

END OF STUDY PROJECT REPORT

Bachelors in Computer Engineering SPECIALITY : IOT AND EMBEDDED SYSTEMS

Empowering Corporate Cyber Defense

Developed By YAHYA ABULHAJ



Mentored By:

Mr. BEN ALI Tarek, Executive Director, Cybersecurity at KPMG

Mrs. MARSIT Imen, MARS, Assistant professor in CS at ISTIC

Defended on 8 December 2023, before the jury composed of :

Mr. Wassim ABBASSI : ISTIC - Rapporteur

Mrs. Sana REKIK : ISTIC - President

Period : 13/07/2022 - 29/12/2023

Promotion — 2022/2023

Tribute

“

TO the person who has never given up,

This study report is dedicated to myself, to my strong resilience, and constant pursuit of knowledge. I have been my own cheerleader, motivator, and supporter throughout this difficult journey always.

TL;DR To myself for believing in my abilities even when self-doubt tried to cloud my mind, and for remaining committed to my goals when no one actually cared.

I am grateful for the times when I searched for knowledge outside of textbooks, for the positive and challenging experiences that have shaped my development.

Each setback taught me endurance, each victory fueled my passion, and each lesson contributed to my personal and intellectual growth.

The dedication symbolizes the culmination of my academic journey thus far, serving as a reminder that academic achievements are not the sole factor. Instead, it is my intellectual curiosity and relentless pursuit of understanding that have propelled me in here.

”

- Yaya

قصة نجاح

مرحبًا، أنا يحيى على الطريق إلى ديفوبس، نشأت وترعرعت وسط ظروف اجتماعية صعبة، حيث لم تكن لدي أية ميزة اجتماعية تُعتبر مساعدة. بدأت رحلتي ببناء ذاتي من الصفر، متخذًا من هذه الصعوبات تحديًا لبناء مستقبلي بنجاح. ظللت مصممًا على تحقيق أهدافي بأفعالي، وبنيت خطوة بخطوة طريقي نحو التطور والنجاح.

عملي بجد واجتهاد، مدعومًا بإصرار لا يلين، لتطوير مهاراتي وقدراتي. كان هدفي النهائي هو اكتساب مهارات تقنية متقدمة، وقد أمضيت ساعات وساعات طويلة في دراسة وتطوير مهارات الحوسبة السحابية. تعلمت استخدام أحدث التقنيات والأدوات المتاحة، مما جعلني أتقن هذا المجال.

في كل مرحلة من مراحل رحلتي، واجهت تحديات وصعوبات لم أكن أتوقعها. لكنني لم أستسلم أبدًا، بل عملت بجدية على التغلب على هذه الصعاب. استخدمت خبراتي السابقة والمهارات التي اكتسبتها للنمو والتطور.

اليوم، أنا فخور بما حققته بنفسي. لقد بنيت مسارًا مهنيًا ناجحًا واكتسبت مهارات متقدمة في مجال الحوسبة السحابية. تجربتي تُظهر أن العزيمة والعمل الجاد يمكن أن يتجاوزا أي عقبات.

أثبتت رحلتي أن الإرادة الصلبة والتصميم يمكن أن يحولا الصعوبات إلى فرص. أنا متحمس لمستقبل مشرق، حيث سأستمر في تطوير نفسي ومساهمة ما أستطيع في المجتمع والعالم من حولي.

كلمات مفتاحية :

تكنولوجيا، حوسبة سحابية، ديفوبس، تطوير، مهارات، تقنيات، تكنولوجيا المعلومات، تحسين، برمجة، شبكات، بنية تحتية، أتمتة، سحابة، تخزين سحابي، تطبيقات ويب، أمان المعلومات، تحليل بيانات.

Abstract

In this document, we trace and, present a comprehensive exploration of the author's firsthand expertise and adeptness in navigating and strategizing within the cyberspace. The focus is on advising, executing, and deploying Security Information and Event Management (SIEM) solutions, with a specific emphasis on the latest Microsoft cloud technologies tailored to meet organizational needs.

Our central objective in this account is not only to share insightful observations, challenges, and achievements encountered during our interaction with these security technologies but also to delve into the capacities, attributes, and merits of these tools in bolstering the security frameworks and methodologies.

Our journey starts with the introduction of our organization, where we provide a comprehensive overview of the array of services extended to our valued clientele. Following this, we seamlessly transition into a detailed case study, presenting an in-depth analysis of the methodologies we have employed.

Following that, we present an all-encompassing SIEM setup. This including and not limited to the deployment process, data collection, and analysis. Furthermore, we delve into the intricate correlation of security events aimed at detecting and promptly responding to potential breaches. Practical examples drawn from our extensive experience illustrate how Microsoft Sentinel, a cloud-native SIEM solution, empowers organizations with comprehensive visibility, threat intelligence, and a proactive incident response.

In summary, we deliver actionable recommendations and share invaluable insights. This armament of knowledge empowers you to enhance your security strategies, proactively mitigate risks, and effectively safeguard your organization against the dynamic landscape of cyber threats.

Keywords: Route Optimization, Salesman Problem, Machine Learning, Classification, Security Operations Center, Threat Intelligence, Incident Response, Compliance, Governance, Security Architecture, Threat Hunting, SIEM, Security Policies.

