QinetiQ Employment Experience

Ava Baratz
QinetiQ Inc
CYSE 368 Cybersecurity Internship
Professor Duvall
October 12, 2024
Fall 2024 Term

Table of Contents

Why I chose QinetiQ

When I first began searching for internships, I came across a position for a cybersecurity intern at QinetiQ on LinkedIn. After researching the company a bit more, I decided to apply. I knew that an internship was essential for building the foundational knowledge I needed for cybersecurity and gaining invaluable hands-on experience. I wanted to prepare myself for my career. I revised my resume, hoping to be successful. A couple of weeks later, I interviewed with the internship recruiter. It went well, and I was hired as an intern in June 2023, completing the program by August 2023. After passing my CompTIA Security+, I was rehired in January as a full-time cybersecurity analyst for the organization. Before starting the job, I set several objectives, including building technical skills, understanding cybersecurity frameworks, learning incident response procedures, and professionally collaborating and communicating with a team. In this paper, I will discuss my experience working full-time at QinetiQ, including the type of company it is, the management environment, my work duties, the level of preparation from the ODU cybersecurity curriculum, the most motivating, discouraging, and challenging aspects of the job, and my recommendations for future candidates.

Who is QinetiQ

QinetiQ is a global defense and security contracting organization that works with various federal agencies, including the Department of Defense, the National Security Agency, and the Central Intelligence Agency. QinetiQ focuses on providing engineering and cybersecurity services to government clients. It is considered a mid-size company within the government contracting industry and has merged with and acquired several smaller companies. The organization emphasizes having an impactful work culture where everyone is a leader. It offers considerate employee benefits, including PTO, 401k contributions, paid holidays, and paid maternity leave. QinetiQ encourages employees to build close professional relationships through several employee resource groups that allow individuals to connect and bond over shared interests. The company values diversity, equity, and inclusion and makes significant efforts to ensure that employees from all backgrounds are represented within the organization.

QinetiQ Leadership

QinetiQ employs an organizational leadership chart to outline the roles within the company. Each business unit, such as security, cybersecurity, HR, and communications, is led by a director who reports directly to the CEO. Managers, who report to these directors, oversee teams that range from small to medium in size. In my role, I report directly to the Chief Information Security Officer (CISO). My team consists of three full-time employees and one part-time contractor. I provide daily updates to my manager on the tasks I am working on and address any questions related to my duties.

QinetiQ also follows a structured job architecture that all employees adhere to. There are different career tracks, including professional, technical, and managerial. The professional track involves roles that don’t require extensive technical knowledge, while technical roles are for engineers and hands-on analysts. The managerial track includes leadership roles ranging from

team leads to directors. I am currently on the technical track as a level-one associate engineer and hope to progress to the staff engineer level by next year, after my performance review. All employees set goals around the five company pillars once every fiscal year with their supervisor. Employees must establish impactful goals and try their best to accomplish it by the end of the fiscal year. If all goals are met, the employee is likely to receive a promotion.

Work Duties

I supported the Tethered Aerostat Radar System (TARS) government contract for U.S. Customs and Border Protection (CBP) after joining QinetiQ in January. This program operates aerostats along the U.S.-Mexico border to monitor drug trafficking. The contract has two primary components: operations, which encompass all activities related to flying the aerostats, and infrastructure, which covers the underlying network and technology that sustain the program. I worked on the technology side, completing various responsibilities to ensure the infrastructure proactively supported the mission. In addition to my work on the contract, I also supported the enterprise corporate network. Although I have since transitioned fully to the corporate network, I dedicated 80% of my time to TARS and 20% to the corporate network while working on the contract.

QinetiQ won the TARS contract in December 2024. At that time, the company did not inherit the previous infrastructure and received only a limited number of licenses from the prior contractor. This created a significant amount of work to rebuild the technology infrastructure, including servers, workstations, routers, and more, to support the mission. The team faced tight deadlines and limited resources, making efficient planning essential for success. My manager brought me onto the contract to assist with the transition and reduce the workload on the team of system administrators and network engineers. My involvement allowed us to tackle tasks more effectively and ensure that key components were implemented on schedule.

