microsoft sentinel workbooks github

microsoft sentinel workbooks github is an essential resource for organizations looking to enhance their security operations through efficient monitoring and reporting. Microsoft Sentinel provides a robust platform for security information and event management (SIEM), and workbooks are a critical component that allows users to visualize and analyze their security data effectively. By utilizing Microsoft Sentinel workbooks available on GitHub, organizations can leverage community-driven templates and solutions, ensuring they get the most out of their security analytics. This article will explore the functionalities of Microsoft Sentinel workbooks, the advantages of using GitHub for accessing these resources, and how to implement them effectively in your organization.

Understanding Microsoft Sentinel Workbooks

Microsoft Sentinel workbooks are interactive dashboards that provide visual insights into your security data. They are built on the Azure Monitor workbooks framework, allowing users to create customized visualizations and reports based on their security logs and alerts. Workbooks can pull data from various sources, enabling a comprehensive view of security posture across an organization.

Key Features of Microsoft Sentinel Workbooks

Some of the key features of Microsoft Sentinel workbooks include:

- **Data Visualization:** Workbooks offer a range of visualization options, including charts, graphs, and tables, helping users interpret data quickly.
- **Custom Queries:** Users can create custom Kusto Query Language (KQL) queries to retrieve specific data relevant to their security needs.

- **Collaboration:** Workbooks can be shared across teams, fostering collaboration and allowing different stakeholders to access vital security information.
- **Template Availability:** Microsoft Sentinel provides built-in workbook templates, which can be customized according to specific requirements.

Benefits of Using GitHub for Workbooks

GitHub serves as a powerful platform for managing Microsoft Sentinel workbooks due to its collaborative features and extensive community support. By hosting workbooks on GitHub, users can access a wealth of resources created by security professionals and enthusiasts.

Community Contributions

One of the primary benefits of using GitHub is the ability to tap into community contributions. Users can find a variety of workbooks shared by others, which can serve as a starting point for their own customizations. This collaborative environment encourages innovation and the sharing of best practices.

Version Control

GitHub's version control system allows users to track changes made to workbooks, making it easier to manage updates and revert to previous versions if necessary. This feature is particularly valuable in a security context, where changes may need to be audited for compliance purposes.

How to Access Microsoft Sentinel Workbooks on GitHub

Accessing Microsoft Sentinel workbooks on GitHub is straightforward. Users can search for repositories that contain workbooks specific to Microsoft Sentinel, often tagged with relevant keywords.

Finding Workbooks on GitHub

To find relevant workbooks, users can follow these steps:

1. Navigate to the GitHub website.
2. Use the search bar to enter keywords such as "Microsoft Sentinel workbooks".
3. Filter results by repositories to find those specifically focused on Sentinel.
4. Explore the repositories to find workbooks that suit your needs.

Cloning Repositories

Once users identify suitable workbooks, they can clone the repositories to their local machines or directly import them into their Azure environment. This process typically involves the following steps:

1. Select the repository you want to clone.
2. Click the "Code" button and copy the URL provided.
3. Use Git on your local machine to clone the repository using the command line.

Implementing Workbooks in Microsoft Sentinel

After accessing the desired workbooks, the next step is to implement them within Microsoft Sentinel. This process allows organizations to visualize their security data effectively.

Importing Workbooks into Microsoft Sentinel

To import workbooks into Microsoft Sentinel, users can follow this procedure:

1. Log in to the Microsoft Sentinel portal.
2. Navigate to the "Workbooks" section.
3. Select "Add new" and choose "Import from GitHub".
4. Paste the URL of the workbook repository and follow the prompts to complete the import.

Customizing Workbooks

Once imported, workbooks can be customized to meet specific organizational needs. Users can modify queries, change visualizations, and adjust parameters to ensure the workbooks provide the most relevant insights.

Best Practices for Using Microsoft Sentinel Workbooks

To maximize the effectiveness of Microsoft Sentinel workbooks, organizations should adhere to several best practices.

Regular Updates

It is crucial to regularly update workbooks to ensure they reflect the latest threat intelligence and organizational changes. This practice helps in maintaining the relevance and accuracy of security insights.

Training and Documentation

Providing training for users on how to navigate and utilize workbooks effectively can enhance the overall security posture of the organization. Documentation should also be maintained to guide users on leveraging workbook features.

Use Cases of Microsoft Sentinel Workbooks

Microsoft Sentinel workbooks can be utilized in various scenarios across organizations to bolster their security operations.

