microsoft sentinel workbooks

microsoft sentinel workbooks are versatile tools designed to enhance the monitoring and analysis capabilities of Microsoft Sentinel, enabling users to visualize and interpret vast amounts of security data effectively. These workbooks allow security teams to create customized dashboards and reports that provide insights into security incidents, alerts, and system performance. In this article, we will explore the features and capabilities of Microsoft Sentinel workbooks, how to create and customize them, the benefits they offer for security monitoring, and best practices for leveraging them effectively. By the end of this article, you will have a comprehensive understanding of Microsoft Sentinel workbooks and how they can enhance your security operations.

Understanding Microsoft Sentinel Workbooks

Microsoft Sentinel workbooks are interactive reports that allow users to visualize and analyze security data collected by Microsoft Sentinel. They act as a powerful interface for security professionals to gain insights from security logs, alerts, and incidents. Workbooks are built on top of Azure Monitor Workbooks, which means they can leverage various Azure data sources and visualization tools. This integration allows users to create comprehensive reports that can include graphs, tables, and charts, making complex data easier to interpret.

Workbooks are customizable, meaning users can tailor them to fit specific operational needs, making them an essential part of any security operations center (SOC). Microsoft Sentinel workbooks can be used for a variety of purposes, including tracking incident response metrics, analyzing trends in security data, and providing compliance reports. Their flexibility makes them suitable for various industries, including finance, healthcare, and technology.

Key Features of Microsoft Sentinel Workbooks

Microsoft Sentinel workbooks come equipped with several key features that enhance their functionality and usability. Understanding these features can help organizations maximize their effectiveness in monitoring and responding to security incidents.

Interactive Visualizations

One of the standout features of Microsoft Sentinel workbooks is their ability to create interactive visualizations. Users can choose from a variety of visualization types, including pie charts, bar graphs, and time charts. These visualizations allow users to drill down into specific data points for a more granular analysis.

Custom Queries

Workbooks allow users to create custom queries using Kusto Query Language (KQL), enabling them to filter and analyze data tailored to their needs. This flexibility ensures that users can focus on the most relevant information, whether it’s related to specific incidents, asset types, or timeframes.

Integration with Azure Services

Microsoft Sentinel workbooks seamlessly integrate with other Azure services, allowing for enhanced data collection and reporting capabilities. This integration can include importing data from Azure Security Center, Azure Active Directory logs, and various third-party security solutions.

Creating and Customizing Microsoft Sentinel Workbooks

Creating and customizing Microsoft Sentinel workbooks involves several steps that allow users to tailor the workbook to meet their specific needs. The process is straightforward, making it accessible for security professionals of varying skill levels.

Step-by-Step Creation Process

1. **Access the Microsoft Sentinel Portal:** Begin by logging into the Microsoft Sentinel portal and navigating to the "Workbooks" section.

2. **Create a New Workbook:** Click on "Add new" to start a new workbook. You can choose from pre-built templates or start from scratch.

3. **Define Data Sources:** Select the data sources you want to include in the workbook.

These can be logs from various Azure services or external data sources.

4. **Design the Layout:** Use the drag-and-drop interface to arrange the visualizations, tables, and text boxes as needed. Customize the layout to prioritize the most important information.

5. **Save and Share:** Once the workbook is complete, save it and share it with team members or stakeholders for collaborative analysis.

Customizing Workbooks for Specific Needs

Customizing workbooks is crucial for ensuring that they meet the specific requirements of an organization. Users can adjust the following elements:

- **Visualization Types:** Choose different types of charts and tables based on the data being analyzed.
- **Data Filtering:** Implement filters to display only relevant data, which can enhance clarity and focus.
- **Interactive Elements:** Add interactive elements that allow users to drill down into specifics, making the workbook more engaging.

Benefits of Using Microsoft Sentinel Workbooks

Utilizing Microsoft Sentinel workbooks provides numerous advantages that can significantly enhance an organization's security posture. These benefits are not only operational but also strategic in nature.

Enhanced Visibility and Insights

Workbooks provide enhanced visibility into security metrics and trends, enabling security teams to identify potential threats quickly. By visualizing data in an intuitive format, teams can make informed decisions based on real-time information.

Improved Incident Response

With the ability to track incidents, alerts, and response times, workbooks facilitate improved incident response. Security teams can analyze past incidents to refine future response strategies, thereby increasing overall efficiency and effectiveness.

Streamlined Reporting

Microsoft Sentinel workbooks simplify the reporting process by allowing users to generate comprehensive reports quickly. These reports can be tailored for various stakeholders, from technical teams to executive leadership, ensuring that everyone has access to the information they need.

Best Practices for Microsoft Sentinel Workbooks

To maximize the effectiveness of Microsoft Sentinel workbooks, organizations should follow best practices that enhance usability and relevance.

Regular Updates and Maintenance

It is essential to regularly update and maintain workbooks to ensure they reflect the current security landscape and organizational needs. This includes revisiting queries, data sources, and visualizations to keep them relevant.

Involve Stakeholders

Engaging stakeholders during the creation and customization of workbooks can enhance their effectiveness. By understanding the needs of different users, teams can create workbooks that serve varied purposes across the organization.

Training and Documentation

Providing training and comprehensive documentation for users can increase adoption and effective use of workbooks. This ensures that all team members can leverage the full capabilities of Microsoft Sentinel workbooks.

Conclusion

Microsoft Sentinel workbooks are powerful tools for security monitoring and analysis, offering customized dashboards that enhance visibility into security data. By understanding their features, learning how to create and customize them, and recognizing their benefits, organizations can significantly improve their security operations. Following best practices will ensure that these workbooks remain effective and relevant, ultimately leading to a more robust security posture. Embracing Microsoft Sentinel workbooks is a strategic move for any organization looking to enhance its security capabilities.

Q: What are Microsoft Sentinel workbooks?

A: Microsoft Sentinel workbooks are customizable reports and dashboards that allow users to visualize and analyze security data collected by Microsoft Sentinel. They enable security teams to gain insights into incidents, alerts, and system performance.

Q: How do I create a Microsoft Sentinel workbook?

A: To create a Microsoft Sentinel workbook, access the Microsoft Sentinel portal, select the "Workbooks" section, click "Add new," define your data sources, design the layout, and then save and share the workbook.

Q: What types of visualizations can I create with Microsoft Sentinel workbooks?

A: You can create various types of visualizations in Microsoft Sentinel workbooks, including pie charts, bar graphs, line charts, and tables, to effectively present your security data.

Q: Can I use custom queries in Microsoft Sentinel workbooks?

A: Yes, Microsoft Sentinel workbooks allow users to create custom queries using Kusto Query Language (KQL) to filter and analyze security data according to specific needs.

Q: What are the benefits of using Microsoft Sentinel workbooks?

