Month 1 at CyberTalos: Building the Foundation

My first month at CyberTalos has been an incredible journey of learning, exploration, and hands-on experiences. The training focused on understanding the company's operations, mastering key tools, and delving into the fundamentals of SOC (Security Operations Center) operations. Here's a week-by-week breakdown of my first month:

Week 1: Introduction and Onboarding

The first week was all about getting acquainted with the company's structure, culture, and tools.

Highlights:

- Attended onboarding sessions to learn about CyberTalos' objectives and how its proprietary software integrates with datacenters and servers.
- Started exploring the Elastic Stack, a critical tool for data search, analysis, and visualization.
- Watched a six-part video series on Elastic Stack to understand its features and practical use cases.
- Observed live demonstrations of the software in action, gaining insights into real-time applications.

Key Takeaways:
This week was foundational. I developed a clear understanding of how the Elastic Stack operates and its role in ensuring system health and security. The learning curve was steep, but it laid the groundwork for more advanced tasks in the following weeks.

Week 2: Hands-On with Tools and Systems

In the second week, I transitioned from theoretical learning to hands-on experiences.

Highlights:

- Worked directly with the Elastic Stack, exploring its functionalities and understanding the companies CyberTalos serves.
- Participated in a session with Vinod Sir, who explained server operations, terms like Disk Bay, RAID configurations (0/1/5/10), and details about TATA and Blazenet servers.

- Visited the datacenter at GIFT City in Gandhinagar. This visit was eye-opening as I learned about datacenter management and saw how multiple companies' data is securely stored.

Key Takeaways:
Seeing the datacenter in person was an unforgettable experience. It brought the concepts we'd studied to life and deepened my understanding of datacenter operations.

Week 3: Exploring the SOC Monitoring Web

This week, I delved deeper into SOC operations and monitoring tools.

Highlights:

- Explored the SOC web interface and learned to access it remotely via the remote desktop feature.
- Analyzed the monitoring dashboard, studying the data and understanding its significance.
- Successfully identified my first alert: multiple failed login attempts (3,000 attempts in 15 minutes) that indicated potential malware activity. Reporting this was a great achievement and a confidence booster.

Key Takeaways:
Detecting and reporting the malware alert reinforced the importance of vigilance in SOC operations. Monitoring tools like Elastic Stack proved invaluable in maintaining system security.

Week 4: Advanced Tools and Concepts

The final week of the month was all about diving into advanced tools and concepts.

Highlights:

- Learned about firewalls, focusing on Fortinet firewall services, and explored Proxmox for virtualized environment management.
- Studied Hyper-V in detail, including its installation and functionalities.
- Understood Proxmox's demo setup, features, and practical applications.

Key Takeaways:
This week solidified my knowledge of advanced tools used in SOC operations. The combination of Proxmox, Hyper-V, and firewalls provided a comprehensive understanding of system monitoring and management.

Conclusion

The first month at CyberTalos has been a remarkable learning experience. From understanding foundational tools to working hands-on with advanced systems, every week offered something new. While challenging at times, these experiences have built a strong base for the months ahead.

Month 2 at CyberTalos: Overcoming Challenges and Building Confidence

The second month of my internship at CyberTalos was a transformative phase. It marked the shift from foundational learning to active involvement in real-world tasks. This period challenged me to apply what I had learned, work on live systems, and gradually gain confidence in handling complex SOC operations. Here's how my journey unfolded, week by week.

Week 1: Building Hands-On Skills

This week was all about stepping into practical work and gaining real-world exposure.

Highlights:

- Set up a physical server at the office, learning the foundational steps in server configuration and deployment.
- Completed the Proxmox training series and got access to a live Proxmox server, enabling me to explore its functionalities in a real-world environment.
- Started working with the Proxmox server for hands-on tasks, including testing and troubleshooting.

Key Takeaways:
Setting up and working on servers gave me a deeper understanding of their architecture and how they interact with other systems. It was the first real test of my theoretical knowledge.

Week 2: Exploring Fortinet and Cloud Computing

The second week expanded my understanding of cybersecurity tools and introduced me to cloud technologies.

Highlights:

- Learned about the Fortinet gateway, widely used by CyberTalos and other companies for server and datacenter management.
- Watched Fortinet setup and use-case videos, gaining insights into its diverse applications beyond monitoring.
- Started exploring cloud computing, setting up an AWS free trial server to practice cloud-based tools like Docker, Azure, and GCP.

Key Takeaways:
This week was a turning point as I ventured into cloud computing, which is critical for

modern SOC operations. It also strengthened my understanding of Fortinet and its role in ensuring server stability and security.

Week 3: Monitoring and First VAPT Tasks

The third week was intense, as I began taking on more responsibilities and participated in my first vulnerability assessment and penetration testing (VAPT) task.