Contents

| | |
|--|-------------|
| Tribute | II |
| Acknowledgment | III |
| Forging Greatness from Adversity | IV |
| Metamorphosis: A Year in Review | V |
| VI | ملخص |
| Abstract | VII |
| General Introduction | 1 |
| 1 Scope Definition and Context | 6 |
| Scope Definition and Context | 6 |
| 1.1 Core Business Activities | 6 |
| 1.2 Presenting the Organism | 7 |
| 1.2.1 NxCi - Startups Merge for Empowerment | 7 |
| 1.2.2 Cybersecurity Architecture For The Cloud | 8 |
| 1.2.3 Cloud Computing Security Catalog | 9 |
| 1.2.4 Author Offering DevSecOps Services | 10 |
| 1.2.5 Swift and Effective Threat Response Solutions | 11 |
| 1.2.6 Exclusive Network Security Offering | 12 |
| 1.2.7 Unwrap the Gift of Consulting and Audit Services | 13 |
| 1.3 Project Odyssey in Pursuit of Knowledge | 14 |
| 1.3.1 Comprehensive Exploration of the Cybersecurity | 14 |
| 1.3.2 Unlocking the Secrets of Azure Cloud | 17 |
| 1.3.3 Mastering Key Azure Cloud Technical Aspects | 18 |
| 1.3.4 Diving Deep into Cybersecurity Products | 19 |
| 1.3.5 Understanding Core Cyber Mechanics | 20 |
| 1.4 Microsoft's Influence on Author Journey | 21 |
| 1.4.1 Foundations Laid Correctly | 21 |
| 1.4.2 Charting My Course To Cybersecurity | 22 |
| 1.4.3 The Make-or-Break: This Specific Exam's Impact | 23 |
| 1.5 Problem Statement and Market Analysis | 24 |
| 1.6 Factors Driving Hacker Activities | 26 |
| 1.7 Methodologies | 27 |

| | | |
|----------|---|-----------|
| 1.8 | Transforming Threats into Frameworks | 28 |
| 1.8.1 | TOGAF Framework Implementation | 29 |
| 1.8.2 | Incident Response Framework | 29 |
| 1.8.3 | Continuous Training | 31 |
| 1.8.4 | Skill Enhancement | 32 |
| 1.8.5 | Championing Cybersecurity Excellence | 33 |
| 2 | Strategic Requirement Assessment | 34 |
| | Strategic Requirement Assessment | 34 |
| 2.1 | Introduction | 35 |
| 2.1.1 | The Significance of this Analysis | 35 |
| 2.1.2 | From Aspiration to Attainment | 35 |
| 2.2 | Exploring the Requirements Landscape | 36 |
| 2.2.1 | Unveiling Functional Needs | 36 |
| 2.2.2 | Non-functional Requirements | 37 |
| 2.3 | Agile Excellence | 38 |
| 2.3.1 | The Symphony of Scrum Roles | 38 |
| 2.3.2 | The Three Pillars of Scrum Artifacts | 39 |
| 2.3.3 | Events Drive Project Momentum | 39 |
| 2.4 | Building A Product Backlog | 40 |
| 2.5 | The Dynamic Landscape of Startup Work | 42 |
| 2.6 | Startups Behind the Scenes | 43 |
| 2.7 | Deconstructing Pieces of Progress | 44 |
| 2.8 | Sprint I: Setting the Foundations | 44 |
| 2.9 | Sprint II: Vigilance and Swift Response | 44 |
| 2.10 | Sprint III: The Art of Refinement | 45 |
| 2.11 | Sprint IV: Customizing, Empower the Shield | 45 |
| 2.12 | Sprint V: DevSecOps, The Never-Ending Vigil | 45 |
| 2.13 | Decoding The 365-Day Gantt Roadmap | 46 |
| 2.14 | The Project Ecosystem | 47 |
| 2.14.1 | The Hardware Realm | 47 |
| 2.14.2 | Team Reconnects in the Real World | 49 |
| 2.14.3 | Software Foundations | 50 |
| 2.14.4 | Tool and Tech of the Trade | 51 |
| 2.15 | Stepping Stones to Sprint Success | 52 |
| 3 | Sprint I: Product Setup and Initial Data Ingestion | 53 |
| | Sprint I: Product Setup and Initial Data Ingestion | 53 |
| 3.1 | Introduction | 54 |
| 3.1.1 | Fine-Tuning Application-Level | 54 |
| 3.1.2 | Securing Data at Its Core | 55 |
| 3.1.3 | Granular Identity Management | 57 |
| 3.1.4 | Advanced Endpoint-Level Security Techniques | 58 |
| 3.1.5 | Security at the Infrastructure Level | 60 |
| 3.2 | System Requirements | 62 |

| | | |
|----------|--|-----------|
| 3.3 | Installation and Configuration | 62 |
| 3.3.1 | Setup Azure Log Analytics Workspace | 62 |
| 3.3.2 | Enable Diagnostic Settings | 63 |
| 3.3.3 | Setup Microsoft Sentinel Instance | 64 |
| 3.3.4 | Data Source Ingestion Pathways | 65 |
| 3.3.5 | Establishing Data Source Connections | 66 |
| 3.3.6 | Building and Visualizing Security Dashboards | 67 |
| 3.3.7 | Get Started With Workbooks | 68 |
| 3.3.8 | Handcrafted Reporting Workbooks | 69 |
| 3.3.9 | Security Reports Exhibition Center | 71 |
| 4 | Foundational Release: SIEM and SOAR in Tandem | 72 |
| 4.1 | Sprint II: Threat Detection and Response | 73 |
| 4.2 | SOCs, Guardians of Cybersecurity | 74 |
| 4.3 | Deciphering Sprint Two | 75 |
| 4.3.1 | Elucidating Operational Strategies | 75 |
| 4.3.2 | Real-Time Incident Response | 75 |
| 4.4 | Threat Detection | 76 |
| 4.5 | Intrusion Detection Systems | 77 |
| 4.6 | Intrusion Prevention Systems | 78 |
| 4.7 | The Unified Security Trinity Systems | 78 |
| 4.8 | Our Approach To Threat Assessment | 79 |
| 4.9 | Creating Built-In Analytics Rules | 81 |
| 4.10 | Code Custom Analytics Rules | 82 |
| 4.10.1 | Prerequisites | 82 |
| 4.10.2 | Creating the Rule using KQL | 82 |
| 4.11 | Manual Incident Response | 85 |
| 4.12 | Incident Severity Exposed | 86 |
| 4.13 | Response Strategy | 87 |
| 4.13.1 | Critical Incidents | 87 |
| 4.13.2 | High-Priority Incidents | 88 |
| 4.13.3 | Medium and Low-Priority Incidents | 88 |
| 4.13.4 | Lessons Drawn from Our Journey | 88 |
| 4.13.5 | A Blueprint for Time Efficiency | 89 |
| 4.14 | Sprint III: Refinement and Automation | 90 |
| 4.15 | The Rise Of UEBA | 92 |
| 4.16 | Create a Cybersecurity Playbook | 94 |
| 4.17 | Logic App Types for Informed Decision-Making | 95 |
| 4.18 | Building a Consumption-Driven Logic App | 96 |
| 4.19 | Next-Gen Connectivity With Azure Logic App | 98 |
| 4.20 | Security Turns Developer Phase | 100 |
| 4.21 | Use Playbooks Templates | 101 |
| 4.22 | Run Playbooks Manually | 102 |
| 4.23 | Unlock SOAR Potential | 104 |
| 4.24 | Navigating Automation Excellence | 104 |
| 4.25 | Create Automation Rules In Sentinel | 105 |