A: The benefits include enhanced visibility into security metrics, improved incident response capabilities, and streamlined reporting processes, making them essential for effective security operations.

Q: How often should I update my Microsoft Sentinel workbooks?

A: It is recommended to regularly update your Microsoft Sentinel workbooks to ensure they reflect the current security landscape and organizational needs, revisiting queries, data sources, and visualizations as necessary.

Q: Can Microsoft Sentinel workbooks integrate with other Azure services?

A: Yes, Microsoft Sentinel workbooks can integrate with various Azure services, allowing

for enhanced data collection and reporting capabilities from sources like Azure Security Center and Azure Active Directory.

Q: What is the best way to share Microsoft Sentinel workbooks with my team?

A: After creating a workbook, you can save it and use the sharing options available within the Microsoft Sentinel portal to share it with team members or stakeholders for collaborative analysis.

Q: Are there any templates available for Microsoft Sentinel workbooks?

A: Yes, Microsoft Sentinel provides pre-built templates for workbooks that can help users get started quickly. These templates can be customized to meet specific organizational needs.

Q: How can I ensure that my team effectively uses Microsoft Sentinel workbooks?

A: Providing training and comprehensive documentation for users, involving stakeholders in the customization process, and regularly maintaining the workbooks can ensure effective usage across your team.

Microsoft Sentinel Workbooks

microsoft sentinel workbooks: Microsoft Sentinel in Action Richard Diver, Gary Bushey, John Perkins, 2022-02-10 Learn how to set up, configure, and use Microsoft Sentinel to provide security incident and event management services for your multi-cloud environment Key FeaturesCollect, normalize, and analyze security information from multiple data sourcesIntegrate AI, machine learning, built-in and custom threat analyses, and automation to build optimal security solutionsDetect and investigate possible security breaches to tackle complex and advanced cyber threatsBook 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 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 learnImplement Log Analytics and enable Microsoft Sentinel and data ingestion from multiple sourcesTackle Kusto Query Language (KQL) codingDiscover how to carry out threat hunting activities in Microsoft SentinelConnect Microsoft Sentinel to ServiceNow for automated ticketingFind out how to detect threats and create automated responses for immediate resolutionUse triggers and actions with Microsoft Sentinel playbooks to perform automationsWho 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.

microsoft sentinel workbooks: Microsoft Azure Sentinel Yuri Diogenes, Nicholas DiCola, Tiander Turpijn, 2022-08-05 Build next-generation security operations with Microsoft Sentinel Microsoft Sentinel is the scalable, cloud-native, security information and event management (SIEM) solution for automating and streamlining threat identification and response across your enterprise. Now, three leading experts guide you step-by-step through planning, deployment, and operations, helping you use Microsoft Sentinel to escape the complexity and scalability challenges of traditional solutions. Fully updated for the latest enhancements, this edition introduces new use cases for investigation, hunting, automation, and orchestration across your enterprise and all your clouds. The authors clearly introduce each service, concisely explain all new concepts, and present proven best practices for maximizing Microsoft Sentinel's value throughout security operations. Three of Microsoft's leading security operations experts show how to: Review emerging challenges that make better cyberdefense an urgent priority See how Microsoft Sentinel responds by unifying alert detection, threat visibility, proactive hunting, and threat response Explore components, architecture, design, and initial configuration Ingest alerts and raw logs from all sources you need to monitor Define and validate rules that prevent alert fatigue Use threat intelligence, machine learning, and automation to triage issues and focus on high-value tasks Add context with User and Entity Behavior Analytics (UEBA) and Watchlists Hunt sophisticated new threats to disrupt cyber kill chains before you're exploited Enrich incident management and threat hunting with Jupyter notebooks Use Playbooks to automate more incident handling and investigation tasks Create visualizations to spot trends, clarify relationships, and speed decisions Simplify integration with point-and-click data connectors that provide normalization, detection rules, queries, and Workbooks About This Book For cybersecurity analysts, security administrators, threat hunters, support professionals, engineers, and other IT professionals concerned with security operations For both Microsoft Azure and non-Azure users at all levels of experience

microsoft sentinel workbooks: Exam Ref AZ-500 Microsoft Azure Security Technologies Yuri Diogenes, Orin Thomas, 2022-04-19 Prepare for Microsoft Exam AZ-500: Demonstrate your real-world knowledge of Microsoft Azure security, including tools and techniques for protecting identity, access, platforms, data, and applications, and for effectively managing security operations. Designed for professionals with Azure security experience, this Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified: Azure Security Engineer Associate level. Focus on the expertise measured by these objectives: Manage identity and access Implement platform protection Manage security operations Secure data and applications This Microsoft Exam Ref: Organizes its coverage by exam objectives Features strategic, what-if scenarios to challenge you Assumes you have expertise implementing security controls and threat protection,

managing identity and access, and protecting assets in cloud and hybrid environments About the Exam Exam AZ-500 focuses on the knowledge needed to manage Azure Active Directory identities; configure secure access with Azure AD; manage application access and access control; implement advanced network security; configure advanced security for compute; monitor security with Azure Monitor, Azure Firewall manager, Azure Security Center, Azure Defender, and Azure Sentinel; configure security policies; configure security for storage and databases; and configure and manage Key Vault. About Microsoft Certification Passing this exam fulfills your requirements for the Microsoft Certified: Azure Security Engineer Associate credential, demonstrating your expertise as an Azure Security Engineer capable of maintaining security posture, identifying and remediating vulnerabilities, implementing threat protection, and responding to incident escalations as part of a cloud-based management and security team. See full details at: microsoft.com/learn

