Tunisian Republic
Ministry of Higher Education
and Scientific Research

University of Carthage

Higher Institute of Information and
Communication Technologies

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 يحي على الطريق إلى ديفوبس، نشأتُ وترعرتُ وسط ظروف اجتماعية صعبة، حيث لم تكن لدي أية ميزة اجتماعية تُعتبر مساعدةً. بدأت رحلتي ببناء ذاتي من الصفر، متخذًا من هذه الصعوبات تحديًا لبناء مستقبلي بنجاح. ظللت مصممًا على تحقيق أهدافي بأفعالي، وبنيتُ 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

List of Figures

List of Tables

List Of Acronyms

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

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 endpoint 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 endpoint 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. Ably 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.

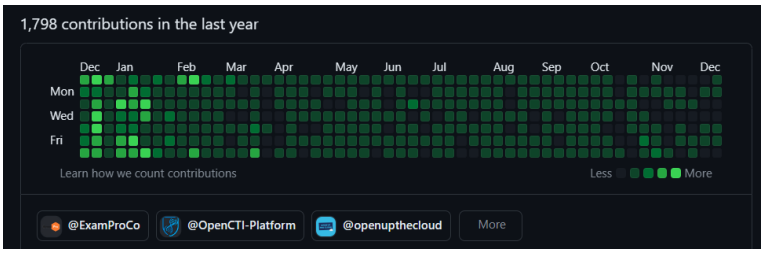

Figure 5.34: **yaya2devops** GitHub Odyssey: Charting the Contributions of 2023

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!