| | | |
|----------|--|------------|
| 4.26 | Empower SOAR With UBEA | 107 |
| 5 | Advancement Release: Integrate and Automate | 109 |
| 5.1 | Sprint VI: Integrate External Technologies | 110 |
| 5.1.1 | A Unified Approach | 110 |
| 5.1.2 | Benefits of Integration | 110 |
| 5.2 | Integrate A Communication Tool | 111 |
| 5.2.1 | Implementation | 111 |
| 5.2.2 | Microsoft Teams From Sentinel Workflow | 112 |
| 5.3 | Integration With Threat Intelligence | 113 |
| 5.4 | A Really One Click Guide | 113 |
| 5.5 | Verify TI Integration | 114 |
| 5.6 | Verify Using TI Indicators | 114 |
| 5.7 | SIEM Theat Intelligence Notify | 115 |
| 5.8 | Visualize TI in SIEM | 116 |
| 5.9 | Microsoft Defender Threat Analytics | 117 |
| 5.10 | Integration With OpenAI | 118 |
| 5.10.1 | Translating Architecture into Actionable Workflow | 119 |
| 5.10.2 | Synergizing Security and AI: | 119 |
| 5.11 | Add a New Step to the Incident Connector | 120 |
| 5.11.1 | Obtain OpenAI API Key | 120 |
| 5.11.2 | Design the Action Prompt | 121 |
| 5.11.3 | Send Output to Sentinel Incident | 121 |
| 5.11.4 | Trigger an Incident | 122 |
| 5.11.5 | Automate OpenAI Target Incident | 123 |
| 5.12 | Exploring Integration and Beyond | 124 |
| 5.13 | Sprint V: Continuous Monitoring, DevSecOps | 125 |
| 5.14 | Sprint Objectives | 126 |
| 5.15 | Closing The IaC Gap | 127 |
| 5.16 | Pre-Coding Preparations | 128 |
| 5.16.1 | Providers In Terraform | 128 |
| 5.16.2 | The Azure Cloud Provider Configuration | 128 |
| 5.17 | Provisioning Microsoft Sentinel | 129 |
| 5.18 | Configuring Connectors | 130 |
| 5.19 | All-In-One DevUnityOps Platform | 131 |
| 5.20 | Design Your Own Pipeline | 132 |
| 5.21 | Trigger Pipeline for Terraform Workflow | 133 |
| 5.22 | Sentinel Version Controllable | 134 |
| 5.23 | Monitoring and Maintenance | 137 |
| 5.24 | Wrapping Up DevSecOps Insights | 138 |
| | Webography | 145 |

List of Figures

| | | |
|------|--|----|
| 1 | Author Helping You Face The Future Threats | 3 |
| 2 | Author Journey Through Life's Wilderness of Endurance | 5 |
| 1.1 | Author Subject Matter Expert - Overall Mission | 6 |
| 1.2 | NGCSC - Next Generation Cybersecurity Consulting Canada | 7 |
| 1.3 | NxCi - Next Generation Consulting International | 7 |
| 1.4 | Author Subject Matter Expert - Cybersecurity ransomware Architecture . | 8 |
| 1.5 | Author Subject Matter Expert - Cloud Computing Security | 9 |
| 1.6 | Author Subject Matter Expert - DevSecOps and beyond | 10 |
| 1.7 | Author Subject Matter Expert - SOAR and SIEM | 11 |
| 1.8 | Author Subject Matter Expert - Networking Security | 12 |
| 1.9 | Author Subject Matter Expert - IT Audits and Consulting | 13 |
| 1.10 | Global Cybersecurity Spending: A Decade Of Potential Growth | 14 |
| 1.11 | Gartner Insights to Develop Your Ideal Security Strategy | 16 |
| 1.12 | Overview of the Great Microsoft Azure | 17 |
| 1.13 | Why Security Products are good for cybersecurity professionals | 19 |
| 1.14 | The Author Microsoft Fundamentals Exams Passing Dates | 21 |
| 1.15 | CIA Triad: A Key Part In Your Cybersecurity Journey | 22 |
| 1.16 | Certificate For passing 180 min exam in just ten with 800+ | 23 |
| 1.17 | Financial Consequences of Cybercrime | 24 |
| 1.18 | Comprehensive Overview of AI Potential Threats and Responsible Apps. . | 25 |
| 1.19 | Data Protection Security Controls | 27 |
| 1.20 | A TOGAF Perspective: Navigating Enterprise Security Architecture . . . | 29 |
| 1.21 | Cyber Incident Response Plan | 30 |
| 1.22 | Key Elements Of Cybersecurity Education | 31 |
| 1.23 | HR Tells Why Training Is Good For YOU | 32 |
| 1.24 | Promoting Collaboration Among Your Team | 33 |
| 2.1 | Project Pioneering: How Needs Analysis Steers the Way Forward | 35 |
| 2.2 | Unlocking Value: Scrum Methodologies and Approach | 38 |
| 2.3 | Easing the Team's Journey to Success: A Tale of A Humble Leadership . . | 42 |
| 2.4 | Team Spotlight: A Personal Look Within | 43 |
| 2.5 | Agile Time-Tested Security: SIEM Implementation Chronology | 46 |
| 2.6 | Gant Chart for SIEM Project Task Management | 46 |
| 2.7 | The untold union, A one year old machine | 47 |
| 2.8 | About the Device System and Hardware | 48 |
| 2.9 | Computer Windows Operating System Specifications | 48 |
| 2.10 | NGCSC Branded Essentials: Cup And, Bag Bundle | 49 |