microsoft sentinel workbooks: Microsoft Security Operations Analyst Associate (SC-200) Certification Guide Aditya Katira, 2025-06-12 TAGLINE Detect, Investigate, and Respond to Threats with Microsoft tools KEY FEATURES ● In-depth coverage of Microsoft SC 200 Certification to secure identities, endpoints, and cloud workloads across hybrid environments. ● Hands-on guidance with KQL, threat hunting, and automation to simulate real-world security operations. ● Exclusive insights on AI-powered security using Microsoft Copilot and emerging trends shaping the future of SOC operations. DESCRIPTION The Microsoft Security Operations Analyst certification (SC-200) is a vital credential for anyone aiming to excel in modern cybersecurity roles. The Microsoft Security Operations Analyst Associate (SC-200) Certification Guide is your companion for mastering the skills and tools needed to pass the exam and thrive as a Security Operations Analyst in Microsoft environments. Through in-depth coverage of Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender, you'll learn to detect, investigate, and respond to threats across hybrid and cloud infrastructures. With a focus on real-world use cases, this book walks you through key concepts such as threat mitigation, incident response, and security monitoring—all aligned with the latest SC-200 objectives. You'll gain hands-on experience configuring Microsoft's security tools, writing queries using Kusto Query Language (KQL), creating custom detection rules, and automating responses for streamlined SOC operations. Each chapter builds your expertise through practical examples and exercises, helping bridge the gap between certification prep and operational readiness. Whether you're looking to boost your cybersecurity career or strengthen your organization's defenses, this guide provides the knowledge and exam confidence you need. Take the next step to become a Microsoft Security Operations Analyst expert. WHAT WILL YOU LEARN ● Configure and operationalize Microsoft Defender for Identity, Endpoint, and Cloud to protect users and resources. ● Leverage Microsoft Copilot for Security to enhance investigation and response using generative AI capabilities. ● Implement Data Loss Prevention (DLP), Insider Risk Management, and eDiscovery for robust information protection. ● Use Kusto Query Language (KQL) to analyze logs, hunt threats, and develop custom queries. ● Enhance security visibility through effective use of data connectors and threat intelligence feeds in Microsoft Sentinel. ● Automate detection and response workflows using Sentinel's playbooks, analytics rules, and notebooks for advanced threat management. WHO IS THIS BOOK FOR? This book is ideal for security analysts, system administrators, and IT professionals preparing for the SC-200: Microsoft Security Operations Analyst certification. It is also valuable for those looking to deepen their expertise in Microsoft security solutions. A working knowledge of Microsoft Azure, Microsoft 365, and core cybersecurity concepts is recommended to get the most from this guide. TABLE OF CONTENTS 1. Microsoft Defender Identity Endpoint Cloud and More 2. Microsoft Copilot for Security with AI Assistance 3. Mastering Data Protection with Data Loss Prevention, Insider Risk, and Content Search 4. Securing Endpoint Deployment Management and Investigation 5. Managing Security Posture Across Platforms 6. KQL Mastery for Querying Analyzing and Working with Security Data 7. Optimizing Security Operations with Log Management Watchlists and Threat Intelligence 8. Expanding Security Visibility with Data Connectors in Microsoft Sentinel 9. Tactical Threat Management with Detection Automation and Response 10. Decoding Threat

Hunting by Leveraging Search Jobs and Notebooks 11. Future Trends in Security Operations Index

microsoft sentinel workbooks: *Microsoft Security Operations Analyst Associate (SC-200) Certification Guide: Master Microsoft Security Operations, Threat Response, and Cloud Defense to ace the SC-200 Certification Exam* Aditya Katira, 2025-06-12 Detect, Investigate, and Respond to Threats with Microsoft tools Key Features● In-depth coverage of Microsoft SC 200 Certification to secure identities, endpoints, and cloud workloads across hybrid environments.● Hands-on guidance with KQL, threat hunting, and automation to simulate real-world security operations.● Exclusive insights on AI-powered security using Microsoft Copilot and emerging trends shaping the future of SOC operations. Book DescriptionThe Microsoft Security Operations Analyst certification (SC-200) is a vital credential for anyone aiming to excel in modern cybersecurity roles. The Microsoft Security Operations Analyst Associate (SC-200) Certification Guide is your companion for mastering the skills and tools needed to pass the exam and thrive as a Security Operations Analyst in Microsoft environments. Through in-depth coverage of Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender, you'll learn to detect, investigate, and respond to threats across hybrid and cloud infrastructures. With a focus on real-world use cases, this book walks you through key concepts such as threat mitigation, incident response, and security monitoring—all aligned with the latest SC-200 objectives. You'll gain hands-on experience configuring Microsoft's security tools, writing queries using Kusto Query Language (KQL), creating custom detection rules, and automating responses for streamlined SOC operations. Each chapter builds your expertise through practical examples and exercises, helping bridge the gap between certification prep and operational readiness. Whether you're looking to boost your cybersecurity career or strengthen your organization's defenses, this guide provides the knowledge and exam confidence you need. Take the next step to become a Microsoft Security Operations Analyst expert. What you will learn● Configure and operationalize Microsoft Defender for Identity, Endpoint, and Cloud to protect users and resources.● Leverage Microsoft Copilot for Security to enhance investigation and response using generative AI capabilities.● Implement Data Loss Prevention (DLP), Insider Risk Management, and eDiscovery for robust information protection.● Use Kusto Query Language (KQL) to analyze logs, hunt threats, and develop custom queries.● Enhance security visibility through effective use of data connectors and threat intelligence feeds in Microsoft Sentinel.● Automate detection and response workflows using Sentinel's playbooks, analytics rules, and notebooks for advanced threat management. Table of Contents1. Microsoft Defender Identity Endpoint Cloud and More2. Microsoft Copilot for Security with AI Assistance3. Mastering Data Protection with Data Loss Prevention, Insider Risk, and Content Search4. Securing Endpoint Deployment Management and Investigation5. Managing Security Posture Across Platforms6. KQL Mastery for Querying Analyzing and Working with Security Data7. Optimizing Security Operations with Log Management Watchlists and Threat Intelligence8. Expanding Security Visibility with Data Connectors in Microsoft Sentinel9. Tactical Threat Management with Detection Automation and Response10. Decoding Threat Hunting by Leveraging Search Jobs and Notebooks11. Future Trends in Security Operations Index

microsoft sentinel workbooks: Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals Yuri Diogenes, Nicholas DiCola, Kevin McKinnerney, Mark Morowczynski, 2021-11-22 Prepare for Microsoft Exam SC-900 and help demonstrate your real-world knowledge of the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services. Designed for business stakeholders, new and existing IT professionals, functional consultants, and students, this Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified: Security, Compliance, and Identity Fundamentals level. Focus on the expertise measured by these objectives: • Describe the concepts of security, compliance, and identity • Describe the capabilities of Microsoft identity and access management solutions • Describe the capabilities of Microsoft security solutions • Describe the capabilities of Microsoft compliance solutions This Microsoft Exam Ref: • Organizes its coverage by exam objectives • Features strategic, what-if scenarios to challenge you • Assumes you are a business user, stakeholder, consultant, professional, or student who wants to create holistic,

end-to-end solutions with Microsoft security, compliance, and identity technologies About the Exam Exam SC-900 focuses on knowledge needed to describe: security and compliance concepts and methods; identity concepts; Azure AD identity services/types, authentication, access management, identity protection, and governance; Azure, Azure Sentinel, and Microsoft 365 security management; Microsoft 365 Defender threat protection and Intune endpoint security; Microsoft 365 compliance management, information protection, governance, insider risk, eDiscovery, and audit capabilities; and Azure resource governance. About Microsoft Certification Passing this exam fulfills your requirements for the Microsoft Certified: Security, Compliance, and Identity Fundamentals certification, helping to demonstrate your understanding of the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services. With this certification, you can move on to earn more advanced related Associate-level role-based certifications. See full details at: microsoft.com/learn

