Completed application form – a perfect example (Principal Title)

The following is an example of what good looks like in a completed application form from an individual applying for the **Principal Title in the Security Testing specialism**. The individual provided clear, structured STAR evidence, against each of the professional competencies.

A: Knowledge, Understanding & Experience

A1: Are engaged in a role or have practical experience of activities that have a degree of complexity within their Specialism.

Situation: Recently, I was approached by a government agency that had just experienced a significant security breach within their on-premises IT environment. The breach raised critical concerns about the security of their entire infrastructure, leading the agency to fast-track their ongoing migration to the cloud. They had already deployed two Azure cloud environments but needed assurance that these environments were secure before going live. The agency was particularly concerned about potential vulnerabilities and wanted to ensure that the configurations were robust enough to withstand similar attacks that had compromised their on-premises systems.
Given the high stakes, the agency sought a security assessment. They tasked me with planning and executing a thorough review of these Azure environments from both an external, red team perspective and an internal configuration audit. The goal was to identify and mitigate any vulnerabilities that could be exploited by attackers, whether from outside or within the organisation. This required careful planning and precise execution, as the environments needed to be tested without causing disruption or downtime. The agency relied on my expertise to ensure that the transition to the cloud would not replicate the security flaws that had led to their recent breach.
Task: I led multiple asset discovery exercises and penetration tests against their production lines. The results of this needed to feed into the detailed risk assessments our Risk team was compiling for the wider business.

Action: Testing in OT environments is complex. There is a generally higher risk of causing costly disruption due to the nature of the equipment within the networks. This is largely due to the use of legacy equipment which expects only given inputs and break if unexpected data reaches them.
I took appropriate precautions when connecting to each production line in line with my specialist training and experience. This included selecting suitable tools for the task based on my knowledge of how different tooling may affect the OT network.
I started by running passive tooling to understand the network and the risks that I was likely to pose to its operations. I progressed to very targeted active techniques against certain low-risk assets in agreement with the system owners. Some of the activities I conducted included:

- Establishing what "normal" looked like on the network.
- Understanding what protocols and devices were transmitting data across the network.
- Understanding what devices were likely to pose the highest risk if they were to receive malformed packets/unexpected data.
- Taking a manual and very cautious approach to probing the network to identify any other devices and attempting to identify any potential routes to other networks/the internet in line with the penetration testing scope.

Result: The culmination of my efforts was a comprehensive and detailed report, which I personally presented to the client through a structured walkthrough. During this session, I led the team in highlighting the key findings and areas of concern within the Azure environments. Our assessment revealed that several aspects of the configuration did not meet compliance standards and that the overall attack surface had not been sufficiently minimised. Specific issues, such as overly permissive NSGs and weak access controls, were identified as critical vulnerabilities that needed immediate attention. The lack of MFA across all users was also a significant issue, with a proof of concept supplied to list brute force attacks.
In addition to identifying these vulnerabilities, I provided actionable recommendations to strengthen the environment. I and the team worked closely with the client to revise and implement a more robust ruleset that limited who could access the cloud environment. This included enhancing the security of the Azure VPN to ensure that only authorised users could connect to the network, thereby reducing the risk of unauthorised access, MFA, IP whitelisting played an important factor here. I also addressed issues related to the rotation of access keys and the enforcement of stricter permissions on storage accounts, which are often overlooked but can be significant points of failure if not properly managed.
The client was highly impressed with the depth and thoroughness of the review. They particularly appreciated my expertise in Azure and the practical solutions provided to secure their cloud

environment. The feedback from the agency was overwhelmingly positive, and they expressed their confidence in the work by offering the opportunity to conduct annual reviews. This ongoing relationship will ensure that their cloud environment remains secure and that any emerging threats are promptly addressed, providing them with the peace of mind they need to operate securely in the cloud.

A2: Applied problem solving tools and techniques in meeting customer / organisational requirements.

Situation: I was faced with two challenging situations where my ability to apply analytical problem-solving was critical to meeting the client's security assessment requirements. The first scenario involved a client who had a highly locked-down internal environment. Their infrastructure was accessible only through virtual desktop infrastructure, which severely limited what I could run due to restrictive internal policies and the presence of Windows Defender. These restrictions made it difficult to conduct the necessary active directory review and run the essential tools for a complete and professional security assessment. The situation demanded an innovative approach that could bypass these security measures without triggering alerts or violating the client's security protocols.
In a separate case, I was engaged by a client who required a security assessment of their internal cloud environment. However, the client's strict security policies only allowed onsite access to their cloud environment, and external consultants were not permitted to be physically onsite. This restriction posed a challenge, as it meant that the necessary security tools and techniques, such as Nessus for vulnerability scanning and Nmap for network exploration, could not be directly deployed within the client's environment. The client's security policies were non-negotiable, so I had to devise a solution that would allow me to conduct a thorough assessment remotely while respecting their access constraints.
Task: In both scenarios, my primary task was to find secure and effective methods to conduct the required security assessments despite the limitations imposed by the clients' environments. For the first client, I needed to bypass the restrictions of the VDI environment to gather the necessary data for an Active Directory review. This involved overcoming the defences set by Windows Defender and the internal policies that limited the execution of tools. The goal was to ensure that the AD review could be conducted without compromising the integrity of the client's security systems.
For the second client, my task was to establish a secure remote access solution that would enable me to run the necessary security tools from a distance. Given that the client's internal cloud environment was accessible only onsite, I had to create a method to securely connect to their environment remotely. This would involve setting up an infrastructure that could simulate onsite access while adhering to the client's strict security protocols. My goal was to ensure that the entire internal cloud

environment was thoroughly reviewed, including all hosts and networks, without needing physical access.

Action: In the first scenario involving the VDI environment, I began by thoroughly analysing the security measures in place, particularly focusing on how Windows Defender and the internal policies operated. I realized that a direct approach would likely trigger alerts or be blocked entirely, so I opted for a more sophisticated method. I deployed a Command and Control (C2) framework, which allowed me to establish a secure communication channel with the remote environment. This approach enabled me to run necessary tools for the Active Directory review without triggering security defences. I carefully selected C2 techniques that would remain under the radar, ensuring that the client's security systems would not flag the activity as malicious. Through this method, I successfully gathered the required data for a comprehensive AD review, providing valuable insights to the client without compromising their security posture.

For the second scenario, where onsite access to the internal cloud environment was restricted, I approached the problem by leveraging my expertise in Azure cloud technologies. I set up an Azure VM within my organisation's cloud environment, configuring it to be highly secure and compliant with both my organisations and the client's security policies and exported this to be sent to the client. The VM was locked down to only allow access through our company VPN, ensuring that it was protected from unauthorised access. I then implemented port forwarding techniques to establish a connection from the Azure VM to the client's internal cloud environment. This setup effectively simulated onsite access, allowing me to run security tools like Nessus and Nmap remotely.

In addition to setting up the remote access, I engaged in discussions with the client about the possibility of VPN peering. By establishing a secure VPN peering connection between our environments, I was able to gain full visibility of all hosts within the client's cloud infrastructure. This allowed me to perform a thorough assessment, including automated scans and manual inspections using tools like RDP, to identify any vulnerabilities or misconfigurations. This approach not only met the client's security assessment requirements but also respected their stringent access controls.

Result: The outcome of these efforts was highly successful in both scenarios. In the first case, the use of the C2 framework allowed me to bypass the restrictive environment and complete the Active Directory review without any disruptions to the client's operations. The detailed insights provided by the review helped the client to address potential vulnerabilities in their AD setup, significantly improving their overall security posture. The client appreciated the innovative approach taken to overcome the restrictions and was impressed by the depth of the assessment provided.

In the second scenario, the solution I devised enabled a comprehensive security assessment of the client's internal cloud environment without requiring physical onsite access. The setup of the Azure VM and the implementation of VPN peering allowed for full visibility and control, ensuring that all

aspects of the environment were thoroughly reviewed. The client was particularly pleased with how the solution adhered to their security policies while still providing a detailed analysis of their cloud infrastructure. As a result, the client was able to identify and remediate several key vulnerabilities, leading to a stronger and more secure cloud environment.
Moreover, the success of these projects not only met but exceeded the clients' expectations, leading to positive feedback.

A3: Have planned or delivered continuous improvement to cyber security.

Situation: As the field of cybersecurity constantly evolves, staying ahead of potential threats and ensuring the latest and greatest security practices are followed is a continuous challenge. In my role, I have taken the initiative to lead and coordinate several ongoing cybersecurity improvement efforts, both for the clients I serve and within the company I work for. Recognising the importance of proactive measures, I have consistently engaged in activities aimed at enhancing security awareness and fortifying both cloud and internal environments. This includes delivering targeted talks, conducting live demonstrations, and creating hands-on lab environments where vulnerabilities are intentionally exposed for educational purposes.
One particular focus of mine has been on cloud and internal environments, in one case AWS was the targeted area, where misconfigurations and overlooked vulnerabilities can lead to significant security breaches. I have also extended my efforts beyond professional engagements by creating personal guides designed to educate vulnerable populations, such as the elderly and social media users, about online safety. These initiatives aim to address the diverse spectrum of cybersecurity challenges, from technical cloud security to everyday online practices that can protect individuals from common threats like phishing, identity theft, and unauthorised data access or cloning.
Task: My primary task has been to lead the continuous improvement of cybersecurity practices by educating both clients and colleagues about the latest threats and mitigation techniques. This involved organising and delivering presentations, setting up vulnerable lab environments for hands-on learning, and providing detailed walkthroughs on how to secure cloud and internal infrastructures. My goal was to ensure that all users, whether they were IT professionals, business leaders, or everyday users had a clear understanding of the importance of strong security practices and knew how to implement them effectively.
In the context of cloud security, my task was to demonstrate the potential risks associated with AWS environments and provide actionable guidance on how to lock them down. This included a live "hack" demonstrations where I showed, in real-time, how an AWS environment could be breached from an external perspective. I needed to clearly illustrate how attackers could exploit common

vulnerabilities, such as misconfigured S3 buckets or exposed APIs, to gain unauthorised access and escalate privileges within the cloud environment. Beyond technical demonstrations, I also aimed to foster a culture of cybersecurity awareness within my organisation and among clients and personal friends, family, users by providing practical advice on online safety, particularly targeting those less familiar with digital threats.

