YOUR BEGINNER'S GUIDE TO BECOMING A SOC ANALYST

BY IZZMIER IZZUDDIN

Table of Contents

CHECKLIST FOR FUTURE SOC ANALYSTS!

PATH 1: FOR INDIVIDUALS WITHOUT IT EXPERIENCE

1. **Basic IT Knowledge**

□ **Computer Hardware Basics**

- Understand components like CPU, RAM, storage, etc.
- Assemble and troubleshoot basic hardware issues.

□ **Operating Systems**

- Learn the basics of Windows (navigation, file systems, basic commands).
- Get comfortable with Linux (basic commands, navigating the file system).

□ **Networking Fundamentals**

- Understand how networks work (LAN, WAN, TCP/IP).
- Learn about common network devices (routers, switches, firewalls).
- Familiarise yourself with basic networking protocols (HTTP, DNS, DHCP).

2. **Introduction to Cybersecurity**

□ **Cybersecurity Fundamentals**

- Learn the CIA Triad (Confidentiality, Integrity, Availability).
- Understand common threats (malware, phishing, DDoS).

□ **Security Architecture**

- Get familiar with the layered security approach.
- Understand how firewalls, IDS/IPS and antivirus work together.

□ **Security Policies and Governance**

- Learn about basic security policies and compliance (ISO 27001, NIST).

3. **SOC-Specific Knowledge**

□ **SIEM (Security Information and Event Management)**

- Understand the role of SIEM in a SOC.
- Learn how to use SIEM tools (Splunk, QRadar).
- Practice log analysis and creating alerts.

□ **Incident Response (IR)**

- Learn the phases of incident response.
- Practice responding to simulated incidents.
- Understand the importance of documentation.

□ **IDS/IPS (Intrusion Detection and Prevention Systems):**

- Understand how IDS/IPS work.
- Learn to configure and tune IDS/IPS systems.

4. **Developing Analytical and Monitoring Skills**

□ **Alert Analysis**

- Learn to triage and prioritise alerts.
- Understand how to deal with false positives.

□ **Threat Intelligence**

- Learn where to source threat intelligence.
- Practice using threat intelligence in SOC operations.

5. **Hands-On Practice (Home Lab)**

□ **Set Up a Home Lab**

- Install and configure virtual machines.
- Set up SIEM, IDS/IPS and other security tools.

□ **Simulate Security Incidents**

- Practice detecting and responding to attacks in your lab.

□ **Documentation and Reporting**

- Practice writing incident reports and logs.

6. **Continuous Learning**

□ **Join Cybersecurity Communities**

- Participate in forums, meetups or online communities.

□ **Stay Updated on Cybersecurity Trends**

- Follow blogs, news sites and forums.

□ **Engage in Continuous Learning**

- Take online courses, attend webinars.
- Use LinkedIn Learning for access to a variety of cybersecurity courses and resources.

PATH 2: FOR INDIVIDUALS WITH IT EXPERIENCE

1. **Advanced IT Knowledge**

☐ **Operating Systems:**

- Deepen your knowledge of Windows and Linux systems.
- Learn about system administration tasks (user management, security settings).

☐ **Advanced Networking:**

- Get deeper into networking protocols and technologies (VPN, VLAN, IPv6).
- Learn about network security measures (SSL/TLS, IDS/IPS configurations).

☐ **Virtualisation and Cloud Computing:**

- Understand the basics of virtual environments (VMware, Hyper-V).
- Learn about cloud security fundamentals (AWS, Azure).

2. **Advanced Cybersecurity Knowledge**

☐ **Advanced Security Concepts:**

- Learn about encryption, hashing and secure communications.
- Understand advanced threat types (Advanced Persistent Threats, Zero-Day Exploits).

☐ **Security Policies and Compliance:**

- Dive into specific frameworks relevant to SOC operations (PCI-DSS, HIPAA).

3. **SOC-Specific Knowledge (Deeper Focus)**

☐ **SIEM Mastery:**

- Become proficient with advanced SIEM features (correlation searches, dashboards).
- Learn how to integrate SIEM with other security tools.

☐ **Advanced Incident Response:**

- Practice advanced incident response scenarios.
- Learn forensic analysis basics.

