Tatum Evans: Cybersecurity Analyst I

I am interviewing Tatum, a Cybersecurity Analyst on the Security Operations Center (SOC) team. I work closely with Tatum; she is the professional I've trained under most. Much of my training concerns the responsibilities of Tatum's position. When I asked her how she got into the cyber/IT field, she said she was always interested in figuring out puzzles and solving problems, so naturally, pursuing cybersecurity and security operations was fitting. The investigative aspects of the job were what caught her eye. Tatum was previously in the Navy and got her position by interning through SkillBridge, and she is passing on the knowledge she learned to me.

When asked about the most important knowledge, skills, and abilities needed in cybersecurity, Tatum said it is essential to know incident detection and response, threat intelligence and hunting, some digital forensics, and the city's cybersecurity policies and procedures. These skills and abilities are pertinent to the cybersecurity team on the SOC side because they are responsible for triage and incident response. With this knowledge, a cybersecurity analyst can resolve alerts, mitigate threats, and investigate malicious activity. Some soft skills Tatum mentioned that are important to have are critical thinking, communication, teamwork, adaptability, and attention to detail. As a cybersecurity analyst, I know there could be a new problem to solve daily, so excellent teamwork, critical thinking, and attention to detail will be helpful. Tatum also stresses that adaptability and willingness to learn were soft skills that helped her get the job. They showed her interest in the work and drive to improve.

Technical skills are some of the most important in this field. Tatum brought up some technical skills necessary for the job, most of which she teaches me. As a SOC team analyst, it is important to build a foundation with Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Open-Source Intelligence (OSINT) tools. The primary SIEM tool I've learned about is Splunk, a cloud-based service that collects and organizes big data that could later be useful in threat response and investigations. EDR tools I have been using are Microsoft Defender and Azure to investigate and resolve low-level alerts, phishing submissions, and risky sign-ins. To assist with my task, I used OSINT tools like VirusTotal, Scamalytics, AbuseIPDB, ANY.RUN, and URLScan to scan IPs and links. Tatum and Kris, the SOC team manager, have introduced me to all these tools and taught me. Tatum's Cybersecurity Analyst I position is an entry-level job. It is a great entry-level job to gain experience in cybersecurity and security operations. Kris was a SOC analyst at Dominoes before taking a management position at Virginia Beach.