As a cyber analyst for TARS, I had a technical role that involved governance, risk, and compliance responsibilities, as well as hands-on security engineering tasks. In addition to these duties, I took on a management role, directing the system administrators' activities and presenting the contract’s security status during the weekly operations brief to government clients. This dual responsibility allowed me to bridge the gap between technical execution and strategic oversight, ensuring that our cybersecurity measures were aligned with client expectations. Furthermore, the experience enhanced my leadership skills, as I learned to motivate and guide my team while fostering an environment of collaboration and accountability.

One of my primary responsibilities each week was completing the required cyber deliverables. There were four main deliverables: Vulnerability and Host Discovery Scans, Endpoint Module Security Reports, Asset List, and Network Availability and Latency Reports. Vulnerability scans were performed using licensed vulnerability scanning software, which analyzed each system on the network and generated a list of weaknesses categorized by severity—critical, high, medium, low, or informational. These scans illustrated the security posture of the network assets. We were required to ensure all vulnerabilities were remediated according to system flaw remediation requirements. The system administrators received these vulnerabilities weekly to address and validate their remediation efforts.

The vulnerability scanning software also performed a weekly host discovery scan that reported all IP addresses of systems found on the network, ensuring no unauthorized devices were present. These scans took a considerable amount of time to complete, so I reconfigured them to run during periods of low network activity, preventing disruption to regular operations. By scheduling these scans strategically, I was able to minimize any impact on system performance and maintain a seamless user experience. This proactive approach not only enhanced our network security posture but also demonstrated our commitment to diligent monitoring practices. Additionally, the timely identification of unauthorized devices allowed the team to address potential security risks promptly, further strengthening our overall defense strategy.

The endpoint module security report was generated using Endpoint Detection and Response (EDR) software. This software provided antivirus protection for all network assets and enforced security measures through group policy objects (GPOs). All systems on the network checked in with the EDR server hourly to receive the latest antivirus policies. If a device failed to check in, it became non-compliant. I would remotely access non-compliant devices to troubleshoot their connection with the EDR server, often using the command line to install the latest agent from the EDR server. Once all devices were compliant, I generated a CSV file listing each device's compliance status and the last users to access the systems. This systematic reporting allowed for effective tracking of security compliance across the network, providing valuable insights into potential vulnerabilities. Additionally, the CSV file served as a crucial documentation tool for audits and compliance reviews, ensuring accountability in our security measures. By regularly reviewing this data, I could identify trends and proactively address any issues related to device compliance and security

Additionally, I updated the asset list weekly to ensure an accurate inventory of all devices on the network. I began by gathering the program’s baseline inventory and identifying devices from the host discovery scans. This process involved cross-referencing multiple data sources to confirm that no devices were overlooked. Each device was then listed in the asset list with the correct operating system, firmware, serial number, and make and model. After the team performed system patching, I reviewed the vulnerability scan reports to verify the operating system version and updated the list accordingly. This approach ensured that our records remained up-to-date and facilitated compliance with security protocols.

The final deliverable was the network availability and latency report, created using a network monitoring tool. This tool monitored network routers and reported the mean uptime for the week, as well as any traffic delays. I used this software to help network engineers troubleshoot connectivity issues with routers. By analyzing the data, I was able to identify patterns that indicated potential problems in the network. This information was essential for planning maintenance and ensuring optimal performance. Overall, the report played a key role in maintaining the reliability of our network infrastructure.

I completed these deliverables each Monday and sent them to the Information System Security Officer (ISSO) and the CBP cyber lead for the program. Afterward, I analyzed the vulnerability scan results and endpoint module compliance. I prepared weekly slides that included cyber action items, vulnerability scan results, endpoint security compliance, and endpoint security threats. The vulnerability report provided a high-level overview of the week’s findings, listing compliant vulnerabilities within the patching window and non-compliant vulnerabilities outside

of it. For endpoint threats, I reviewed all software alerts and ensured that users adhered to the required procedures and the computer use policy. I presented these results during the weekly call with government stakeholders for the program.

Additionally, I hosted the weekly change control meeting with the system administrators and network engineers to inform them of the action items for the week and the required remediation. The team raised any concerns about patching or other security issues related to the program. Occasionally, the team explained that they were unable to perform patching due to licensing issues. In such cases, I coordinated with my supervisor to obtain a quote from a vendor, submit a purchase request, and wait for government approval. I also handled ad-hoc requests from the CBP cyber lead and the ISSO, such as conducting network speed discovery at all sites, gathering router configurations, collecting cyber training requirements for all employees in the program, and confirming the security status for various security advisories.