Incident Response

During incident response, workbooks can provide real-time insights into security alerts, enabling teams to act swiftly and effectively. Customized dashboards can highlight critical incidents and correlate data from multiple sources.

Compliance Reporting

Workbooks can assist in generating compliance reports by visualizing data related to security controls and regulatory requirements. This capability is essential for organizations that need to demonstrate adherence to standards such as GDPR or HIPAA.

Conclusion

Microsoft Sentinel workbooks, especially those available on GitHub, are invaluable tools for organizations aiming to enhance their security analytics and monitoring capabilities. By understanding how to access, implement, and customize these workbooks, organizations can better utilize their security data for informed decision-making. The community-driven aspect of GitHub enriches the availability of templates and solutions, fostering collaboration and innovation in security practices. As cyber threats continue to evolve, leveraging Microsoft Sentinel workbooks will be crucial for maintaining a robust security posture.

Q: What are Microsoft Sentinel workbooks?

A: Microsoft Sentinel workbooks are interactive dashboards that allow users to visualize and analyze security data within the Microsoft Sentinel platform. They provide customizable visualizations and reports based on security logs and alerts.

Q: How can I find Microsoft Sentinel workbooks on GitHub?

A: You can find Microsoft Sentinel workbooks on GitHub by searching for relevant keywords like "Microsoft Sentinel workbooks" and filtering the results to repositories. This will help you locate community-contributed workbooks that you can use or customize.

Q: Can I customize Microsoft Sentinel workbooks?

A: Yes, Microsoft Sentinel workbooks can be customized to fit specific organizational needs. Users can modify queries, change visualizations, and adjust parameters to ensure the workbooks provide relevant insights.

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

A: Using GitHub for Microsoft Sentinel workbooks allows users to access community contributions, benefit from version control, and collaborate with other security professionals, enhancing the overall effectiveness of their security monitoring.

Q: How do I import a workbook from GitHub into Microsoft Sentinel?

A: To import a workbook from GitHub into Microsoft Sentinel, you log in to the Microsoft Sentinel portal, navigate to the "Workbooks" section, select "Add new," and choose "Import from GitHub," pasting the URL of the workbook repository.

Q: What are the best practices for using Microsoft Sentinel workbooks?

A: Best practices include regularly updating workbooks, providing training for users, maintaining documentation, and customizing workbooks to fit the organization's specific needs.

Q: What are some common use cases for Microsoft Sentinel workbooks?

A: Common use cases for Microsoft Sentinel workbooks include incident response to provide real-time insights into security alerts and compliance reporting to visualize data related to security controls and regulatory requirements.

Q: Can I collaborate with others when using Microsoft Sentinel workbooks?

A: Yes, Microsoft Sentinel workbooks can be shared across teams, promoting collaboration and enabling various stakeholders to access vital security information.

Q: How do Microsoft Sentinel workbooks enhance security operations?

A: Microsoft Sentinel workbooks enhance security operations by providing visual insights, facilitating real-time data analysis, and enabling organizations to respond effectively to security incidents and compliance requirements.

Q: Are there any built-in templates for Microsoft Sentinel workbooks?

A: Yes, Microsoft Sentinel provides built-in workbook templates that users can utilize as a foundation for their customizations, streamlining the process of creating effective dashboards and reports.

