sentinel workbooks

sentinel workbooks are essential tools designed to enhance the monitoring, management, and analysis of data within cloud environments. As organizations increasingly rely on cloud services, the need for effective data management solutions has never been more critical. Sentinel workbooks provide users with a powerful way to visualize data, gain insights, and automate reporting processes, leading to improved operational efficiency. This article will delve into the core functionalities of sentinel workbooks, their benefits, best practices for implementation, and how they can be tailored to meet specific organizational needs. With a focus on practical applications and strategic usage, this comprehensive guide will equip you with the knowledge to leverage sentinel workbooks effectively.

Introduction to Sentinel Workbooks

Sentinel workbooks are part of the Azure Sentinel platform, a cloud-native security information and event management (SIEM) solution. They allow users to create custom dashboards and reports that visualize data collected from various sources, including security logs, user activities, and threat intelligence feeds. By utilizing sentinel workbooks, organizations can gain deeper insights into their security posture, identify potential threats, and respond more effectively to incidents.

The design of sentinel workbooks is user-friendly, enabling both technical and non-technical users to generate meaningful insights without extensive coding knowledge. With a wide array of templates and customization options, users can tailor their workbooks to reflect the specific data and metrics

that matter most to their organization.

Core Features of Sentinel Workbooks

Custom Visualizations

One of the standout features of sentinel workbooks is the ability to create custom visualizations. Users can choose from various chart types, including bar charts, line graphs, and pie charts, to represent their data in a way that is easy to understand. These visualizations help stakeholders quickly grasp complex data sets and make informed decisions based on real-time insights.

Integration with Azure Services

Sentinel workbooks seamlessly integrate with other Azure services, enabling users to pull data from various sources within the Azure ecosystem. This integration allows for a comprehensive view of an organization’s security landscape, making it easier to correlate data and identify trends.

Template Library

To simplify the process of creating workbooks, Azure Sentinel provides a template library filled with pre-built workbooks. These templates cover a range of common security scenarios, such as monitoring user activity, tracking threats, and analyzing system logs. Users can customize these templates to suit their specific needs, saving time and effort in the reporting process.

Benefits of Using Sentinel Workbooks

Enhanced Data Analysis

Sentinel workbooks facilitate enhanced data analysis by providing users with the tools needed to visualize and interpret large volumes of data. With the ability to drill down into specifics, organizations can identify patterns and anomalies that may indicate security threats or operational inefficiencies.

Improved Incident Response

By utilizing sentinel workbooks, organizations can improve their incident response capabilities. The visualizations and insights provided by the workbooks allow security teams to quickly assess incidents, prioritize responses, and track the effectiveness of their actions over time.

Streamlined Reporting

Creating reports can be a time-consuming task. Sentinel workbooks streamline this process by allowing users to automate reporting based on specific metrics and timelines. This automation not only saves time but also ensures that stakeholders receive timely updates on critical security issues.

Best Practices for Implementing Sentinel Workbooks

Define Clear Objectives

Before implementing sentinel workbooks, organizations should define clear objectives for what they aim to achieve. This involves identifying key metrics that need monitoring and understanding the specific insights that stakeholders require. Setting these objectives will guide the design and implementation of the workbooks.

Utilize Templates Wisely

While the template library is a valuable resource, it is important for users to customize these templates to align with their organizational needs. Modifying templates to include relevant metrics and visualizations will enhance their usefulness and ensure that the data presented is actionable.

Regularly Update Workbooks

Data and security landscapes are constantly evolving. Regularly updating sentinel workbooks to reflect new threats, changes in data sources, or shifts in organizational priorities is essential. This practice ensures that workbooks remain relevant and continue to provide valuable insights.

Customizing Sentinel Workbooks for Your Needs

Incorporating Organizational Branding

Customizing sentinel workbooks to incorporate organizational branding can enhance their impact. This includes adjusting color schemes, logos, and overall design elements to create a cohesive look that aligns with the organization’s identity.

Adding Custom Queries

Sentinel workbooks allow users to add custom queries to pull specific data from Azure logs. This feature enables organizations to focus on the data that matters most to them, enhancing the relevance and utility of the insights generated.

Use Cases for Sentinel Workbooks

Incident Monitoring

One of the primary use cases for sentinel workbooks is incident monitoring. Organizations can set up workbooks to track specific incidents over time, allowing security teams to assess trends and make data-driven decisions about resource allocation and incident response strategies.