microsoft sentinel workbooks: Defending APIs Colin Domoney, 2024-02-09 Get up to speed with API security using this comprehensive guide full of best practices for building safer and secure APIs Key Features Develop a profound understanding of the inner workings of APIs with a sharp focus on security Learn the tools and techniques employed by API security testers and hackers, establishing your own hacking laboratory Master the art of building robust APIs with shift-left and shield-right approaches, spanning the API lifecycle Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionAlong with the exponential growth of API adoption comes a rise in security concerns about their implementation and inherent vulnerabilities. For those seeking comprehensive insights into building, deploying, and managing APIs as the first line of cyber defense, this book offers invaluable guidance. Written by a seasoned DevSecOps expert, Defending APIs addresses the imperative task of API security with innovative approaches and techniques designed to combat API-specific safety challenges. The initial chapters are dedicated to API building blocks, hacking APIs by exploiting vulnerabilities, and case studies of recent breaches, while the subsequent sections of the book focus on building the skills necessary for securing APIs in real-world scenarios. Guided by clear step-by-step instructions, you'll explore offensive techniques for testing vulnerabilities, attacking, and exploiting APIs. Transitioning to defensive techniques, the book equips you with effective methods to guard against common attacks. There are plenty of case studies peppered throughout the book to help you apply the techniques you're learning in practice, complemented by in-depth insights and a wealth of best practices for building better APIs from the ground up. By the end of this book, you'll have the expertise to develop secure APIs and test them against various cyber threats targeting APIs.What you will learn Explore the core elements of APIs and their collaborative role in API development Understand the OWASP API Security Top 10, dissecting the root causes of API vulnerabilities Obtain insights into high-profile API security breaches with practical examples and in-depth analysis Use API attacking techniques adversaries use to attack APIs to enhance your defensive strategies Employ shield-right security approaches such as API gateways and firewalls Defend against common API vulnerabilities across several frameworks and languages, such as .NET, Python, and Java Who this book is for This book is for application security engineers, blue teamers, and security professionals looking forward to building an application security program targeting API security. For red teamers and pentesters, it provides insights into exploiting API vulnerabilities. API developers will benefit understanding, anticipating, and defending against potential threats and attacks on their APIs. While basic knowledge of software and security is required to understand the attack vectors and defensive techniques explained in the book, a thorough understanding of API security is all you need to get started.

microsoft sentinel workbooks: Azure Security Bojan Magusic, 2024-01-09 Azure Security is a practical guide to the native security services of Microsoft Azure written for software and security engineers building and securing Azure applications. Readers will learn how to use Azure tools to improve your systems security and get an insider's perspective on establishing a DevSecOps program using the capabilities of Microsoft Defender for Cloud.

microsoft sentinel workbooks: Microsoft Security, Compliance, and Identity

Fundamentals Exam Ref SC-900 Dwayne Natwick, Sonia Cuff, 2022-05-26 Understand the fundamentals of security, compliance, and identity solutions across Microsoft Azure, Microsoft 365, and related cloud-based Microsoft services Key Features • Grasp Azure AD services and identity principles, secure authentication, and access management • Understand threat protection with Microsoft 365 Defender and Microsoft Defender for Cloud security management • Learn about security capabilities in Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Intune Book Description Cloud technologies have made building a defense-in-depth security strategy of paramount importance. Without proper planning and discipline in deploying the security posture across Microsoft 365 and Azure, you are compromising your infrastructure and data. Microsoft Security, Compliance, and Identity Fundamentals is a comprehensive guide that covers all of the exam objectives for the SC-900 exam while walking you through the core security services available for Microsoft 365 and Azure. This book starts by simplifying the concepts of security, compliance, and identity before helping you get to grips with Azure Active Directory, covering the capabilities of Microsoft's identity and access management (IAM) solutions. You'll then advance to compliance center, information protection, and governance in Microsoft 365. You'll find out all you need to know about the services available within Azure and Microsoft 365 for building a defense-in-depth security posture, and finally become familiar with Microsoft's compliance monitoring capabilities. By the end of the book, you'll have gained the knowledge you need to take the SC-900 certification exam and implement solutions in real-life scenarios. What you will learn • Become well-versed with security, compliance, and identity principles • Explore the authentication, access control, and identity management capabilities of Azure Active Directory • Understand the identity protection and governance aspects of Azure and Microsoft 365 • Get to grips with the basic security capabilities for networks, VMs, and data • Discover security management through Microsoft Defender for Cloud • Work with Microsoft Sentinel and Microsoft 365 Defender • Deal with compliance, governance, and risk in Microsoft 365 and Azure Who this book is for This book is for cloud security engineers, Microsoft 365 administrators, Azure administrators, and anyone in between who wants to get up to speed with the security, compliance, and identity fundamentals to achieve the SC-900 certification. A basic understanding of the fundamental services within Microsoft 365 and Azure will be helpful but not essential. Table of Contents • Preparing for Your Microsoft Exam • Describing Security Methodologies • Understanding Key Security Concepts • Key Microsoft Security and Compliance Principles • Defining Identity Principles/Concepts and the Identity Services within Azure AD • Describing the Authentication and Access Management Capabilities of Azure AD • Describing the Identity Protection and Governance Capabilities of Azure AD • Describing Basic Security Services and Management Capabilities in Azure • Describing Security Management and Capabilities of Azure • Describing Threat Protection with Microsoft 365 Defender • Describing the Security Capabilities of Microsoft Sentinel • Describing Security Management and the Endpoint Security Capabilities of Microsoft 365 • Compliance Management Capabilities in Microsoft • Describing Information Protection and Governance Capabilities of Microsoft 365 (N.B. Please use the Look Inside option to see further chapters)

microsoft sentinel workbooks: Microsoft Azure Security Technologies (AZ-500) - A Certification Guide Jayant Sharma, 2021-10-14 With Azure security, you can build a prosperous career in IT security. KEY FEATURES ● In-detail practical steps to fully grasp Azure Security concepts. ● Wide coverage of Azure Architecture, Azure Security services, and Azure Security implementation techniques. ● Covers multiple topics from other Azure certifications (AZ-303, AZ-304, and SC series). DESCRIPTION 'Microsoft Azure Security Technologies (AZ-500) - A Certification Guide' is a certification guide that helps IT professionals to start their careers as Azure Security Specialists by clearing the AZ-500 certification and proving their knowledge of Azure security services. Authored by an Azure security professional, this book takes readers through a series of steps to gain a deeper insight into Azure security services. This book will help readers to understand key concepts of the Azure AD architecture and various methods of hybrid authentication. It will help readers to use Azure AD security solutions like Azure MFA, Conditional Access, and PIM.