I was also responsible for Windows system patching for the program. I patched offline Windows workstations and validated the results using vulnerability software. Patching could only be completed at specific times to avoid disrupting mission operations. Therefore, I coordinated with site personnel and other technology stakeholders to schedule patching windows during low-impact times. This careful planning ensured that all updates were applied efficiently without interfering with critical tasks. I also communicated with users to inform them about the patching schedule and any necessary downtime.

Additionally, I conducted monthly phishing campaigns for the program to test employees' cyber hygiene. These campaigns mimicked fraudulent emails commonly seen in inboxes, attempting to trick users into providing sensitive information. The phishing reports included data on the number of employees who clicked on links, submitted information, or simply read or deleted the message. Based on their actions, specific training was assigned to the employees. All employees received bi-weekly notifications and had one month to complete the training. I monitored training compliance and responded to any user questions regarding the phishing campaign.

Since this is a government-owned network, the program followed a more restrictive security framework: the National Institute of Standards and Technology (NIST) 800-53 Security and Privacy Controls for Information Systems and Organizations. This framework consists of hundreds of security requirements, called controls, which are grouped by category. These controls cover a wide range of areas, including access management, incident response, and system integrity. Regular assessments and audits are conducted to ensure that all security measures are effectively implemented and maintained. Adherence to this framework is essential for maintaining program compliance and operations. Government programs must obtain an Authorization to Operate (ATO), demonstrating compliance with NIST 800-53.

In May 2024, I conducted a comprehensive one-week security assessment with a small group of cyber team members to evaluate the program's security compliance. We assessed system configurations, vulnerabilities, and NIST 800-53 controls. I led the planning of the assessment, delegating specific responsibilities to each team member. After briefing the plan to my supervisor and obtaining approval from CBP, we proceeded. For security configurations, we followed the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) as best practices for securing all devices on the network. I remotely executed

automated Security Content Automation Protocol (SCAP) benchmarks for the majority of security checks and completed the remaining manual checks onsite using my administrator account. Additionally, I performed printer STIG checks and consolidated the team's findings into an executive brief. I reviewed vulnerability reports and organized a remediation plan. Finally, we hosted group discussions to verify the compliance of each NIST 800-53 control. Once the assessment was complete, I documented all findings in a comprehensive Plan of Action and Milestones (POA&M) for remediation and briefed the results to the government clients.

I transitioned off TARS in early October 2024 to assist my supervisor with enterprise-wide efforts. I trained another analyst on the corporate team to take over my responsibilities for TARS, ensuring she could successfully fulfill the position. This transition gave me more bandwidth to work on other tasks, including a recent pre-assessment engagement for our company's Community Maturity Model Certification (CMMC) Level 2 certification. My company follows the NIST 800-171 framework, which governs the protection of Controlled Unclassified Information (CUI) for non-federal systems and organizations. While less restrictive than NIST 800-53, NIST 800-171 encompasses a variety of security controls.

The CMMC pre-assessment helped QinetiQ Cyber evaluate readiness for certification, which is mandatory for government contractors to confirm compliance with required security controls and regulations. The pre-assessment involved over 100 evidence requests, mapped to NIST 800-171 controls, requiring technical documentation such as policies, firewall configurations, and account management procedures. I organized the evidence requests in a tracker and delegated tasks to the cyber and IT teams. Over a two-week period, I coordinated efforts to gather the necessary documentation and created a SharePoint site with labeled folders for each evidence request. After the teams uploaded the documents, I performed quality assurance to ensure they met the requirements of the control and request. I then submitted the documentation in the compliance portal for review by the third-party assessor. As additional documentation or clarification was requested, I proactively responded to ensure the assessor had the required information. As the compliance administrator for this engagement, I was responsible for ensuring all documentation was submitted and reviewing the assessor's comments.

At the end of the engagement, the assessor provided feedback on controls that were not compliant. Some controls had been implemented but lacked sufficient documentation, so I gathered additional materials to demonstrate compliance. After the review, the assessor re-evaluated and marked those controls as compliant. A few remaining controls were still non-compliant, which were later incorporated into our POA&M for the corporate network. Overall, the engagement was highly successful and provided valuable insight into our enterprise's security posture.