| | | |
|------|--|-----|
| 2.11 | Unveiling the Software that Shaped My Path and Can Ignite Yours | 50 |
| 2.12 | Computer Essentials: Yaya Potent Instruments | 51 |
| 3.1 | The Initial Security Assessment: Application-Level Focus | 54 |
| 3.2 | The Second Security Assessment: Data-Level Focus | 55 |
| 3.3 | Azure PIM Mechanics: Take Control | 56 |
| 3.4 | The Third Security Assessment: Identity-Level Focus | 57 |
| 3.5 | The Fourth Security Assessment: Endpoint-Level Focus | 58 |
| 3.6 | The Fifth Security Assessment: Infra-Level Focus | 60 |
| 3.7 | Deploy DevSecOps For Infrastructure As Code | 61 |
| 3.8 | Microsoft Azure Log Analytics Workspace Resource Creation | 62 |
| 3.9 | Microsoft Azure Log Analytics Workspace Diagnostic Settings | 63 |
| 3.10 | Microsoft Azure Sentinel Instance Setup | 64 |
| 3.11 | Navigating Event Source Onboarding for Microsoft Sentinel | 65 |
| 3.12 | Onboarding Data: Your First Steps with Microsoft 365 Services | 66 |
| 3.13 | Save Microsoft's Workbook Templates in Sentinel | 68 |
| 3.14 | Create Microsoft's Workbook Templates in Sentinel | 69 |
| 3.15 | Edit Microsoft's Custom Workbook in Sentinel | 69 |
| 3.16 | Accessing and Using Microsoft's Workbook Templates in Sentinel | 70 |
| 3.17 | Azure Portal Company Sign-In Activity Overtime | 71 |
| 4.1 | The Emerge and Advance Of Cybersecurity Since Computer Birth | 73 |
| 4.2 | Security Operations Center, IBM USA Office | 74 |
| 4.3 | Threat Detection Flow Through Network | 76 |
| 4.4 | Intrusion Detection Systems | 77 |
| 4.5 | Inventing the Deep: Jacques Cousteau's Underwater Breathing Apparatus | 79 |
| 4.6 | Heartbeat Dataset Transformation into Timecharts | 80 |
| 4.7 | Configuring Microsoft's Built-In Analytics Rules in Sentinel | 81 |
| 4.8 | Creating a Scheduled Query Analytics Rule In Sentinel | 82 |
| 4.9 | Analytics Rules Tcatics, Techniques and Severity | 83 |
| 4.10 | Analytics Rule Logic In KQL query | 83 |
| 4.11 | Configuring Alert Enrichment and Entity Mapping in Sentinel | 84 |
| 4.12 | Incident Settings Page Configuration | 84 |
| 4.13 | Incident Response Processes | 85 |
| 4.14 | Security Operations, About Incident Severity | 86 |
| 4.15 | Microsoft Sentinel Incident Investigations | 87 |
| 4.16 | SOAR Power Of Combination | 90 |
| 4.17 | Unpacking SOAR Capabilities for Cybersecurity Resilience | 91 |
| 4.18 | A Comprehensive Analysis of User Behavior and Entity Analytics | 92 |
| 4.19 | Quick start playbooks from Automation in left pane | 94 |
| 4.20 | Initial Playbook Creation Steps | 96 |
| 4.21 | Connection Tab in Playbook Creation | 97 |
| 4.22 | Freshly Created LogicApp From Sentinel Playbook | 97 |
| 4.23 | Inside The Idenity Windows Of Logic Apps | 98 |
| 4.24 | Role Assignments For Logic App Connector | 98 |
| 4.25 | Process of Authenticating with Logic App Connector | 99 |
| 4.26 | Code Editor Within The Logic App Designer | 100 |

