Andrew T. Antles
https://www.linkedin.com/in/andrew-antles | https://github.com/andrewantles

Work Experience

Senior Application Security Engineer July 2022 – *Present*
Flatiron Health

- Dynamic and static source code analysis, and remediation plan hand-off.
- Developed internal security training based on LLM research.
- Developed vulnerability management program to address significant backlog.
- Participate in threat modeling exercises.

Senior Application Security Consultant July 2019 – July 2022
Optiv Security, Inc.

- Manual and automated penetration testing of web, API, and mobile apps for Fortune 500 firms.
- Discovered major vulnerabilities and provided remediation steps for:
  - Production data leak allowing unauthenticated access to PII (online banking)
  - Authentication bypass in two mobile applications (airline, and consumer financial)
  - eCommerce checkout bypass allowing free subscription services (auto manufacturer)
  - Misc. high-profile vulns: XXE, cross-site scripting, SQL injection, authorization bypass, etc.
- Tool development in Python and JavaScript: CAPTCHA bypass tool, custom BurpSuite extensions, web requests, file operations, RegEx, etc.
- Developed internal trainings: Attacking CORS mis-configurations; How to exploit CSRF.
- Delivered clear, concise reporting and walkthroughs to technical and non-technical teams.

SIEM Security Consultant April 2018 – July 2019
Optiv Security, Inc.

- Architected SIEM deployments, working with technical and non-technical teams.
- Advanced scripting: API & SQL interaction, ad-hoc automation, etc.
- One of three selected to spearhead new Optiv delivery practice of UEBA platform, Exabeam.
- Team mentor and extensive contributor to internal documentation.

Senior Security Engineer December 2014 – April 2018
NDM Technologies

- SOC Team Lead – developed new SOC practice and mentored junior engineers.
- Senior Networking Engineer: Routing, switching, VLAN, wireless, VPN, DNS, etc.

Other Relevant Experience

- Community: Coach at Spokane Cyber Cup competition: Feb 2022-2024
- Community: Organizer at local DefCon509 group: 2017 – 2021
- Community: Mentor at local Cyber Patriots program: 2017 – 2018

References

Maxwell Dulin – Spokane Cyber Cup organizer MaxwellDulin.com
Senior Security Engineer, Security Innovation

Greg Leonard – Colleague at Optiv Security, Inc.
Managing Principal Consultant, DirectDefense; SANS Instructor

Garrett Freibott – Colleague at Optiv Security, Inc.
Security Engineer, Praetorian Security