# Jake **Derkowski**

## CYBER SECURITY ENGINEER · SECURITY OPERATIONS CENTER ANALYST

832-702-9498  |  ✉ jakederkowski12@gmail.com  |  🏠 jderkowski.com  |  JakeDerkowski96  |  jake-derkowski2020

## Professional Experience

**5Q Partners**                                                                                     *Remote, Texas*
JUNIOR CYBER SECURITY ENGINEER                                                           *Jan. 2021 - Present*
- Utilized Logic Applications, tailored KQL queries, and customized analytic rules to increase SIEM efficiency by lowering false positives and automating incident response
- Upheld triage requirements defined by service-level agreements
- Created regular reports illustrating security operation metrics and used log data as basis for the recommendations provided
- Maintained and grew client relations by providing clear and precise communication when escalating incidents

**Website, Inc.**                                                                                   *Houston, Texas*
SYSTEM ADMINISTRATOR                                                                       *May 2020 - Nov. 2020*
- Transferred clients' resources to an updated server where troubleshooting with clients was also a high priority
- Managed a Linux (CentOS) server environment that primarily used Apache2, MySQL databases, and PHP, over 100 client sites
- Quickly responded to customer's concerns and tickets by explaining or troubleshooting over the phone or SSH into their server

## Skills

| | |
|---|---|
| **Languages** | Ada, Agile Methodologies, Bash, C++, Java, PowerShell, Python, Kusto (KQl), SQL |
| **Systems** | Administration and maintenance of Linux/UNIX OS (Kali, Ubuntu, CentOS), Windows 10, and Server 2012R2/2016 |
| **Tools** | Ettercap, exploit-db, M365/O365, Power BI, Git, Metasploit, Nmap, Snort, VMware, WireShark |
| **Network** | Active Directory, Azure, Cloud Computing & Migration,DNS, Firewalls, Group Policy, TCP/IP, Virtualization, |
| **Security** | SIEMs, Basic Splunk Queries, Azure Sentinel, Microsoft Security & Compliance, Threat hunting |

## Education

**Sam Houston State University**                                                                   *Huntsville, Texas*
MASTER OF SCIENCE, INFORMATION ASSURANCE & SECURITY                                       *August 2020 - May 2022*
- Center of Academic Excellence in Cyber Defense Education                                              *(Online)*

**Sam Houston State University**                                                                   *Huntsville, Texas*
BACHELOR OF SCIENCE, COMPUTER SCIENCE                                                      *June 2018 - May 2020*
- Concentrated studies in Information Assurance and Digital Forensics, ABET Accredited
- Philosophy Minor                                                                                **GPA: 3.33**

## Honors & Awards

| | | |
|---|---|---|
| 2020 | **Best Project**, Information Security Class Competition, Sam Houston State University | *Huntsville, Texas* |
| 2020 | **Regional Qualifiers**, Collegiate Cyber Defense Competition | *Remote, U.S.A* |
| 2020 | **Dean's List**, Sam Houston State University | *Huntsville, Texas* |
| 2019 | **Dean's List**, Sam Houston State University | *Huntsville, Texas* |

## Projects

**Cyber Warfare**                                                                                   *Class Project*
SAM HOUSTON STATE UNIVERSITY                                                               *Jan. 2020 - May 2020*
- Constructed a secure, fully functional virtual network using CentOS and Windows Server 2016 systems
- Successfully penetrated opponent's network using social engineering, scanning, enumeration, and exploit db

**Zoom Project**                                                                                    *Research Project*
SAM HOUSTON STATE UNIVERSITY                                                               *Jan. 2020 - May 2020*
- Identified vulnerabilities within the Zoom Video Conferencing application through extensive research
- Captured user credentials via packet poisoning and filtering; cracked with hash-cat
- Successfully discovered the cause of the vulnerability, then provided possible remediation