Blue Team Study Plan

1. Build Foundational Knowledge

- **Study Detection Engineering**
  Learn how to identify, create, and tune detection rules for threats. Start with:
  - MITRE ATT&CK framework
  - Sigma rules
  - YARA rules
- **Beginner Blue Team Topics**
  Focus on:
  - Incident response basics
  - Log analysis (Windows Event Logs, Sysmon, etc.)
  - SIEM fundamentals (e.g., Splunk, Elastic, Sentinel)
- **Deepen Networking Knowledge**
  - Study OSI model, TCP/IP, DNS, HTTP/S, VPNs, firewalls
  - Use tools like Wireshark to analyze traffic
- **Learn Basic Scripting/Programming**
  - Python (focus on automation, log parsing, and scripting)
  - Bash (for Linux environments)

🔹 **2. Get Certified**

- **BTL1 (Blue Team Level 1)** from Security Blue Team
  - Entry-level, hands-on certification for blue teamers
  - Covers SOC fundamentals, threat intelligence, and more

🔹 **3. Join Communities**

- **Black Hills Information Security Discord**

- Great for networking, mentorship, and learning
- Look into their **Antisyphon Training** for affordable, high-quality courses

---

🔹 4. Leverage Internal Opportunities

- **Reach Out to TechSec Support Team**
  - They act as a bridge between Support and the SOC
  - Ask to shadow or assist with product-related security issues
  - This will expose you to internal security processes and tools

---

🔹 5. Create a Learning Schedule

Break your time into weekly goals. For example:

Week	Focus Area
1–2	Networking fundamentals
3–4	Basic scripting (Python/Bash)
5–6	Blue team basics + log analysis
7–8	Detection engineering intro
9–10	BTL1 prep
Ongoing	Join Discords, explore Antisyphon, connect with TechSec