Compliance Reporting

Sentinel workbooks are also valuable for compliance reporting. Organizations can create workbooks that aggregate data related to regulatory requirements, helping to ensure that they meet necessary compliance standards and can easily provide documentation when required.

Conclusion

Sentinel workbooks represent a powerful solution for organizations looking to enhance their data monitoring and analysis capabilities within cloud

environments. With their ability to provide custom visualizations, streamline reporting, and improve incident response, they are an invaluable tool for any organization serious about maintaining a robust security posture. By following best practices and customizing workbooks to fit specific needs, organizations can leverage sentinel workbooks to drive meaningful insights and improve overall operational effectiveness.

Frequently Asked Questions

Q: What are sentinel workbooks used for?

A: Sentinel workbooks are used for visualizing and analyzing data from Azure Sentinel, enabling organizations to monitor security incidents, track user activities, and generate reports for enhanced decision-making.

Q: How do I create a sentinel workbook?

A: To create a sentinel workbook, navigate to the Azure Sentinel portal, select the "Workbooks" section, and choose to create a new workbook. From there, you can use templates or start from scratch to design your custom visualizations.

Q: Can sentinel workbooks integrate with third-party data sources?

A: Yes, sentinel workbooks can integrate with various data sources, including third-party solutions, through Azure's data connectors, allowing for a comprehensive view of an organization's security data.

Q: What types of visualizations can be created in sentinel workbooks?

A: Sentinel workbooks offer various visualization options, including bar charts, line graphs, pie charts, tables, and maps, allowing users to represent data in the most effective way for analysis.

Q: Are there any costs associated with using sentinel workbooks?

A: While creating and using sentinel workbooks is part of the Azure Sentinel service, costs may be associated with the data ingested and stored in Azure. It’s advisable to review Azure's pricing model for specific details.

Q: How can sentinel workbooks improve incident response times?

A: By providing real-time data visualizations and insights, sentinel workbooks enable security teams to quickly identify, assess, and respond to incidents, thereby reducing overall response times.

Q: What is the importance of regularly updating sentinel workbooks?

A: Regularly updating sentinel workbooks is crucial to ensure they reflect the latest data, threats, and organizational priorities, maintaining their relevance and effectiveness in providing actionable insights.

Q: Can I share sentinel workbooks with other team members?

A: Yes, sentinel workbooks can be shared with team members, allowing for collaboration and collective analysis of security data within the organization.

Q: What are some common challenges when using sentinel workbooks?

A: Common challenges include ensuring data accuracy, maintaining up-to-date workbooks, and customizing templates effectively to meet specific organizational needs. Addressing these challenges is essential for maximizing the benefits of sentinel workbooks.

Sentinel Workbooks

sentinel workbooks: Learn Azure Sentinel Richard Diver, Gary Bushey, 2020-04-07 Understand how to set up, configure, and use Azure Sentinel to provide security incident and event management services for your environment Key FeaturesSecure your network, infrastructure, data, and applications on Microsoft Azure effectivelyIntegrate artificial intelligence, threat analysis, and automation for optimal security solutionsInvestigate possible security breaches and gather forensic evidence to prevent modern cyber threatsBook Description Azure Sentinel is a Security Information

and Event Management (SIEM) tool developed by Microsoft to integrate cloud security and artificial intelligence (AI). Azure Sentinel not only helps clients identify security issues in their environment, but also uses automation to help resolve these issues. With this book, you'll implement Azure Sentinel and understand how it can help find security incidents in your environment with integrated artificial intelligence, threat analysis, and built-in and community-driven logic. This book starts with an introduction to Azure Sentinel and Log Analytics. You'll get to grips with data collection and management, before learning how to create effective Azure Sentinel queries to detect anomalous behaviors and patterns of activity. As you make progress, you'll understand how to develop solutions that automate the responses required to handle security incidents. Finally, you'll grasp the latest developments in security, discover 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 Azure Sentinel to fit your needs and be able to protect your environment from cyber threats and other security issues. What you will learnUnderstand how to design and build a security operations centerDiscover the key components of a cloud security architectureManage and investigate Azure Sentinel incidentsUse playbooks to automate incident responsesUnderstand how to set up Azure Monitor Log Analytics and Azure SentinelIngest data into Azure Sentinel from the cloud and on-premises devicesPerform threat hunting in Azure SentinelWho this book is for This book is for solution architects and system administrators who are responsible for implementing new solutions in their infrastructure. Security analysts who need to monitor and provide immediate security solutions or threat hunters looking to learn how to use Azure Sentinel to investigate possible security breaches and gather forensic evidence will also benefit from this book. Prior experience with cloud security, particularly Azure, is necessary.

