

Automated Threat Management Vectra Networks

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network. Artificial intelligence (AI) and data mining is the fastest growing field in computer science. AI and data mining algorithms and techniques are found to be useful in different areas like pattern recognition, automatic threat detection, automatic problem solving, visual recognition, fraud detection, detecting developmental delay in children, and many other applications. However, applying AI and data mining techniques or algorithms successfully in these areas needs a concerted effort, fostering integrative research between experts ranging from diverse disciplines from data science to Artificial Intelligence. Successful application of security frameworks to enable meaningful, cost effective, personalize security service is a primary aim of engineers and researchers today. However realizing this goal requires effective understanding, application and amalgamation of AI and Data Mining and several other computing technologies to

Download File PDF Automated Threat Management Vectra Networks

deploy such system in an effective manner. This book provides state of the art approaches of artificial intelligence and data mining in these areas. It includes areas of detection, prediction, as well as future framework identification, development, building service systems and analytical aspects. In all these topics, applications of AI and data mining, such as artificial neural networks, fuzzy logic, genetic algorithm and hybrid mechanisms, are explained and explored. This book is aimed at the modeling and performance prediction of efficient security framework systems, bringing to light a new dimension in the theory and practice. This groundbreaking new volume presents these topics and trends, bridging the research gap on AI and data mining to enable wide-scale implementation. Whether for the veteran engineer or the student, this is a must-have for any library.

Artificial Intelligence in Banking

Artificial Intelligence in Society

The emergence of cloud computing, internet of things, mobile technologies, and social networking have created better-connected members of the public who are digitally linked with each other in real time. Establishing this two-way interaction between citizens and governments has thus become attractive and an expected feature of governments worldwide. Previously, federal and local governments relied on first-generation technologies to provide basic levels of automation and digitization. Now,

Download File PDF Automated Threat Management Vectra Networks

because of their desire to become more open, transparent, accountable, and connected, newer technologies including cloud computing, mobile networking, big data analytics, Web 2.0, and social media must be developed and utilized. Web 2.0 and Cloud Technologies for Implementing Connected Government is an essential reference source that presents various dimensions of connected government and connected e-governance visions as well as the latest emerging technologies. Offering development methodologies, practical examples, best practices, case studies, and the latest research, this book covers new strategies for implementing better-connected government models and the technologies that serve to establish these frameworks, including in-depth examinations of mobile technologies, automation, business intelligence, etc. as well as the various ethical and security issues surrounding the use and protection of data. This book is essential for federal, state, and local government officials; policymakers; civil servants; IT specialists; security analysts; academicians; researchers; and students.

PCMag.com is a leading authority on technology, delivering Labs-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

Microsoft Sentinel in Action

PC Mag

Architect, design, implement, and operate Microsoft Sentinel as the core of your security solutions

Download File PDF Automated Threat Management Vectra Networks

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

Download File PDF Automated Threat Management Vectra Networks

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.

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

AI in Cybersecurity

Cyber Criminology

Download File PDF Automated Threat Management Vectra Networks

Intelligent Computing Theories and Application

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."

This book presents a collection of state-of-the-art AI approaches to cybersecurity and cyberthreat intelligence, offering strategic defense mechanisms for malware, addressing cybercrime, and assessing vulnerabilities to yield proactive rather than reactive countermeasures. The current variety and scope of cybersecurity threats far exceed the capabilities of even the most skilled security professionals. In addition, analyzing yesterday's security incidents no longer enables experts to predict and prevent tomorrow's attacks, which necessitates approaches that go far beyond identifying known threats. Nevertheless, there are promising avenues: complex behavior matching can isolate threats based on the actions

Download File PDF Automated Threat Management Vectra Networks

taken, while machine learning can help detect anomalies, prevent malware infections, discover signs of illicit activities, and protect assets from hackers. In turn, knowledge representation enables automated reasoning over network data, helping achieve cybersituational awareness. Bringing together contributions by high-caliber experts, this book suggests new research directions in this critical and rapidly growing field.

Research Anthology on Cross-Disciplinary Designs and Applications of Automation

Canadian Library Handbook

ICCWS 2019 14th International Conference on Cyber Warfare and Security

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations.

Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Safety, Reliability and Risk Analysis. Theory, Methods and Applications contains the papers presented at the joint ESREL (European Safety and Reliability) and SRA-Europe (Society for Risk Analysis Europe) Conference (Valencia, Spain, 22-25 September 2008). The book covers a wide range of topics, including: Accident and

***Incident Investigation; Crisi
InfoWorld***

***Guide Des Bibliothèques Canadiennes
Transforming Cybersecurity: Using COBIT 5***

This two-volume set of LNCS 12836 and LNCS 12837 constitutes - in conjunction with the volume LNAI 12838 - the refereed proceedings of the 17th International Conference on Intelligent Computing, ICIC 2021, held in Shenzhen, China in August 2021. The 192 full papers of the three proceedings volumes were carefully reviewed and selected from 458 submissions. The ICIC theme unifies the picture of contemporary intelligent computing techniques as an integral concept that highlights the trends in advanced computational intelligence and bridges theoretical research with applications. The theme for this conference is Advanced Intelligent Computing Methodologies and Applications. The papers are organized in the following subsections: Artificial Intelligence in Real World Applications, Biomedical Informatics Theory and Methods, Complex Diseases Informatics, Gene Regulation Modeling and Analysis, Intelligent Computing in Computational Biology, and Protein Structure and Function Prediction. Cyber Defence in the Age of AI, Smart Societies and Augmented HumanitySpringer Nature Web 2.0 and Cloud Technologies for Implementing Connected Government Computerworld The Independent Guide to IBM-standard Personal Computing

Download File PDF Automated Threat Management Vectra Networks

The artificial intelligence (AI) landscape has evolved significantly from 1950 when Alan Turing first posed the question of whether machines can think. Today, AI is transforming societies and economies. It promises to generate productivity gains, improve well-being and help address global challenges, such as climate change, resource scarcity and health crises.