Highlights:

- Monitored SOC activities for CyberTalos and its clients, such as Ventura and Master Trust.
- Worked on my first VAPT task, collaborating with my co-worker Samarth to identify and filter vulnerabilities like true positives and false positives.
- Built my first VAPT report for a client, which took two days due to the steep learning curve.

Key Takeaways:
The VAPT task was a significant milestone. It tested my ability to analyze vulnerabilities and prepare detailed reports, reinforcing the importance of accuracy and attention to detail.

Week 4: Advanced VAPT and Proxmox Exploration

The final week of the month pushed me to apply my skills further, with a mix of advanced VAPT tasks and deeper exploration of Proxmox.

Highlights:

- Conducted a VAPT scan for another client's website, identifying a vulnerability at the login page related to SQLite injection.
- Worked on exploiting the vulnerability further, as recommended by the client, and documented the findings for their reference.
- Received credentials for Proxmox webserver monitoring, providing insights into all client servers.
- Monitored and analyzed the Proxmox system throughout the day to learn its features and outcomes.

Key Takeaways:
This week solidified my understanding of VAPT and enhanced my skills in identifying and documenting vulnerabilities. Monitoring Proxmox gave me a comprehensive view of its capabilities, preparing me for more independent tasks.

Conclusion

Month 2 was a challenging but rewarding phase. From working on live systems to conducting VAPT scans and building reports, I gained hands-on experience that boosted my confidence and skills. Every challenge was a learning opportunity, and with the guidance of my mentors and teammates, I navigated this phase successfully.

Month 3 at CyberTalos: Tackling Real-World Challenges and Refining Skills

The third month at CyberTalos was an exciting phase of deeper involvement in vulnerability assessment and penetration testing (VAPT) projects. It was a period of significant growth as I handled client interactions, worked on large-scale projects, and honed my technical skills. Here's a week-by-week breakdown of my experiences:

Week 1: Client Interaction and First Major VAPT Project

This week marked my first experience handling client calls and managing a full VAPT project independently with my team.

Highlights:

- Handled client calls, addressing issues related to Proxmox functionality and managing server gateway flow problems.
- Took on my first major VAPT project for a company site named Qmetry. The scanning process revealed a large number of vulnerabilities, which required careful analysis.
- Worked on separating true positives and false positives from the 40+ vulnerabilities identified.
- Collaborated with my mentor and teammate Samarth to conduct penetration testing, narrowing the focus to three critical vulnerabilities that were communicated to the client.

Key Takeaways:
This week was a milestone in my journey. I learned how to efficiently prioritize and validate vulnerabilities, a critical skill in SOC operations. The experience of handling client calls also boosted my confidence in addressing technical issues.

Week 2: Completing Qmetry VAPT and Strengthening Skills

This week involved wrapping up the Qmetry project and using my free time to sharpen my skills.

Highlights:

- Completed the Qmetry VAPT project by creating a detailed report that demonstrated real-time exploitation of vulnerabilities.
- Supported my mentor in preparing for a client meeting with Qmetry professionals, where the findings were presented.

- Used the downtime to enhance my skills in Linux OS, which is vital for SOC tasks.

Key Takeaways:
Finishing my first VAPT project was a rewarding experience. It gave me valuable insights into the reporting process and the importance of clear communication in client interactions.

Week 3: Starting the Otsuka VAPT Project

The third week introduced a new VAPT project for a company named Otsuka, which required a thorough and systematic approach.

Highlights:

- Began the VAPT process for Otsuka's site, which had been facing persistent issues.
- Conducted an in-depth vulnerability scan and initiated the process of separating false positives.
- Faced challenges due to the size and complexity of the site, which required extensive analysis.

Key Takeaways:
This week emphasized the importance of patience and attention to detail in handling large-scale projects. Collaborating with my team was crucial in managing the workload and ensuring accuracy.

Week 4: Filtering Vulnerabilities and Finalizing the Otsuka Project

The final week was dedicated to refining the Otsuka VAPT project and learning from my mentors' guidance.

Highlights:

- Continued filtering the vulnerabilities, which totaled 1,154. Many were duplicates with similar solutions, requiring further consolidation.
- Worked under my mentor's guidance to prioritize critical vulnerabilities and streamline the process.
- Focused on organizing and presenting the findings clearly, ensuring the data was actionable for the client.

Key Takeaways:
This week highlighted the importance of mentorship and systematic problem-solving in large projects. The Otsuka VAPT project tested my ability to manage time, collaborate effectively, and produce accurate results under pressure.

Conclusion

Month 3 was packed with challenges and opportunities to grow. From handling client calls to managing large-scale VAPT projects, every task was a stepping stone toward becoming more proficient in SOC operations. The collaborative efforts with my mentors and teammates played a significant role in my success.

