****

* +971-502160203
* Dubai, UAE
* [firnas.ahammad@outlook.com](mailto:firnas.ahammad@outlook.com)
* firnasahammad

 firnasata

Abdulla Firnas

Information Security analyst

**ABOUT ME** “Hello, I’m Abdulla Firnas, a techno-savvy professional with 4+ years of experience as Information Security Analyst. I live in Dubai, but I work with people around the world to deliver the services. I have been involved in the information technology And Cyber Security field and holds professional International certification Like CEH,CSA,Security+. I have strong technical skills in Splunk montoring tool as well as excellent interpersonal skills, enabling me to interact with a wide range of clients. I am eager to be challenged in order to grow and further improve my IT skills. My greatest passion is in life is using my technical know-how to benefit other people and organisations.

**WORK EXPERIENCE** 

Nov 2020 – Present  **Information Security Analyst**

# **Mediclinic Middle East, Dubai (United Arab Emirates)**



* Monitor, triage, prioritize and investigate security events and alerts that are populated in McAfee and Vectra AI.
* Investigating and resolving security incidents and coordinating with different teams for resolution.
* Responsible for end to end security, ensuring that the confidentiality, integrity and availability of all Hospital information data is not breached, infected or compromised in anyway by outside malicious users.
* Create Log monitoring reports on daily, weekly and monthly basis in order to maintain strict SLA adherence.
* Monitor external event sources for security intelligence and actionable events/incidents (DOH, CISA and other sources)
* Develop and implement security policies, procedures, and protocols to safeguard company data and systems
* Conduct regular vulnerability assessments, penetration testing, and risk assessments to identify potential threats
* Provide advice and guidance to the users and stakeholders around threats, vulnerabilities, and security changes
* Maintaining and updating security policies and procedures.
* Monitoring of the security consoles from various SOC entry channels (SIEM, Tickets, Email and Phone).
* Provide an additional layer of monitoring for any events generated through the SOC monitoring tools.
* Monitor network security through multiple devices and solutions such as Network Grade Firewall, IDS/IPS System, Anti-Phishing Solution, Advance Malware Protection System, Security Information and Event Management Monitoring Tool, Vulnerability Assessment Tool, Infrastructure Management Monitoring Tool and Network Access Control.
* URL reviewing and categorization by protecting websites and networks from cyber threats such as malware, denial-of-service attacks, hacks and viruses.
* check for security intelligence feeds and other external event sources.  
  Create, manage, discard and/or dispatch cyber security incident tickets and cases.
* Assist the penetration testing team when it is required.
* Contributing to the development of the security awareness training program for employees.
* Conducting regular security audits and risk assessments. (ADHICS, Pwc)
* Conducting vulnerability assessments and penetration testing.Managed vulnerability for IT and non IT environment. [network/applications/systems na dBiomed devices], ensuring timely completion and effective prioritization.Analyzed vulnerability reports, translating complex technical details into clear and concise explanations
* Escalated critical vulnerabilities to appropriate teams and tracked remediation progress
* Reduced unpatched vulnerabilities by 100% through improved communication and prioritization strategies.



**CERTIFICATION**

Cybersecurity Analyst+ (CySA+)

Certified Ethical Hacker (CEH)

Security+

Certified SOC Analyst (CSA)

**EDUCATION AND TRAINING** 

Aug 2014 – July 2017 Bachelor of Computer Application

# Cochin, Kerala- (India)

**PERSONAL SKILLS** 

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Mother tongue(s) | Malayalam |  | | | | |
| Foreign language(s) | UNDERSTANDING | | | SPEAKING | | WRITING |
|  | Listening | | Reading | Spoken interaction | Spoken production |  |
| English |  | C1 | C2 | C1 | C2 | C1 |
| Arabic |  | A1 | A1 | A1 | A1 | A1 |
| Hindi |  | A1 | A1 | A1 | A1 | A1 |

Organisational Skills

* Security tools: SIEM, IDS/IPS, DLP and endpoint protection.
* Network protocols: TCP/IP, HTTP, HTTPS, DNS, SMTP, FTP, SSH, and SSL/TLS.
* Threat intelligence and vulnerability management.
* Security audits and risk assessments.
* Analytical and problem-solving skills.
* Excellent communication and teamwork skills.Splunk, HP Arcsight, Vectra
* Endpoint solutions McAfee
* Experience with tools: Metasploit, Nmap, Solarwinds, Nesuss, VECTRA AI.

Job-related skills    

Interests   