It will help readers to maintain various industry standards for an Azure environment through Azure Policies and Azure Blueprints. This book will also help to build a secure Azure network using Azure VPN, Azure Firewall, Azure Front Door, Azure WAF, and other services. It will provide readers with a clear understanding of various security services, including Azure Key vault, Update management, Microsoft Endpoint Protection, Azure Security Center, and Azure Sentinel in detail. This book will facilitate the improvement of readers' abilities with Azure Security services to sprint to a rewarding career. WHAT YOU WILL LEARN ● Configuring secure authentication and authorization for Azure AD identities. ● Advanced security configuration for Azure compute and network services. ● Hosting and authorizing secure applications in Azure. ● Best practices to secure Azure SQL and storage services. ● Monitoring Azure services through Azure monitor, security center, and Sentinel. ● Designing and maintaining a secure Azure IT infrastructure. WHO THIS BOOK IS FOR This book is for security engineers who want to enhance their career growth in implementing security controls, maintaining the security posture, managing identity and access, and protecting data, applications, and networks of Microsoft Azure. Intermediate-level knowledge of Azure terminology, concepts, networking, storage, and virtualization is required. TABLE OF CONTENTS 1. Managing Azure AD Identities and Application Access 2. Configuring Secure Access by Using Azure Active Directory 3. Managing Azure Access Control 4. Implementing Advance Network Security 5. Configuring Advance Security for Compute 6. Configuring Container Security 7. Monitoring Security by Using Azure Monitor 8. Monitoring Security by Using Azure Security Center 9. Monitoring Security by Using Azure Sentinel 10. Configuring Security for Azure Storage 11. Configuring Security for Azure SQL Databases

microsoft sentinel workbooks: *Microsoft Identity and Access Administrator Exam Guide* Dwayne Natwick, Shannon Kuehn, 2022-03-10 This certification guide focuses on identity solutions and strategies that will help you prepare for Microsoft Identity and Access Administrator certification, while enabling you to implement what you've learned in real-world scenarios Key FeaturesDesign, implement, and operate identity and access management systems using Azure ADProvide secure authentication and authorization access to enterprise applicationsImplement access and authentication for cloud-only and hybrid infrastructuresBook Description Cloud technologies have made identity and access the new control plane for securing data. Without proper planning and discipline in deploying, monitoring, and managing identity and access for users, administrators, and guests, you may be compromising your infrastructure and data. This book is a preparation guide that covers all the objectives of the SC-300 exam, while teaching you about the identity and access services that are available from Microsoft and preparing you for real-world challenges. The book starts with an overview of the SC-300 exam and helps you understand identity and access management. As you progress to the implementation of IAM solutions, you'll learn to deploy secure identity and access within Microsoft 365 and Azure Active Directory. The book will take you from legacy on-premises identity solutions to modern and password-less authentication solutions that provide high-level security for identity and access. You'll focus on implementing access and authentication for cloud-only and hybrid infrastructures as well as understand how to protect them using the principles of zero trust. The book also features mock tests toward the end to help you prepare effectively for the exam. By the end of this book, you'll have learned how to plan, deploy, and manage identity and access solutions for Microsoft and hybrid infrastructures. What you will learnUnderstand core exam objectives to pass the SC-300 examImplement an identity management solution with MS Azure ADManage identity with multi-factor authentication (MFA), conditional access, and identity protectionDesign, implement, and monitor the integration of enterprise apps for Single Sign-On (SSO)Add apps to your identity and access solution with app registrationDesign and implement identity governance for your identity solutionWho this book is for This book is for cloud security engineers, Microsoft 365 administrators, Microsoft 365 users, Microsoft 365 identity administrators, and anyone who wants to learn identity and access management and gain SC-300 certification. You should have a basic understanding of the fundamental services within Microsoft 365 and Azure Active Directory before getting started with

this Microsoft book.

microsoft sentinel workbooks: *Microsoft Teams Administration Cookbook* Fabrizio Volpe, 2023-08-22 Microsoft Teams is used in hundreds of thousands of organizations to help keep remote and hybrid workplaces with dispersed workforces running smoothly. But while Microsoft Teams can seem easy for the user, Teams administrators must stay on top of a wide range of topics, including device administration techniques, quality benchmarks, and security and compliance measures. With this handy cookbook, author Fabrizio Volpe provides a clear, concise overview of administrative tasks in Teams-along with step-by-step recipes to help you solve many of the common problems that system administrators, project managers, solution architects, and IT consultants may face when configuring, implementing, and managing Microsoft Teams. Think of this book as a detailed, immensely practical cheat sheet for Microsoft Teams administrators. Recipes in the book will show you how to: Apply Teams best practices, compliance, and security Automate administrative tasks Successfully deploy Teams Implement Teams collaboration Deploy and manage Microsoft Teams Rooms Leverage the monitoring, productivity, and accessibility features Foresee roadblocks in migrations to Teams and Teams Voice Optimize Teams on virtual machines

microsoft sentinel workbooks: Security Orchestration, Automation, and Response for Security Analysts Benjamin Kovacevic, Nicholas DiCola, 2023-07-21 Become a security automation expert and build solutions that save time while making your organization more secure Key Features What's inside An exploration of the SOAR platform's full features to streamline your security operations Lots of automation techniques to improve your investigative ability Actionable advice on how to leverage the capabilities of SOAR technologies such as incident management and automation to improve security posture Book Description What your journey will look like With the help of this expert-led book, you'll become well versed with SOAR, acquire new skills, and make your organization's security posture more robust. You'll start with a refresher on the importance of understanding cyber security, diving into why traditional tools are no longer helpful and how SOAR can help. Next, you'll learn how SOAR works and what its benefits are, including optimized threat intelligence, incident response, and utilizing threat hunting in investigations. You'll also get to grips with advanced automated scenarios and explore useful tools such as Microsoft Sentinel, Splunk SOAR, and Google Chronicle SOAR. The final portion of this book will guide you through best practices and case studies that you can implement in real-world scenarios. By the end of this book, you will be able to successfully automate security tasks, overcome challenges, and stay ahead of threats. What you will learn Reap the general benefits of using the SOAR platform Transform manual investigations into automated scenarios Learn how to manage known false positives and low-severity incidents for faster resolution Explore tips and tricks using various Microsoft Sentinel playbook actions Get an overview of tools such as Palo Alto XSOAR, Microsoft Sentinel, and Splunk SOAR Who this book is for You'll get the most out of this book if You're a junior SOC engineer, junior SOC analyst, a DevSecOps professional, or anyone working in the security ecosystem who wants to upskill toward automating security tasks You often feel overwhelmed with security events and incidents You have general knowledge of SIEM and SOAR, which is a prerequisite You're a beginner, in which case this book will give you a head start You've been working in the field for a while, in which case you'll add new tools to your arsenal

microsoft sentinel workbooks: Exam Ref SC-200 Microsoft Security Operations Analyst Yuri Diogenes, Jake Mowrer, Sarah Young, 2021-08-31 Prepare for Microsoft Exam SC-200—and help demonstrate your real-world mastery of skills and knowledge required to work with stakeholders to secure IT systems, and to rapidly remediate active attacks. Designed for Windows administrators, Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified Associate level. Focus on the expertise measured by these objectives: Mitigate threats using Microsoft 365 Defender Mitigate threats using Microsoft Defender for Cloud Mitigate threats using Microsoft Sentinel This Microsoft Exam Ref: Organizes its coverage by exam objectives Features strategic, what-if scenarios to challenge you Assumes you have experience with threat management, monitoring, and/or response in Microsoft 365 environments About the Exam Exam