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.

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

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

sentinel workbooks: Threat Hunting in the Cloud Chris Peiris, Binil Pillai, Abbas Kudrati,

2021-08-31 Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure how to solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, Threat Hunting in the Cloud is also an indispensable guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy.

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

sentinel workbooks: Microsoft 365 Security Administration: MS-500 Exam Guide Peter Rising,

2020-06-19 Get up to speed with expert tips and techniques to help you prepare effectively for the MS-500 Exam Key FeaturesGet the right guidance and discover techniques to improve the effectiveness of your studying and prepare for the examExplore a wide variety of strategies for security and complianceGain knowledge that can be applied in real-world situationsBook Description The Microsoft 365 Security Administration (MS-500) exam is designed to measure your ability to perform technical tasks such as managing, implementing, and monitoring security and compliance solutions for Microsoft 365 environments. This book starts by showing you how to configure and administer identity and access within Microsoft 365. You will learn about hybrid identity, authentication methods, and conditional access policies with Microsoft Intune. Next, the book shows you how RBAC and Azure AD Identity Protection can be used to help you detect risks and secure information in your organization. You will also explore concepts, such as Advanced Threat Protection, Windows Defender ATP, and Threat Intelligence. As you progress, you will learn about additional tools and techniques to configure and manage Microsoft 365, including Azure Information Protection, Data Loss Prevention, and Cloud App Discovery and Security. The book also ensures you are well prepared to take the exam by giving you the opportunity to work through a mock paper, topic summaries, illustrations that briefly review key points, and real-world scenarios. By the end of this Microsoft 365 book, you will be able to apply your skills in the real world, while also being well prepared to achieve Microsoft certification. What you will learnGet up to speed with implementing and managing identity and accessUnderstand how to employ and manage threat protectionGet to grips with managing governance and compliance features in Microsoft 365Explore best practices for effective configuration and deploymentImplement and manage information protectionPrepare to pass the Microsoft exam and achieve certification with the help of self-assessment questions and a mock examWho this book is for This Microsoft certification book is designed to help IT professionals, administrators, or anyone looking to pursue a career in security administration by becoming certified with Microsoft's role-based qualification. Those trying to validate their skills and improve their competitive advantage with Microsoft 365 Security Administration will also find this book to be a useful resource.

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

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

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

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

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

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

sentinel workbooks: Microsoft Certified Exam guide - Azure Administrator Associate (AZ-104) Cybellium , Master Azure Administration and Elevate Your Career! Are you ready to become a Microsoft Azure Administrator Associate and take your career to new heights? Look no further than the Microsoft Certified Exam Guide - Azure Administrator Associate (AZ-104). This

comprehensive book is your essential companion on the journey to mastering Azure administration and achieving certification success. In today's digital age, cloud technology is the backbone of modern business operations, and Microsoft Azure is a leading force in the world of cloud computing. Whether you're a seasoned IT professional or just starting your cloud journey, this book provides the knowledge and skills you need to excel in the AZ-104 exam and thrive in the world of Azure administration. Inside this book, you will find: In-Depth Coverage: A thorough exploration of all the critical concepts, tools, and best practices required for effective Azure administration. Real-World Scenarios: Practical examples and case studies that illustrate how to manage and optimize Azure resources in real business environments. Exam-Ready Preparation: Comprehensive coverage of AZ-104 exam objectives, along with practice questions and expert tips to ensure you're fully prepared for the test. Proven Expertise: Written by Azure professionals who not only hold the certification but also have hands-on experience in deploying and managing Azure solutions, offering you valuable insights and practical wisdom. Whether you're looking to enhance your skills, advance your career, or simply master Azure administration, Microsoft Certified Exam Guide - Azure Administrator Associate (AZ-104) is your trusted roadmap to success. Don't miss this opportunity to become a sought-after Azure Administrator in a competitive job market. Prepare, practice, and succeed with the ultimate resource for AZ-104 certification. Order your copy today and unlock a world of possibilities in Azure administration! www.cybellium.com

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.