☐ **Advanced IDS/IPS Management:**

- Get into the specifics of tuning IDS/IPS to your network environment.
- Learn about integrating IDS/IPS with SIEM and other tools.

4. **Developing Advanced Analytical and Monitoring Skills**

□ **Advanced Alert Analysis:**

- Learn to identify patterns and behaviours in alerts.
- Practice threat hunting techniques.

□ **Threat Intelligence Application:**

- Deepen your understanding of threat intelligence platforms.
- Practice using threat intelligence to improve SOC detection capabilities.

5. **Advanced Hands-On Practice**

□ **Advanced Home Lab Setup:**

- Create a more complex lab environment (include multiple networks, servers, firewalls).
- Practice incident response with real-world scenarios.

□ **Documentation and Reporting:**

- Develop advanced incident reports that include detailed analysis and remediation steps.

6. **Continuous Learning**

□ **Engage in Advanced Learning:**

- Take part in cybersecurity competitions (Capture the Flag).

PATH 1: FOR INDIVIDUALS WITHOUT IT EXPERIENCE

1. Basic IT Knowledge

Computer Hardware Basics

Key Concepts to Learn:

- **Central Processing Unit (CPU):**
    - Learn about the CPU, the "brain" of the computer, which processes instructions from programs and performs calculations. Understand how CPU performance affects overall system performance.
- **Random Access Memory (RAM):**
    - Understand how RAM temporarily stores data that the CPU needs quick access to. Learn how the amount of RAM can affect system performance, especially when running multiple applications.
- **Storage Devices:**
    - Get familiar with different types of storage devices like Hard Disk Drives (HDDs), Solid State Drives (SSDs) and external storage. Understand the difference between storage and memory and how data is stored and retrieved.
- **Motherboard and Power Supply:**
    - Learn about the motherboard, which connects all the components of the computer and the power supply, which provides the necessary power for all components to function.

Practical Steps:

- **Assemble a Computer:**
    - If possible, try assembling a basic computer. This hands-on experience will help you understand how each component fits and works together.
- **Troubleshooting:**
    - Practice troubleshooting common hardware issues like replacing faulty RAM, upgrading storage or identifying why a computer isn't powering on. This experience is invaluable for understanding hardware-related security incidents.

Operating Systems

Key Concepts to Learn:

- **Windows Operating System:**
    - Learn the basics of the Windows OS, including navigation, file management and system settings.
    - Understand the Windows file system (NTFS), how files and directories are organised and basic commands (e.g., creating files, navigating directories).
    - Familiarise yourself with system administration tools like Task Manager, Control Panel and Event Viewer.
- **Linux Operating System:**
    - Get comfortable with Linux, as it's widely used in cybersecurity for its flexibility and powerful command-line interface (CLI).
    - Learn basic Linux commands (e.g., ls, cd, pwd, cp, mv) and how to navigate the file system.
    - Understand file permissions and how they impact security (e.g., chmod, chown commands).
    - Explore different Linux distributions like Ubuntu, CentOS and Kali Linux and understand their use cases in cybersecurity.

Practical Steps:

- **Set Up Virtual Machines:**
    - Use virtual machines (VMs) to practice installing and configuring both Windows and Linux operating systems. Tools like VirtualBox or VMware Workstation can help you create these environments.
- **Command-Line Practice:**
    - Spend time working in the command-line interface of both Windows (Command Prompt, PowerShell) and Linux. Practice common tasks like file management, system monitoring and process control.

Networking Fundamentals

Key Concepts to Learn:

- **Local Area Network (LAN) and Wide Area Network (WAN):**
    - Understand the difference between LAN (a network within a small geographic area like an office) and WAN (a network spread across a larger geographic area, like the internet).