| | | |
|------|---|-----|
| 4.27 | Where To Look For Playbooks Templates | 101 |
| 4.28 | Run Playbooks Manually Against Specific Incidents | 102 |
| 4.29 | Run Playbooks Failed Because You Need Permission | 103 |
| 4.30 | Assign the required Permission So You can Run Playbooks | 103 |
| 4.31 | Create Automation Rules In Microsoft Sentinel | 105 |
| 4.32 | Types Of Automation Rules Trigger | 105 |
| 4.33 | Types Of Automation Rules Conditions | 106 |
| 4.34 | Types Of Automation Rules Actions | 106 |
| 4.35 | UBEA Microsoft Sentinel Settings Pane | 107 |
| 4.36 | Enable UBEA In Your Organisation | 108 |
| | | |
| 5.1 | Pre-Post Logic App Teams Workflow and Custom Message | 111 |
| 5.2 | Post Sentinel Incidents To Microsoft Teams | 112 |
| 5.3 | Microsoft Threat Analytics Built-In Connector | 113 |
| 5.4 | Microsoft Sentinel Threat Intelligence Custom Query | 114 |
| 5.5 | Defender Threat Intelligence SIEM Indicator | 114 |
| 5.6 | Defender Threat Intelligence SIEM Analytics Rule | 115 |
| 5.7 | Get The Built-In Threat Intelligence Workbook | 116 |
| 5.8 | Defender Threat Analytics Realtime Dashboards | 116 |
| 5.9 | Microsoft Defender Threat Analytics Platform | 117 |
| 5.10 | Sentinel and OpenAI, The Integration Of The Future | 118 |
| 5.11 | Complete Custom LogicApp OpenAI Workflow | 119 |
| 5.12 | Innovation-Driven Incident Response With OpenAI | 119 |
| 5.13 | Create API Secret From OpenAI Platform | 120 |
| 5.14 | Incident and OpenAI Completion Connectors | 121 |
| 5.15 | Add Sentinel Incident Comment Connector To Your Flow | 121 |
| 5.16 | OpenAI Resolved Incident Tactics and Techniques | 122 |
| 5.17 | OpenAI Prompt Design and Incident Shoot | 122 |
| 5.18 | OpenAI Rule Trigger, Condition and Action Spec | 123 |
| 5.19 | OpenAI Automation Rule Listed in Sentinel | 123 |
| 5.20 | Taking a moment to Reflect on Sprint Number Four | 124 |
| 5.21 | Me and The Team Doing DevOps With Sec In mind | 125 |
| 5.22 | Ultimate Benefits Of Using Terraform As Your IaC | 127 |
| 5.23 | Azure DevOps, The All In One Developer Product | 131 |
| 5.24 | Azure DevOps Pipelines Success Jobs | 133 |
| 5.25 | Create Version Control Connection To Sentinel | 134 |
| 5.26 | Use GitHub Authentication As Service | 135 |
| 5.27 | Microsoft Sentinel Version Control Settings | 135 |
| 5.28 | Deployed Sentinel Workbook As Code Via GitHub | 136 |
| 5.29 | The way to Continously Security Monitoring | 137 |
| 5.30 | A DevSecOps Journey of Strategic Reflection | 138 |
| 5.31 | Aurora Aspirations: A Signature Melody for Radiant Futures | 139 |
| 5.32 | Second Consecutive Year as Microsoft Certified Trainer | 152 |
| 5.33 | An Embrace of Excellence: GitHub's Heartfelt Ode to Yahya | 154 |
| 5.34 | yaya2devops GitHub Odyssey: Charting the Contributions of 2023 | 154 |
| 5.35 | AWS Community Builder Welcome Kit 2023 | 155 |

List of Tables

| | | |
|------|---|-----|
| 1.1 | Statistics on Cybersecurity Loses | 15 |
| 1.2 | Key Trends in the Future of Cybersecurity | 16 |
| 1.3 | Microsoft Azure Interesting Facts | 17 |
| 1.4 | Revenue figures for Microsoft Azure from 2017 to 2022. | 18 |
| 1.5 | Early Challenges and Lessons in Product Based Security Evolution. | 19 |
| 1.6 | Understanding SIEM and SOAR in Cybersecurity. | 20 |
| 1.7 | The People Skills of Cybercriminals | 26 |
| 1.8 | Security Frameworks: Cybersecurity Professional Adoption | 27 |
| 1.9 | Overview of Security Frameworks | 28 |
| 1.10 | Technical Skills Required For Your Team. | 31 |
| 2.1 | Product Backlog Batch Initial Sprints | 40 |
| 2.2 | Sprint-End Product Backlog Empowering | 41 |
| 2.3 | Sprint 1: Initial Setup and Data Ingestion | 44 |
| 2.4 | Sprint 2: Threat Detection and Incident Response—Release II | 44 |
| 2.5 | Sprint 3—Release I: Optimization and Training | 45 |
| 2.6 | Sprint 4—Release II: Customization and Integration | 45 |
| 2.7 | Sprint 5—Release II: Continuous Monitoring and DevSecOps | 45 |
| 2.8 | Aspects Considered in the Holistic View of Security | 52 |
| 3.1 | Contributions to Infrastructure Fortification in Sprint 1 | 61 |
| 3.2 | Data Sources for Microsoft Sentinel | 64 |
| 4.1 | Summary of Key Findings and Actions Taken | 76 |
| 4.2 | Comparison of Intrusion Detection And Prevention Systems | 78 |
| 4.3 | Startups on Fire: SOAR Solutions Transforming Cybersecurity Landscape | 91 |
| 4.4 | SOAR Playbooks: Enhancing Cybersecurity Operations | 93 |
| 4.5 | Logic App Types Key Differentiation | 94 |
| 4.6 | Azure LogicApps Consumption Vs Standard Comparison | 95 |
| 4.7 | Matching Logic App Types to Scenarios | 95 |
| 4.8 | Comparison between System-assigned and User-assigned Managed Identities | 99 |
| 4.9 | Many Reasons Why You Got To Try Code Editor | 100 |
| 4.10 | List of Sentinel Playbooks Templates For Quick SecOps | 101 |
| 4.11 | Benefits of Manually Triggering Playbooks in Incident Response | 103 |
| 5.1 | SIEM Empowerment Through Integrations | 110 |
| 5.2 | Example of What Terraform Call Big Providers Of Infrastructure | 128 |

List Of Acronyms

| | |
|------------------|---|
| CoB | <i>Close of Business</i> |
| XSS | <i>Cross-Site Scripting</i> |
| ASAP | <i>As Soon As Possible</i> |
| CEO | <i>Chief Executive Officer</i> |
| VPN | <i>Virtual Private Network</i> |
| SOC | <i>Security Operations Center</i> |
| R&D | <i>Research and Development</i> |
| KPI | <i>Key Performance Indicator</i> |
| APT | <i>Advanced Persistent Threat</i> |
| JSON | <i>JavaScript Object Notation</i> |
| DDoS | <i>Distributed Denial of Service</i> |
| MFA | <i>Multi-Factor Authentication</i> |
| ETTC | <i>Estimated Time To Completion</i> |
| EDR | <i>Endpoint Detection and Response</i> |
| UEBA | <i>User and Entity Behavior Analytics</i> |
| GDPR | <i>General Data Protection Regulation</i> |
| SIEM | <i>Security Information and Event Management</i> |
| ISO 27001 | <i>International Organization for Standardization 27001</i> |