sentinel workbooks: *Azure Security* Bojan Magusic, 2024-02-06 Secure your Azure applications the right way. The expert DevSecOps techniques you'll learn in this essential handbook make it easy to keep your data safe. As a Program Manager at Microsoft, Bojan Magusic has helped numerous Fortune 500 companies improve their security posture in Azure. Now, in Azure Security he brings his experience from the cyber security frontline to ensure your Azure cloud-based systems are safe and secure. In Azure Security you'll learn vital security skills, including how to: Set up secure access through Conditional Access policiesImplement Azure WAF on Application Gateway and Front Door

Deploy Azure Firewall Premium for monitoring network activities Enable Microsoft Defender for Cloud to assess workload configurations Utilize Microsoft Sentinel for threat detection and analytics Establish Azure Policy for compliance with business rules Correctly set up out-of-the-box Azure services to protect your web apps against both common and sophisticated threats, learn to continuously assess your systems for vulnerabilities, and discover cutting-edge operations for security hygiene, monitoring, and DevSecOps. Each stage is made clear and easy to follow with step-by-step instructions, complemented by helpful screenshots and diagrams. About the technology Securing cloud-hosted applications requires a mix of tools, techniques, and platform-specific services. The Azure platform provides built-in security tools to keep your systems safe, but proper implementation requires a foundational strategy and tactical guidance. About the book Azure Security details best practices for configuring and deploying Azure's native security services—from a zero-trust foundation to defense in depth (DiD). Learn from a Microsoft security insider how to establish a DevSecOps program using Microsoft Defender for Cloud. Realistic scenarios and hands-on examples help demystify tricky security concepts, while clever exercises help reinforce what you've learned. What's inside Set up secure access policies Implement a Web Application Firewall Deploy MS Sentinel for monitoring and threat detection Establish compliance with business rules About the reader For software and security engineers building and securing Azure applications. About the author Bojan Magusic is a Product Manager with Microsoft on the Security Customer Experience Engineering Team. Table of Contents PART 1 FIRST STEPS 1 About Azure security 2 Securing identities in Azure: The four pillars of identity and Azure Active Directory PART 2 SECURING AZURE RESOURCES 3 Implementing network security in Azure: Firewall, WAF, and DDoS protection 4 Securing compute resources in Azure: Azure Bastion, Kubernetes, and Azure App Service 5 Securing data in Azure Storage accounts: Azure Key Vault 6 Implementing good security hygiene: Microsoft Defender for Cloud and Defender CSPM 7 Security monitoring for Azure resources: Microsoft Defender for Cloud plans PART 3 GOING FURTHER 8 Security operations and response: Microsoft Sentinel 9 Audit and log data: Azure Monitor 10 Importance of governance: Azure Policy and Azure Blueprints 11 DevSecOps: Microsoft Defender for DevOps

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

sentinel workbooks: *Mastering Azure Security* Arnav Sharma, 2025-09-30 DESCRIPTION The adoption of the Cloud brings many security challenges. Securing identities, data, and workloads while trying to stay on the right side of compliance regulations has become a priority for organizations. Mastering Azure Security is your essential handbook for defending applications and data against a complex threat landscape. Starting with the fundamentals, this book guides you through Azure security from the ground up. You will begin with core concepts like the shared responsibility model and Zero Trust, then apply these to secure key service layers, such as identity and access with Entra ID, networks with NSGs and Azure Firewall, compute for VMs and containers, and data with encryption and access controls. Furthermore, you will look at security governance, learning to manage your environment at scale using Azure Policy and Azure Landing Zones. Finally,

you will learn about posture management with Microsoft Defender for Cloud and detect threats using Microsoft Sentinel. By the end of this book, readers will gain an understanding of Azure security and develop the practical skills required to design, implement, and maintain a secure and compliant cloud infrastructure. Whether you are trying to nail down compliance, make systems more resilient, or know how to handle the latest threats, this book will give you the skills to make it happen. WHAT YOU WILL LEARN ● Secure Azure compute and virtual networks with policies and controls. ● Implement data encryption, masking, and auditing in Azure. ● Protect workloads with Microsoft Defender for Cloud services. ● Apply Zero Trust principles to users and applications. ● Govern resources with Azure Policy, CAF, and WAF. ● Manage secrets and keys using Azure Key Vault. ● Strengthen security posture with monitoring and automation. WHO THIS BOOK IS FOR This book is for cloud engineers, IT professionals, security architects, consultants, and risk managers who work with Microsoft Azure. It is equally useful for administrators, security teams, and learners aiming to master practical Azure security. Whether you focus on compliance, Zero Trust, or workload protection, this book offers hands-on strategies to build and maintain secure Azure environments. TABLE OF CONTENTS 1. Introduction to Azure Security 2. Securing Identity and Access 3. Securing Networks 4. Securing Compute 5. Securing Data 6. Security Governance 7. Security Posture 8. Workload Protection 9. Security Monitoring 10. Security Best Practices

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)

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.

