS) Configure and use the Q1 Labs QRadar SIEM system Implement ArcSight Enterprise Security Management (ESM) v4.5 Develop your SIEM security analyst skills

The Practice of Network Security Monitoring Syngress

This book constitutes the revised selected papers of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, held in Funchal - Madeira, Portugal, in January 2018. The 15 full papers presented were

carefully reviewed and selected from a total of 71 submissions. They are dealing with topics such as data and software security; privacy and confidentiality; mobile systems security; biometric authentication; information systems security and privacy; authentication, privacy and security models; data mining and knowledge discovery; phishing; security architecture and design analysis; security testing; vulnerability analysis and countermeasures; web applications and services.
Springer
The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.
Sustainable Innovation, Disruption, and Change Newnes
Zero-day vulnerabilities--software vulnerabilities for which no patch or fix has been publicly released-- and their exploits are useful in cyber operations--whether by criminals, militaries, or governments--as well as in defensive and academic settings. This report provides findings from real-world zero-day vulnerability and exploit data that could augment conventional proxy examples and expert opinion, complement current efforts to create a framework for deciding whether to disclose or retain a cache of zero-day vulnerabilities and exploits, inform ongoing policy debates regarding stockpiling and vulnerability disclosure, and add extra context for those examining the implications and resulting liability of attacks and data breaches for U.S. consumers, companies, insurers, and for the civil justice system broadly. The authors provide insights about the zero-day vulnerability research and exploit development industry; give information on what proportion of zero-day vulnerabilities are alive (undisclosed), dead (known), or somewhere in between; and establish some baseline metrics regarding the average lifespan of zero-day vulnerabilities, the likelihood of another party discovering a vulnerability within a given time period, and the time and

costs involved in developing an exploit for a zero-day vulnerability"--Publisher's description.

Microsoft Azure Sentinel CRC Press

This book includes the proceedings of the 15th International Conference on Complex, Intelligent, and Software Intensive Systems, which took place in Asan, Korea, on July 1–3, 2021. Software intensive systems are systems, which heavily interact with other systems, sensors, actuators, devices, and other software systems and users. More and more domains are involved with software intensive systems, e.g., automotive, telecommunication systems, embedded systems in general, industrial automation systems, and business applications. Moreover, the outcome of web services delivers a new platform for enabling software intensive systems. Complex systems research is focused on the overall understanding of systems rather than its components. Complex systems are very much characterized by the changing environments in which they act by their multiple internal and external interactions. They evolve and adapt through internal and external dynamic interactions. The development of intelligent systems and agents, which is each time more characterized by the use of ontologies and their logical foundations build a fruitful impulse for both software intensive systems and complex systems. Recent research in the field of intelligent systems, robotics, neuroscience, artificial intelligence, and cognitive sciences is very important factor for the future development and innovation of software intensive and complex systems. The aim of the book is to deliver a platform of scientific interaction between the three interwoven challenging areas of research and development of future ICT-enabled applications: Software intensive systems, complex systems, and intelligent systems.

4th International Conference, ICISSP 2018, Funchal - Madeira, Portugal, January 22-24, 2018, Revised Selected Papers No Starch Press

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shinder show how to apply Azure Security Center’s full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You’ll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. Whatever your role in Azure security, you’ll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft’s leading cloud security experts show how to: • Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and risk management • Master a new security paradigm for a world without traditional perimeters • Gain visibility and control to secure compute, network, storage, and application workloads • Incorporate Azure Security Center into your security operations center • Integrate Azure Security Center with Azure AD Identity Protection Center and third-party solutions • Adapt Azure Security Center’s built-in policies and definitions for your organization • Perform security assessments and implement Azure Security Center recommendations • Use

incident response features to detect, investigate, and address threats • Create high-fidelity fusion alerts to focus attention on your most urgent security issues • Implement application whitelisting and just-in-time VM access • Monitor user behavior and access, and investigate compromised or misused credentials • Customize and perform operating system security baseline assessments • Leverage integrated threat intelligence to identify known bad actors

Know Your Network Rand Corporation Emerging Trends in ICT Security, an edited volume, discusses the foundations and theoretical aspects of ICT security; covers trends, analytics, assessments and frameworks necessary for performance analysis and evaluation; and gives you the state-of-the-art knowledge needed for successful deployment of security solutions in many environments. Application scenarios provide you with an insider’s look at security solutions deployed in real-life scenarios, including but limited to smart devices, biometrics, social media, big data security, and crowd sourcing. Provides a multidisciplinary approach to security with coverage of communication systems, information mining, policy making, and management infrastructures Discusses deployment of numerous security solutions, including, cyber defense techniques and defense against malicious code and mobile attacks Addresses application of security solutions in real-life scenarios in several environments, such as social media, big data and crowd sourcing

Related with Product Matrix For 2017 Fortinet:
• New Math Inheriting Parents House : click here