Researched Webography

1. [Microsoft Cybersecurity](#) - Comprehensive cybersecurity solutions and resources provided by Microsoft.
2. [Microsoft Security Orchestration, Automation, and Response](#) - Overview of Microsoft's SOAR capabilities and how they can enhance security operations through automation.
3. [Gartner Cybersecurity Reports](#) - Cybersecurity reports and research from Gartner, providing industry insights and analysis.
4. [Gartner SIEM Magic Quadrant](#) - Gartner's evaluation of Security Information and Event Management (SIEM) solutions in the cybersecurity landscape.
5. [Gartner SOAR Market Guide](#) - Gartner's market guide providing insights into the Security Orchestration, Automation, and Response (SOAR) landscape.
6. [Ms 365 Security](#) - Resources and documentation for securing Microsoft 365 environments and services.
7. [Microsoft Sentinel Documentation](#) - Documentation for Microsoft Azure Sentinel, a cloud-native SIEM and SOAR solution.
8. [Azure SOAR Solutions](#) - Explore SOAR solutions available on the Microsoft Azure Marketplace for enhancing security operations.
9. [Microsoft Threat Intelligence and SIEM](#) - Insights into leveraging threat intelligence with Microsoft's Security Information and Event Management (SIEM) solutions.
10. [Gartner on Cybersecurity Trends](#) - Gartner's insights and forecasts on the growth of worldwide information security spending in 2023.
11. [Microsoft Cybersecurity Blog](#) - Articles and updates from Microsoft's cybersecurity experts covering a wide range of topics in the field.
12. [MITRE ATTCK Framework](#) - Comprehensive knowledge base for adversary tactics and techniques.
13. [SANS Institute](#) - Training and resources on information security and cybersecurity.
14. [CIS Critical Security Controls](#) - Best practices to enhance cybersecurity posture.
15. [Dark Reading](#) - Cybersecurity news, analysis, and insights.

16. [Krebs on Security](#) - Investigative journalism on cybersecurity and online crime.
17. [FireEye Cyber Threat Map](#) - Real-time view of global cyber threats.
18. [TheHackerNews](#) - Cybersecurity news and analysis.
19. [SecurityWeek](#) - News, analysis, and insights on cybersecurity.
20. [ISACA Cybersecurity Resources](#) - Resources and guidance from the Information Systems Audit and Control Association.
21. [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework](#) - Framework for improving cybersecurity in organizations.
22. [Threatpost](#) - Cybersecurity news, insights, and analysis.
23. [CrowdStrike](#) - Industry-leading cybersecurity technology company providing end-point protection and threat intelligence.
24. [Recorded Future](#) - Specializing in threat intelligence, using machine learning to analyze data and predict cyber threats.
25. [CyberArk](#) - A global leader in privileged access management, securing critical assets and sensitive information.
26. [Tanium](#) - Endpoint security and systems management platform offering real-time visibility and control.
27. [Splunk](#) - Known for its powerful data analytics platform, Splunk is widely used for security information and event management (SIEM).
28. [Darktrace](#) - Utilizes artificial intelligence to autonomously detect and respond to cyber threats in real-time.
29. [Palo Alto Networks](#) - Provides next-generation firewalls, cloud security, and advanced threat prevention solutions.
30. [Qualys](#) - Cloud-based security and compliance platform offering vulnerability management and threat intelligence.
31. [Veracode](#) - Focuses on application security, providing automated solutions for secure software development.
32. [McAfee](#) - A global cybersecurity company offering antivirus, encryption, and end-point security solutions.
33. [Dragos](#) - Specializes in industrial control system (ICS) cybersecurity, providing solutions for critical infrastructure protection.
34. [UpGuard](#) - Focuses on third-party risk and attack surface management, helping organizations secure their digital footprint.

35. [Sqreen](#) - Offers application security solutions with a focus on runtime application self-protection (RASP) and real-time monitoring.
36. [IBM Security](#) - Comprehensive cybersecurity solutions and services from IBM.
37. [Check Point Software Technologies](#) - Provider of network security solutions, including firewalls and threat prevention.
38. [Fortinet](#) - Offers cybersecurity solutions, including next-generation firewalls and security-driven networking.
39. [Symantec \(now NortonLifeLock\)](#) - Provides cybersecurity solutions, including antivirus and identity theft protection.
40. [Trend Micro](#) - Specializes in cloud and internet security, with a focus on threat intelligence.
41. [Cylance \(by BlackBerry\)](#) - Utilizes artificial intelligence to provide endpoint security and threat prevention.
42. [Akamai Technologies](#) - Offers cloud security solutions, including DDoS protection and web application firewall.
43. [Rapid7](#) - Provides cybersecurity analytics and automation solutions for threat detection and response.
44. [Forcepoint](#) - Focuses on human-centric cybersecurity, offering solutions for data loss prevention and insider threat protection.
45. [Digital Shadows](#) - Specializes in digital risk protection, helping organizations monitor and manage their digital footprints.
46. [Neustar](#) - Offers security solutions, including DDoS protection and identity resolution services.
47. [Arbor Networks \(NETSCOUT\)](#) - Provides DDoS protection and advanced threat intelligence for networks.
48. [Cybereason](#) - Focuses on endpoint detection and response, using behavioral analytics for threat hunting.
49. [Exabeam](#) - Specializes in user and entity behavior analytics (UEBA) for security information and event management.
50. [Zscaler](#) - Offers cloud security services, including secure web gateways and zero-trust network access.
51. [Sophos](#) - Provides cybersecurity solutions, including endpoint protection, encryption, and email security.
52. [Pulse Secure](#) - Specializes in secure access solutions, including VPN and network visibility for remote and mobile users.

