Esdras Borba

SECURITY ANALYST

Details

Recife
Brazil
+55(81)981035626
esdras.borba@gmail.com

Links

Portfolio

Github

Linkedin

Skills

SIEM tools

Cyber Defense Frameworks

MITRE

OSINT

Snort

Wireshark

Endpoint security

Splunk

Digital Forensics

Phishing analysis and prevention

Tcpdump

Sysmon

Python

Linux

SQL

Languages

Portuguese

English

Profile

Passionate about security.

Anxious to investigate and solve the foremost problems.

Eager to work in a team environment building safe solutions.

Yearning to start my career under the supervision of an innovation driven institution, willing to learn quickly and help in the growth of the company.

Experience

Cyber Security Student, Part Time, Recife

JANUARY 2023 — PRESENT

Projects

Utilized tcpdump to capture and analyze TCP traffic.

Utilized wireshark to analyze HTTP/s and RDP traffic.

Configured groups and performed administrative tasks with Microsoft Active Directory

Used Sysmon and Event Logs to detect and analyze malicious activities on Windows server, including identifying DLL hijacking.

Used Event Tracing for Windows(ETW) to identify parent-child relationships and malicious .NET assembly loading.

Education

Bachelor's in history, Universidade Federal de Pernambuco, Recife

FEBRUARY 2014 — DECEMBER 2018

Courses

Google Cybersecurity Certificate, Coursera

JUNE 2023 — JULY 2023

Algorithms and Programming Logic from Basic to Advanced, Geek University

FEBRUARY 2022 — FEBRUARY 2022

Python Programming from Basic to Advanced, Geek University

MARCH 2022 — MAY 2022

Basic to Advanced SQL and NoSQL Databases, Geek University

AUGUST 2022 — OCTOBER 2022

Git and Github Developer Essentials, Geek university

NOVEMBER 2022 — DECEMBER 2022

Learn all about Linux! Complete and updated v2023!, Vitor Mazuco

JANUARY 2023 — MARCH 2023