Microsoft Sentinel Workbooks Github

microsoft sentinel workbooks github: 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 github: *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 github: 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 github: Microsoft Defender for Cloud Cookbook Sasha Kranjac, 2022-07-22 Effectively secure their cloud and hybrid infrastructure, how to centrally manage security, and improve organizational security posture Key Features • Implement and optimize security posture in Azure, hybrid, and multi-cloud environments • Understand Microsoft Defender for Cloud and its features • Protect workloads using Microsoft Defender for Cloud's threat detection and prevention capabilities Book Description Microsoft Defender for Cloud is a multi-cloud and hybrid cloud security posture management solution that enables security administrators to build cyber defense for their Azure and non-Azure resources by providing both recommendations and security protection capabilities. This book will start with a foundational overview of Microsoft Defender for Cloud and its core capabilities. Then, the reader is taken on a journey from enabling the service, selecting the correct tier, and configuring the data collection, to working on remediation. Next, we will continue with hands-on guidance on how to implement several security features of Microsoft Defender for Cloud, finishing with monitoring and maintenance-related topics, gaining visibility in advanced threat protection in distributed infrastructure and preventing security failures through automation. By the end of this book, you will know how to get a view of your security posture and where to optimize security protection in your environment as well as the ins and outs of Microsoft Defender for Cloud. What you will learn • Understand Microsoft Defender for Cloud features and capabilities • Understand the fundamentals of building a cloud security posture and defending your cloud and on-premises resources • Implement and optimize security in Azure, multi-cloud and hybrid environments through the single pane of glass - Microsoft Defender for Cloud • Harden your security posture, identify, track and remediate vulnerabilities • Improve and harden your security and services security posture with Microsoft Defender for Cloud benchmarks and best practices • Detect and fix threats to services and resources Who this book is for This book is for Security engineers, systems administrators, security professionals, IT professionals, system architects, and developers. Anyone whose responsibilities include maintaining security posture, identifying, and remediating vulnerabilities, and securing cloud and hybrid infrastructure. Anyone who is willing to learn about security in Azure and to build secure Azure and hybrid infrastructure, to improve their security posture in Azure, hybrid and multi-cloud environments by leveraging all the features within Microsoft Defender for Cloud.

microsoft sentinel workbooks github: *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 github: Mastering Microsoft 365 Security Technologies Pramiti Bhatnagar, 2025-05-28 DESCRIPTION Microsoft security technologies provide a robust, integrated defense against evolving cyber threats, spanning identity, endpoints, applications, and data across hybrid environments. It offers a unified and intelligent defense across an organization's digital landscape. This book will introduce readers to Microsoft security solutions. It covers Microsoft Defender, Microsoft Entra ID, and Microsoft Purview. Readers will learn how they can protect their organization across different attack vectors such as email, identity, data, endpoints, and applications. It discusses how to protect the user identities using Microsoft Entra ID, protect devices and applications using Microsoft Defender and Microsoft Sentinel, and protect organization data using Microsoft Purview. With a focus on real-world scenarios, hands-on labs, and expert guidance, cybersecurity professionals will gain a deep understanding of Microsoft security solutions and how to use them to protect their organizations from bad actors. By the end of this book, you will possess the practical knowledge and skills to design, implement, and manage a strong security posture across your organization's Microsoft infrastructure, confidently protecting identities, data, and applications from modern cyberattacks. WHAT YOU WILL LEARN ● Data security and governance using Microsoft Purview information protection and DLP. ● Protecting devices, identities, M365, and non-M365 applications using Microsoft Defender. ● Microsoft's Zero Trust Network Access solution – secure services edge. ● Manage Entra ID users, groups, RBAC, Admin Units, Protected Actions effectively. ● Managing regulatory compliance and privacy. WHO THIS BOOK IS FOR This book is ideal for IT professionals and administrators seeking careers in security administration using Microsoft security technologies. Readers need foundational cloud computing knowledge (IaaS, PaaS, SaaS), basic M365 cloud and Azure familiarity, plus awareness of Zero Trust, identity and access, and platform protection. TABLE OF CONTENTS 1. Introduction to Microsoft Entra 2. Implementing Identity 3. Identity Management 4. Identity Protection 5. Identity Governance 6. Microsoft Defender XDR 7. Protecting Identities 8. Protecting Endpoints 9. Protecting M365 Apps 10. Protecting Non-Microsoft Cloud Apps 11. Security Management Using Microsoft Sentinel 12. Protect and Govern Sensitive Data 13. Managing Insider Risks 14. Managing eDiscovery Cases 15. Managing Regulatory Compliance 16. Managing Privacy 17. Best Practices