Action: To address the task of continuous improvement in cybersecurity, I took a multi-faceted approach. For cloud security, I developed and conducted a series of interactive sessions where participants could engage with vulnerable lab environments that I had set up. These labs were designed to simulate real-world scenarios where cloud environments were intentionally left exposed or misconfigured, allowing participants to see firsthand how vulnerabilities could be exploited. During these sessions, I walked through each step of the attack process, explaining how an attacker could breach an AWS environment, from gaining access to an S3 bucket to exploiting an API to reach internal resources. I also demonstrated how misconfigured Lambda functions could lead to privilege escalation, turning a low-privilege user into a global admin.

To complement these technical sessions, I delivered live "hack" demonstrations where I simulated external attacks on AWS environments. These live sessions were particularly effective in driving home the importance of proper security configurations. For instance, I showed how sensitive information could be extracted from a publicly accessible S3 bucket, which was then used to pivot and exploit an exposed API. By exploiting these weaknesses, I was able to demonstrate the chain of attacks that could lead to full compromise of the cloud environment. After the demonstrations, I provided detailed guidance on how to prevent such attacks, including best practices for configuring S3 buckets, securing APIs, and implementing least privilege principles in Lambda functions.

Beyond technical demonstrations, I also took the initiative to create cybersecurity guides targeted at vulnerable populations, such as the elderly and social media users. These guides focused on practical tips for staying safe online, such as identifying fake accounts, limiting the exposure of personal information on social media, and understanding how attackers use OSINT techniques to gather information. I emphasised the importance of using multi-factor authentication, creating strong passwords, and being cautious about clicking on links or downloading attachments from unknown sources. These efforts were aimed at raising awareness and providing actionable steps that could significantly reduce the risk of falling victim to online threats.

Result: The continuous improvement initiatives I led had a significant impact on both the clients and the company I work for. The vulnerable lab environments and live "hack" demonstrations were particularly well-received, as they provided practical, hands-on experience that reinforced the importance of proper security configurations in cloud environments. Clients who participated in these sessions gained a deeper understanding of the specific risks associated with AWS and left with

actionable steps to better secure their cloud infrastructures. Many of these clients reported implementing the security recommendations I provided, leading to a measurable improvement in their overall security posture.

The personal guides I created for the elderly and social media users also made a significant impact. Feedback from those who received the guides indicated that they felt more confident in their ability to navigate the online world safely. They were better equipped to recognize potential threats, such as phishing attempts or fake social media accounts, and understood the importance of using MFA and strong passwords to protect their accounts. This initiative not only helped individuals protect themselves online but also contributed to a broader effort to reduce the overall risk of cybercrime in the community.

Overall, my efforts to lead, manage, and coordinate continuous improvements to cybersecurity have resulted in tangible benefits for both the clients I serve and the organisation I work for. By providing education, practical tools, and clear guidance, I have helped to elevate the security standards of the environments we manage and have empowered individuals to take control of their online safety. These initiatives have not only addressed immediate security concerns but have also laid the groundwork for ongoing improvements in cybersecurity practices.

B: Communication & Interpersonal Skills

B1: Have the ability to explain cyber security effectively to non- technical audiences.

Situation: In my role, I am frequently involved in both the initial scoping calls and the final end-of-testing calls with clients. These interactions complete understanding of the client's needs, the environment to be tested, and for conveying the results of our cybersecurity assessments in a manner that is clear and actionable for the client. Scoping calls can vary greatly depending on the participants, ranging from highly technical discussions with IT teams showing me detailed network maps and internal configurations, to more high-level conversations with CEOs or account managers who may not have a deep technical background but need to understand the risks and implications of potential security breaches. These scenarios require me to tailor my communication style to effectively engage with the audience, ensuring that I both gather the necessary information and provide appropriate explanations.

The ability to navigate these conversations is critical, as it sets the tone for the entire testing engagement and ensures that the client's needs are fully understood and addressed. For technical teams, it's about diving deep into the specifics of their infrastructure, discussing the best methodologies for testing, whether it's a build review, internal or external penetration testing, mobile

application review, or something else. On the other hand, when speaking with non-technical stakeholders like CEOs, the focus shifts to discussing common breach scenarios, the importance of different testing approaches, and the potential impact of security issues on the business. These conversations require not only technical knowledge but also the ability to simplify complex concepts and relate them to the client's business objectives.

Task: My task during these scoping and end-of-testing calls is to ensure that I accurately capture the client's requirements and concerns, regardless of their technical proficiency. I must ask the right questions to gain a full understanding of the environment and any specific areas of concern that need to be tested. This involves active listening, where I pay close attention to the details provided by the client, whether they are discussing technical configurations or business risks. Once the testing is completed, my task is to summarise the findings in a way that is tailored to the audience, whether that means providing a detailed technical breakdown for the IT team or delivering a high-level overview that focuses on financial and operational impacts for the executive team.

This requires a careful balance of questioning and listening, ensuring that I fully understand the client's environment and concerns before testing begins. It also involves the ability to communicate complex cybersecurity issues in a way that is accessible and relevant to the client, whether they are technical experts or business leaders. Ultimately, my task is to bridge the gap between technical cybersecurity assessments and the client's understanding, ensuring that they are fully informed and able to take appropriate action based on the results.

Action: During scoping calls, I begin by assessing the technical level of the participants and adjusting my approach accordingly. When dealing with technical teams, I delve into the specifics of their network architecture, security controls, and any existing vulnerabilities they may be aware of. I ask probing questions to uncover any areas that might require special attention, such as recent changes to the infrastructure or specific compliance requirements they need to meet. For instance, I might inquire about the types of systems in use, the sensitivity of the data they handle, and any previous incidents of concern. This helps me tailor the testing methodology to their specific needs, whether it's focusing on internal network security, external threats, or application-level vulnerabilities.

In contrast, when speaking with non-technical stakeholders like CEOs or account managers, my approach shifts to focus on the broader business implications of cybersecurity. I explain the purpose of different types of testing in terms of how they can protect the business from financial loss, reputational damage, and operational disruptions. For example, I might discuss how an external penetration test can help identify vulnerabilities that could be exploited by hackers to gain unauthorised access to sensitive data, or how a mobile application review can prevent potential breaches that could harm customer trust. I ensure that my explanations are clear and relatable,

avoiding technical jargon and instead focusing on real-world scenarios and outcomes that resonate with their responsibilities and concerns.

Once testing is completed, I take the time to carefully summarise the results based on the audience. For technical teams, I provide detailed reports that include specific vulnerabilities, the methods used to exploit them, and recommendations for remediation. I also make myself available for follow-up discussions to go over any complex findings or to assist with implementing the recommended fixes.

For non-technical stakeholders, I distill the findings into high-level summaries that emphasise the potential business impact of the issues identified, such as the risk of data breaches, the potential cost of remediation, and the strategic importance of maintaining robust security practices. I also highlight how addressing these issues can protect the organisation's reputation and bottom line, ensuring that they understand the importance of taking action.

Result:

The approach I take in these scoping and end-of-testing calls has consistently led to successful engagements and satisfied clients. By tailoring my communication to the technical proficiency of the audience, I ensure that both technical teams and business leaders feel understood and supported.

Technical teams appreciate the depth of understanding and the precise, actionable insights provided, which help them to effectively address the vulnerabilities identified. This often leads to more efficient remediation processes and stronger overall security postures within their environments.

For non-technical stakeholders, my ability to explain cybersecurity issues in business terms fosters a greater understanding of the importance of cybersecurity at the executive level. CEOs and account managers gain clarity on how potential security breaches could impact their business operations, finances, and reputation. This understanding often results in a stronger commitment to investing in cybersecurity measures and more proactive approaches to managing risks. Additionally, my clear and concise summaries help these stakeholders make informed decisions about prioritising security improvements, leading to better alignment between business objectives and security strategies.

As a result of this approach, clients consistently provide positive feedback on the clarity and relevance of the information presented. They value the way I bridge the gap between technical details and business impact, which enhances their ability to make informed decisions about cybersecurity. This not only strengthens the relationship between myself and the client but also often leads to repeat engagements and long-term partnerships as clients recognise the value of the clear, effective communication and tailored cybersecurity advice I provide.

B2: Explain cyber security advice and direction in a way that is clearly understood by the intended audience.

Situation: As a cybersecurity professional, one of my key responsibilities is to communicate complex security concepts and findings to a diverse audience, which often includes both technical and non-technical users. This is particularly important during end-of-testing calls, where I present the results of a cybersecurity assessment to the client. The challenge lies in ensuring that each audience, whether IT professionals, account managers, or CEOs, clearly understands the issues identified, their potential impact, and the steps required to address them. The goal is to go beyond just delivering a basic report; I strive to provide a tailored, comprehensive explanation that resonates with each group's specific concerns and knowledge levels.

One specific example of this occurred during an engagement with a company transitioning from an on-premises environment to Azure. The client requested a security assessment of their new Azure environment and was particularly interested in understanding Azure's native defences, network segregation, and the variety of services offered by the platform. This was an important moment for the client, as they were moving to the cloud for the first time and needed reassurance that their environment was secure. My task was to not only identify any vulnerabilities but also to explain Azure's security mechanisms in a way that the client's IT team could implement confidently. Additionally, I had to communicate the business risks to the company's leadership in a manner that highlighted the strategic importance of cybersecurity within this new infrastructure. This meant not being biased to cloud infrastructure and also showing positives and weaknesses and the need for constant review.

