Nicholas B. **Anderson**

Security Engineer · Host Based Security Detection and Response · Malware Reverse Engineering

nanderson7@gmail.com | brewfault.io | muffins | nanderson7 | @poppyseedplehzr

Experience

Apple Product Security Engineer, Ecosystem Integrity Protection *Seattle, WA Mar. 2020 - Current*

- Reverse Engineered malware samples affecting the macOS platform
- Developed automation infrastructure of response workflows using AWS cloud infrastructure
- Developed standardized libraries for analyst and investigator workflows

Facebook Security Engineer, Detection Infrastructure *Menlo Park, CA Feb. 2016 - Mar. 2020*

- Architected and executed EDR cluster infrastructre on-prem to cloud migration
- Purchase and integration of third-party Detection-as-a-Service capabilities
- Core developer and maintainer of osquery project - https://osquery.io
- Developed and maintained host-based endpoint monitoring agents, logging infrastructure, and deployment mechanisms
- Administered and orchestrated Carbon Black backend infrastructure
- Built endpoint detections leveraging host-based endpoint telemetry
- Mentor for Facebook Open Source Mentorship program
- Rearchitected corporate DNS blacklisting capability
- Developed security education curriculum for lockpicking and CTF challenges for use in Hacktober security awareness month
- Developed osquery workshop curriculum delivered at conferences to teach endpoint detection at scale

Sandia National Laboratories Cyber Security R&D Scientist and Engineer *Albuquerque, NM Jan. 2015 - Jan. 2016*

- Malware Reverse Engineer on Security Incident Response Teams
- Reverse Engineered and developed C2 generation script for detection of Hammertoss malware
- Mentored Albuquerque High School CyberPatriot team

Sandia National Laboratories Graduate Student Intern *Albuquerque, NM June. 2014 - Aug. 2014*

- Member of the TITANS Center for Cyber Defenders (CCD) Program
- Developed fuzzing framework for email detection engine to test detection rulesets

Trail of Bits Security Intern *New York, NY Jan. 2014 - Aug. 2014*

- Developed platform testing framework for Windows Virtual Machines

Handel IT Software Developer, Systems Administrator *Laramie, WY Sep. 2012 - Aug. 2013*

- C# and .NET software development of RiteTrack5 software suite
- Systems Administrator for Windows 2003, 7, 2008, 2012, and FreeBSD(pfSense) Operating Systems
- Deployed and Administered Nagios Core, monitoring and alerting engine
- Administered Windows SCCM server for agent and software deployments

University of Wyoming, Mathematics Dept. Academic Lecturer *Laramie, WY Dec. 2009 - Apr. 2010*

- Responsible for lectures, student grades, and preparing and issuing class quizzes

University of Wyoming IT Technicianfor Academic Support Unit *Laramie, WY Feb. 2008 - July. 2009*

- Troubleshooting computer issues, maintaining computer labs, and tech support

Education

New York University, Polytechnic Master of Science in Cybersecurity, 3.889 GPA *Brooklyn, NY*

- SFS ASPIRE Fellowship

University of Wyoming Master of Science in Mathematics, **Did Not Complete**, 3.42 GPA *Laramie, WY*

- Computing the refined stability condition, Quarterly of Applied Mathematics - https://goo.gl/A4LCgP
- Upsilon Pi Epsilon Special Recognition Scholarship Recipient, Fall 2012

University of Wyoming Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA *Laramie, WY*

- Outstanding Graduate, College of Arts & Sciences Top 20 in Class, Spring 2010
- Honor Roll, U.W. President's List, 4.0 Semester GPA, Spring 2007, 08, 09
- Varineau Memorial Math Scholarship Recipient, Spring 2009