microsoft sentinel workbooks github: 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 github: *Microsoft Azure Sentinel* Yuri Diogenes, Nicholas DiCola, Jonathan Trull, 2020-02-25 Microsoft Azure Sentinel Plan, deploy, and operate Azure Sentinel, Microsoft's advanced cloud-based SIEM Microsoft's cloud-based Azure Sentinel helps you fully leverage advanced AI to automate threat identification and response – without the complexity and scalability challenges of traditional Security Information and Event Management (SIEM) solutions. Now, three of Microsoft's leading experts review all it can do, and guide you step by step through planning, deployment, and daily operations. Leveraging in-the-trenches experience supporting early customers, they cover everything from configuration to data ingestion, rule development to incident management… even proactive threat hunting to disrupt attacks before you're exploited. Three of Microsoft's leading security operations experts show how to: • Use Azure Sentinel to respond to today's fast-evolving cybersecurity environment, and leverage the benefits of its cloud-native architecture • Review threat intelligence essentials: attacker motivations, potential targets, and tactics, techniques, and procedures • Explore Azure Sentinel components, architecture, design considerations, and initial configuration • Ingest alert log data from services and endpoints you need to monitor • Build and validate rules to analyze ingested data and create cases for investigation • Prevent alert fatigue by projecting how many incidents each rule will generate • Help Security Operation Centers (SOCs) seamlessly manage each incident's lifecycle • Move towards proactive threat hunting: identify sophisticated threat behaviors and disrupt cyber kill chains before you're exploited • Do more with data: use programmable Jupyter notebooks and their libraries for machine learning, visualization, and data analysis • Use Playbooks to perform Security Orchestration, Automation and Response (SOAR) • Save resources by automating responses to low-level events • Create visualizations to spot trends, identify or clarify relationships, and speed decisions • Integrate with partners and other third-parties, including Fortinet, AWS, and Palo Alto

microsoft sentinel workbooks github: Mastering DevOps on Microsoft Power Platform Uroš Kastelic, József Zoltán Vadkerti, 2024-09-05 Learn from Microsoft Power Platform experts how to leverage GitHub, Azure DevOps, and GenAI tools like Microsoft Copilots to develop and deliver secure, enterprise-scale solutions Key Features Customize Power Platform for secure large-scale deployments with the help of DevSecOps practices Implement code-first fusion projects with ALM and infuse AI in Power Platform using copilots and ChatOps Get hands-on experience through real-world examples using Azure DevOps and GitHub Purchase of the print or Kindle book includes a

free PDF eBook Book Description Mastering DevOps on Microsoft Power Platform is your guide to revolutionizing business-critical solution development. Written by two Microsoft Technology Specialists with extensive experience in enterprise-scale Power Platform implementations and DevOps practices, this book teaches you how to design, build, and secure efficient DevOps processes by adapting custom software development practices to the Power Platform toolset, dramatically reducing time, cost, and errors in app modernization and quality assurance. The book introduces application life cycle management (ALM) and DevOps-enabled architecture, design patterns, and CI/CD practices, showing you why companies adopt DevOps with Power Platform. You'll master environment and solution management using Dataverse, Git, the Power Platform CLI, Azure DevOps, and GitHub Copilot. Implementing the shift-left approach in DevSecOps using GitHub Advanced Security features, you'll create a Power Platform tenant governed by controls, automated tests, and backlog management. You'll also discover advanced concepts, such as fusion architecture, pro-dev extensibility, and AI-infused applications, along with tips to avoid common pitfalls. By the end of this book, you'll be able to build CI/CD pipelines from development to production, enhancing the life cycle of your business solutions on Power Platform. What you will learn Gain insights into ALM and DevOps on Microsoft Power Platform Set up Power Platform pipelines and environments by leveraging best practices Automate, test, monitor, and secure CI/CD pipelines using DevSecOps tools, such as VS Code and GitHub Advanced Security, on Power Platform Enable pro-developer extensibility using fusion development to integrate Azure and Power Platform Provision enterprise landing zones and build well-architected workloads Discover GenAI capabilities in Power Platform and support ChatOps with the copilot stack Who this book is for If you are a DevOps engineer, cloud architect, site reliability engineer, solutions architect, software developer, or low-code engineer looking to master end-to-end DevSecOps implementation on Microsoft Power Platform from basic to advanced levels, this book is for you. Prior knowledge of software development processes and tools is necessary. A basic understanding of Power Platform and DevOps processes will also be beneficial.