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

Data Sources

Safety, Reliability and Risk Analysis

Cyber Defence in the Age of AI, Smart Societies and

Augmented Humanity

Cyber Risk Leaders: Global C-Suite Insights - Leadership and Influence in the Cyber Age, by Shamane Tan - explores the art of communicating with executives, tips on navigating through corporate challenges, and reveals what the C-Suite looks for in professional partners. For those who are interested in learning from top industry leaders, or an aspiring or current CISO, this book is gold for your career. It's the go-to book and your CISO kit for the season. This book provides a comprehensive overview of the current and emerging challenges of cyber criminology, victimization and profiling. It is a compilation of the outcomes of the collaboration between researchers and practitioners in the cyber criminology field, IT law and security field. As Governments, corporations, security firms, and individuals look to tomorrow's cyber security challenges, this book provides a reference point for experts and forward-thinking analysts at a time when the debate over how we plan for the cyber-security of the future has become a major concern. Many criminological perspectives define crime in terms of social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition has allowed crime to be characterised, and crime prevention, mapping and measurement methods to be tailored to specific target audiences. However, this characterisation cannot be carried over to cybercrime, because the environment in which such crime is committed cannot be pinpointed to a geographical location, or distinctive social or cultural groups. Due to the rapid changes in technology, cyber criminals' behaviour has become dynamic, making it necessary to reclassify the typology being currently used. Essentially, cyber criminals' behaviour is evolving over

Download File PDF Automated Threat Management Vectra Networks

time as they learn from their actions and others' experiences, and enhance their skills. The offender signature, which is a repetitive ritualistic behaviour that offenders often display at the crime scene, provides law enforcement agencies an appropriate profiling tool and offers investigators the opportunity to understand the motivations that perpetrate such crimes. This has helped researchers classify the type of perpetrator being sought. This book offers readers insights into the psychology of cyber criminals, and understanding and analysing their motives and the methodologies they adopt. With an understanding of these motives, researchers, governments and practitioners can take effective measures to tackle cybercrime and reduce victimization.

Datapro Reports on Data Communications

*17th International Conference, ICIC 2021, Shenzhen, China, August 12-15, 2021, Proceedings, Part III
ICCWS 2019*

Learn how to set up, configure, and use Microsoft Sentinel to provide security incident and event management services for your multi-cloud environment
Key Features Collect, normalize, and analyze security information from multiple data sources
Integrate AI, machine learning, built-in and custom threat analyses, and automation to build optimal security solutions
Detect and investigate possible security breaches to tackle complex and advanced cyber threats
Book Description Microsoft Sentinel is a security information and event management (SIEM) tool developed by Microsoft that helps you integrate cloud security and artificial intelligence (AI). This book will teach you how to implement Microsoft Sentinel and understand how it can help detect security incidents in your environment with integrated AI, threat analysis, and built-in and community-driven logic. The first part of this book will introduce you to Microsoft Sentinel and Log Analytics, then move on to understanding data collection and management, as well as how to create effective Microsoft Sentinel queries to detect anomalous

Download File PDF Automated Threat Management Vectra Networks

behaviors and activity patterns. The next part will focus on useful features, such as entity behavior analytics and Microsoft Sentinel playbooks, along with exploring the new bi-directional connector for ServiceNow. In the next part, you'll be learning how to develop solutions that automate responses needed to handle security incidents and find out more about the latest developments in security, techniques to enhance your cloud security architecture, and explore how you can contribute to the security community. By the end of this book, you'll have learned how to implement Microsoft Sentinel to fit your needs and protect your environment from cyber threats and other security issues. What you will learn

Implement Log Analytics and enable Microsoft Sentinel and data ingestion from multiple sources

Tackle Kusto Query Language (KQL) coding

Discover how to carry out threat hunting activities in Microsoft Sentinel

Connect Microsoft Sentinel to ServiceNow for automated ticketing

Find out how to detect threats and create automated responses for immediate resolution

Use triggers and actions with Microsoft Sentinel playbooks to perform automations

Who this book is for

You'll get the most out of this book if you have a good grasp on other Microsoft security products and Azure, and are now looking to expand your knowledge to incorporate Microsoft Sentinel. Security experts who use an alternative SIEM tool and want to adopt Microsoft Sentinel as an additional or a replacement service will also find this book useful.

Throughout human history, technological advancements have been made for the ease of human labor. With our most recent advancements, it has been the work of scholars to discover ways for machines to take over a large part of this labor and reduce human intervention. These advancements may become essential processes to nearly every industry. It is essential to be knowledgeable about automation so that it may be applied. Research Anthology on Cross-Disciplinary Designs and Applications of Automation is a comprehensive resource on the emerging designs and application of automation. This collection features a number of authors spanning multiple disciplines such as home automation, healthcare automation,

Download File PDF Automated Threat Management Vectra Networks

government automation, and more. Covering topics such as human-machine interaction, trust calibration, and sensors, this research anthology is an excellent resource for technologists, IT specialists, computer engineers, systems and software engineers, manufacturers, engineers, government officials, professors, students, healthcare administration, managers, CEOs, researchers, and academicians.

PC Magazine

Artificial Intelligence and Data Mining Approaches in Security Frameworks

Newsletter