Month 4 at CyberTalos: Consolidating Knowledge and Handling Professional Milestones

The fourth month at CyberTalos was a mix of finalizing major projects, handling client interactions, and balancing personal milestones. It was a month that emphasized the importance of professionalism, teamwork, and adaptability. Here's a week-by-week breakdown:

Week 1: Finalizing the Otsuka VAPT Project

Highlights:

- Completed the filtering process for Otsuka's vulnerabilities. This task required a thorough review of 1,154 vulnerabilities to ensure the final report contained only critical and actionable issues.
- Worked on formatting the final VAPT report, which included detailed sections on IT systems, website vulnerabilities, and open or vulnerable ports.
- Collaborated with my mentor and teammates to add the finishing touches to the report. The final version was polished and prepared for presentation during the upcoming meeting with Otsuka's IT team.

Key Takeaways:
The week underscored the importance of attention to detail in delivering professional-quality reports. This experience taught me how to present technical findings in a clear and structured manner.

Week 2: Client Presentation and Downtime

Highlights:

- The Otsuka VAPT report was successfully presented during a meeting with their IT team. The feedback was overwhelmingly positive, with the client expressing interest in future collaborations.
- While my seniors attended the meeting, my team and I were tasked with monitoring operations and handling any issues that might arise. It was a quiet day, as no major calls or problems came in, likely due to it being a Saturday when many client offices were closed.

Key Takeaways:
This week offered insights into how client-facing presentations are conducted and how effective teamwork ensures smooth operations even in the absence of senior members.

Week 3: Personal Milestones and Adaptability

Highlights:

- Took a day off to participate in a placement drive test, an important step in my professional journey.
- The week also brought unexpected challenges, such as navigating through heavy rains, which forced me to take another day off due to getting drenched on my way to the office.

Key Takeaways:
Balancing personal responsibilities with professional commitments can be challenging, but it’s an essential aspect of growth. This week taught me the value of time management and adaptability.

Week 4: Reflection and Learning

Highlights:

- With major projects completed and fewer tasks at hand, I spent time reflecting on the journey so far. This period allowed me to consolidate my learnings and identify areas for improvement.
- Reviewed previous project reports and notes to enhance my understanding of VAPT processes and SOC operations.
- Focused on self-improvement and preparing for upcoming challenges by exploring new tools and technologies in the SOC domain.

Key Takeaways:
This week emphasized the importance of continuous learning and self-assessment. Even in quieter times, there’s always room to grow and prepare for future opportunities.

Conclusion

Month 4 was a blend of wrapping up significant projects and managing personal responsibilities. The successful completion of the Otsuka VAPT project and the positive client feedback were highlights of the month. Additionally, the downtime allowed me to reflect on my progress and prepare for the road ahead.

Month 5 at CyberTalos: Transition to Active Monitoring

The fifth month at CyberTalos marked a significant transition in my role. Having gained foundational knowledge over the previous months, I stepped into active monitoring and reporting, with a stronger focus on client security and hands-on operational tasks. Here's a snapshot of the first two weeks of this phase:

Week 1: Active Monitoring and On-Site Operations

This week, I took on the responsibility of monitoring our company's SOC and client servers daily. My tasks involved analyzing system logs, tracking potential malicious activities, and reporting any anomalies to ensure system integrity. During this time, I successfully identified and flagged several malicious IPs attempting unauthorized access to client systems. By reporting these issues promptly, I helped our clients block high-traffic threats and secure their environments.

Additionally, I participated in a physical setup at our data center in GIFT City. This involved installing new storage infrastructure for a client requiring extensive resources. It was a rewarding experience that combined hands-on work with a better understanding of the physical components supporting SOC operations.

Week 2: Routine Monitoring and Weekend Insights

This week emphasized the importance of routine. Monitoring tasks focused on maintaining consistent vigilance over SOC systems, ensuring stable performance and reporting any abnormalities in IP traffic or server loads. While weekdays were busy with regular system checks, weekends brought quieter times due to reduced traffic from client offices.

The lighter workload on the weekend allowed for brief moments of downtime. It provided an opportunity to recharge while remaining on alert for potential emergencies. This balance between high-alert weekdays and calmer weekends highlighted the variability in SOC operations and the adaptability required for the role.

Conclusion: A Gratifying Journey Ends

As I wrap up my internship at CyberTalos, I look back with immense gratitude and pride. This journey has been a transformative experience, helping me grow both professionally and personally. Over the past five months, I've gained hands-on expertise in monitoring tools like Elastic Stack, Proxmox, and Zabbix, as well as valuable experience in SOC operations, vulnerability assessments, and client management.

The guidance of my mentors and the collaborative spirit of my team were instrumental in shaping my skills and building my confidence. This internship not only deepened my understanding of cybersecurity but also instilled in me the resilience and adaptability required to thrive in this field.

As I step forward into the next phase of my career, I carry with me the lessons learned and the satisfaction of having contributed meaningfully to the organization. I am thankful for this opportunity and excited about the challenges and growth that lie ahead.