Théo Dufour

+33 6 04 16 11 92 | theo.a.dufour@gmail.com | Lyon, France

Summary

Information security engineer with over 4 years experience as an analyst in Security Operations Centers (SOC) in France and Canada. Worked with multiple SIEM and SOAR solutions to detect and respond to security incidents in a wide range of sectors (energy, manufacturing, health).
Now seeking for a new opportunity, preferably in incident response (CSIRT/CERT) or operational security (SOC) worldwide.

Experience

SQUAD | Lyon, France
Security Consultant | 10/2024 - Present

- Investigation and remediation of security incidents for a client in the energy sector
- Made Splunk dashboards to improve reporting
- Configured the security policy of IPS (Intrusion Protection Systems)

I-Tracing | Montréal, QC, Canada
Security Analyst | 08/2022 - 04/2024

- Developed detection rules to monitor information systems
- Handled alerts and managed incident response in a follow-the-sun model (providing 24/7 SOC services)
- Organised weekly committees with clients to review incidents and service developments
- Improved investigation and response capabilities by automating processes (case format, IOC enrichment) using a SOAR

Cdiscount | Bordeaux, France
Security Engineer | 02/2021 - 06/2022

- Security Operations Center automation (SOAR)
  - PoC using open-source applications exclusively (TheHive, N8N)
  - Deployed and configured a high-availability SOAR solution
  - Python scripts development to automate incident management
- Malware sandboxing : deployed and configured a distributed Cuckoo instance
- Handled security incidents for Cdiscount and clients as a SOC analyst

TEHTRIS | Bordeaux, France
Swift Developer Intern | 07/2020 - 09/2020

- Developed a Mobile Threat Defense (MTD) iOS application to assess the security of a mobile device (iOS, iPadOS)
- Configuration checks, intrusion detection and integration to an XDR platform to manage multiple devices from a single interface

Skills

Splunk, Azure Sentinel, Chronicle SIEM, Python, Chronicle SOAR, Cortex XSOAR, SentinelOne, Crowdstrike

Education

ENSEIRB-MATMECA | Bordeaux, France
Engineering degree | 09/2021
Computer science, specialised in information security, systems and networks

La Prépa des INP | Bordeaux, France
Bachelor degree | 09/2018
Preparatory class in general engineering

Languages

French, English