Conference Talks & Workshops

Oct. 2018	**OSDFcon**, The osquery file carver	*Herndon, VA, USA*
Oct. 2018	**OSDFcon**, Docker Detection and Forensics, 'Gotta catch them all'!	*Herndon, VA, USA*
June 2018	**QueryCon**, Keynote - Evolving Our Open Source Community	*San Francisco, CA, USA*
Nov. 2018	**BlueHat**, Detecting compromise on Windows endpoints with osquery	*Redmond, WA, USA*
Oct. 2016	**Brucon 0x8**, Hunting Malware at Scale with osquery	*Ghent, Belgium*
Sep. 2016	**Structure Security**, Open Source Security Panel	*San Francisco, CA, USA*
Aug. 2016	**DEFCON 24**, Hunting Malware at Scale with osquery	*Las Vegas, Nevada, USA*
Aug. 2015	**DEFCON 23**, Hardware and Trust Security: Explain it like I'm 5	*Las Vegas, Nevada, USA*

Publications

Introducing osquery for Windows *Facebook Protect the Graph Blog* *Sept. 27th, 2016*
https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/

Computing the refined stability condition https://arxiv.org/abs/1207.4101 *University of Wyoming* *July 17th, 2012*

Skills

Programming	Python, C/C++, x86/x64 Assembly, Powershell, Hacklang, sqlite, R
Security Tools	IDA Pro, BinaryNinja, WinDBG, gdb, Wireshark, tshark, nmap, x64dbg, ollydbg, Metasploit, Empyre
Enterprise Tools	osquery, Chef, Splunk, Graylog, AWS, MD-ATP, Windows Active Directory, GPO, SCCM, pfSense, Carbon Black
Skillsets	Malware Reverse Engineering, Infrastructure, Automation, Digital Forensics, SOAR, Lockpicking, Exploitation, CTFs

Honors & Awards

2019	**Regional Winners**, Splunk Boss of the SoC competition	*Seattle, Washington, US*
2017	**Winners**, Splunk Boss of the SoC competition	*San Jose, California, US*
2017	**O'Reilly Security Project Defender Award**, O'Reilly Security Conference	*New York, New York, US*
2014, 15, 17	**Completed and Honor Roll**, FireEye FLARE Reverse Engineering Challenge Competition	*flare-on.com*

Associations

2009 - 2010	**Researcher**, Cryptography Research Cohort	*University of Wyoming Mathematics Dept.*
2009	**Researcher**, NSF EPSCoR Research Fellowship	*University of Wyoming Mathematics Dept.*
2009 - 2012	**Founding Charter Member**, Upsilon Pi Epsilon	*University of Wyoming Computer Science Dept.*
2009 - 2012	**Founding Member and Co-Captain**, Cyber Defense Action League, University of Wyoming Cybersecurity Team	*University of Wyoming*

Extracurricular Activity

Brooklynt Overflow, NYU OSIRIS Lab Co-Captian and Team Lead *Brooklyn, NY* *2013 - 2015*

- Curator of educational program Hack Night, teaching new students about security
- Organizer of CSAW Security Conference
- CTF Challenge author for DHS Forensics competition

Cyber Defense Action League, Univ of Wyo Cyber Security team Core and Founding Member *Laramie, WY* *2009 - 2012*

- Helped found and establish the University of Wyoming Cybersecurity team
- Awarded $15,271.26 for grant proposal to construct Cyber Security Lab
- 1st Place Winner of the North Central Collegiate Cyber Defense Competition in Spring 2011, 12
- Competed in CTF competitions such as CSAW, ASIS, Plaid, and ruCTF
- Gave educational demos around exploitation and malware reverse engineering

Upsilon Pi Epsilon Founding Charter Member *Laramie, WY* *2009 - 2012*

- Helped found and establish the University of Upsilon Pi Epsilon (Computer Science Honor Society) chapter

University of Wyoming Cryptography Research Cohort Researcher *Laramie, WY* *Academic year 2009 - 2010*

- Worked with cohort on deep dives into asymetric crypto routines and co-prime primitives
- Wrote R code for running numerical analysis of research work

NSF EPSCoR Research Fellowship Researcher *Laramie, WY* *Spring 2009*

- Senior research project on the question ”can you hear the shape of a drum?”, analysis of eigen values of wave forms