Task: My task during the end-of-testing call was to provide clear, actionable cybersecurity advice that was tailored to the varying levels of technical expertise within the client's organisation. For the IT professionals, I needed to dive deep into the specifics of the identified vulnerabilities, offering detailed explanations and guidance on how to address them within the Azure environment. This involved discussing Azure's built-in security features, such as network security groups, identity and access management, and how these could be leveraged to mitigate risks. Given that the client's team was still relatively new to Azure, it was also my responsibility to educate them on how these services worked, drawing on my own certifications like AZ-900 and AZ-500 training, which equipped me with a comprehensive understanding of Azure's offerings.

Simultaneously, I had to prepare to explain the findings to the company's account managers and CEOs, who were more concerned with the business implications of any security issues. My task here was to translate the technical details into language that highlighted the potential financial and reputational risks, helping them understand why certain vulnerabilities needed to be addressed urgently, and how their mitigation could protect the company's bottom line. This required not only a

solid understanding of the technical aspects but also the ability to convey the strategic importance of cybersecurity in a way that aligned with the company's overall business goals.

Action: During the end-of-testing call, I began by presenting a comprehensive overview of the assessment, ensuring that both the technical team and the executives were on the same page about the scope of the testing and the general findings. For the IT professionals, I provided an in-depth analysis of each identified vulnerability, explaining how these issues could be exploited in the Azure environment. I detailed how Azure's security features could be configured to prevent such exploitation, discussing specific services like NSGs for network segmentation, Azure Defender for threat detection, and Azure Policy for ensuring compliance. I used examples from my AZ-900 certification and AZ-500 training to clarify how these services work together to create a secure cloud environment, offering practical advice on best practices for their implementation.

Recognising that the IT team might benefit from a more interactive session, I went beyond the standard report or PowerPoint presentation. I organised a live walkthrough of one of the vulnerabilities using a lab environment, demonstrating how an attacker might exploit it and how the mitigation steps would prevent such an attack. This hands-on approach not only reinforced the technical concepts but also provided the team with a practical understanding of how to secure their environment. I encouraged questions throughout the session, fostering an open dialogue where the team could discuss their specific concerns and scenarios. This ensured that they left the call with a clear, actionable plan for addressing the vulnerabilities.

For the account managers and CEOs, I shifted my focus to the broader business implications of the findings. I explained how the vulnerabilities could lead to potential data breaches, financial losses, or damage to the company's reputation if left unaddressed. I provided scenarios that illustrated the impact of such breaches on the organisation's operations, highlighting the importance of proactive security measures in safeguarding the company's assets and customer trust. I also highlighted how investing in these security improvements could ultimately save the company from the much higher costs associated with a potential breach. By framing the technical issues within the context of business risk, I ensured that the leadership understood the critical importance of the recommendations.

Result: The approach I took during the end-of-testing call had a significant positive impact on the client's understanding and response to the cybersecurity assessment. The IT professionals gained a deeper knowledge of Azure's security features and felt more confident in their ability to secure their cloud environment. The interactive lab session was particularly well-received, as it provided them with a tangible example of how to address vulnerabilities in real time. This hands-on experience, combined with the detailed explanations I provided, empowered the team to take immediate action

to strengthen their Azure defences. They implemented the recommended security configurations promptly, which significantly reduced their risk of exposure to potential threats.
For the executives, the discussion around business risks and the strategic importance of cybersecurity resonated strongly. By translating the technical vulnerabilities into financial and reputational risks, I helped them understand why it was crucial to prioritise these security improvements. As a result, they were more willing to allocate the necessary resources to support the IT team's efforts, viewing it as a critical investment in the company's future stability and success. The call concluded with the leadership expressing their appreciation for the clarity and relevance of the information provided, and their commitment to making cybersecurity a key component of their ongoing business strategy.
The success of this call went beyond just addressing the immediate vulnerabilities. It established a foundation of trust and collaboration between myself and the client, leading to further engagements where I continued to provide expert advice tailored to their evolving needs. The client's proactive approach to cybersecurity, guided by the detailed and accessible explanations I provided, significantly improved their overall security posture and positioned them as a more resilient organisation in the face of emerging threats.

B3: Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.

Situation: I interact with a wide range of clients and users from diverse backgrounds, including different countries, cultures, and even specific charitable organisations that have unique needs and challenges. These interactions often require not only technical expertise but also strong personal and social skills to ensure that all clients feel understood, respected, and valued, regardless of their background or technical proficiency. I regularly work with teams and clients across different time zones, which sometimes requires adjusting my schedule to accommodate their working hours. This commitment to flexibility and understanding is essential in building strong, inclusive relationships that foster collaboration and trust.
One example of this is when I worked with a charitable organisation that supported vulnerable populations. The organisation had users from various cultural backgrounds, some of whom had limited technical knowledge but were deeply invested in the security and privacy of their data due to the sensitive nature of their work. My task was to guide them through a cybersecurity assessment and help them implement necessary measures to protect their digital assets. This required me to not only provide technical guidance but also to demonstrate empathy and understanding for their unique situation. I had to ensure that all communication was clear, respectful, and inclusive, taking into account the diverse backgrounds of the users involved.

Task: My task in these interactions is to ensure that I provide cybersecurity services in a way that is sensitive to the diverse needs and backgrounds of the clients I work with. This involves tailoring my communication style to suit the specific audience, whether that means simplifying technical jargon for non-technical users, being culturally aware and respectful in my interactions, or being flexible with my working hours to accommodate clients in different time zones. It also requires demonstrating empathy, especially when working with organisations that support vulnerable populations, where the stakes are often higher, and the need for understanding and sensitivity is paramount.

In the case of the charitable organisation, my task was to not only conduct the cybersecurity assessment but also to deliver the findings in a way that was accessible and reassuring to all users. I needed to ensure that everyone, regardless of their technical background or cultural perspective, felt included in the conversation and understood the importance of the security measures being recommended. This meant being patient, listening actively to their concerns, and providing explanations that were both clear and considerate of their unique challenges. My goal was to empower them with the knowledge and tools they needed to protect their organisation while fostering an environment of trust and inclusivity.

Action: To achieve these goals, I took several steps to ensure that my interactions with the clients were inclusive and empathetic. First, I made a point to learn about the cultural backgrounds and specific needs of the users I was working with. This involved researching cultural norms, being aware of potential language barriers, and understanding the broader context in which these users operated. For example, when working with clients from different countries, I adjusted my communication style to be more formal or informal depending on what was culturally appropriate. I also made sure to speak slowly and clearly when language barriers were present, and I used visual aids and written summaries to reinforce key points.

In the case of the charitable organisation, I scheduled multiple meetings at times that were convenient for them, even if it meant working outside of my usual hours. During these meetings, I practiced active listening, making sure to address their concerns thoroughly and respectfully. I also made a conscious effort to involve all users in the conversation, asking for their input and feedback to ensure that they felt heard and valued. When explaining technical concepts, I used analogies and simple language to make the information more accessible, and I was careful to check in frequently to ensure that everyone was following along. I highlighted that their concerns were valid and important, reinforcing my commitment to helping them secure their environment in a way that made sense for their organisation.

Additionally, I provided follow-up support after the initial assessment, offering additional training sessions and resources to help them implement the recommended security measures. I tailored these sessions to the specific needs of the organisation, recognising that some users needed more hands-

on guidance while others were more comfortable with the material. Throughout the process, I maintained a focus on inclusivity, ensuring that all users, regardless of their technical expertise, felt empowered to take part in the security process.

Result: The approach I took in these interactions led to highly positive outcomes for both the clients and myself. The charitable organisation, in particular, expressed deep appreciation for the way I handled the assessment and the subsequent guidance. By tailoring my communication and demonstrating empathy and understanding, I was able to build a strong rapport with the organisation, which led to a successful implementation of the recommended security measures. The users felt more confident in their ability to protect their digital assets, and they appreciated the extra effort I made to accommodate their needs and ensure that everyone was included in the process. My commitment to inclusivity and empathy also strengthened the trust and collaboration between myself and the clients. They felt that I genuinely cared about their concerns and were more willing to engage with the security recommendations as a result. The cultural awareness and flexibility I demonstrated helped to bridge any potential gaps, making the interactions smoother and more productive. As a result, the organisation not only improved its cybersecurity posture but also gained a greater understanding of how to maintain it in the future.

This experience reinforced the importance of good personal and social skills in cybersecurity work. It showed that by being empathetic, inclusive, and culturally aware, I could not only deliver technical solutions but also build lasting relationships that are based on trust and mutual respect. These skills are crucial in a field that often involves working with diverse clients and users, and they play a key role in ensuring that cybersecurity advice is not only heard but also acted upon in a meaningful way.

B4: Have good oral and written communication skills for both technical and non- technical audiences.

Situation: In my role, I am responsible for ensuring that all communications, both oral and written, are clear, accurate, and appropriately tailored to the audience, whether they are technical experts or non-technical users potentially as CEOs or end users. One of the key responsibilities I hold is the quality assurance of reports generated by my team. With 35 testers under my supervision, each engagement requires a thorough review of their reports before they are sent out to clients. These reports must be technically precise, well-organised, and accessible to the intended audience, which can range from IT professionals to business leaders with limited technical knowledge. Additionally, I am tasked with drafting and sending daily communications, including start-of-day and end-of-day emails that outline the testing activities, methodologies, and any issues identified.

This situation requires me to consistently demonstrate strong written and oral communication skills. Whether it's providing detailed feedback on a report, explaining complex technical issues over email

or a call, or crafting guides and references for less technical audiences, my communication must be clear, concise, and effective. The ability to bridge the gap between technical detail and broader business implications is crucial, particularly when communicating with non-technical users who need to understand the impact of our findings without getting lost in the technical jargon.