SC-200 focuses on knowledge needed to detect, investigate, respond, and remediate threats to productivity, endpoints, identity, and applications; design and configure Azure Defender implementations; plan and use data connectors to ingest data sources into Azure Defender and Azure Sentinel; manage Azure Defender alert rules; configure automation and remediation; investigate alerts and incidents; design and configure Azure Sentinel workspaces; manage Azure Sentinel rules and incidents; configure SOAR in Azure Sentinel; use workbooks to analyze and interpret data; and hunt for threats in the Azure Sentinel portal. About Microsoft Certification Passing this exam fulfills your requirements for the Microsoft 365 Certified: Security Operations Analyst Associate certification credential, demonstrating your ability to collaborate with organizational stakeholders to reduce organizational risk, advise on threat protection improvements, and address violations of organizational policies. See full details at: microsoft.com/learn

microsoft sentinel workbooks: *Application Delivery and Load Balancing in Microsoft Azure* Derek DeJonghe, Arlan Nugara, 2020-12-04 With more and more companies moving on-premises applications to the cloud, software and cloud solution architects alike are busy investigating ways to improve load balancing, performance, security, and high availability for workloads. This practical book describes Microsoft Azure's load balancing options and explains how NGINX can contribute to a comprehensive solution. Cloud architects Derek DeJonghe and Arlan Nugara take you through the steps necessary to design a practical solution for your network. Software developers and technical managers will learn how these technologies have a direct impact on application development and architecture. While the examples are specific to Azure, these load balancing concepts and implementations also apply to cloud providers such as AWS, Google Cloud, DigitalOcean, and IBM Cloud. Understand application delivery and load balancing--and why they're important Explore Azure's managed load balancing options Learn how to run NGINX OSS and NGINX Plus on Azure Examine similarities and complementing features between Azure-managed solutions and NGINX Use Azure Front Door to define, manage, and monitor global routing for your web traffic Monitor application performance using Azure and NGINX tools and plug-ins Explore security choices using NGINX and Azure Firewall solutions

microsoft sentinel workbooks: Ultimate Microsoft XDR for Full Spectrum Cyber Defence Ian David Hanley, 2025-09-11 TAGLINE Unify Your Cyber Defense, Hunt Smarter and Respond Faster with Microsoft XDR! KEY FEATURES ● Learn every component of the Defender suite, Entra ID, and Microsoft Sentinel, from fundamentals to advanced automation. ● Build real-world detections, hunt threats, and automate response with guided labs and step-by-step workflows. ● Master KQL query design, cross-platform signal correlation, and threat-informed defense strategies. ● Design, deploy, and manage a mature, unified XDR strategy for organizations of any size. DESCRIPTION Extended Detection and Response (XDR) is essential for unifying security signals, accelerating investigations, and stopping attacks, before they spread. This book, Ultimate Microsoft XDR for Full Spectrum Cyber Defence shows you how to harness Microsoft’s powerful XDR stack to protect identities, endpoints, cloud workloads, and collaboration platforms. You will progress from mastering the core Defender products and Entra ID security features to unlocking Microsoft Sentinel’s SIEM and SOAR capabilities. Along the way, you will also build high-fidelity detections with KQL, automate responses with playbooks, and apply Zero Trust principles to secure modern, hybrid environments. Each chapter combines real-world scenarios with step-by-step guidance, so that you can confidently operationalize Microsoft XDR in your own organization. Hence, whether you are a security analyst, architect, SOC leader, or MSSP team, this guide equips you to design, deploy, and scale a unified detection and response strategy—reducing complexity, improving visibility, and neutralizing threats at machine speed. Thus, build a security operation that is proactive, resilient, and Microsoft-native. WHAT WILL YOU LEARN ● Design and deploy Microsoft XDR across cloud and hybrid environments. ● Detects threats, using Defender tools and cross-platform signal correlation. ● Write optimized KQL queries for threat hunting and cost control. ● Automate incident response, using Sentinel SOAR playbooks and Logic Apps. ● Secure identities, endpoints, and SaaS apps with Zero Trust principles. ● Operationalize your SOC with real-world Microsoft security use cases. WHO IS

THIS BOOK FOR? This book is tailored for SOC analysts/engineers, architects, Azure and MS 365 admins, and MSSP teams to design and run scalable Microsoft XDR defenses. Centered on Defender, Sentinel, and Entra ID, it teaches you to secure identities, endpoints, and cloud workloads with practical, Zero Trust–driven strategies for any organization size. TABLE OF CONTENTS 1. Understanding Microsoft XDR 2. Defender for Endpoint 3. Defender for Identity 4. Defender for Cloud Apps 5. Defender for Office 365 6. Entra ID Security 7. Introduction to Microsoft Sentinel 8. Microsoft Sentinel SIEM Capabilities 9. Microsoft Sentinel SOAR Capabilities 10. Efficient KQL Query Design and Optimization 11. Hands-On Lab Setup 12. Building and Operating a Mature Unified XDR Strategy Index

microsoft sentinel workbooks: *SC-200 Microsoft Security Operations Analyst Exam Full Preparation (Latest Version)* G Skills, This Book will give you’re the opportunity to Pass Your Exam on the First Try (Latest Exclusive Questions & Explanation) In this Book we offer the Latest, Exclusive and the most Recurrent Questions & detailed Explanation, Study Cases and References. This Book is a study guide for the new Microsoft SC-200 Microsoft Security Operations Analyst certification exam. This SC-200: Microsoft Security Operations Analyst Preparation book offers professional-level preparation that helps candidates maximize their exam performance and sharpen their skills on the job. Skills measured: The content of this exam will be updated periodically: Mitigate threats using Microsoft 365 Defender (25-30%) Mitigate threats using Azure Defender (25-30%) Mitigate threats using Azure Sentinel (40-45%) This Book: Target professional-level SC-200 exam candidates with content focused on their needs. Streamline study by organizing material according to the exam objective domain (OD), covering one functional group and its objectives in each chapter. Provide guidance from Microsoft, the creator of Microsoft certification exams. Provide Lastest Exam Questions & Study Cases. Provide Detailed Explanation for every question Important References. Welcome!