    - Learn how devices within a LAN communicate with each other and how LANs connect to WANs.
- **TCP/IP Model:**
    - Study the Transmission Control Protocol/Internet Protocol (TCP/IP) model, which is the foundation of internet communication. Understand the four layers (Application, Transport, Internet and Network Access) and how data flows through them.
    - Learn about the IP addressing system (IPv4 and IPv6) and how data packets are routed from the source to the destination.
- **Common Networking Devices:**
    - Familiarise yourself with routers, which direct traffic between networks and switches, which manage data flow within a network. Understand the role of firewalls in protecting networks by controlling incoming and outgoing traffic.
- **Basic Networking Protocols:**
    - Learn about essential networking protocols such as:
        - **HTTP/HTTPS:** Protocols for web communication. HTTPS adds encryption for secure data transmission.
        - **DNS (Domain Name System):** Translates domain names (like www.example.com) into IP addresses.
        - **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices on a network.

Practical Steps:

- **Network Simulation Tools:**
    - Use network simulation tools like Cisco Packet Tracer or GNS3 to create and configure virtual networks. Practice setting up routers, switches and firewalls.
- **Configure Home Network:**
    - Work on your home network by setting up a router, configuring Wi-Fi and understanding how your devices connect to the internet.
- **Analyse Network Traffic:**

    - Use tools like Wireshark to capture and analyse network traffic. This will help you understand how data moves across the network and identify common protocols in action.

2. Introduction to Cybersecurity

Cybersecurity Fundamentals

Key Concepts to Learn:

- **CIA Triad (Confidentiality, Integrity, Availability):**
    - **Confidentiality:**
        - Ensures that sensitive information is accessible only to authorised individuals. Learn about encryption, access controls and the importance of protecting data from unauthorised access.
        - Example: Encryption is used to protect data stored on a device or transmitted over the internet.
    - **Integrity:**
        - Ensures that information remains accurate and unaltered. Understand the importance of data integrity checks and the role of hashing in verifying data authenticity.
        - Example: Hashing is used to verify that a downloaded file has not been tampered with.
    - **Availability:**
        - Ensures that information and systems are accessible when needed. Learn about redundancy, backups and disaster recovery plans that help maintain system availability even during attacks or failures.
        - Example: Redundant servers and backup power supplies ensure that critical systems remain operational during outages.
- **Common Cyber Threats:**
    - **Malware:**
        - Learn about different types of malicious software, including viruses, worms, Trojans, ransomware and spyware. Understand how malware infects systems and how it can be prevented or removed.

        - Example: Ransomware encrypts files on a victim's computer and demands payment to restore access.

    - **Phishing:**

        - Understand how attackers use deceptive emails or messages to trick individuals into revealing sensitive information, such as login credentials or financial details. Learn to recognise common phishing tactics and how to protect against them.

        - Example: An email that appears to be from a legitimate source but contains a link to a fake login page designed to steal your credentials.

    - **Distributed Denial of Service (DDoS) Attacks:**

        - Learn how attackers overwhelm a target system with excessive traffic, rendering it unavailable to legitimate users. Understand the basic techniques used in DDoS attacks and the measures that can be taken to mitigate them.

        - Example: A website is flooded with traffic from multiple sources, causing it to crash and become unavailable.

Practical Steps:

- **Interactive Learning:**

    - Use online platforms like Cybrary or Udemy to take introductory courses on cybersecurity fundamentals. Many of these platforms offer interactive lessons and quizzes to reinforce your learning.

- **Case Studies:**

    - Study real-world cyber incidents to see how the CIA Triad and common threats play out in actual scenarios. Analyse how organisations responded and what could have been done differently.

Security Architecture

Key Concepts to Learn:

- **Layered Security Approach (Defence in Depth):**

    - Understand the concept of layered security, where multiple security measures are implemented at different levels (e.g., network, application, endpoint) to protect systems from various threats. This approach ensures that if one layer is compromised, others can still provide protection.

    - Example: A corporate network may have firewalls to block unauthorised access, intrusion detection systems to monitor for suspicious activity and antivirus software to detect and remove malware.