Task: My task is to ensure that all written and oral communications are of the highest quality, accurately conveying technical information while being understandable to the target audience. For the reports produced by my team, I need to review and refine the content to ensure it meets our standards for technical accuracy and clarity. This involves not only checking for errors or omissions but also ensuring that the reports are structured in a way that makes the information accessible to the client, regardless of their technical background.

In addition to report QA, I am responsible for drafting and sending out start-of-day and end-of-day emails for engagements. These communications need to clearly outline what will be tested, the techniques and tools that will be used, and any preliminary findings or issues encountered. For technical audiences, this requires detailed explanations of methodologies and technical results. For non-technical users, I must distill this information into key points that emphasise the business impact of any findings. Moreover, I often provide verbal explanations during calls, where I must be prepared to adjust my communication style based on the audience's level of technical understanding.

Action: To achieve these goals, I employ a systematic approach to communication. For report QA, I start by thoroughly reviewing each document for technical accuracy. I ensure that all findings are clearly explained, with appropriate context provided so that the reader can understand the significance of the issue and the recommended remediation steps. I focus on clarity and conciseness, eliminating any unnecessary jargon or overly complex language that might confuse the reader. If a report is intended for a non-technical audience, I work to translate technical findings into plain language, highlighting the potential risks and impacts in terms that resonate with business leaders. This might involve providing analogies or simplified explanations that help non-technical users grasp the importance of the issues identified.

When drafting start-of-day and end-of-day emails, I tailor my communication to the audience's needs. For technical recipients, I include detailed information about the testing procedures, tools used, and any technical challenges encountered. I might explain, for instance, how a specific penetration testing tool was employed to identify vulnerabilities and why certain techniques were chosen based on the client's environment. For non-technical recipients, I focus on the broader implications of the testing activities, such as the potential business impact of any vulnerabilities found, or the overall security posture of the environment being tested. I ensure that these emails are not only informative but also actionable, providing clear next steps or recommendations where necessary.

During calls, I practice active listening to gauge the audience's level of understanding and adjust my explanations accordingly. For technical discussions, I delve into the specifics, using precise terminology and detailed descriptions of the testing processes. For non-technical discussions, I focus on the high-level outcomes and their relevance to the organisation's goals, avoiding technical details unless specifically asked. I also make use of visual aids, such as slides or diagrams, to help convey complex ideas in a more digestible format. This adaptability in communication helps ensure that all users are well-informed and can make decisions based on a clear understanding of the issues at hand.

Result: The result of these efforts is a consistently high standard of communication across all engagements. The reports I QA are well-received by clients, as they are both technically accurate and accessible to the intended audience. Technical teams appreciate the clarity and detail provided, which helps them to effectively address the issues identified. Non-technical users, such as CEOs and account managers, value the way complex information is distilled into key points that are relevant to their business objectives, allowing them to make informed decisions without needing to wade through technical jargon.

The daily emails I send out ensure that clients are kept fully informed throughout the testing process. Technical recipients benefit from the detailed explanations of the testing activities and methodologies, which help them understand the technical aspects of the engagement. Non-technical recipients, on the other hand, appreciate the clear and concise summaries that focus on the business impact of the findings. This transparency and clarity help build trust with the client, as they feel confident that they are kept in the loop and understand the significance of the work being done.

In verbal communications, whether during scoping calls, end-of-testing reviews, or ad-hoc discussions, my ability to adjust my communication style to the audience has led to more effective and productive interactions. Technical teams feel understood and supported, as I am able to speak their language and address their specific concerns. Non-technical users, meanwhile, feel reassured and informed, as I provide them with the insights they need to make strategic decisions without overwhelming them with unnecessary technical details. This adaptability and clarity in communication have strengthened client relationships, leading to positive feedback, repeat engagements, and a strong reputation for my ability to effectively bridge the gap between technical and non-technical audiences.

C: Collaborative Management, Leadership & Mentoring

C1: Are able to manage resource, people, budgets in a cyber security environment.

Situation: In my career, I have consistently been promoted to senior roles due to my ability to manage resources, people, and budgets effectively, particularly in complex and high-pressure cybersecurity environments. Most recently, I was promoted to the role of Service Delivery Lead, where I am responsible for overseeing a team of 35+ cybersecurity testers. This role demands a high level of responsibility, as I am tasked with ensuring that each tester performs their assigned tasks to the highest standards, while also managing the various logistical and financial aspects of our operations. The environments we work in are often under significant pressure, either due to tight deadlines, the critical nature of the systems being tested, or the need to meet stringent compliance requirements.

One of the biggest challenges in this role is balancing the need for thorough and effective security testing with the constraints imposed by client budgets. Clients often have specific needs and limited resources, requiring us to tailor our testing services to fit within their financial constraints while still delivering high-quality results. This situation requires me to be strategic in resource allocation, ensuring that we can meet client expectations without compromising the quality of our work or the well-being of my team. Managing these complex dynamics is essential for maintaining client satisfaction and upholding the reputation of our services.

Task: As the Service Delivery Lead, my task is to ensure that our team of testers is efficiently managed, that resources are allocated effectively, and that we stay within the budgets set by our clients. This involves a range of responsibilities, including assigning tasks to the appropriate testers based on their skills and experience, monitoring the progress of testing activities, and making adjustments as needed to ensure that deadlines are met without sacrificing quality. I am also responsible for communicating with clients to understand their specific needs and constraints, and then developing testing plans that align with their budgets while still addressing all critical security concerns.

Additionally, I must ensure that the team is not only productive but also motivated and supported, especially in high-pressure situations. This involves regular check-ins with the testers to assess their workload, providing guidance and support when they encounter challenges, and managing any interpersonal dynamics that might arise. My role also requires me to be vigilant about the financial aspects of our operations, ensuring that we stay within the agreed-upon budgets while still delivering comprehensive and effective security testing. This often means making tough decisions about where to allocate resources and how to optimise our processes to get the best results within the constraints we face.

Action: To manage these responsibilities effectively, I implemented a structured approach to resource and people management. First, I developed a detailed overview of each tester's strengths, experience, and current workload. This allowed me to assign tasks more strategically, ensuring that each tester was working on projects that matched their expertise while also balancing the overall team workload to prevent burnout. For example, when dealing with a particularly complex environment that required specialised knowledge, I assigned it to testers who had demonstrated proficiency in that area, ensuring the client received the highest quality of service.

In terms of budget management, I worked closely with clients to understand their financial constraints and priorities. This involved detailed discussions about their security needs, the potential risks they faced, and the compliance requirements they needed to meet. Based on these discussions, I developed customised testing plans that aligned with their budgets. For instance, if a client had a limited budget but needed comprehensive coverage, I might suggest a phased approach, where we focus on the most critical areas first and plan additional testing for later phases as their budget allows. This approach not only helped in meeting the client's budgetary constraints but also ensured that their security needs were addressed in a systematic and effective manner.

To ensure that the team remained motivated and capable of performing under pressure, I fostered a supportive and communicative environment. I held regular team meetings to discuss progress, share insights, and address any challenges that testers were facing. I also encouraged an open-door policy where testers could come to me with any concerns, whether they were technical or personal. By being accessible and supportive, I was able to help the team navigate high-pressure situations more effectively, ensuring that they could maintain the quality of their work even under tight deadlines or challenging conditions.

Result: The result of these efforts has been highly positive, both in terms of client satisfaction and team performance. By carefully managing resources and aligning testing plans with client budgets, we were able to consistently deliver high-quality cybersecurity assessments that met or exceeded client expectations. Clients appreciated the tailored approach we took, recognising that we were not only mindful of their financial constraints but also committed to providing comprehensive security coverage. This led to strong client relationships, repeat business, and positive referrals, all of which contributed to the ongoing success of our service delivery.

Within the team, the structured and supportive approach to management resulted in a highly motivated and efficient group of testers. By aligning tasks with each tester's strengths and ensuring that workloads were balanced, we were able to maintain a high standard of work across all engagements. Testers felt supported and valued, which contributed to a positive work environment where they could perform at their best, even in high-pressure situations. The regular communication

and collaborative problem-solving also helped to resolve any issues quickly, minimising disruptions and ensuring that projects stayed on track.
Overall, my ability to manage resources, people, and budgets effectively in complex and high-pressure cybersecurity environments has not only led to successful project outcomes but has also strengthened the team's capabilities and enhanced client trust in our services. This role has solidified my reputation as a reliable and strategic leader who can deliver results in challenging situations, further reinforcing the value I bring to the organisation and its clients.

C2: Are able to lead, manage and develop people.

Situation: As the Service Delivery Lead in a cybersecurity organisation, I am responsible for overseeing a team of 35+ testers. This role goes beyond just managing the day-to-day activities; it involves leading, coaching, and mentoring the team to ensure their continuous development and success. The team is diverse in terms of experience and expertise, with some members being junior testers who are still building their skills, while others are more seasoned professionals with specialised knowledge. My goal is to create a collaborative environment where everyone feels supported and encouraged to grow, both individually and as part of the team.
One of the key challenges in this role is balancing the need to provide guidance and oversight without micromanaging. Each tester needs the freedom to take ownership of their work, but they also need access to support and feedback to help them improve. To address this, I have implemented a system of regular check-ins, both as a team and on a one-to-one basis, to ensure that everyone is on track and feels supported. Additionally, I have created a network within the team where individuals with specific areas of expertise can mentor and guide junior testers, fostering a culture of continuous learning and collaboration.
Task: My task as a leader is to not only manage the team's workload but also to actively contribute to their professional development through coaching and mentoring. This involves offering constructive feedback, recognising achievements, and providing opportunities for growth. I need to ensure that each team member feels valued and has the resources they need to succeed, while also encouraging them to take on new challenges and expand their skill sets. Additionally, I am tasked with creating and leading both formal and informal teams, as well as establishing collaborative links within the team to enhance communication and knowledge sharing.
Another important aspect of my role is to advise and influence others, both within my team and in the broader organisation. This involves guiding the team in their decision-making processes, helping them navigate complex challenges, and ensuring that they are aligned with the organisation's goals and

standards. My influence is not just about directing their actions but also about inspiring confidence and motivating them to achieve their best.