53. [SANS Resources](#) - Cybersecurity training and resources.
54. [Cisco Security](#) - Cybersecurity solutions and products by Cisco.
55. [Juniper Networks Security Solutions](#) - Network security solutions from Juniper Networks.
56. [ESET](#) - Antivirus and internet security solutions.
57. [Bitdefender](#) - Cybersecurity solutions, including antivirus and anti-malware.
58. [F-Secure](#) - Offers cybersecurity solutions, including endpoint protection and threat intelligence.
59. [Palo Alto Networks Cortex XSOAR](#) - Security orchestration, automation, and response platform.
60. [AlienVault \(ATT Cybersecurity\)](#) - Unified Security Management for threat detection and response.
61. [CISA \(Cybersecurity & Infrastructure Security Agency\)](#) - U.S. government agency providing cybersecurity resources.
62. [Cybersecurity & Infrastructure Security Agency \(UK\)](#) - National Cyber Security Centre for the UK.
63. [SophosLabs](#) - Threat intelligence and research by Sophos.
64. [AWS Security Hub](#) - Amazon Web Services (AWS) security hub for centralized security management.
65. [U.S. National Cyber Strategy](#) - Official strategy documents on cybersecurity.
66. [IBM Cybersecurity Services](#) - Professional cybersecurity services by IBM.
67. [MITRE Corporation](#) - Research and development center with a focus on cybersecurity.
68. [UK National Cyber Security Centre](#) - Guidance and resources for cybersecurity.
69. [Canadian Centre for Cyber Security](#) - Cybersecurity information and guidance for Canadians.
70. [National Security Agency \(NSA\)](#) - U.S. government agency providing cybersecurity guidance.
71. [EUROCONTROL Cyber Security](#) - Information on cybersecurity in air traffic management.
72. [European Union Agency for Cybersecurity \(ENISA\)](#) - Agency providing cybersecurity expertise.
73. [US-CERT \(United States Computer Emergency Readiness Team\)](#) - Alerts and tips for enhancing cybersecurity.

74. [Cloud Security Alliance](#) - Promoting security best practices for cloud computing.
75. [OpenStack](#) - Open-source cloud computing platform.
76. [Cloudera](#) - Enterprise data cloud platform.
77. [VMware Cloud Management](#) - Solutions for cloud management and automation.
78. [Alibaba Cloud](#) - Cloud computing services from Alibaba Group.
79. [Linux Foundation](#) - Supports the development of open-source software, including cloud-related projects.
80. [OpenAI](#) - Artificial intelligence research lab working on cloud-based AI solutions.
81. [Red Hat Cloud Computing](#) - Open-source solutions for cloud computing.
82. [Google Cloud vs. AWS](#) - A comparison of Google Cloud and Amazon Web Services.
83. [Ansible](#) - Automation platform for cloud provisioning and configuration management.
84. [DZone](#) - DevOps articles, tutorials, and resources.
85. [DEV Community](#) - Community platform for programmers, including DevOps professionals.
86. [Puppet](#) - Automation software for managing the infrastructure.
87. [TeamCity by JetBrains](#) - Continuous Integration and Continuous Deployment (CI/CD) server.
88. [Prometheus](#) - An open-source monitoring and alerting toolkit designed for reliability and scalability of containers and microservices.
89. [Travis CI](#) - Cloud-based CI/CD service for open-source projects.
90. [Jenkins Plugins](#) - Directory of plugins for the Jenkins CI/CD platform.
91. [CircleCI](#) - Cloud-based CI/CD platform.
92. [GitLab Learn](#) - Resources and documentation for GitLab CI/CD.
93. [Docker Blog](#) - Articles and updates on Docker and container technology.
94. [Terraform by HashiCorp](#) - Infrastructure as Code (IaC) tool for cloud provisioning.
95. [Google Cloud Security](#) - Security solutions for Google Cloud Platform.
96. [Microsoft Azure Security](#) - Security solutions for Microsoft Azure.
97. [IBM Cloud Security](#) - Security offerings and solutions for IBM Cloud.
98. [Oracle Cloud Security](#) - Security services and features for Oracle Cloud.

99. [Oracle Cloud Infrastructure Security](#) - Security practices for Oracle Cloud Infrastructure.
100. [AWS DevOps](#) - DevOps practices and tools on Amazon Web Services.
101. [Google Cloud DevOps](#) - DevOps solutions and practices on Google Cloud Platform.
102. [Microsoft Azure DevOps](#) - DevOps services and tools for Microsoft Azure.
103. [Docker](#) - Platform for developing, shipping, and running applications in containers.
104. [Kubernetes](#) - Open-source container orchestration for automating the deployment, scaling, and management of containerized applications.
105. [Atlassian Continuous Delivery](#) - DevOps practices and tools by Atlassian.
106. [SonarQube](#) - Continuous inspection of code quality during the development process.
107. [GitLab](#) - Web-based Git repository manager with CI/CD pipeline features.
108. [Checkmarx](#) - Application security testing solutions.
109. [Veracode](#) - Application security testing and analysis.
110. [WhiteHat Security](#) - Application security solutions.
111. [Sysdig](#) - Container security and monitoring.
112. [AWS Lambda](#) - Serverless compute service by Amazon Web Services.
113. [Serverless Framework](#) - Open-source framework for building applications with serverless architecture.
114. [Azure Functions](#) - Serverless compute service by Microsoft Azure.
115. [OpenFaaS](#) - Serverless functions made simple for Docker and Kubernetes.
116. [IBM Cloud Functions](#) - Serverless compute service on IBM Cloud.
117. [Google Cloud Functions](#) - Serverless execution environment on Google Cloud Platform.
118. [ZEIT Now](#) - Serverless deployment platform with a focus on simplicity.
119. [Netlify](#) - Hosting and automation platform for modern web projects, including serverless functions.
120. [Azure Logic Apps](#) - Serverless workflow automation platform by Microsoft Azure.
121. [Cloudflare Workers](#) - Serverless computing on the Cloudflare network.
122. [Abyl Realtime](#) - Serverless messaging platform for real-time data streaming.
123. [FaunaDB](#) - Serverless NoSQL database with built-in global distribution.