- **Firewalls:**
    - Learn how firewalls act as a barrier between internal networks and external threats. Understand the different types of firewalls (e.g., packet-filtering, stateful inspection, proxy) and how they enforce security policies by controlling incoming and outgoing traffic.
    - Example: A firewall may block traffic from known malicious IP addresses or only allow specific types of traffic (e.g., HTTP, HTTPS) to pass through.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):**
    - Understand how IDS and IPS work together to detect and prevent unauthorised access or attacks. IDS monitors network traffic for suspicious activity and alerts administrators, while IPS actively blocks or mitigates detected threats.
    - Example: An IDS might alert you to unusual traffic patterns indicative of a potential attack, while an IPS could automatically block traffic from the offending source.
- **Antivirus and Endpoint Security:**
    - Learn about the role of antivirus software in detecting, preventing and removing malware. Understand how modern endpoint security solutions extend beyond traditional antivirus to include features like behaviour analysis and threat intelligence.
    - Example: Antivirus software scans files and applications on a computer for known malware signatures and quarantines any detected threats.

Practical Steps:

- **Hands-On Labs:**
    - Set up a home lab where you can experiment with configuring firewalls, IDS/IPS systems and antivirus solutions. Practice creating security rules and responding to simulated attacks.
- **Network Simulation Tools:**
    - Use tools like Cisco Packet Tracer or GNS3 to simulate network environments and implement layered security measures. Experiment with different configurations to understand how each component works.

Security Policies and Governance

Key Concepts to Learn:

- **Security Policies:**
  - Learn about the importance of having clear and comprehensive security policies that outline how data should be protected, how incidents should be handled and what employees' roles and responsibilities are regarding cybersecurity.
  - Example: A data protection policy may specify how sensitive data should be encrypted and who has access to it.
- **Compliance and Regulatory Frameworks:**
  - Understand the key regulatory frameworks that govern cybersecurity practices, such as:
    - **ISO 27001:** A widely recognised standard that provides requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS).
    - **NIST (National Institute of Standards and Technology):** The NIST Cybersecurity Framework offers a policy framework of computer security guidance for how private sector organisations in the U.S. can assess and improve their ability to prevent, detect and respond to cyber-attacks.
- **Risk Management:**
  - Learn how organisations assess and manage risks through processes like risk assessment, risk treatment and continuous monitoring. Understand the importance of regularly reviewing and updating security policies to adapt to new threats and technologies.
  - Example: A risk assessment might identify that employees frequently use weak passwords, leading to the implementation of a strong password policy.

Practical Steps:

- **Policy Development:**
  - Draft a basic security policy for a hypothetical organisation. Include sections on data protection, access control and incident response. Review examples of real-world security policies to guide your efforts.

- **Compliance Simulation:**
    - Use online tools and resources to simulate compliance audits or assessments. Understand how organisations prepare for audits and ensure they meet regulatory requirements.

3. **SOC-Specific Knowledge**

SIEM (Security Information and Event Management)
Key Concepts to Learn:

- **Role of SIEM in a SOC:**
    - **Centralised Monitoring:**
        - SIEMs provide a centralised platform for monitoring security events across an organisation. They aggregate logs from various devices like firewalls, intrusion detection systems (IDS), servers and applications, allowing analysts to see the bigger picture of what's happening in the network.
    - **Correlation and Alerting:**
        - SIEMs use correlation rules to identify patterns or sequences of events that could indicate a security incident. For example, multiple failed login attempts followed by a successful one might trigger an alert for a potential brute force attack.
    - **Incident Detection:**
        - SIEMs help in the early detection of security incidents by analysing logs and generating alerts based on predefined rules. Analysts then investigate these alerts to determine if they represent actual threats.
- **Using SIEM Tools (Splunk, QRadar):**
    - **Splunk:**
        - Learn how to use Splunk, one of the most popular SIEM tools. Understand how to ingest and search logs, create dashboards and set up alerts.
        - Example: Use Splunk to monitor login attempts across the network and create a dashboard that visualises failed and successful logins.
    - **QRadar:**

        - QRadar is another widely used SIEM tool. Learn how to configure data sources, write custom correlation rules and investigate incidents using QRadar's user interface.
        - Example: Configure QRadar to correlate events from firewalls and IDS to detect potential intrusion attempts.