Action: To effectively lead and develop my team, I implemented a structured approach that balances guidance with autonomy. I begin each day with check-ins, where I connect with each tester individually to discuss their progress, any challenges they are facing, and how I can support them. Rather than micromanaging, I focus on offering assistance and reviewing their work and reports, providing constructive feedback where needed and praising them for their achievements. This approach helps to build trust and ensures that the testers feel confident in their work while knowing that I am available to help them navigate any difficulties.

I also hold weekly team calls where we discuss broader issues, share insights, and celebrate successes. These meetings are an opportunity for the team to come together, exchange ideas, and learn from each other. In addition to these group sessions, I conduct one-to-one meetings with team members who may need more personalised support. These meetings provide a safe space for testers to discuss any concerns or areas where they feel they need additional guidance, allowing me to tailor my coaching to their specific needs.

Recognising the importance of leveraging the expertise within the team, I created a network where testers with specific areas of expertise act as mentors to junior testers. This initiative not only supports the development of the junior testers but also empowers the more experienced members of the team to take on leadership roles and share their knowledge. I oversee this network, ensuring that it functions smoothly and that both mentors and mentees are benefiting from the arrangement. By fostering these collaborative links, I encourage the team to work together, learn from one another, and build a stronger, more cohesive unit.

Result: The results of these efforts have been highly positive, both in terms of individual development and overall team performance. The daily check-ins and regular feedback have created an environment where testers feel supported and motivated. They are more confident in their work, knowing that they have the guidance and resources they need to succeed. The constructive feedback and recognition of their achievements have also contributed to higher morale and job satisfaction, which has been reflected in the quality of their work and their willingness to take on new challenges.

The weekly team meetings and one-to-one sessions have strengthened the sense of community within the team. Testers feel more connected to each other and are more willing to collaborate and share their knowledge. The network of expertise that I established has been particularly effective in helping junior testers develop their skills. By connecting them with more experienced mentors, I have facilitated a learning environment where knowledge is shared, and skills are continuously developed.

This has not only accelerated the growth of the junior testers but has also enhanced the leadership and mentoring skills of the senior testers.
Overall, my approach to leading, managing, and developing the team has resulted in a more cohesive, skilled, and motivated group of professionals. The team is better equipped to handle the complexities and pressures of our work, and they feel more valued and supported in their roles. This, in turn, has led to improved performance, greater client satisfaction, and a stronger reputation for our team within the organisation. By focusing on coaching, mentoring, and fostering collaboration, I have been able to create a positive and productive environment where everyone has the opportunity to thrive.

C3: Have good organisational and time management skills.

Situation: In my role as a Service Delivery Lead, managing time and staying organised is crucial, not just for my own success, but for the success of the entire team. With a large team of testers to oversee, numerous client engagements, and various tasks to coordinate, maintaining a high level of organisation and time management is essential. My responsibilities include scheduling and conducting scoping calls, performing quality assurance checks on reports, ensuring timely delivery of results to clients, and being available to support my team members. The dynamic nature of the cybersecurity environment, coupled with the global reach of our clients, often requires flexibility, with days starting early and ending late to accommodate different time zones and urgent client needs. The complexity of this role means that if I'm not organised, it could have a ripple effect, delaying deliverables and potentially compromising the quality of our work. Given that my time management serves as a guideline for other testers, I have to be meticulous in planning my day, setting clear priorities, and ensuring that everything runs smoothly. My ability to manage time effectively is crucial in maintaining the high standards expected by both our clients and my organisation.
Task: My task is to ensure that my day is structured in a way that maximises productivity while allowing flexibility to handle unexpected challenges. This involves creating detailed workbooks, logs, and schedules that outline what tasks need to be completed and when. For instance, I need to allocate time for scoping calls with clients, ensuring these fit within the overall schedule without disrupting other activities. Similarly, QA checks on reports require dedicated focus, and I need to ensure these are completed in a timely manner to meet client deadlines.
In addition to managing my own time, I am also responsible for setting the pace for the rest of the team. This includes being available to assist testers who may be struggling with their workload or need guidance on specific tasks. Given the global nature of our work, I often need to adjust my schedule

to accommodate client meetings or support team members in different time zones. The task at hand is not just about managing my own time effectively, but also about ensuring that the entire team operates efficiently and that client needs are met promptly.

Action: To manage my time effectively, I start each day by reviewing and updating my workbook, which outlines the key tasks and priorities for the day. This workbook includes timeframes for each task, ensuring that I allocate enough time to focus on each activity without overlap or unnecessary delays. For example, I schedule scoping calls early in the day when I am most focused, allowing me to engage with clients and gather important information that will guide the testing process. These calls are scheduled in advance and slotted into my calendar to avoid conflicts with other tasks.

I also use logs to track the progress of various activities, such as QA checks on reports. By maintaining these logs, I can quickly see which reports are due, which ones are in progress, and which have been completed. This allows me to prioritise my QA work and ensure that reports are reviewed and sent to clients on time. I have developed a system where I block out specific times of the day for QA work, minimising distractions and ensuring that I can give these tasks the attention they require.

In addition to managing my tasks, I regularly check in with my team to assess their workload and offer assistance where needed. This often means starting my day earlier or staying late to provide support, especially when dealing with clients in different time zones. By doing so, I ensure that the team remains on track and that any issues are addressed promptly. This approach allows me to stay ahead of potential challenges and ensure that both my own work and the team's work are completed efficiently.

Result: The result of these organisational and time management efforts is a consistently high level of productivity and efficiency, both for myself and the team. By structuring my day with detailed workbooks, logs, and schedules, I am able to manage a large volume of tasks without becoming overwhelmed or missing deadlines. Clients appreciate the timely delivery of reports and the smooth coordination of scoping calls, which builds trust and strengthens our relationships.

My ability to manage my time effectively also sets a positive example for the rest of the team. Testers see how I structure my day and use it as a guideline for managing their own time, leading to a more organised and efficient team overall. The proactive support I provide, particularly in accommodating different time zones, ensures that we are responsive to client needs regardless of their location. This flexibility has been crucial in maintaining high client satisfaction and ensuring that we can meet the demands of a global client base.

C4: Maintain a professional and secure working environment.

Situation: In my new lead role, I maintain a working environment that is not only productive and professional but also secure. The nature of our work demands the highest levels of professionalism in every aspect; from how we conduct ourselves in client interactions to how we manage and protect sensitive information. The teams I oversee are often involved in both remote and onsite engagements, which require careful planning and adherence to security protocols to ensure that our work is carried out efficiently and safely. My role involves setting the standard for these practices and ensuring that every team member is equipped to maintain these standards consistently.
Weekly calls and one-on-one meetings with clients are integral to this process. These interactions are opportunities to reinforce expectations around professionalism and security, ensuring that our team members understand and embody these values in their daily duties. Additionally, I have been involved in implementing various tools and procedures designed to enhance the security of our operations, such as secure file upload facilities and Mobile Device Management systems. These tools aid in protecting data and ensuring that devices remain secure, especially when team members are working remotely or onsite at client locations. Furthermore, I have taken proactive steps to ensure the safety of testers when they are onsite by assisting with risk assessments and implementing regular check-ins, even just a quick phone call or morning message to ensure they are onsite and do not require assistance.
Task: My task is to ensure that the working environment remains productive, professional, and secure at all times. This involves setting clear expectations for the team regarding professionalism, which includes everything from how they communicate with clients to how they present themselves in terms of mannerisms and attire. I must also ensure that our testing approach is thorough and precise, reflecting the high standards of the organisation. Beyond professionalism, a key part of my task is to implement and maintain security measures that protect both our team and the sensitive information we handle.
This includes working with teams to implement secure communication tools, such as encrypted file upload facilities, and ensuring that all devices used in our operations are managed through MDM systems to prevent non-compliance. Additionally, I must ensure that the safety of our testers is prioritised during onsite engagements. This involves conducting risk assessments to identify potential hazards and establishing protocols for regular check-ins to ensure their well-being. My task is to create an environment where team members can work efficiently and securely, knowing that they are supported and that all necessary precautions have been taken.
Action: To maintain a productive, professional, and secure working environment, I implemented several key practices and procedures. During our weekly team calls, I emphasize the importance of

professionalism in every interaction with clients. I discuss the expectations around communication, both written and verbal, and the importance of presenting oneself professionally, whether working onsite or remotely. I also cover the need for a meticulous approach to testing, ensuring that every aspect of our work is conducted with precision and attention to detail. These calls are also an opportunity to address any challenges the team may be facing and to provide guidance on how to overcome them while maintaining our professional standards.

In terms of security, I worked with our IT team to implement a secure file upload facility that allows us to exchange sensitive information with clients while ensuring that the data remains encrypted and protected from unauthorised access or man-in-the-middle attacks. I also collaborated with teams to deploy Mobile Device Management systems across all devices used by our testers. This ensures that all devices are regularly updated, virus-free, and compliant with our security policies. These measures are particularly important for remote work, where the risks of data breaches and other security incidents are higher.

For onsite engagements, I assist in conducting thorough risk assessments to identify any potential hazards that testers might encounter. Based on these assessments, I help to implement safety protocols, including regular check-ins, so that we are always aware of the testers' status and can respond quickly if any issues arise. This not only ensures the security of the work being done but also the personal safety of our team members, which is a top priority. By taking these steps, I ensure that the working environment is not only secure but also supportive and conducive to high performance.

Result: The actions I have taken to maintain a productive, professional, and secure working environment have had a significant positive impact on both the team and our clients. The regular reinforcement of professionalism during our weekly calls has led to a noticeable improvement in how team members conduct themselves in client interactions. Clients have provided positive feedback on the clarity and professionalism of our communication, and our meticulous approach to testing has been recognised as a key strength. This has not only enhanced our reputation but also strengthened client trust and satisfaction.

