Five Marketing Modules

**About Me:**

Brandon Krause, I have a Bachelor’s Degree in Communications from California State University, Dominguez Hills. I have four years of experience in Cyber Security.

**Unique Selling Proposition (USP):**

I think like a catcher. As a catcher, it isn’t enough to just know what your job is on the field. You also need to know the jobs of everyone else so you can have a better understanding of how each situation needs to be handled given the surrounding circumstances. I apply this in cyber security because it is the job of a security analyst to know the responsibilities of each IT department and how they interact with each other to create a cohesive and productive technical environment. Understanding the responsibilities of each department allows me to better secure them, and by extension, the system as a whole.

**Skills:**

As the catcher, I use tools to help me monitor the situation and keep an eye on all players and positions. I use Wireshark, Nmap, Splunk, Metasploit. I know what things should look like and what is out of place. I use vulnerability management framework assessment, penetration testing, threat detection and malware detection to help me immediately spot any anomalies. My skills in incident response and malware eradication let me apprehend anomalies before they become issues. I use security related awareness training, incident response plan creation and playbook creation to create a finely tuned security system.

**Projects Summary:**

Have worked as a security analyst for Nordstrom, Labcorp, Infusionsoft and AT&T. Moved from following playbook and procedures to mitigate and prevent security threats to evaluating existing procedures to writing new plans and procedures to help guide lower level analysts.

**Summary of Project:**

Junior SOC Analyst – Monitored SOC systems, including IDS and Splunk and ran vulnerability scans with Nessus to identify weaknesses and prevent attacks, and to detect attacks and mitigate them or escalate them to higher level analysts as needed.

SOC Analyst I – Worked with multiple IT departments to assess their status in terms of security in order to harden their systems. Provided cyber security awareness training to employees so they could follow security best practices. Helped with the creation of playbooks to help guide analysts in their detection and remediation decisions.

Information Security Analyst – Developed Plan of Action and Milestones for threats and weaknesses that we found during vulnerability scans. Performed penetration tests and vulnerability scans regularly, then used those findings to report to management about updating security policies and data loss prevention methods.

Cyber Security Analyst II – Interviewed security team and general IT members to get a feel for common practices in order to reform behavior to harden security operations. Wrote Splunk queries to visualize the most relevant data for easy log monitoring. Tracked forensic efforts to ensure they were being handled properly.

Cyber Security Analyst III – Created plans to remediate discovered vulnerabilities. Conducted penetration tests using Cobalt Strike, Metasploit and Burp Suite. Redefined rules and changed configuration settings in Splunk and Snort. Performed IT risk assessments and worked with various departments to reduce risk.