Abdullah M. AlGhalib AlSharif
Cybersecurity Professional

Nationality	Saudi
Address	Jeddah, Saudi Arabia
DOB	Jan/6/1994
E-Mail	info@alsharifabdullah.net
Website	alsharifabdullah.net
Mobile No.	+966-53-3060-950

ABOUT

Cybersecurity professional with 5+ years of experience in several industries. Experienced different IT & OT Cybersecurity fields as monitoring, incident and vulnerability management. Powerful and versatile thinker who can enhance Cybersecurity posture in the organization.

EDUCATION

Bachelor of Computing and Information Technology in Network Administration and Security
King Abdulaziz University, 2017, (GPA 4.22)

EXPERIENCE

Head of Cybersecurity Monitoring
Saudi Air Navigation Services (SANS)
May 2022 – Present

- Develop plan, procedure, guidelines and playbook
- Ensure to build and enable team for security event/incident identification, risk assessment, quantification, reporting, communication, escalation, monitoring and mitigation.
- Develop dashboards and reports to identify potential threats, suspicious/anomalous activity, malware, etc.
- Assist in the design, evaluation, and implementation of new security technologies.
- Work collaboratively within Cybersecurity to perform event / incident analysis, prepare root cause analysis report and communicate to key stakeholders
- Review detailed investigation and analysis reports for cybersecurity consumption and delivery to management.
- Provide expert analytic investigative support of large scale and complex security incidents.
- Review queries and alerts to detect adversary actions.
- Support in monitoring day-to-day activities to ensure compliance with stipulated policies and procedures.
- Contribute to the identification of opportunities for continuous improvement of systems and processes considering leading practices, changes in business environment, cost reduction and productivity improvement.
- Actively participate in on-the-job training, mentoring and coaching of subordinates.
- Provide clear direction, prioritize tasks, assign and delegate responsibility and monitor the workflow.

Cybersecurity Incident Responder
Saudi Air Navigation Services (SANS)
February 2021 – Present

- Responsible to manage the lifecycle of the cybersecurity incident resolution from CSIRT activation, incident containment, mitigation, full equipment restoration to post incident analysis.
- Leads coordination with asset owners, performs preliminary impact analysis and incident triage
- Act as subject matter expert to provide insight and guidance to colleagues engaging in prevention measures

- Proactive coordinate with appropriate departments during a security incident management, legal, security, operations, and others
- Develop automation algorithm for the remediation of the low-level cybersecurity incidents
- Collaborate and give insight to GRC and Vulnerability Management team
- Maintain incident response documentation and reports
- Conduct and participate table-top and drill exercise to improve the response effectiveness during actual incident
- Contribute to the identification of opportunities for continuous improvement of systems, processes considering leading practices, changes in business environment, cost reduction and productivity improvement.

Manager, Information Security
Middle East and North Africa Beverage (PEPSI)
April 2019 – February 2021

- Develop information security risk assessments and controls activities.
- Design and re-engineer information security policies and SOPs
- Educate, advice and give guidance on information security.
- Manage and provide leadership for the information security function, ranging from planning and budgeting to motivational and promotional activities expounding the value of information security.
- Leads activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with relevant.

Global Shift Lead, Cyber Security Analyst
Saudi Basic Industries Corporation (SABIC)
April 2018 – March 2019

Additional with the previous role :
- Leading and managing my team globally.
- Perform technical quality check to my team members.
- Create, improve and enhanced 12 SOC SOP's.
- Captured incidents recommendation in order to enhance our security controls and rules.
- Handle High incidents.

Global Cyber Security Analyst
Saudi Basic Industries Corporation (SABIC)
July 2017 – March 2018

- Responsible for Investigate, identify, analyze, and remediate exposed security issues using SIEM solution monitoring and detection features.
- Incident handling includes Detection, Analysis, Identification of FPs & TPs, Incident Creation, remediation, follow up and engage with other teams, resolving and closure of incidents.
- Creation of the Daily Report.
- Creation RCA, incident and threat report.
- Work in shifts 24x7 operations.

PROJECTS

- Implementing Full-Cycle Advance Email Protection.
- Improve, Develop and Review Cybersecurity policies, Plans, procedure and playbooks.
- Implementing Network Access Control (NAC) in OT.
- Develop and Execute Security Awareness Program and Training.
- Deployment of Vulnerability Management in IT/OT.
- Implementing EDR Solution in IT/OT.
- Data Center & Disaster Recovery Migration.
- Cyber Security Center Workload Distribution System.