The implementation of secure communication tools and MDM systems has significantly reduced the risk of security incidents, particularly in remote work scenarios. The encrypted file upload facility has been particularly effective, allowing us to securely share sensitive data with clients without compromising its integrity. The MDM systems have ensured that all devices are compliant with our security policies, reducing the likelihood of breaches and ensuring that our operations remain secure at all times.

The safety protocols established for onsite engagements have also been successful. The risk assessments and regular check-ins have provided peace of mind to our testers, knowing that their safety is a priority. This has led to a more confident and focused approach to onsite work, as testers

feel supported and secure in their environment. Overall, the measures I have implemented have created a working environment where productivity, professionalism, and security are consistently maintained, leading to better outcomes for both the team and our clients.

D: Integrity

D1: Have personal and professional honesty and integrity.

Situation: Early in my career as an IT technician at a college, I encountered a challenging situation that tested my personal and professional honesty and integrity. While performing my regular duties, I began noticing discrepancies in the inventory of equipment, including missing printers, laptops, and other valuable items. Initially, I thought these discrepancies might have been due to clerical errors or misplacements, but as I continued to monitor the situation, it became evident that something more serious was occurring. The equipment wasn't just misplaced; it was being systematically stolen. My investigation led me to suspect that a colleague was involved in the theft and was selling the stolen equipment on eBay. This discovery placed me in a difficult position, as it was a serious allegation that could have significant consequences for the colleague involved and the institution as a whole.
The situation required me to make a critical decision: whether to ignore the issue and avoid potential conflict, or to act with honesty and integrity by reporting my findings to the appropriate authorities. Given my values and commitment to ethical behaviour, I knew that I had to take the right course of action, even though it was uncomfortable and could potentially lead to tensions in the workplace. This scenario was not just about upholding the rules; it was about maintaining the trust that the institution had placed in me and ensuring that the environment remained one of integrity and honesty.
Task: My task in this situation was twofold. First, I needed to gather enough evidence to substantiate my concerns before raising the issue with management. I understood that making such a serious allegation without concrete proof could lead to unjust accusations and potential harm to innocent parties. Therefore, it was important to approach the situation with care and diligence, ensuring that my actions were based on facts and not just suspicions.
Second, once I had gathered sufficient evidence, my task was to report the matter to the appropriate authorities within the college, demonstrating my commitment to honesty and integrity. This also meant being prepared to face any consequences that might arise from making the report, including possible backlash from colleagues or the individual involved. My goal was to ensure that the institution's resources were protected and that the environment remained one where ethical

behaviour was upheld. Additionally, I wanted to set an example for others by showing that it's important to stand up for what's right, even when it's difficult.

Action: To address the situation, I began by meticulously tracking the inventory and documenting the missing items. I cross-referenced the inventory records with purchase orders and recent deliveries, noting any discrepancies. I also paid closer attention to the colleague's behaviour and activities, looking for patterns that might confirm my suspicions. Over time, I gathered enough evidence, including proof of the stolen items being sold online, which clearly indicated that my colleague was involved in the theft.

Once I was confident that I had gathered sufficient evidence, I approached the college's management with my findings. I provided them with the documentation I had compiled, including records of the missing items and screenshots of the eBay listings where the stolen equipment was being sold. I made it clear that my intention was not to falsely accuse anyone, but rather to protect the institution's assets and maintain an ethical working environment. I was transparent about my actions and motivations, emphasising that honesty and integrity were my guiding principles in this situation.

Throughout the process, I remained professional and focused on the facts, avoiding any personal attacks or assumptions about the colleague's motivations. I also made it clear that I was willing to cooperate fully with any investigation and that I was committed to resolving the issue in a fair and just manner. My approach was to let the evidence speak for itself, trusting that the truth would come to light through the proper channels.

Result: The evidence I provided led to a thorough investigation by the college's management and security team. As a result of the investigation, my colleague was found guilty of stealing and selling the equipment. The college took appropriate legal action, which ultimately led to the colleague's conviction. While it was a difficult situation, the outcome affirmed the importance of honesty and integrity in the workplace. The college management thanked me for my diligence and courage in bringing the issue to their attention, and my actions helped to protect the institution's resources and maintain the integrity of the workplace.

This experience reinforced my commitment to honesty and integrity in all aspects of my professional life. It also highlighted the importance of being willing to admit when something is wrong and to take the necessary steps to correct it, even when it's uncomfortable. This principle has continued to guide me throughout my career. I am always the first to admit if I make a mistake, and I work diligently to correct it. I believe that acknowledging errors and learning from them is crucial for personal and professional growth.

Moreover, this experience shaped how I lead and manage my team today. I emphasize the importance of honesty and integrity in our work, encouraging my team members to come forward

with any issues or mistakes they encounter. I strive to create an environment where everyone feels safe to admit faults without fear of retribution, knowing that the goal is always to find solutions and improve. By fostering a culture of transparency and accountability, I ensure that we can address challenges effectively and maintain the trust of our clients and colleagues.

D2: Comply with codes of conduct of their professional membership organisation

Situation: Adherence to the codes of conduct set forth by various professional membership organisations is paramount. This commitment is especially known when conducting penetration testing and other security assessments, which are governed by strict rules and regulations to ensure that these activities are performed ethically and legally. One of the primary frameworks I work under is the CHECK scheme by NCSC, which sets specific rules around how penetration testing should be conducted, particularly in terms of encryption, data storage, and reporting practices. Additionally, my organisation has its own internal code of conduct, which aligns with these external standards but also utilises our unique values and commitments to clients.

The complexity of the environments I test, particularly cloud environments, adds another layer of regulatory requirements. For instance, when I test Microsoft Azure this allows penetration testing without explicit permission from Microsoft for client environments, there are strict prohibitions against denial-of-service or distributed denial-of-service attacks and will still require authorisation via the client but not from Microsoft themselves. Oracle is another example that has its own specific ruleset for penetration testing, often requiring testers to have completed their certified courses and added to an exclusive list.

D3: Understand and comply with the appropriate legal and regulatory requirements

Situation: I have been privileged to work within numerous sensitive environments. Two particular scenarios underscore the importance of this compliance. The first involved when I conducted a penetration test for a government agency responsible for managing sensitive child welfare information. Given the nature of the data involved, it was essential to comply with various UK laws, including the Data Protection Act 2018 and the Computer Misuse Act 1990, to ensure the security of the information and adherence to strict non-disclosure agreements.

The second scenario I was involved with was performing a breakout review within a prison's computer systems. The goal was to ensure that prisoners could not bypass the security controls in place to access restricted resources, such as the internet, internal servers, or sensitive prisoner information. This situation presented unique legal challenges, requiring strict adherence to laws governing the

operation within a prison environment, such as the Prisons (Interference with Wireless Telegraphy) Act 2012, the Computer Misuse Act 1990, and the Data Protection Act 2018. Additionally, I had to follow specific protocols for handling and safeguarding sensitive data related to the prison and its inmates in addition to follow in house protocols like screening, auditing of equipment, etc.

Task: In these scenarios, my primary task was to ensure that all activities were conducted in full compliance with the relevant UK legal and regulatory requirements. For the government agency, this involved conducting the penetration test while safeguarding sensitive child welfare data and adhering to the Computer Misuse Act 1990 and the Data Protection Act 2018. I also needed to ensure that the NDAs protecting this information were strictly followed.

For the prison breakout review, my task was to ensure that the technical testing complied with legal standards while also meeting the specific legal requirements for operating within a prison. This included obtaining all necessary permissions under the Computer Misuse Act 1990, ensuring compliance with the Data Protection Act 2018 for handling sensitive data, and following the Prisons (Interference with Wireless Telegraphy) Act 2012, which governs the control of wireless communications in prison settings. My responsibility was to ensure that these legal frameworks were fully respected throughout the engagement.

Action: To ensure compliance with these legal and regulatory requirements, I took several careful and deliberate actions. For the government agency's penetration test, I began by thoroughly reviewing the relevant UK laws, including the Computer Misuse Act 1990 and the Data Protection Act 2018. These laws guided our approach to ensure that all testing methods were legally compliant, and that sensitive data was protected. I collaborated closely with the agency's legal team to fully understand the terms of the NDAs and any additional legal constraints related to handling child welfare information. During the testing process, I implemented strict data handling procedures, ensuring that all data was encrypted, securely stored, and only accessible by authorised personnel. Every action was documented meticulously to create a clear audit trail demonstrating our adherence to the relevant legal frameworks.

In the case of the prison breakout review, I first ensured that all necessary legal permissions were secured under the Computer Misuse Act 1990. This involved coordinating with prison officials and legal advisors to ensure that our activities were fully authorised and compliant with the Prisons (Interference with Wireless Telegraphy) Act 2012. I conducted a thorough risk assessment to identify any potential legal or security risks associated with the testing. Throughout the review, I implemented stringent security measures to prevent unauthorised access to sensitive data and ensured that the testing did not interfere with the prison's operations. All data was handled in accordance with the Data Protection Act 2018, ensuring that sensitive information about the prison and its inmates remained secure.

In both scenarios, I maintained open and transparent communication with the relevant legal teams and authorities, ensuring that our actions were fully aligned with the applicable laws. I provided detailed reports at the conclusion of each project, outlining the steps taken to ensure legal compliance and the results of our testing. This transparency helped to build trust with the government agency and prison authorities, demonstrating our commitment to operating within the bounds of the law.

Result: The meticulous attention to legal and regulatory compliance in these scenarios led to successful outcomes. For the government agency, the penetration test was completed without incident, and all sensitive child welfare information remained secure throughout the process. The agency appreciated our careful approach to legal compliance and data protection, which ensured that they met their regulatory obligations while gaining valuable insights into their security posture. This successful engagement reinforced our reputation as a trusted and ethical cybersecurity provider.