For the corporate network, I am responsible for developing, maintaining, and updating all cybersecurity policies. During my internship in the summer of 2023, I created 15 policies, which aligned with the security control families of NIST 800-171 and covered various other areas, including employee resignations, terminations, and the computer use policy. In my current role, I frequently develop policies based on my supervisor's requests. Most recently, I wrote an Artificial Intelligence (AI) policy that outlines the requirements and limitations for AI use at QinetiQ, following the NIST AI Risk Management Framework (RMF). Moreover, I update all

policies annually, as required by NIST 800-171. All policies I develop are published in a central document repository on the company's SharePoint page for employees to access.

In addition to policy creation, I oversee ongoing monitoring to ensure compliance with NIST 800-171 controls within the corporate network. I established a folder repository where each cyber team member uploads control compliance evidence, which is reviewed weekly. This process ensures we continue adhering to the NIST 800-171 controls implemented across the enterprise to meet regulatory compliance requirements.

One of the specific controls I manage is access control. I ensure that users only have access to necessary systems and do not have unnecessary privileges. Additionally, I review all administrative accounts and their permissions to verify they do not exceed what is required. I also ensure administrators complete privileged user requirements, which include signing access agreements outlining restrictions for admin accounts and completing privileged user training. For contractors and partners working with QinetiQ, I ensure they submit required compliance forms, including non-disclosure agreements, network access forms listing authorized personnel, and cloud computing questionnaires verifying compliance with regulations such as NIST 800-171 and ISO 27001 certification for Information Security Management Systems.

Along with access control, I oversee compliance for QinetiQ's Bring Your Own Device (BYOD) program, which allows employees to enroll personal devices for accessing corporate data, such as emails or Microsoft Teams messages. To manage this, I cross-check the list of enrolled devices from our asset management system with the list of users who have completed required BYOD training. Only employees who have completed training are allowed to enroll. When I identify non-compliant users, I collaborate with the integrated talent management team to assign the necessary training. Furthermore, I review the technical configurations of the BYOD policies enforced through our Mobile Device Manager (MDM) to ensure they meet proper access control standards.

One of my primary responsibilities is incident response. We utilize a range of endpoint security tools to monitor compliance with technical policies and alignment with employee computer use policies. These tools track and alert on various security events, such as administrative actions, malware detection, system failures, and unauthorized activities. My role involves monitoring and responding to these alerts. Upon receiving an alert about suspicious activity, I investigate by identifying the user and device involved and reviewing logs that document the event and related system activity. Once I determine the nature of the security incident, I follow the company's incident handling playbook, which outlines required actions based on the threat type. I document each incident by creating a ServiceDesk IT ticket, which includes incident details for tracking. After executing the appropriate response procedures, I provide an updated report to my supervisor and continue monitoring the affected user's security logs for several days to ensure the issue does not recur.

I also contribute to proposal development to support QinetiQ in winning contracts. Recently, I authored a ten-page System Security Plan (SSP) that outlines QinetiQ's cybersecurity program and the technical measures implemented throughout the organization. In this document, I highlighted how we exceed minimum requirements by incorporating additional frameworks beyond what is mandated. I explained how our network is configured according to Department

of Defense (DoD) best practices and industry standards, ensuring resilience against emerging cyber threats. This in-depth documentation distinguishes QinetiQ from other contracting companies, showcasing our commitment to a robust cybersecurity program and giving us a competitive edge in securing contracts. During the proposal process, I participated in daily calls with selected writers and reviewers, provided daily status updates, and relayed information to my supervisor. Once I completed the draft, it was reviewed by the team, who offered both general comments and specific recommendations. Ultimately, three reviewers praised the draft, giving it an "excellent" rating, with one reviewer identifying it as a strength of the overall proposal. Only minimal edits were needed before finalizing the document.

Beyond my work duties, I am an active member of QinetiQ's Toastmasters public speaking group. I joined to continue developing my professional communication skills and to prepare for future leadership roles. The group provides constructive feedback on various aspects of public speaking, helping me to improve my clarity and effectiveness. Our structured meetings occur monthly, with each member assigned a specific role and responsibilities. The meeting includes an introduction, two main speeches, impromptu table topics, and general evaluations. Roles within the group include the Toastmaster, who organizes and introduces participants, the general evaluator, who monitors punctuality and overall meeting flow, the grammarian, who highlights incorrect word usage or grammar, and the ah-counter, who tracks filler words used by speakers.

