Resume_Date: 1-28-2022

Brandon J. Tobalski
GLEN BURNIE, MD 21061
Cell Phone : 321.243.1763
Email : btobalskii@gmail.com
Clearance Level : TS/SCI plus Full-Scope Polygraph (Lifestyle)

Resume:
Brandon J. Tobalski
Glen Burnie, MD 21061
BTobalskii@gmail.com
321.243.1763
www.linkedin.com/in/brandontobalski

Professional Summary

Vision-driven candidate with exemplary record of cybersecurity success

Proven talent for aligning organizational strategy and objectives with established cybersecurity paradigms to achieve maximum operational impacts with minimum resource expenditures. Results-focused team leader with a solid military background, recognized for active defensive and offensive posture, enumeration, and analysis skills. Holds marked interest in remote-based managerial opportunities within the industry. Champions innovative solutions to integrate best practices, drive continuous improvement, analyze data, and provide key insights to inform strategic plans. Exceptionally dedicated professional with keen interpersonal and communication skills for the modern information security landscape.

Core Competencies

* Offensive Cyber Capabilities and Strategies
* Team & Project Leadership
* Training & Development
* UNIX, Windows & Mac Command Line Execution & Interpretation
* Reporting & Analytics
* Penetration Testing and Vulnerability Assessment

Professional Experience

Markesman Group LLC, Fort George G. Meade, MD,
SENIOR RED TEAM INTERACTIVE OPERATOR (Federal Contractor), August 2021 - Present

* Excel in the development of operation training networks and exercises for a wide variety of worldwide customers.
* Responsible for providing opposing force actions during live exercise events, in addition to allowing cyber protection teams the chance to experience live network threats.
* Craft detailed TTPs and scenarios based off of Mitre Att&ck Framework adversary data.
* Generate detailed after-action reports.
* Facilitate functions of cyber protection team certification events.

RED TEAM INTERACTIVE OPERATOR, USAF/FEDERAL AGENCY, August 2019 - August 2021
* Orchestrated adversarial emulation against DoD client networks.
* Tasked with maintaining up-to-date training on C2 tool platforms.
* Secured initial foothold on DoD systems, elevating privileges to create system-level persistence for current and future operations.
* Carried out detailed activity logging.
* Leveraged Windows registry manipulation skills.
* Accountable for having surveyed potential threats currently or previously located within client systems.

UNIX BLUE TEAM INTERACTIVE OPERATOR, USAF/FEDERAL AGENCY, March 2017 - August 2019
* Conducted on-site insider threat assessment and analysis, along with onsite vulnerability analysis.
* Devised analytical procedures for the collection of Apple Mac systems for analysis.
* Produced detailed reports and remediations to better secure DoD networks, and assumed responsibility for presenting information to high-level management.

WINDOWS BLUE TEAM ANALYST, USAF/FEDERAL AGENCY, January 2016 - March 2017
* Spearheaded the design of team-wide operational Windows OS to be used in all vulnerability assessments.
* Customized Splunk dashboards to parse DoD customer information for analysis.
* Contributed actively to creating a Blue Team classification guide, as well as streamlining report writing and creation.

Additional Experience

United States Air Force, Patrick AFB, FL, June 2010 - March 2015 | MILITARY POLICE PATROLMAN

Education and Credentials

Bachelor's Degree in Computer Networks and Cybersecurity, 2021

-University of Maryland Global Campus, Adelphi, MD
-Earned Presidential Scholarship and Deans List
Associate Degree in Cybersecurity, 2018
-Community College of the Air Force, Montgomery, AL
Security+ Certification
-COMPTIA Certifications, held from May 2015 - May 2024
GCIH Certification
-SANS Certifications, held from February 2021 - February 2025

Professional Training
Beginners Python programming
Splunk Fundamentals 1 & 2
Basic UNIX fundamentals, System Admin, Power user & RedHat Certified Systems Administration
Certified Ethical Hacking and Countermeasures
SANS Hacker Tools, Techniques, Exploits and Incident Handling (SANS504)
Cisco CCNA Routing and Switching (Expired Certification 2019)
CompTIA A+, Network+, Security+ & Pentest+
Advanced Cyber Defense Operator courses via USAF Technical Training
Dedicated Red Team Tools, Tactics and Techniques course
*Education on various tools used in defensive and offensive roles (can expand upon request)

Additional Information
Technical Proficiencies: Windows command line, Linux command line, Mac OS file system, Active Directory, Microsoft Office Suite, Vulnerability assessment report writing, NMap scanning, Nessus scanning, Burp Suite, Wireshark, Metasploit, Cobalt Strike, VMWare, other various Kali Linux tools.

Interests: Woodworking, Star Wars, Hiking, Travel

References Available Upon Request

CLEARANCE
Intel Agency - Full Scope Polygraph

Resume from V-Source