ALI ALAMRI

Security Researcher

@ 0xalamri@gmail.com 0540449442 layer0.xyz https://github.com/sh1dow3r www.linkedin.com/in/ali-alamri

OBJECTIVE

Computer security researcher specializing in incident response. Passionate about detection engineering and defensive methodologies. Blackhat speaker and GMON, GDAT, OSCP certified.

EXPERIENCE

Threat Detection & Research Director

Cipher Company for CyberSecurity

Oct 24' - Current Riyadh, SA

- Overseeing operation from DFIR, DE, and CTI departments.
- Developed proactive services to help clients enhance their security posture within the evolving threat landscape.

DFIR Manger

Cipher Company for CyberSecurity

Jan 24' - Sep 24' Riyadh, SA

- Established DFIR department within Cipher including Process, People, Technology.
- Managed incident response and compromise assessment engagements as a team leader.

SOC Team Lead

Cipher Company for CyberSecurity

Aug 23' - Jan 24' Riyadh, SA

- Led security incident investigations, conducted root cause analysis, and formulated prevention strategies.
- Automated playbook workflows using SOAR Platform.

IR Consultant

X-Force IR, IBM

July 22' - Aug 23' Remote

- Managed incident response and compromise assessment engagements as a team leader.
- Conducted proactive services, including tabletop exercises, incident response plan and cybersecurity training.

DFIR Senior Analyst

Saudi Information Technology Company, SITE

July 21' - July 22' Riyadh, SA

- Lead and supported incident response and compromise assessment engagements.
- Developed internal tools and parsers to expedite the investigation process.
- Designed and implemented TheZoo Platform.

Cyber SOC Analyst

Cyber Defense Labs, LCC

Sep 20' - July 21' Dallas, TX

EDUCATION

Rochester Institute of Technology

B.S. in Computing Security

Dec 20'

- Minor in Networking & System Administration
- Overall GPA: 3.70

M.S. in Computing Security

May 21'

- Overall GPA: 4.00
- Master Capstonee: Scalable Infrastructure as Code for Blue/Red Competitions

PROJECTS

layer0.xyz

- Personal website for projects and things I find interesting.

Home Lab

- vSphere cluster deployed on personal server to simulate Security Operations Center environment, Red Teaming environment, and Air-gapped network for malware analysis.

VASE

- Design an automated infrastructure as Code(IaC) to deploy an Airgapped infrastructure using VMware vSphere suite.

TheZoo

- Automated and scalable platform for malware collection and analysis in a unified place.

TCC

- Twitter Covert Communication hidden in plain sight by abusing twitter API

RanSim

- Cross-platform ransomware simulator made to assess organization's security posture and response against ransomware attacks.

Forenware

- Automated collection of forensics images and memory images from VMware vSphere suite.

SKILLS

Languages

- Python, GoLang, Bash, PowerShell, LaTeX

Tools/Software

- Linux & Windows Servers, VMware vSphere Suite, Cisco OS, Palo Alto, PfSense, Ansible, Vagrant, Terraform, Docker, Git, Visio

Certification & Courses

- CCNA R&S, GDAT, GMON, OSCP