Preparation is key for our Toastmasters group. Members must review the meeting agenda in advance and notify the leaders two weeks ahead of time if they cannot attend, allowing for role reassignment. Each member completes an icebreaker speech within a couple of months of joining, which typically includes personal information, such as their role in the company and their reasons for joining Toastmasters. Following this, members deliver a 5-7 minute speech on any topic of their choice. Evaluators assigned to each speaker offer constructive feedback at the end of the meeting.

I am also part of the Toastmasters public relations group, which promotes our activities within the company and helps recruit new members. We meet bi-weekly to discuss strategies for reaching our public relations goals, including hosting open houses to introduce the group and developing marketing plans to reach our target membership. During these meetings, we brainstorm creative ideas to engage potential members and highlight the benefits of joining Toastmasters. We also review feedback from previous events to improve our future outreach efforts and ensure they resonate with employees. Additionally, we collaborate on crafting messages that effectively communicate our group's mission and the skills participants can gain through public speaking.

Preparation from ODU

The Old Dominion University (ODU) Cybersecurity curriculum equipped me with essential soft skills for collaborating with team members and communicating effectively with management. Throughout my time at ODU, I participated in numerous group projects that required teamwork, careful planning, coordination, and collaboration to divide the workload and complete the assignments efficiently. These experiences not only enhanced my ability to work cohesively within a team but also fostered a deeper understanding of diverse perspectives and problem-solving approaches. Engaging with peers from different backgrounds allowed me to

appreciate the importance of adaptability and open communication in achieving common goals. Furthermore, the challenges we faced as a team strengthened my resilience and commitment to excellence, preparing me for the collaborative nature of the cybersecurity field.

Moreover, the time management skills I developed at ODU have been invaluable in my current position. During my busiest semesters, I often faced multiple assignments due each week. To stay on top of deadlines, I meticulously planned my schedule, dedicating specific time slots throughout the week for each task. Sometimes, I needed to adjust my schedule when assignments took longer than expected. This ability to manage and re-prioritize my time has been equally critical in my current role, allowing me to meet deadlines and stay organized. It has enabled me to complete my tasks in a timely manner while also providing the flexibility to focus on other projects.

However, I believe the ODU Cybersecurity curriculum lacked the technical depth necessary for my position. While the program provided foundational knowledge in areas such as the CIA triad and basic networking concepts, it did not cover practical skills, like configuring vulnerability scans or applying patches, that I need in my job. I found that hands-on experience is the most effective way to learn these skills, which are challenging to grasp in a classroom setting without live practice. Additionally, much of my role revolves around understanding complex frameworks and regulations. Although the curriculum introduced a few basic frameworks, it didn't provide the level of detail my job requires. Early in my position at QinetiQ, one of my primary tasks was studying entire frameworks, such as NIST 800-171, to fully understand the comprehensive security requirements.

Similarly, many of the labs I completed at ODU focused on Linux and Python, including password cracking using tools like Cain and Abel and John the Ripper, ethical hacking with the Metasploit framework, and developing client-server scripts in Python. In my current role, however, I do not use Linux or Python, as QinetiQ assigns specific roles for these technologies, such as database administrators and network engineers. Instead, I work primarily in Windows. Since I didn't perform any Windows administration labs during my time at ODU, I had to learn various aspects of Windows administration on the job. This included becoming familiar with the Windows registry, Local Group Policy settings for security configurations, and using the Windows Event Viewer to review logs.

Discouraging, Challenging, and Encouraging Aspects of the Job

One of the challenging parts of my job is handling unexpected problems as they come up. Recently, I was involved in supporting contingency planning for the upcoming Hurricane Milton to ensure that our disaster recovery solution was effective. I helped my supervisor plan a series of priority actions for the team to complete and ensured that the team were properly documenting the actions taken with the correct time stamps. Similarly, incident response requires attention right away, which can be stressful, especially when there's no time to waste. In situations like this, it's important to stay calm and focused to make the right decisions. Also, coordinating with different teams and making sure everyone understands their role adds to the challenge. Overall, these experiences show me how important it is to be flexible and prepared for anything that might happen.