microsoft sentinel workbooks github: Microsoft Azure Security Technologies Certification and Beyond David Okeyode, 2021-11-04 Excel at AZ-500 and implement multi-layered security controls to protect against rapidly evolving threats to Azure environments – now with the the latest updates to the certification Key FeaturesMaster AZ-500 exam objectives and learn real-world Azure security strategiesDevelop practical skills to protect your organization from constantly evolving security threatsEffectively manage security governance, policies, and operations in AzureBook Description Exam preparation for the AZ-500 means you'll need to master all aspects of the Azure cloud platform and know how to implement them. With the help of this book, you'll gain both the knowledge and the practical skills to significantly reduce the attack surface of your Azure workloads and protect your organization from constantly evolving threats to public cloud environments like Azure. While exam preparation is one of its focuses, this book isn't just a comprehensive security guide for those looking to take the Azure Security Engineer certification exam, but also a valuable resource for those interested in securing their Azure infrastructure and keeping up with the latest updates. Complete with hands-on tutorials, projects, and self-assessment questions, this easy-to-follow guide builds a solid foundation of Azure security. You'll not only learn about security technologies in Azure but also be able to configure and manage them. Moreover, you'll develop a clear understanding of how to identify different attack vectors and mitigate risks. By the end of this book, you'll be well-versed with implementing multi-layered security to protect identities, networks, hosts, containers, databases, and storage in Azure – and more than ready to tackle the AZ-500. What you will learnManage users, groups, service principals, and roles effectively in Azure ADExplore Azure AD identity security and governance capabilitiesUnderstand how platform perimeter protection secures Azure workloadsImplement network security best practices for IaaS and PaaSDiscover various options to protect against DDoS attacksSecure hosts and containers against evolving security threatsConfigure platform governance with cloud-native toolsMonitor security operations with Azure Security Center and Azure SentinelWho this book is for This book is a comprehensive resource aimed at those preparing for the Azure Security Engineer (AZ-500)

certification exam, as well as security professionals who want to keep up to date with the latest updates. Whether you're a newly qualified or experienced security professional, cloud administrator, architect, or developer who wants to understand how to secure your Azure environment and workloads, this book is for you. Beginners without foundational knowledge of the Azure cloud platform might progress more slowly, but those who know the basics will have no trouble following along.

microsoft sentinel workbooks github: Windows Ransomware Detection and Protection Marius Sandbu, 2023-03-17 Protect your end users and IT infrastructure against common ransomware attack vectors and efficiently monitor future threats Purchase of the print or Kindle book includes a free PDF eBook Key FeaturesLearn to build security monitoring solutions based on Microsoft 365 and SentinelUnderstand how Zero-Trust access and SASE services can help in mitigating risksBuild a secure foundation for Windows endpoints, email, infrastructure, and cloud servicesBook Description If you're looking for an effective way to secure your environment against ransomware attacks, this is the book for you. From teaching you how to monitor security threats to establishing countermeasures to protect against ransomware attacks, Windows Ransomware Detection and Protection has it all covered. The book begins by helping you understand how ransomware attacks work, identifying different attack vectors, and showing you how to build a secure network foundation and Windows environment. You'll then explore ransomware countermeasures in different segments, such as Identity and Access Management, networking, Endpoint Manager, cloud, and infrastructure, and learn how to protect against attacks. As you move forward, you'll get to grips with the forensics involved in making important considerations when your system is attacked or compromised with ransomware, the steps you should follow, and how you can monitor the threat landscape for future threats by exploring different online data sources and building processes. By the end of this ransomware book, you'll have learned how configuration settings and scripts can be used to protect Windows from ransomware attacks with 50 tips on security settings to secure your Windows workload. What you will learnUnderstand how ransomware has evolved into a larger threatSecure identity-based access using services like multifactor authenticationEnrich data with threat intelligence and other external data sourcesProtect devices with Microsoft Defender and Network ProtectionFind out how to secure users in Active Directory and Azure Active DirectorySecure your Windows endpoints using Endpoint ManagerDesign network architecture in Azure to reduce the risk of lateral movementWho this book is for This book is for Windows administrators, cloud administrators, CISOs, and blue team members looking to understand the ransomware problem, how attackers execute intrusions, and how you can use the techniques to counteract attacks. Security administrators who want more insights into how they can secure their environment will also find this book useful. Basic Windows and cloud experience is needed to understand the concepts in this book.

microsoft sentinel workbooks github: *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 github: 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 github: 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

microsoft sentinel workbooks github: *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.

microsoft sentinel workbooks github: 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.

