Andre J. Maccarone

andre@rootninja.com

PROFESSIONAL EXPERIENCE

Stroz Friedberg, an Aon company *Washington, DC*

Manager *(July 2021 – Present)*

- Lead complex incident response and digital forensic engagements including ransomware incidents, business email compromises, APT incidents, and data theft incidents
- Strategize, prioritize, and coordinate analysis on complex and large scale network intrusions to determine root cause and the extent of the breach
- Produce high-quality oral and written work product and deliver expert opinions based on analysis
- Advise clients on remediation efforts and best practices
- Support the mentorship and technical development of junior DFIR staff
- Firm's subject matter expert in AWS forensics

Senior Consultant *(May 2020 – June 2021)*

- Performed deep-dive host forensics across Windows, Linux, and Mac systems
- Examined firewall, web, database, and other log sources to identify evidence and artifacts of malicious activity
- Performed static and dynamic analysis of malware samples and malicious code
- Performed threat hunts across Windows, Linux, and Mac environments using various EDR solutions and artifact collection tools
- Contributed to in-house training sessions and documentation to contribute to the firms development of talent and processes

Consultant *(June 2018 – May 2020)*

- Forensically collected and preserved servers, endpoints, mobile devices, storage devices, and cloud accounts
- Worked on a wide range of DFIR engagements alongside colleagues and client representatives

Cyber Associate *(August 2017 – June 2018)*

- Performed tasks related to technical consulting engagements involving digital forensics, incident response and information security
- Develop and broaden skills through training and research.
- Conduct statistical analysis of large data sets and other investigative components of cases.

Summer Cyber Associate *(June 2016 – August 2016)*

- Performed risk assessments, external and internal penetration tests
- Documentation of methodology and findings
- Created automated log analysis platform for incident response cases

Andre J. Maccarone

andre@rootninja.com

- Worked with teams remotely in 14 different cities
- Presented technical topics to an audience with broad technological understanding
- Created python/bash/PowerShell scripts to automate redundant tasks

Senator Patrick Leahy Center for Digital Investigations *Burlington, VT*

Network Administrator *(August 2013 – May 2017)*

- Managed a Windows domain controller with approximately 50 users
- Managed an air gapped forensic network
- Performed incremental and full backups
- Imaged computers across a network using WDS
- Maintained a Virtualized server environment using ESXI
- Assisted in creating compressive documentation for user policies
- Diagnosed and fixed computer hardware and software related issues
- Setup and managed a centralized SIEM using ELK

EDUCATION

Champlain College[1], Burlington, VT (*May 2017)*

Bachelor of Science in Computer Networking and Cyber Security

Specialization in Cyber Security, Minor in Digital Forensic

ACHIEVEMENTS AND ACTIVITIES

GIAC Certified Penetration Tester (GPEN) (January 2020)

GIAC Certified Forensic Analyst (GCFA) (March 2019)

GIAC Certified Forensic Examiner (GCFE) (March 2018)

2x Participant in North Eastern Collegiate Cyber Defense Competition (NECCDC) (2016 | 2017)

- Tasked with maintaining and defending a network and its services from a team of industry professionals
- Won 3rd place along with 7 other members.

[1] Designated a National Center of Academic Excellence in Information Assurance Education by the National Security Agency and the Department of Homeland Security