

Ricardo Camargo De Felice Martin

CYBER SECURITY ANALYST

Profile

Results-driven cybersecurity analyst with a sharp eye for detail and a solid background in troubleshooting. Known for being a dedicated team player who excels at identifying and resolving IT issues. I'm organized and self-motivated, contributing to a secure and collaborative work environment. I'm also passionate about DevOps and PowerShell, with a keen interest in automation to streamline processes and improve efficiency.

Employment History

Cyber Security Analyst, Avatara LLC, St. Louis

JANUARY 2024 – PRESENT

- Deploy and monitor endpoints via Intune and Defender XDR
- Responsible for filling out security questionnaires
- Built custom SIEM infrastructure to monitor network traffic and user behavior.
- Developed custom tools to continuously scan the internal and external networks.
- Responsible for deploying Sophos endpoint protection to servers and workstations
- Sophos certified Engineer
- Develop custom tools to monitor threats and zero-day vulnerabilities
- Investigate incidents and respond quickly in response to events
- Responsible for making detailed incident reaction reports
- Automation of daily reports
- Development of a Secure environment for the Cybersecurity Maturity Model Certification (CMMC)
- Internal Penetration testing
- Web Application testing (OWASP top 10)
- Azure Monitoring

Cybersecurity Lead (Lind Engage), Lindenwood University + Avatara LLC, St. Louis

JANUARY 2023 – DECEMBER 2023

- Developed custom tools to continuously scan the internal and external networks.
- Develop custom tools to monitor threats and zero-day vulnerabilities
- Investigate incidents and respond quickly in response to events
- Responsible for making detailed incident reaction reports

Details

USA

rcfmartin@rcfmartin.com

Links

<https://linkedin.com/in/rcfmartin>

<https://rcfmartin.com/portfolio>

Skills

CMMC Registered Practitioner

Indicators of Compromise (IOCs) Integration

Automation/DevOps/Version Control

Alert Triage and Malicious Actor Identification

Threat Lifecycle Understanding

Networking Proficiency

Malware Analysis

Technical Report Generation

Problem Solving and Solution Pursuit

Effective Communication

Team Player

Intrusion Detection/Prevention Systems

Email Security

Languages

English

Portuguese

Cyber Security Analyst, Avatara LLC, St. Louis

MAY 2021 – JANUARY 2023

- Built custom SIEM infrastructure to monitor network traffic and user behavior.
- Developed custom tools to continuously scan the internal and external networks.
- Responsible for deploying Sophos endpoint protection to servers and workstations
- Sophos certified Engineer
- Develop custom tools to monitor threats and zero-day vulnerabilities
- Investigate incidents and respond quickly in response to events
- Responsible for making detailed incident reaction reports
- Automation of daily reports
- Development of a Secure environment for the Cybersecurity Maturity Model Certification (CMMC)
- Internal Penetration testing
- Web Application testing (OWASP top 10)
- Azure Monitoring

Information Technology Support Specialist, Avatara LLC

JANUARY 2020 – MAY 2021

- Active Directory, DNS, DHCP, Group Policy Management, Print Management, Exchange 2010 – 2019
- Microsoft Windows Operating Systems
- Provide support for desktop hardware & software, laptops, mobile devices, & office appliances such as printers & wireless access points

Education

Information Technology, Missouri Baptist University, St. Luis

JANUARY 2016 – DECEMBER 2019