In the prison breakout review, the testing was conducted successfully with no breaches of legal or security protocols. The findings provided the prison with insights into potential vulnerabilities, with one being access to the control panel via repeated clicks on the time clock, allowing them to enhance their security measures and prevent breakouts by prisoners. The prison authorities valued our thoroughness, particularly our strict adherence to the legal requirements for operating within such a sensitive environment. The successful completion of this review demonstrated our ability to conduct complex cybersecurity assessments within highly regulated environments, further solidifying our credibility and expertise in the field.

Overall, these experiences highlighted the importance of understanding and complying with the appropriate legal and regulatory requirements in cybersecurity. By ensuring that all activities were conducted within the legal framework, we were able to achieve our objectives while maintaining the highest standards of integrity and professionalism.

D4: Are able to identify and implement appropriate standards

Situation: Last year, I took on the responsibility of becoming a Cyber Essentials assessor, a certification provided by the UK government that helps organisations protect themselves against the most common cyber threats. Passing the Cyber Essentials assessor exam was a significant milestone in my career, as it equipped me with the knowledge and authority to guide organisations through the process of achieving Cyber Essentials and Cyber Essentials Plus certifications.

This certification process is important for many organisations, due to personal funding for companies and particularly those that handle sensitive data or need to demonstrate a strong security posture to their clients and partners. The challenge lies in identifying the specific standards that each

organisation must meet and implementing them effectively to ensure compliance. My role involves not only assessing organisations against these standards but also helping them understand the requirements and guiding them through the process of achieving and maintaining their certification. This process requires a deep understanding of the Cyber Essentials framework, as well as the ability to translate these standards into actionable steps that organisations can implement.

Task: My primary task as a Cyber Essentials assessor is to evaluate organisations against the Cyber Essentials and Cyber Essentials Plus standards, ensuring they meet the required criteria for certification. This involves a thorough assessment of their security measures, including their firewall and internet gateway configurations, secure configuration of devices and software, user access controls, malware protection, and patch management. I must identify any areas where the organisation falls short of the required standards and provide clear, actionable guidance on how to address these gaps. In most cases, I am happy to jump on a call and talk through the failures, how they can be addressed and why they are issues. I have worked with huge organisations that require numerous separate CE certifications, and always ensure I am talking through the framework with them to meet the objectives.

Additionally, I am tasked with helping organisations implement these standards in a way that aligns with their specific operational needs. This often involves working closely with their IT teams to develop and refine their security practices, ensuring that they not only achieve certification but also maintain a significant security posture going forward. My goal is to ensure that these organisations are not just compliant with the Cyber Essentials standards but are also genuinely protected against cyber threats. This is usually followed by a more sophisticated penetration test to ensure security is met with more than just CE frameworks.

Action: To fulfil this task, I begin by conducting the assessment of the organisation's current security practices. This involves a detailed review of their infrastructure, including network configurations, device management, and user access controls. I use the Cyber Essentials standards as a benchmark, identifying any areas where the organisation does not meet the required criteria. For instance, I assess whether their firewall configurations are correctly set up to prevent unauthorised access, if their devices are securely configured and updated, and if their malware protection measures are sufficient.

Once the assessment is complete, I provide the organisation with a detailed report outlining the areas where they need to improve to meet the Cyber Essentials or Cyber Essentials Plus standards. I don't just stop at identifying the gaps; I work closely with their IT team to develop a plan for implementing the necessary changes. This might involve recommending specific tools or technologies, providing guidance on best practices for secure configuration, or offering training to help staff understand the importance of these measures.

For organisations pursuing Cyber Essentials Plus, I conduct additional testing to verify that the standards have been implemented correctly and that the security measures are effective in practice. This includes vulnerability scans, penetration testing, and other hands-on assessments to ensure that the organisation's defences are locked down and up to date. Throughout the process, I maintain clear communication with the organisation's leadership and IT teams, ensuring they understand the importance of each standard and how it contributes to their overall security posture.

Result: The results of these efforts have been highly successful, with numerous organisations achieving their Cyber Essentials and Cyber Essentials Plus certifications under my guidance. For companies that fail, I ensure that they know the process and requirements for passing next time, consulting professionally. By carefully identifying the appropriate standards and working closely with organisations to implement them, I have helped these companies significantly enhance their cybersecurity measures. This has not only enabled them to achieve certification but has also improved their overall security posture, making them better protected against cyber threats.

Organisations have expressed their appreciation for the clear, actionable guidance I provided throughout the certification process. They valued the way I broke down the Cyber Essentials standards into manageable steps and worked with them to implement these standards effectively. This collaborative approach has not only helped them achieve compliance but has also helped their IT teams to maintain these standards over the long term, ensuring ongoing protection against cyber threats.

Furthermore, the organisations I have worked with have reported increased confidence in their security measures and have been able to demonstrate this to their clients and partners. Achieving Cyber Essentials certification has also opened up new business opportunities for many of these organisations, as it serves as a trusted indicator of their commitment to cybersecurity. Overall, my ability to identify and implement appropriate standards has had a lasting impact on the security and success of the organisations I have worked with, reinforcing the importance of adhering to industry standards.

E: Personal Commitment

E1: Carry out and record Continuing Professional Development (CPD) or an acceptable equivalent.

Situation: Staying current with the latest trends, tools, and techniques is essential. To ensure that I remain at the forefront of the industry, I have made it a priority to actively pursue Continuing Professional Development. This commitment involves not only attending formal training sessions but also engaging in self-directed learning through various platforms and participating in conferences where I both learn and share my expertise. My approach to CPD is comprehensive, encompassing everything from attending masterclasses organised by NCSC to hands-on practice on platforms like Hack The Box, Try Hack Me, and Pentester Academy.

In addition to structured learning, I regularly read cybersecurity blogs and whitepapers to stay informed about the latest developments and emerging threats. I also actively participate in conferences where I contribute by explaining cybersecurity concepts and conducting vulnerable lab walkthroughs. These activities not only enhance my own skills but also allow me to give back to the community by sharing knowledge. Over the years, I have also obtained several certifications from recognised organisations such as Pentester Academy, Microsoft, and CompTIA, further validating my skills and commitment to continuous learning.

Task: My primary task is to ensure that I continually develop my professional skills and knowledge to stay ahead in the field of cybersecurity. This involves identifying relevant opportunities for CPD, such as attending masterclasses, engaging in hands-on training, and earning certifications. It is also important to record and reflect on these activities to track my progress and ensure that my learning is aligned with my career goals and the needs of the industry.

Another key aspect of my task is to share the knowledge I gain through CPD with others in the cybersecurity community. This includes presenting at conferences, writing blogs, and mentoring less experienced professionals. By doing so, I contribute to the growth of the community while reinforcing my own understanding of complex topics. Additionally, I must ensure that all my CPD activities are properly documented, both for my own records and to meet any professional requirements for maintaining certifications or memberships in professional organisations.

Action: To fulfil my commitment to CPD, I actively seek out and participate in a variety of learning opportunities. One of my regular activities is attending masterclasses provided by the NCSC. These sessions offer deep insights into the latest cybersecurity challenges and solutions, helping me to stay informed about national and global security trends. I make it a point to attend these sessions regularly, taking detailed notes and reflecting on how the information can be applied to my work.

In addition to formal training, I engage in hands-on practice through platforms like Hack The Box, Try Hack Me, and Pentester Academy. These platforms provide a practical, interactive way to hone my

skills in real-world scenarios, allowing me to stay sharp and experiment with new techniques. I set aside time each week to work on challenges and labs, documenting my progress and any new strategies I learn. This hands-on experience is invaluable, as it helps bridge the gap between theoretical knowledge and practical application.

To further enhance my learning, I regularly read blogs and whitepapers from leading cybersecurity experts and organisations. This helps me stay updated on the latest threats, tools, and industry best practices. I also actively participate in cybersecurity conferences, where I both learn from others and share my own knowledge. For example, I have presented at conferences, explaining cybersecurity concepts and leading vulnerable lab walkthroughs. These presentations not only reinforce my understanding of the material but also allow me to contribute to the professional development of others in the field.

Additionally, I have earned several certifications from reputable institutions, including Pentester Academy, Microsoft, and CompTIA. These certifications validate my skills and provide formal recognition of my expertise. I ensure that all my CPD activities, including certifications, training sessions, and conferences, are meticulously recorded. I maintain a detailed log of my CPD activities, noting the date, content, and relevance of each activity to my professional development. This log serves as a valuable resource for tracking my progress and ensuring that I meet the requirements for maintaining my certifications and professional memberships.

Result: As a result of my commitment to CPD, I have developed a deep and broad skill set that allows me to stay at the cutting edge of the cybersecurity field. The knowledge and skills I gain through these activities enable me to approach complex challenges with confidence and provide high-quality solutions to the organisations I work with. My participation in masterclasses, hands-on training, and conferences has kept me well-informed about the latest trends and techniques, ensuring that I can adapt to new developments in the field.

The certifications I have earned from organisations like Pentester Academy, Microsoft, and CompTIA serve as formal recognition of my expertise and commitment to continuous learning. These certifications not only enhance my professional credibility but also open up new opportunities for career advancement and specialization. Furthermore, my efforts to share knowledge through conference presentations and other activities have contributed to the growth of the cybersecurity community, helping others develop their skills and understanding of key concepts.

By maintaining a detailed record of my CPD activities, I can clearly demonstrate my ongoing commitment to professional development. This documentation not only helps me track my progress but also ensures that I meet any professional requirements for certification and membership in industry organizations. Overall, my dedication to CPD has been instrumental in my success as a cybersecurity professional, enabling me to continually grow my expertise and contribute meaningfully to the field.