- **Log Analysis and Creating Alerts:**
    - **Log Analysis:**
        - Practice analysing logs from different sources to identify unusual patterns or activities. Understand the structure of common log formats (e.g., syslog, Windows Event Logs) and what each field represents.
        - Example: Analyse web server logs to identify potential SQL injection attempts by looking for suspicious query strings.
    - **Creating Alerts:**
        - Learn how to create alerts in a SIEM system based on specific criteria. For example, you might create an alert for a high number of failed login attempts from the same IP address within a short period.
        - Example: Set up an alert in Splunk to notify you if more than five failed login attempts occur within a minute on any server.

Practical Steps:

- **SIEM Labs:**
    - Use online labs or virtual environments to practice setting up and using SIEM tools. Sites like CyberDefenders or RangeForce offer hands-on exercises with SIEM tools.
- **Log Analysis Practice:**
    - Obtain sample logs (many security websites provide these) and practice analysing them for potential security events. Practice creating correlation rules and alerts in a SIEM environment.

Incident Response (IR)

Key Concepts to Learn:

- **Phases of Incident Response:**
    - **Preparation:**

    - This phase involves establishing and training an incident response team, developing incident response policies and procedures and ensuring the necessary tools and resources are in place.
    - Example: Preparing an incident response plan that includes contact information for key personnel, communication protocols and a list of critical assets.
- **Identification:**
    - Detecting and identifying potential security incidents is the first active step in incident response. This involves monitoring alerts, investigating suspicious activities and confirming whether an incident has occurred.
    - Example: Investigating an alert generated by the SIEM system that indicates unusual network traffic to determine if it represents an actual threat.
- **Containment:**
    - Once an incident is identified, the next step is to contain it to prevent further damage. This can involve isolating affected systems, disabling compromised accounts or blocking malicious IP addresses.
    - Example: Quarantining an infected server to prevent malware from spreading to other systems on the network.
- **Eradication:**
    - After containing the incident, the goal is to eliminate the root cause. This might involve removing malware, applying patches or changing compromised passwords.
    - Example: Removing malicious code from a web server and applying security patches to prevent future exploitation.
- **Recovery:**
    - Recovery involves restoring affected systems to normal operation and verifying that they are secure. This could include restoring data from backups, reconfiguring systems and monitoring for signs of reinfection.
    - Example: Restoring a compromised server from a clean backup and closely monitoring its activity post-recovery.

  - **Lessons Learned:**
    - After the incident is resolved, it’s essential to review what happened and how it was handled. This phase involves documenting the incident, identifying lessons learned and updating response plans to improve future responses.
    - Example: Conducting a post-incident review to determine what worked well and what could be improved and updating the incident response plan accordingly.
- **Simulating Incident Response:**
  - **Tabletop Exercises:**
    - Participate in or organise tabletop exercises where a hypothetical incident is discussed and the response is planned. This helps in understanding the decision-making process and the roles of different team members during an actual incident.
    - Example: Run a tabletop exercise simulating a ransomware attack, discussing how each phase of incident response would be handled.
  - **Live Simulations:**
    - Engage in live simulations where you respond to simulated incidents in real-time. These exercises provide hands-on experience in detecting, containing and resolving security incidents.
    - Example: Use a cyber range platform like **Immersive Labs** to practice responding to a simulated phishing attack that has led to a data breach.
- **Importance of Documentation:**
  - **Incident Reports:**
    - Learn how to document incidents thoroughly, including what was observed, actions taken and the outcome. Proper documentation is crucial for learning from incidents and for regulatory compliance.
    - Example: After containing and eradicating a malware infection, write a detailed report outlining the timeline of events, the steps taken and recommendations for future prevention.

    - **Post-Incident Reviews:**
        - Conduct post-incident reviews to analyse the effectiveness of the response and identify areas for improvement. These reviews are valuable for refining incident response processes.
        - Example: Hold a meeting after a security incident to review the response and discuss what changes could be made to improve future incident handling.

Practical Steps:

- **IR Labs:**
    - Engage in incident response labs and simulations available on platforms like TryHackMe or Hack The Box. These platforms often include scenarios that require you to go through all phases of incident response.
- **Documentation Practice:**
    - Practice writing incident reports and conducting post-incident reviews based on real or simulated incidents. Pay attention to detail, ensuring that your documentation is clear, concise and actionable.