microsoft sentinel workbooks github: Microsoft Unified XDR and SIEM Solution Handbook Raghu Boddu, Sami Lamppu, 2024-02-29 A practical guide to deploying, managing, and leveraging the power of Microsoft's unified security solution Key Features Learn how to leverage Microsoft's XDR and SIEM for long-term resilience Explore ways to elevate your security posture using Microsoft Defender tools such as MDI, MDE, MDO, MDA, and MDC Discover strategies for proactive threat hunting and rapid incident response Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionTired of dealing with fragmented security tools and navigating endless threat escalations? Take charge of your cyber defenses with the power of Microsoft's unified XDR and SIEM solution. This comprehensive guide offers an actionable roadmap to implementing, managing, and leveraging the full potential of the powerful unified XDR + SIEM solution, starting with an overview of Zero Trust principles and the necessity of XDR + SIEM solutions in modern cybersecurity. From understanding concepts like EDR, MDR, and NDR and the benefits of the unified XDR + SIEM solution for SOC modernization to threat scenarios and response, you'll gain real-world insights and strategies for addressing security vulnerabilities. Additionally, the book will show you how to enhance Secure Score, outline implementation strategies and best practices, and emphasize the value of managed XDR and SIEM solutions. That's not all; you'll also find resources for staying updated in the dynamic cybersecurity landscape. By the end of this insightful guide, you'll have a comprehensive understanding of XDR, SIEM, and Microsoft's unified solution to elevate your overall security posture and protect your organization more effectively.What you will learn Optimize your security posture by mastering Microsoft's robust and unified solution Understand the synergy between Microsoft Defender's integrated tools and Sentinel SIEM and SOAR Explore practical use cases and case studies to improve your security posture See how Microsoft's XDR and SIEM proactively disrupt attacks, with examples Implement XDR and SIEM, incorporating assessments and best practices Discover the benefits of managed XDR and SOC services for enhanced protection Who this book is for This comprehensive guide is your key to unlocking the power of Microsoft's unified XDR and SIEM offering. Whether you're a cybersecurity pro, incident responder, SOC analyst, or simply curious about these technologies, this book has you covered. CISOs, IT leaders, and security professionals will gain actionable insights to evaluate and optimize

their security architecture with Microsoft's integrated solution. This book will also assist modernization-minded organizations to maximize existing licenses for a more robust security posture.

microsoft sentinel workbooks github: 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 github: The Definitive Guide to KQL Mark Morowczynski, Rod Trent, Matthew Zorich, 2024-05-16 Turn the avalanche of raw data from Azure Data Explorer, Azure Monitor, Microsoft Sentinel, and other Microsoft data platforms into actionable intelligence with KQL (Kusto Query Language). Experts in information security and analysis guide you through what it takes to automate your approach to risk assessment and remediation, speeding up detection time while reducing manual work using KQL. This accessible and practical guide—designed for a broad range of people with varying experience in KQL—will quickly make KQL second nature for information security. Solve real problems with Kusto Query Language— and build your competitive advantage: Learn the fundamentals of KQL—what it is and where it is used Examine the anatomy of a KQL query Understand why data summation and aggregation is important See examples of data summation, including count, countif, and dcount Learn the benefits of moving from raw data ingestion to a more automated approach for security operations Unlock how to write efficient and effective queries Work with advanced KQL operators, advanced data strings, and multivalued strings Explore KQL for day-to-day admin tasks, performance, and troubleshooting Use KQL across Azure, including app services and function apps Delve into defending and threat hunting using KQL Recognize indicators of compromise and anomaly detection Learn to access and contribute to hunting queries via GitHub and workbooks via Microsoft Entra ID

microsoft sentinel workbooks github: ⬆ Microsoft SC-900 (Security, Compliance, and Identity Fundamentals) Practice Tests Exams 211 Questions & Answers PDF Daniel Danielecki, 2025-04-01 □ IMPORTANT: This PDF is without correct answers marked; that way, you can print it out or solve it digitally before checking the correct answers. We also sell this PDF with answers marked; please check our Shop to find one. □ Short and to the point; why should you buy the PDF with these Practice Tests Exams: 1. Always happy to answer your questions on Google Play Books and outside :) 2. Failed? Please submit a screenshot of your exam result and request a refund;

we'll always accept it. 3. Learn about topics, such as: - Azure Active Directory (Azure AD); - Azure Bastion; - Azure Defender; - Azure Firewall; - Azure Policy; - Azure Security Center; - Conditional Access Policies; - Microsoft Cloud App Security; - Microsoft 365 Compliance Center; - Microsoft Defender; - Multi-Factor Authentication (MFA); - Privileged Identity Management (PIM); - Much More! 4. Questions are similar to the actual exam, without duplications (like in other practice exams ;-)). 5. These tests are not a Microsoft SC-900 (Security, Compliance, and Identity Fundamentals) Exam Dump. Some people use brain dumps or exam dumps, but that's absurd, which we don't practice. 6. 211 unique questions.

Related to microsoft sentinel workbooks github

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

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