microsoft sentinel workbooks: *Microsoft Security Copilot* Bi Yue Xu, Rod Trent, 2025-07-24 Become a Security Copilot expert and harness the power of AI to stay ahead in the evolving landscape of cyber defense Key Features Explore the Security Copilot ecosystem and learn to design effective prompts, promptbooks, and custom plugins Apply your knowledge with real-world case studies that demonstrate Security Copilot in action Transform your security operations with next-generation defense capabilities and automation Access interactive learning paths and GitHub-based examples to build practical expertise Book Description Be at the forefront of cybersecurity innovation with Microsoft Security Copilot, where advanced AI tackles the intricate challenges of digital defense. This book unveils Security Copilot’s powerful features, from AI-powered analytics revolutionizing security operations to comprehensive orchestration tools streamlining incident response and threat management. Through real-world case studies and frontline stories, you’ll learn how to truly harness AI advancements and unlock the full potential of Security Copilot within the expansive Microsoft ecosystem. Designed for security professionals navigating increasingly sophisticated cyber threats, this book equips you with the skills to accelerate threat detection and investigation, refine your security processes, and optimize cyber defense strategies. By the end of this book, you’ll have become a Security Copilot ninja, confidently crafting effective prompts, designing promptbooks, creating custom plugins, and integrating logic apps for enhanced automation. What you will learn Navigate and use the complete range of features in Microsoft Security Copilot Unlock the full potential of Security Copilot's diverse plugin ecosystem Strengthen your prompt engineering skills by designing impactful and precise prompts Create and optimize promptbooks to streamline security workflows Build and customize plugins to meet your organization's specific needs See how AI is transforming threat detection and response for the new era of cyber defense Understand Security Copilot's pricing model for cost-effective solutions Who this book is for This book is for cybersecurity professionals at all experience levels, from beginners seeking foundational knowledge to seasoned experts looking to stay ahead of the curve. While readers with basic cybersecurity knowledge will find the content approachable, experienced practitioners will gain deep insights into advanced features and real-world applications.

microsoft sentinel workbooks: *Microsoft 365 Security, Compliance, and Identity Administration* Peter Rising, 2023-08-18 Explore expert tips and techniques to effectively manage the security, compliance, and identity features within your Microsoft 365 applications Purchase of the print or Kindle book includes a free PDF eBook Key Features Discover techniques to reap the full potential of Microsoft security and compliance suite Explore a range of strategies for effective security and compliance Gain practical knowledge to resolve real-world challenges Book Description The Microsoft 365 Security, Compliance, and Identity Administration is designed to help you manage, implement, and monitor security and compliance solutions for Microsoft 365 environments. With this book, you'll first configure, administer identity and access within Microsoft 365. You'll learn about hybrid identity, authentication methods, and conditional access policies with Microsoft Intune. Next, you'll discover how RBAC and Azure AD Identity Protection can be used to detect risks and secure information in your organization. You'll also explore concepts such as Microsoft Defender for endpoint and identity, along with threat intelligence. As you progress, you'll uncover additional tools and techniques to configure and manage Microsoft 365, including Azure Information Protection, Data Loss Prevention (DLP), and Microsoft Defender for Cloud Apps. By the end of this book, you'll be well-equipped to manage and implement security measures within your Microsoft 365 suite successfully. What you will learn Get up to speed with implementing and managing identity and access Understand how to employ and manage threat protection Manage Microsoft 365's governance and compliance features Implement and manage information protection techniques Explore best practices for effective configuration and deployment Ensure security and compliance at all levels of Microsoft 365 Who this book is for This book is for IT professionals, administrators, or anyone looking to pursue a career in security administration and wants to enhance their skills in utilizing Microsoft 365 Security Administration. A basic understanding of administration principles of Microsoft 365 and Azure Active Directory is a must. A good grip of on-premises Active Directory will be beneficial.

microsoft sentinel workbooks: *Microsoft Azure Network Security* Nicholas DiCola, Anthony Roman, 2021-05-12 Master a complete strategy for protecting any Azure cloud network environment! Network security is crucial to safely deploying and managing Azure cloud resources in any environment. Now, two of Microsoft's leading experts present a comprehensive, cloud-native approach to protecting your network, and safeguarding all your Azure systems and assets. Nicholas DiCola and Anthony Roman begin with a thoughtful overview of network security's role in the cloud. Next, they offer practical, real-world guidance on deploying cloud-native solutions for firewalling, DDOS, WAF, and other foundational services – all within a best-practice secure network architecture based on proven design patterns. Two of Microsoft's leading Azure network security experts show how to: Review Azure components and services for securing network infrastructure, and the threats to consider in using them Layer cloud security into a Zero Trust approach that helps limit or contain attacks Centrally direct and inspect traffic with the managed, stateful, Platform-as-a-Service Azure Firewall Improve visibility into Azure traffic with Deep Packet Inspection Optimize the way network and web application security work together Use Azure DDoS Protection (Basic and Standard) to mitigate Layer 3 (volumetric) and Layer 4 (protocol) DDoS attacks Enable log collection for Firewall, DDoS, WAF, and Bastion; and configure NSG Flow Logs and Traffic Analytics Continually monitor network security with Azure Sentinel, Security Center, and Network Watcher Customize queries, playbooks, workbooks, and alerts when Azure's robust out-of-the-box alerts and tools aren't enough Build and maintain secure architecture designs that scale smoothly to handle growing complexity About This Book For Security Operations (SecOps) analysts, cybersecurity/information security professionals, network security engineers, and other IT professionals For individuals with security responsibilities in any Azure environment, no matter how large, small, simple, or complex

Related to microsoft sentinel workbooks

Sign in to Microsoft 365 Learn how to sign in to Office or Microsoft 365 from a desktop application or your web browser