IDS/IPS (Intrusion Detection and Prevention Systems)

Key Concepts to Learn:

- **How IDS/IPS Work:**
    - **Intrusion Detection Systems (IDS):**
        - IDS are passive systems that monitor network traffic for suspicious activity and generate alerts when potential threats are detected. They do not take direct action to block the threats but instead notify administrators or analysts.
        - Example: An IDS detects a pattern of behaviour that matches a known exploit and sends an alert to the SOC team for further investigation.
    - **Intrusion Prevention Systems (IPS):**
        - IPS are active systems that not only detect but also block or mitigate detected threats in real-time. IPS systems are often placed in line with network traffic, meaning they can directly influence the flow of traffic to prevent attacks.

        - Example: An IPS detects an attempted SQL injection attack and immediately blocks the malicious traffic before it reaches the web server.

- **Configuring and Tuning IDS/IPS Systems:**
    - **Rule Creation and Management:**
        - Learn how to create and manage detection rules for IDS and IPS systems. This involves writing rules that identify specific attack patterns or behaviours and ensuring they are up-to-date with the latest threat intelligence.
        - Example: Write a Snort rule that detects attempts to exploit a known vulnerability in a web application.
    - **Tuning for Accuracy:**
        - Tuning IDS/IPS systems is critical to reducing false positives (legitimate traffic incorrectly flagged as malicious) and false negatives (malicious traffic not detected). Learn how to adjust rules and thresholds to improve the accuracy of these systems.
        - Example: Adjust the sensitivity of an IDS rule that monitors login attempts to avoid triggering alerts on normal user activity, while still catching brute force attempts.
    - **Deployment Strategies:**
        - Understand different deployment strategies for IDS/IPS, such as network-based or host-based and their respective pros and cons. Learn how to strategically place these systems in the network to maximise coverage and effectiveness.
        - Example: Deploying a network-based IDS at the network perimeter to monitor all inbound and outbound traffic.

Practical Steps:

- **IDS/IPS Labs:**
    - Use platforms like Security Onion or Snort to set up your own IDS/IPS environment. Practice configuring rules, tuning the system and responding to alerts generated by real or simulated traffic.
- **Real-Time Monitoring:**

    - Implement IDS/IPS in a home lab or sandbox environment and monitor network traffic in real-time. Analyse alerts, adjust rules as needed and refine your skills in detecting and preventing intrusions.

4. Developing Analytical and Monitoring Skills

Alert Analysis

Key Concepts to Learn:

- **Alert Triage and Prioritisation:**
    - Understand how to categorise and rank alerts based on risk, severity and potential impact on the organisation.
    - Learn to identify critical alerts that need immediate attention versus lower-priority issues.
    - Use frameworks like the MITRE ATT&CK to classify alerts and link them to possible attacker behaviours.
    - Example: An alert indicating multiple failed login attempts may be prioritised over a less critical alert, like an unusual file download.
- **Handling False Positives:**
    - Learn to recognise patterns that indicate false positives and adjust alerting thresholds accordingly.
    - Understand that too many false positives can lead to alert fatigue, causing genuine threats to be missed.
    - Example: Regular network scanning by IT staff triggering alerts should be tuned out, as it’s a legitimate activity.

Practical Steps:

- **Alert Triage Practice:**
  Use SIEM tools (like Splunk, QRadar) to practice triaging different types of alerts in simulated environments. Set up scenarios where you need to prioritise actions based on real-world use cases.
- **False Positive Reduction:**
  Analyse past incidents of false positives and adjust alerting rules or thresholds. Practice tuning alerts to minimise noise and improve the signal-to-noise ratio.

Threat Intelligence

Key Concepts to Learn:

- **Sourcing Threat Intelligence:**

  - Learn where to find reputable sources of threat intelligence, such as open-source intelligence (OSINT) platforms, industry-specific sharing groups (ISACs) and commercial intelligence feeds.
  - Understand the types of threat intelligence: strategic, operational, tactical and technical.
  - Example: Leveraging feeds from sources like AlienVault OTX, Cisco Talos or government threat advisories.
- **Using Threat Intelligence in SOC Operations:**
  - Integrate threat intelligence into your SIEM or threat detection systems to automatically enrich alerts with additional context.
  - Use threat intelligence to hunt for indicators of compromise (IOCs) such as IP addresses, domain names and file hashes linked to known threats.
  - Understand how to track threat actor TTPs (Tactics, Techniques and Procedures) and use them to enhance your organisation's defences.
  - Example: Threat intelligence indicates that a known threat actor is targeting your sector, leading you to proactively search for their indicators of compromise in your network.