E2: Actively participate and promote the cyber security profession

Situation: As a dedicated cybersecurity professional, I believe it is essential to not only excel in my technical work but also to actively contribute to and promote the cybersecurity profession. This commitment extends beyond my day-to-day responsibilities, as I seek to educate and support various communities on the importance of cybersecurity. Over the years, I have undertaken several initiatives aimed at spreading awareness and providing practical guidance on staying safe online. These efforts include creating personal guides to help the elderly and other vulnerable users navigate the digital world securely, as well as planning future projects focused on protecting children online. Additionally, I have taken part in conferences where I share my knowledge on cloud security and broader cybersecurity practices. My passion for learning about the latest threats drives me to regularly explore blogs and articles that discuss emerging vulnerabilities, including zero-day exploits, and how they can be mitigated. Furthermore, I have volunteered my expertise to support a local charity that was recently targeted by vandals, helping them rebuild their security infrastructure and implement essential safeguards. These activities reflect my ongoing commitment to promoting cybersecurity and supporting those who may not have access to professional resources.

Task: My task is to actively participate in the cybersecurity profession by sharing knowledge, educating various groups, and supporting those in need with my expertise. This involves creating resources like guides for safe online practices, presenting at conferences, and staying informed about the latest threats and best practices in the industry. Additionally, I aim to make a meaningful impact in my local community by offering my services to organisations that may not have the resources to secure their digital environments on their own.

In the case of the elderly and other vulnerable users, my task is to distill complex cybersecurity concepts into easily understandable advice that can help them protect themselves online. For conferences, my task is to present information in a way that is both informative and engaging, helping others in the industry stay updated on key issues like cloud security. For the local charity, my task was to rebuild their security infrastructure after an attack, implementing strong security measures to prevent future incidents. Each of these tasks requires a different approach but all share the common goal of promoting cybersecurity and empowering others with the knowledge and tools they need to stay safe.

Action: To promote cybersecurity among the elderly and vulnerable users, I have created personal guides that offer practical advice on staying safe online. These guides cover essential topics such as recognising phishing attempts, creating strong passwords, and using multi-factor authentication. I have ensured that the language and examples used are simple and relatable, making the content

accessible to those who may not be tech-savvy. These guides have been well-received, and I am currently working on future projects that will focus on keeping children safe online. These projects will provide parents with cybersecurity guidelines and techniques to protect their children on digital devices, addressing concerns like safe browsing, screen time, and the use of parental controls.

In addition to creating these resources, I have actively participated in several conferences, where I have shared my expertise on cloud security and broader cybersecurity practices. I prepare thoroughly for these presentations, ensuring that I deliver content that is both insightful and practical. My goal in these sessions is to not only inform but also inspire others in the industry to adopt best practices and stay vigilant against emerging threats. I have a strong interest in cloud security, but I also make it a point to discuss general cybersecurity trends and the importance of continuous learning.

To stay current with the latest developments, I regularly read blogs and articles that discuss new vulnerabilities and zero-day exploits. I actively seek out information on how these threats were discovered, the potential impact they could have, and what can be done to mitigate them. This knowledge not only helps me stay informed but also allows me to share up-to-date information with others in my presentations and discussions.

In a more hands-on capacity, I offered my cybersecurity services free of charge to a local charity that was recently attacked by vandals. Understanding that they lacked the resources to recover and secure their systems on their own, I stepped in to help them rebuild their IT infrastructure. I implemented strong password policies, enabled BitLocker encryption, and installed reliable antivirus software. I also provided them with training on basic cybersecurity practices to ensure that they could maintain a secure environment going forward. This effort was not just about fixing the immediate problem, but also about empowering the charity to protect itself from future attacks.

Result: The results of my efforts to actively participate in and promote the cybersecurity profession have been highly positive and impactful. The guides I created for the elderly and other vulnerable users have helped them navigate the online world more securely, giving them the confidence to protect themselves from common threats. The feedback I received from these users has been very encouraging, and it has motivated me to continue developing additional resources, such as my upcoming project on keeping children safe online.

My participation in conferences has also yielded significant results. By sharing my knowledge on cloud security and broader cybersecurity practices, I have been able to contribute to the professional development of my peers in the industry. My presentations have been well-received, and I have received positive feedback from attendees who found the content both informative and applicable to their work. These experiences have solidified my desire to continue speaking at conferences and contributing to the wider cybersecurity community.

Through my ongoing efforts to stay informed about the latest threats, I have been able to keep my knowledge current and relevant. This has not only benefited my own professional growth but has also allowed me to provide timely and accurate information to others. By regularly sharing insights from my research with colleagues and at conferences, I help ensure that others in the industry are also aware of and prepared for emerging threats.

Finally, my work with the local charity has had a profound impact. The security measures I implemented have significantly improved their ability to protect their systems and data. The charity is now better equipped to defend against potential cyberattacks, and they have expressed their gratitude for the support I provided. This experience reinforced the importance of using my skills to give back to the community and support organisations that may not have the resources to secure themselves.

Overall, my active participation in the cybersecurity profession has allowed me to make meaningful contributions, both within the industry and in my local community. By sharing knowledge, staying informed, and offering my services to those in need, I have helped to promote cybersecurity and ensure that others are equipped to navigate the digital world safely.

E3: Maintain a working knowledge of technological advancements and threat space

Situation: Due to constant changes within the industry, staying current with technological advancements and the latest threats is essential to providing effective and up-to-date security solutions. As a cybersecurity professional, I am committed to maintaining a deep and current understanding of the threat landscape and the technologies that can mitigate these risks. A significant part of this commitment involves regular recertification in key areas of expertise, such as the CHECK Team Leader certification, which I must renew every three years to ensure I remain proficient in conducting penetration tests to NCSC standards. Additionally, I renew other important certifications, such as the CompTIA Security+, to maintain my credentials and stay recognised as a knowledgeable professional in the field.

Beyond formal certifications, I am actively involved in continuous learning through other means. This includes reading the latest blogs, articles, and posts on emerging threats and new technologies. These resources provide me with insights into the latest attack vectors, vulnerabilities, and defence mechanisms. My role as a penetration tester also contributes to my knowledge, as I encounter a wide variety of environments and scenarios daily, which keeps me sharp and aware of the diverse challenges and threats that organisations face. This combination of formal recertification and daily hands-on experience ensures that I maintain a comprehensive and up-to-date understanding of the cybersecurity landscape.

Task: My task is to ensure that I continuously update my knowledge and skills to remain effective in my role as a cybersecurity professional. This includes meeting the requirements for recertification in areas, such as the CHECK Team Leader certification and CompTIA Security+, to ensure that I am always in line with industry standards. Additionally, I must stay informed about the latest technological advancements and threats by regularly engaging with industry publications, blogs, and other resources. This ongoing education is necessary not only for my professional development but also to ensure that I can provide the most effective security solutions to the organisations I work with.
Another important aspect of my task is to apply this knowledge in my daily work, particularly in penetration testing, where understanding the latest threats and technologies is crucial for identifying vulnerabilities and recommending appropriate defences. By combining formal recertification with continuous self-education and practical experience, I can maintain a high level of proficiency in my field and ensure that I am always prepared to address new and emerging threats.
Action: To maintain my working knowledge of technological advancements and the evolving threat landscape, I take several proactive steps. First, I ensure that I meet all recertification requirements for my key certifications. For the CHECK Team Leader certification, I go through a rigorous recertification process every three years, which includes updated training and assessments to confirm my proficiency in penetration testing according to NCSC standards. This recertification process is important for ensuring that I remain current with the latest methodologies and tools used in cybersecurity assessments.
Similarly, I regularly renew my CompTIA Security+ certification to maintain my standing as a recognised expert in the field. CompTIA certifications require continuous education to stay valid, and I engage in various activities, such as attending webinars, completing courses, and participating in industry events, to earn the necessary continuing education units for recertification. These activities not only help me maintain my certifications but also provide valuable opportunities to learn about the latest security trends and technologies.
In addition to formal recertification, I actively seek out the latest information on emerging threats and technological advancements. I regularly read cybersecurity blogs, follow industry experts on social media, and subscribe to newsletters from reputable sources. These resources keep me informed about the latest vulnerabilities, attack techniques, and defence strategies. I particularly enjoy diving into detailed analysis of zero-day vulnerabilities and new attack vectors, as these insights help me anticipate potential threats and refine my approach to penetration testing.
My daily work as a penetration tester also plays a significant role in maintaining my knowledge. Each engagement presents a unique environment and set of challenges, exposing me to a wide range of technologies and potential vulnerabilities. By applying my knowledge in real-world scenarios, I continually refine my skills and stay updated on the practical implications of the latest threats. This

hands-on experience is invaluable for keeping my knowledge fresh and relevant, ensuring that I can provide effective security solutions to the organisations I work with.

Result: As a result of my commitment to maintaining a working knowledge of technological advancements and the threat landscape, I have been able to consistently deliver high-quality security assessments and recommendations. My certification as a CHECK Team Leader has ensured that I remain proficient in conducting penetration tests according to the latest NCSC standards, which has bolstered my credibility and effectiveness in this critical area. Similarly, maintaining my CompTIA Security+ certification has reinforced my expertise in a broad range of cybersecurity topics, enabling me to provide well-rounded advice and support to clients.

The continuous learning I engage in through reading blogs, following industry experts, and staying informed about new threats has significantly enhanced my ability to anticipate and address emerging risks. This knowledge has directly impacted my work, allowing me to identify vulnerabilities that may not be immediately obvious and to recommend cutting-edge solutions that protect organisations from evolving threats. My regular exposure to different environments through penetration testing further enriches my understanding, as I am constantly applying new knowledge in practical, real-world settings.

Overall, my dedication to maintaining a current and comprehensive understanding of technological advancements and the threat space has enabled me to stay at the forefront of the cybersecurity field. This commitment not only benefits my own professional development but also ensures that the organisations I work with receive the most up-to-date and effective security solutions. By combining formal recertification, continuous learning, and practical experience, I am able to provide the highest level of service and remain a trusted expert in the cybersecurity profession.