On the other hand, the most encouraging aspect of my job is the support I receive from my coworkers. The team consists of highly experienced professionals—many with over 20 years in the field—and they have been incredibly helpful and supportive. Their willingness to share their knowledge and experiences has created a collaborative environment where I feel comfortable asking questions. I regularly meet with each member of the cyber team to learn more about their specific responsibilities and gain insights into different cybersecurity technologies. During these discussions, I have gained practical tips and tricks that have enhanced my understanding of the field. They have also provided valuable advice on improving my resume and introduced me to cybersecurity workshops. Additionally, they've guided me in identifying areas where my skills are best suited and which career paths offer stability and growth opportunities.

Employees can tailor their development paths to align with their personal career goals, whether that involves enhancing technical skills, pursuing leadership training, or staying updated on the latest cybersecurity trends. This flexibility ensures that each team member can cultivate expertise that benefits both their professional journey and the company's objectives. The result is a work environment focused on constant improvement, where team members share knowledge and work together effectively.

Objectives

Overall, my job has met the objectives I set at the start of my role. I have gained a wide range of technical skills and a solid understanding of governance, risk, and compliance procedures, all of which will be beneficial in my next position. I have also learned the key elements of incident response procedures and how to communicate effectively with both my team and management. Over the past year, I have accumulated full-time experience in the cybersecurity field and am grateful to have had this opportunity for professional development before graduating from ODU. I look forward to further honing my technical and soft skills as I work toward entering a security engineering role.

Recommendations

One of the most crucial things that can help a candidate succeed is gaining technical experience prior to starting the job, which can be achieved through certifications. I currently hold the CompTIA Security+, CompTIA CySA+, CompTIA CASP+, and AWS CCP certifications. These credentials have allowed me to better understand my job and participate in more technical conversations with system administrators and network engineers. To pass these certifications, I practiced hands-on skills in virtual labs, which have been instrumental in helping me excel in my role. I highly recommend that future candidates start their careers with at least a CompTIA Security+ certification, as it provides the foundational knowledge required for any entry-level cybersecurity position. This certification is widely recognized as the industry standard for entry-level cyber roles.

I also recommend that candidates network with their coworkers. In cybersecurity, who you know is incredibly important. Building relationships with colleagues can lead to introductions to industry leaders or mentors who can help further your career. These interactions also offer valuable knowledge that would take years of experience to learn independently. Your coworkers

can teach you about different areas within the field, helping you become a well-rounded cybersecurity professional, which ultimately makes you an asset to any organization.

Additionally, candidates must stay well-informed of the emerging industry cyber threats. Cybersecurity is a dynamic industry where new vulnerabilities and sophisticated attack methods are constantly surfacing, often at a rapid pace. Threats like ransomware, phishing schemes, and zero-day exploits continue to evolve, requiring professionals to be proactive in understanding the latest trends. Staying well-informed about these threats is essential because attackers adapt their tactics based on advances in technology and defenses. By keeping up with industry news, threat intelligence reports, and ongoing developments in cybersecurity tools, you can ensure your skills and knowledge remain relevant. Being well-prepared allows you to anticipate and mitigate risks before they escalate, ultimately helping to safeguard sensitive information and maintain trust. In this fast-paced environment, continuous learning is key to maintaining a robust security posture.

Conclusion

My time at QinetiQ has been an invaluable experience, allowing me to acquire extensive knowledge in the cybersecurity field. The hands-on technical skills I've gained, coupled with exposure to real-world challenges, have thoroughly prepared me for future roles in security engineering. The diverse range of projects I've worked on has helped me develop a deeper understanding of key cybersecurity concepts and best practices. I am confident that the knowledge I've accumulated at QinetiQ, along with the mentorship I've received from experienced professionals, has provided me with a strong foundation to excel in my career. Their guidance has not only sharpened my technical abilities but also enhanced my problem-solving and analytical skills.

I look forward to applying these skills as I continue to grow professionally. I am eager to take on new challenges that will help me further refine my expertise and leadership abilities. With the fast-paced nature of cybersecurity, there is always something new to learn, and I'm excited to stay at the forefront of emerging threats and technologies. This journey has not only solidified my passion for cybersecurity but also illuminated a clear path toward achieving my long-term career goals. I am driven to pursue new certifications and specializations, positioning myself as a valuable asset in the ever-evolving security landscape.