124. [AWS App Runner](#) - Fully managed service for building, deploying, and scaling containerized and serverless applications.
125. [Nuclio](#) - Open-source serverless platform that runs on Kubernetes.
126. [Nimbella](#) - Serverless cloud platform with built-in CI/CD.
127. [Architect](#) - Serverless framework for building highly available web applications.
128. [OpenFaaS on Kubernetes \(faasd\)](#) - Lightweight serverless functions for Kubernetes.
129. [Pulumi](#) - Infrastructure as Code (IaC) tool for serverless and cloud resources.
130. [NIST Special Publication 800-207](#) - "Zero Trust Architecture" by NIST.
131. [Forrester's Zero Trust eXtended Ecosystem](#) - Forrester's research report on the extended ecosystem of Zero Trust.
132. [Google Cloud Zero Trust](#) - Google Cloud's approach to Zero Trust security.
133. [CIS Controls for Effective Cyber Defense](#) - Framework by the Center for Internet Security aligned with Zero Trust.
134. [Microsoft Zero Trust Adoption Guide](#) - Microsoft's guide on adopting a Zero Trust model.
135. [Lean Analytics](#) - "Lean Analytics" by Alistair Croll and Benjamin Yoskovitz.
136. [User Story Mapping](#) - User Story Mapping and project mastering.
137. [Atlassian Jira](#) - Project management and issue tracking tool.
138. [Product Coalition](#) - A publication on Medium featuring articles on product management.
139. [Mind the Product](#) - A community and blog for product managers and development professionals.
140. [ProductPlan](#) - Roadmap software for planning, visualizing, and communicating your product strategy.
141. [Aha!](#) - Product management and roadmapping software to set strategy, prioritize features, and share visual plans.
142. [Pragmatic Marketing](#) - A comprehensive framework and training for product management and marketing.
143. [Roman Pichler's Blog](#) - Articles and insights on Agile product management and leadership.
144. [Cleverism](#) - Resources for career development, including articles on product management and leadership.

The Author's Recognition as an MCT

I am proud to share my journey towards achieving the MCT credential, a significant milestone in my professional development. In the upcoming March, I will mark the attainment of the title for the third consecutive year.

My pursuit of the MCT began with a passion for Microsoft technologies and a desire to share that knowledge with fellow professionals. I embarked on a rigorous training program, delving into various Microsoft products and solutions.



Figure 5.32: Second Consecutive Year as Microsoft Certified Trainer

My journey involved mastering key technologies, staying abreast of industry updates, and developing effective communication and teaching skills.

This recognition reflects my commitment to excellence in Microsoft technologies and my dedication to imparting knowledge to others. As I continue to accumulate this over the years, my mission to contributing and giving back only strengthens.

MCT Connect Event Of The Year 2022

I had the incredible opportunity to be part of MCT Connect Event of 2022, a gathering that transcended geographical boundaries to bring together a community of dedicated professionals in the realm of technology and education.

The space buzzed with energy as MCTs from diverse backgrounds, experiences, and regions came together. From seasoned trainers to those just embarking on their MCT journey, the event provided a melting pot of expertise and enthusiasm. The agenda was meticulously crafted, featuring workshops, discussions on the latest Microsoft technologies, and invaluable insights into effective training methodologies.



Bundle From Microsoft MCT Connect Event 2022

What added an extra layer of excitement to the event was the special swag bundle sent as part of the invitation. Unboxing the package revealed a curated collection of Microsoft-branded goodies, from exclusive merchandise to practical tech accessories.

There's also a pocket that wasn't featured in the mentioned assets. I've been using it consistently, and it serves as a secure compartment for my passport. It has become a reliable repository that I check before every Pearson VUE session.

A Showcase of GitHub's Finest Graduate

I'm proud to share that I achieved the distinction of being named GitHub Graduate of the Year 2022, an accolade bestowed upon me in recognition of my impactful open-source contributions. This accomplishment reflects not only my commitment to advancing technology but also the collaborative spirit embedded in the open-source community.



Figure 5.33: An Embrace of Excellence: GitHub's Heartfelt Ode to Yahya

In acknowledgment of and contributions, I received personalized letters that underscored the significance of my work. These letters, addressed specifically to me, served as tokens of appreciation for the dedication and impact I've brought to the open-source landscape.

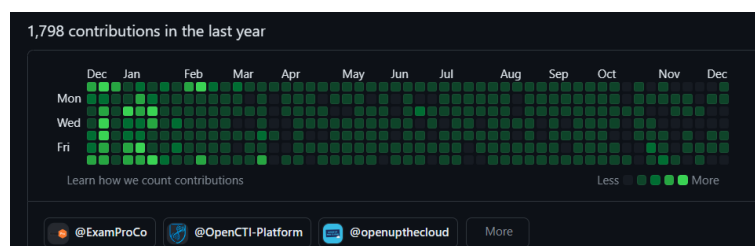


Figure 5.34: **yaya2devops** GitHub Odyssey: Charting the Contributions of 2023

It's immensely rewarding to be recognized at such a level, and it further motivates me to continue my journey of giving my all to the thriving GitHub community.

Final Musings of an AWS Community Builder

In the vast expanse of the cloud, my journey as an Amazon Web Services Community Builder has been an enriching expedition, marked by collaboration, innovation, and recognition on a global scale. Standing among **a select group of only 3,000 Builders worldwide** on march of this 2023, the acknowledgment of my contributions resonates as a testament to the impact we can create as a collective force.

My commitment to fostering a thriving AWS community has taken various forms. From **sharing insights** through blog posts, conducting webinars, to actively engaging in forums and events, I've endeavored to impart knowledge and elevate the understanding of AWS technologies.



Figure 5.35: AWS Community Builder Welcome Kit 2023

As a token of appreciation for my contributions, AWS generously sent a swag package—a tangible acknowledgment that goes beyond the virtual realm.

The swag, adorned with the iconic AWS branding, serves as a reminder of the vibrant community I'm a part of and the impact we collectively make in shaping the future of cloud computing—Let's keep building!

