Christian R. **Crank**

CYBER SECURITY SOLUTIONS ENGINEER

Port Charlotte, Florida

in christian-crank ☎ +1-619-481-8887 ✉ cr4nk@protonmail.com

“I am a Cyber Security Solutions Engineer that uses novel approaches as well as utilizes "out-of-the-box" thinking to mitigate constantly evolving threats. Prior US Navy Cryptologic Technician (Networks) with minor red team and engineering roles for the Cyber Warfare Engineering Team (CWET) in Adelphi, MD under US Navy NIOC MD Department N5-7. I have worked at the National Security Agency (NSA) as a toolset analyst to ensure covertness and obfuscation of said toolsets remained in place. Once out of the military, I have become a security researcher and detection engineer that currently works in the Threat Intelligence sphere to research vulnerabilities and exploits, as well as the indicators of attack and compromise to help create detections for use in Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools. ”

Expertise

Programming	Bash, Python
Operating Systems	Windows Server(2k, 3, 8, 16) Linux(Debian, SuSE, RHEL), FreeBSD, OpenBSD
Virtualization	KVM, podman, docker-compose
Networking	OpenVPN, tcpdump, iptables and nftables, hping3, tcpreplay
AWS	S3, EC2, VPC, IAM
Other	OPSEC, Physical Security Principles, Principle of Least Privilege, Responsible Disclosure

History

Avertium
VIRTUAL

SOLUTIONS ENGINEER, DETECTION ENGINEER
AUG 2018 - PRESENT

- Utilized multiple SIEM technologies to assist customers in creating a security profile, and building rules based on their specific infrastructures.
- Deployed these SIEM technologies on a variety of Hypervisor software, including but not limited to: VMWare/vSphere, Hyper-V, Azure, and AWS.
- Developed dozens of scripts in Python to gather information from multiple APIs including Alienvault Anywhere and BitDefender.
- Developed an API Calling Web Application utilizing Flask for USM Anywhere/Central.
- Worked with EDR teams to assist with SentinelOne, CarbonBlack, and Cisco AMP.
- Assisted in Information Assurance and DFIR during multiple breaches.
- Research into current vulnerabilities and exploits, as well as their indicators to create detections.
- Utilizing EKS to manage a Threat Intelligence platform and bring in information from other sources.

Private Contracting
MCLEAN, VA

PRIVATE CONTRACTOR
AUG 2015 - JAN 2016

- Created and managed a small Search Engine Optimization framework in Python2.
- Utilized using pseudo-randomness to create human-like interlinking and mouse movement to create 'legitimate' looking traffic.

3e Services, LLC
MCLEAN, VA

JUNIOR SOLUTIONS ENGINEER, SUB-CONTRACTOR
SEP 2013 - AUG 2015

- Created multiple STIG (Security Technical Information Guidelines) golden images that adhered to Defense Information Systems Agency (DISA) standards of server safety for a 3rd party while under contract
- Started development on an Electronic Medical Record (EMR) universal translator that would follow specifications in HL7 and FHIR to translate medical coding from one EMR system to another of opposing coding.

TrainACE
GREENBELT, MD

SECURITY RESEARCHER
APR 2013 - SEP 2013

- Leveraged VirtualBox and VMWare to create virtual lab environments for exploitation demos. Utilized custom scripts and known tools such as the MetaSploit Framework, Reaver/Aircrack, Bettercap, Hydra, and mutiple others.
- Stand in instructor for a Certified Ethical Hacker (CEH) Course.

- Created new ideas for PR and Marketing and worked on these ideas to create write-ups and demos to be posted on company blogs and social media to attract customers.
- Spoke for TrainACE at multiple colleges, including Strayer University.

History (continued)

US Navy, NIOC MD Dept. 10/14

NATIONAL SECURITY AGENCY, FORT MEADE, MD

TAILORED ACCESS OPERATIONS/REMOTE OPERATIONS CENTER ANALYST

MAR 2013 - AUG 2012

- Analyzed various agency toolsets and tested them against dummy networks and multiple Personal Security Products (PSPs) and Anti Virus (AV) software to ensure toolset covertness and high-level obfuscation was present.
- Performed analysis on these toolsets due to loss of integrity and provided detailed reports to various high-level developers for further tool development.
- Used Agency-specific debugging tools as well as Windows-specific debugging software to discover malformed code or risks in multiple toolsets and provided extensive reports to assure the toolsets research and development met Agency standards.

US Navy, NIOC MD Dept. N5-7, Cyber Warfare Engineering Team (CWET)

ADELPHI, MD

RED TEAM OPERATOR, SOLUTIONS ENGINEER

NOV 2011 - AUG 2012

- Designed and used penetration testing tools using Perl scripting and physical media, such as wiretaps, "bad USBs", and other I/O devices.
- Directly involved with the development team to create and perform penetration tests against the CWET network infrastructure to assess network security and security policy to identify vulnerabilities and risk.
- Utilized open-source software to develop tools to augment the mission as necessary.
- Steganography using ASCII formatting with Microsoft Paint for use against anti-steganography detection tools to pass messages into the private test network.
- Installed and ran Cat5 Ethernet through the entire workspace, allowing our network infrastructure to scale across the workspace. Improved the networking schema to allow easier access to networking appiances.
- Alpha testing of the virtual 'multi-monitor', a multi-windowed Java platform that allowed different secured networks on one thin-client system. Performed debugging and provided reports to lead developers.

Certifications

Microsoft Azure Security Engineer Associate (AZ-500)

VIRTUAL

JUL 2022 - JUL 2024

Microsoft Azure Fundamentals (AZ-900)

VIRTUAL

FEB 2022 - FEB 2024

Alienvault Certified Security Engineer

VIRTUAL

JUN 2019 - JUN 2022

EC Council Certified Ethical Hacker

VIRTUAL

JAN 2013 - JAN 2014

EC Council Computer Hacking Forensic Investigator

VIRTUAL

JAN 2013 - JAN 2014

Education

US Navy

CORRY STATION, FL

CERTIFICATION, JOINT CYBER ANALYSIS COURSE (JCAC)

- SEP 2011

- 900+ Hour course involving programming, Windows, Unix, Linux, networking, wireless networking, offensive cyber operations, defensive cyber operations, packet analysis, and malicious software analysis. Completed the Joint Cyber Analysis Course without failing any tests and with Honors with a 93% test average.

Will C. Crawford High School

SAN DIEGO, CA

HIGH SCHOOL DIPLOMA

- SEP 2010

- AP Chemistry and Calculus.
- Mu Alpha Theta math honors society.