Related to sentinel workbooks

Visualize your data using workbooks in Microsoft Sentinel Microsoft Sentinel allows you to create custom workbooks across your data or use existing workbook templates available with packaged solutions or as standalone content from

Azure/azure-sentinel/ at main Steps to Build Your Own Workbook: Microsoft Sentinel → Workbooks → + New. Choose Blank Workbook. Add a Query Control: Write a KQL query to pull data. Example: Sign-in failures per

Sentinel Workbooks - Azure Lessons In Azure Sentinel, You can add a new Workbook or use the predefined or inbuilt workbooks templates. Let’s deep dive into a complete tutorial on Azure Sentinel Workbooks

Kinda Technical | A Guide to Azure Sentinel - Creating a Workbook In Azure Sentinel, workbooks provide a flexible canvas for data visualization and analysis. They can include graphs, tables, and text, helping you create a comprehensive view of your data

Create Workbooks for Microsoft Sentinel Solutions This article guides you through the

process of creating and publishing workbooks for Microsoft Sentinel solutions
Create workbooks for explore Sentinel data - KodeKloud Notes This article explains how to create and utilize workbooks in Azure Sentinel for effective data visualization and analysis
Commonly used Microsoft Sentinel workbooks | Azure Docs Learn about the most commonly used workbooks to use popular, out-of-the-box Microsoft Sentinel resources
Sentinel Workbooks to Improve Incident Response Effectiveness In this post, you'll learn how to use Microsoft Sentinel Workbooks to monitor detection effectiveness, measure incident response SLAs, and build dashboards that help both
Commonly used Microsoft Sentinel workbooks | Microsoft Learn Learn about the most commonly used workbooks to use popular, out-of-the-box Microsoft Sentinel resources
Microsoft Sentinel - Workbooks | Cloudutsuk Workbooks in Azure Sentinel are interactive data visualization tools that allow security analysts and administrators to create custom reports, dashboards, and data visualizations based on
Visualize your data using workbooks in Microsoft Sentinel Microsoft Sentinel allows you to create custom workbooks across your data or use existing workbook templates available with packaged solutions or as standalone content from
Azure/azure-sentinel/ at main - GitHub Steps to Build Your Own Workbook: Microsoft Sentinel → Workbooks → + New. Choose Blank Workbook. Add a Query Control: Write a KQL query to pull data. Example: Sign-in failures per
Sentinel Workbooks - Azure Lessons In Azure Sentinel, You can add a new Workbook or use the predefined or inbuilt workbooks templates. Let's deep dive into a complete tutorial on Azure Sentinel Workbooks
Kinda Technical | A Guide to Azure Sentinel - Creating a Workbook In Azure Sentinel, workbooks provide a flexible canvas for data visualization and analysis. They can include graphs, tables, and text, helping you create a comprehensive view of your data
Create Workbooks for Microsoft Sentinel Solutions This article guides you through the process of creating and publishing workbooks for Microsoft Sentinel solutions
Create workbooks for explore Sentinel data - KodeKloud Notes This article explains how to create and utilize workbooks in Azure Sentinel for effective data visualization and analysis
Commonly used Microsoft Sentinel workbooks | Azure Docs Learn about the most commonly used workbooks to use popular, out-of-the-box Microsoft Sentinel resources
Sentinel Workbooks to Improve Incident Response Effectiveness In this post, you'll learn how to use Microsoft Sentinel Workbooks to monitor detection effectiveness, measure incident response SLAs, and build dashboards that help both
Commonly used Microsoft Sentinel workbooks | Microsoft Learn Learn about the most commonly used workbooks to use popular, out-of-the-box Microsoft Sentinel resources
Microsoft Sentinel - Workbooks | Cloudutsuk Workbooks in Azure Sentinel are interactive data visualization tools that allow security analysts and administrators to create custom reports, dashboards, and data visualizations based on

Related to 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 intelligence augments detections by looking at incident
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 intelligence augments detections by looking at incident