Jaazab Ghalob

Cyber Security SOC Analyst

Professional Summary

Enthusiastic SOC analyst experienced in monitoring and responding to cyber threats across a variety of SIEM solutions. Proven ability to effectively manage and triage incidents, as well as develop and implement required mitigation plans. Expertise in analyzing, articulating and solving various problems. Analytical and organized professional individual comfortable working independently or as part of a team.

Employment

2020-05 - 2022-06

Cyber Security SOC Analyst

Novacoast Inc, Manchester, Greater Manchester

- Worked in a 24x7 Security Operation Center.
- Proactively monitoring, conducting investigations and mitigation of security incidents.
- Performed thorough log analysis of security events obtained from various sources (SIEM, Firewall, IDS/IPS, WAF)
- Identified and investigated IPs, domains, phishing emails for potentially malicious behaviour using multiple OSINT tools and recommend mitigation plans.
- Carried out day-to-day duties accurately and efficiently.
- Used critical thinking to break down problems, evaluate solutions and make decisions.
- Worked flexible hours across nights, weekends and holiday shifts.
- Identified issues, analysed information and provided solutions to problems.
- Trained newly onboarded employees in various

Contact

Address

148 Lovely Lane
Warrington, Cheshire, WA5 1PQ

Phone

07532825419

E-mail

jghalob@gmail.com

Skills

Problem-Solving
●●●●○
Very Good

Security / Network Log Analysis
●●●●●
Excellent

Customer Service
●●●●●
Excellent

MS Office
●●●●○
Very Good

Team Building
●●●●○
Very Good

Familiar with Security Regulations and Standards
●●●●○
Very Good

Experience With Intrusion Prevention / Detection Systems
●●●○○
Good

Windows, Unix, Linux (CLI)
●●●●○

SIEM solutions and tools according to company procedures.
- Conducted regular system monitoring and reporting on the status of systems for optimal performance

SIEM Solutions : Logrhythm, Splunk, Alienvault, Carbon Black, Jira, Azure Sentinel, Proofpoint Communities, ServiceNow, NovaSOC
Resources / Tools : Zabbix, OSTicket, Rocketchat / Teams / Chime, Exchange, OSINT (Framework, AbuseIPDB, virustotal, urlscan, Shodan), Nessus / Qualys scanning, Wireshark / Tshark, Proofpoint, Okta

2019-04 - 2020-04

Cyber Security Researcher / Analyst

ECSC Group, Bradford, West Yorkshire

- Worked in a 24x7 Security Operation Center.
- Investigated security events triggering within client environments / systems and provided recommendations on mitigation plans.
- Trained to monitor PCI DSS compliant environments.
- Reviewed violations of computer security procedures and developed mitigation plans.
- Encrypted data and erected firewalls to protect confidential information.
- Monitored use of data files and regulated access to protect secure information.
- Recommended improvements in security systems and procedures.
- Self-taught Linux command line and well-versed in Windows operating systems.

SIEM Solutions and Tools : Wazuh, Ossec, ModSec, PSQL, Apache, Nessus, Qualys, Wireshark / Tshark, Zip / 7-zip, LibreOffice, Thunderbird, Regex, Malwarebytes

2017-09 - 2019-03

Customer Support Analyst Apprentice

European Metal Recycling Ltd, Warrington, Cheshire

- Resolved technical problems, improved operations and provided exceptional customer service as part of a service desk team.

Very Good

SIEM / Firewall configuration and installation

Good

Knowledge of Network and Security Fundamentals

Very Good

Security Operations Experience

Very Good

- Handled 30+ calls per day to address customer inquiries and concerns.
- Produced PO's for client requests and service desk requirements accordingly.
- Increased customer satisfaction and repeat business through relentless pursuit of resolutions to problems arising from various hardware and software sources, ultimately protecting company reputation and loyal client base.
- Worked with internal users to understand requirements and provide exceptional technical / non-technical service.
- Offered friendly and efficient service to customers, handled challenging situations with ease.

Resources / Tools: Ironport, Cisco Jabber, EDR (MS Defender, Sophos), RSA, Cisco Unified CallManager Administration, Avery Weigh-Tronix (Weighman software), Kaspersky, TeamViewer, Cisco Webex

Education

2016-09 - 2017-06

OCR Level 3 Cambridge Technical Extended Diploma: IT

Warrington Collegiate - Winwick Rd, Warrington, Cheshire, WA2 8QA

[2nd Year]
Grades Awarded Per Unit:

- Digital Graphics: **Distinction**
- Communication Technologies: **Distinction**
- IT Technical Support: **Distinction**
- Computer Networks: **Distinction**
- Website Production: **Distinction**
- Spreadsheets Modelling: **Distinction**
- Computer Game Design: **Distinction**
- Developing a Smarter Planet: **Distinction**
- Project Planning in IT: **Distinction**

Overall Grade : **Distinction* Distinction* Distinction***

2015-09 -

OCR Level 3 Cambridge Technical

2016-06

Subsidiary Diploma: IT

Warrington Collegiate - Winwick Rd, Warrington, Cheshire, WA2 8QA

[1st Year]
Grades Awarded Per Unit:

- Communication and Employability Skills for IT: **Distinction**
- Maintaining Computer Systems: **Distinction**
- Information Systems: **Distinction**
- Troubleshooting and Repair: **Distinction**
- Database Design: **Distinction**
- Business Resources: **Distinction**
- Understanding Social Media for Business: **Distinction**
- Computer Game Platforms and Technologies: **Merit**
- Computer Systems: **Merit**

- Awarded 100% Attendance

2012-05 - 2015-08

GCSE

Bridgewater High School - Warrington, Cheshire, Appleton, WA4 3AE

- Achieved 8 A*-C GCSE's including Maths, English and ICT

References & Certificates

References and certificates can be provided upon request.