Contact Us - Microsoft Support Contact Microsoft Support. Find solutions to common problems, or get help from a support agent
Microsoft Support Microsoft Support is here to help you with Microsoft products. Find how-to articles, videos, and training for Microsoft Copilot, Microsoft 365, Windows, Surface, and more
Download, install, or reinstall Microsoft 365 or Office 2024 on a PC Learn how to install, reinstall, or activate Microsoft 365 or Office 2024 on a PC or Mac
Account help - Get help for the account you use with Microsoft. Find how to set up Microsoft account, protect it, and use it to manage your services and subscriptions
How to sign in to a Microsoft account Use your Microsoft account to sign in to Microsoft services like Windows, Microsoft 365, OneDrive, Skype, Outlook, and Xbox Live
Manage devices used with your Microsoft account Learn how to manage your Microsoft devices. Add, remove, register, or rename a device on your Microsoft account
Microsoft account recovery code A Microsoft account recovery code is a 25-digit code used to help you regain access to your account if you forget your password or if your account is compromised
Download and install or reinstall Office 2021, Office 2019, or Office Learn how to install Office 2021, 2019, or 2016 on your PC or Mac
All Products - Find out how to get support for Microsoft apps and services
Sign in to Microsoft 365 Learn how to sign in to Office or Microsoft 365 from a desktop application or your web browser
Contact Us - Microsoft Support Contact Microsoft Support. Find solutions to common problems, or get help from a support agent
Microsoft Support Microsoft Support is here to help you with Microsoft products. Find how-to articles, videos, and training for Microsoft Copilot, Microsoft 365, Windows, Surface, and more
Download, install, or reinstall Microsoft 365 or Office 2024 on a PC Learn how to install, reinstall, or activate Microsoft 365 or Office 2024 on a PC or Mac
Account help - Get help for the account you use with Microsoft. Find how to set up Microsoft account, protect it, and use it to manage your services and subscriptions
How to sign in to a Microsoft account Use your Microsoft account to sign in to Microsoft services like Windows, Microsoft 365, OneDrive, Skype, Outlook, and Xbox Live
Manage devices used with your Microsoft account Learn how to manage your Microsoft devices. Add, remove, register, or rename a device on your Microsoft account
Microsoft account recovery code A Microsoft account recovery code is a 25-digit code used to help you regain access to your account if you forget your password or if your account is compromised
Download and install or reinstall Office 2021, Office 2019, or Office Learn how to install Office 2021, 2019, or 2016 on your PC or Mac
All Products - Find out how to get support for Microsoft apps and services
Sign in to Microsoft 365 Learn how to sign in to Office or Microsoft 365 from a desktop application or your web browser
Contact Us - Microsoft Support Contact Microsoft Support. Find solutions to common problems, or get help from a support agent
Microsoft Support Microsoft Support is here to help you with Microsoft products. Find how-to articles, videos, and training for Microsoft Copilot, Microsoft 365, Windows, Surface, and more
Download, install, or reinstall Microsoft 365 or Office 2024 on a PC Learn how to install, reinstall, or activate Microsoft 365 or Office 2024 on a PC or Mac
Account help - Get help for the account you use with Microsoft. Find how to set up Microsoft account, protect it, and use it to manage your services and subscriptions
How to sign in to a Microsoft account Use your Microsoft account to sign in to Microsoft services like Windows, Microsoft 365, OneDrive, Skype, Outlook, and Xbox Live
Manage devices used with your Microsoft account Learn how to manage your Microsoft

devices. Add, remove, register, or rename a device on your Microsoft account
Microsoft account recovery code A Microsoft account recovery code is a 25-digit code used to help you regain access to your account if you forget your password or if your account is compromised
Download and install or reinstall Office 2021, Office 2019, or Office Learn how to install Office 2021, 2019, or 2016 on your PC or Mac
All Products - Find out how to get support for Microsoft apps and services
Sign in to Microsoft 365 Learn how to sign in to Office or Microsoft 365 from a desktop application or your web browser
Contact Us - Microsoft Support Contact Microsoft Support. Find solutions to common problems, or get help from a support agent
Microsoft Support Microsoft Support is here to help you with Microsoft products. Find how-to articles, videos, and training for Microsoft Copilot, Microsoft 365, Windows, Surface, and more
Download, install, or reinstall Microsoft 365 or Office 2024 on a PC Learn how to install, reinstall, or activate Microsoft 365 or Office 2024 on a PC or Mac
Account help - Get help for the account you use with Microsoft. Find how to set up Microsoft account, protect it, and use it to manage your services and subscriptions
How to sign in to a Microsoft account Use your Microsoft account to sign in to Microsoft services like Windows, Microsoft 365, OneDrive, Skype, Outlook, and Xbox Live
Manage devices used with your Microsoft account Learn how to manage your Microsoft devices. Add, remove, register, or rename a device on your Microsoft account
Microsoft account recovery code A Microsoft account recovery code is a 25-digit code used to help you regain access to your account if you forget your password or if your account is compromised
Download and install or reinstall Office 2021, Office 2019, or Office Learn how to install Office 2021, 2019, or 2016 on your PC or Mac
All Products - Find out how to get support for Microsoft apps and services

Related to microsoft sentinel workbooks

ReversingLabs Joins the Microsoft Security Store Partner Ecosystem (1d) Compare threat intelligence feeds based on indicator quality categories, including indicator age and number of tags.Understand how threat
ReversingLabs Joins the Microsoft Security Store Partner Ecosystem (1d) Compare threat intelligence feeds based on indicator quality categories, including indicator age and number of tags.Understand how threat
Microsoft expands Sentinel and Copilot to secure AI-driven enterprises (4d) This shift allows AI agents, including those in Microsoft Security Copilot, GitHub Copilot and other ecosystems, to reason,
Microsoft expands Sentinel and Copilot to secure AI-driven enterprises (4d) This shift allows AI agents, including those in Microsoft Security Copilot, GitHub Copilot and other ecosystems, to reason,
Microsoft Expands Sentinel Into Agentic Security Platform With Unified Data Lake (The Hacker News4d) Microsoft on Tuesday unveiled the expansion of its Sentinel Security Incidents and Event Management solution (SIEM) as a
Microsoft Expands Sentinel Into Agentic Security Platform With Unified Data Lake (The Hacker News4d) Microsoft on Tuesday unveiled the expansion of its Sentinel Security Incidents and Event Management solution (SIEM) as a
BlueVoyant is a proud participant in the Microsoft Sentinel partner ecosystem (TMCnet3d) BlueVoyant delivers comprehensive cyber defense solutions that help organizations identify, assess, and mitigate risks across their digital ecosystem. Its Third-Party Risk Management platform

provides
BlueVoyant is a proud participant in the Microsoft Sentinel partner ecosystem (TMCnet3d) BlueVoyant delivers comprehensive cyber defense solutions that help organizations identify, assess, and mitigate risks across their digital ecosystem. Its Third-Party Risk Management platform provides
Microsoft Bolstering Sentinel with Workspace Manager and Hunts Previews (Redmond Magazine2y) Microsoft this week announced some Microsoft Sentinel enhancements that are either available as a public preview release or will be coming soon. Microsoft is previewing a "Workspace Manager"
Microsoft Bolstering Sentinel with Workspace Manager and Hunts Previews (Redmond Magazine2y) Microsoft this week announced some Microsoft Sentinel enhancements that are either available as a public preview release or will be coming soon. Microsoft is previewing a "Workspace Manager"

Back to Home: http://www.speargroupllc.com