Practical Steps:

- **Threat Intelligence Exercises:**
  Use platforms like VirusTotal, Shodan or Maltego to search for threat indicators. Practice incorporating this data into your monitoring workflow.
- **Operational Use:**
  Simulate a scenario where an emerging threat is identified through intelligence feeds. Use the information to proactively adjust defences or launch threat hunts in your environment.

5. Hands-On Practice (Home Lab)

Set Up a Home Lab

Key Concepts to Learn:

- **Installing and Configuring Virtual Machines:**
  - Set up virtual machines (VMs) using tools like VirtualBox, VMware or Hyper-V.
  - Install different operating systems, including Linux (e.g., Ubuntu, Kali Linux) and Windows, to simulate diverse environments.

    - Example: Running multiple VMs allows you to simulate a small network with endpoints and servers for monitoring.

- **Setting Up Security Tools:**
    - **SIEM (Security Information and Event Management):**
      Install free versions of SIEM tools like Splunk, Elastic Stack or OSSIM to collect and analyse logs from your VMs.
    - Example: Using Splunk to collect and correlate logs from multiple machines to detect suspicious activities.
    - **IDS/IPS (Intrusion Detection/Prevention Systems):**
      Set up Snort, Suricata or Zeek to monitor network traffic for anomalies and malicious activity.
    - Example: Snort will alert you when it detects a suspicious network scan.
    - **Other Security Tools:**
      Install firewalls, antivirus software and endpoint detection and response (EDR) tools to simulate a complete security architecture.
    - Example: Using pfSense as a firewall to control and monitor network traffic between your VMs.

Practical Steps:

- **Lab Setup Guides:**
  Follow tutorials and guides to set up your home lab environment, ensuring that your VMs and tools are properly configured and communicating.
- **Configuring Alerts and Monitoring:**
  Set up alerting rules in your SIEM and IDS/IPS tools to detect specific events like unauthorised access attempts or malware execution.

Simulate Security Incidents

Key Concepts to Learn:

- **Detecting Attacks:**
    - Simulate attacks like phishing, malware infections, brute force attempts or lateral movement within your lab environment.
    - Monitor logs and alerts in your SIEM to detect these attacks in real-time.
    - Example: Launching a brute-force attack from one VM to another and detecting it with your IDS.
- **Responding to Attacks:**

    - Practice containment, eradication and recovery procedures. Learn how to isolate infected machines, clean up malware and restore systems from backups.
    - Example: Upon detecting malware in your lab, practice isolating the infected VM and removing the malicious software.

Practical Steps:

- **Attack Simulation Tools:**
  Use tools like Metasploit, Kali Linux or Cyber Kill Chain simulators to simulate attacks. Test your incident detection and response skills in a controlled environment.
- **Step-by-Step Exercises:**
  Create detailed attack scenarios, execute them and document each step—from detection to remediation.

Documentation and Reporting

Key Concepts to Learn:

- **Incident Reports:**
    - Learn how to write detailed incident reports that include the nature of the incident, timeline of events, the root cause and the remediation steps taken.
    - Example: An incident report detailing a simulated malware infection, how it was detected and the actions taken to resolve it.
- **Log Management:**
    - Understand how to maintain and analyse logs from your SIEM, network devices and endpoint security tools to support incident investigations and audits.
    - Example: Storing and reviewing logs from multiple VMs to identify anomalies during an attack simulation.

Practical Steps:

- **Practice Writing Reports:**
  After each simulated incident, write a full incident report. Include all relevant information, from initial detection to recovery and any recommendations for preventing future incidents.

- **Review and Analyse Logs:**
  Regularly review logs generated in your lab to practice identifying patterns, correlating events and spotting potential incidents.

6. **Continuous Learning**

Join Cybersecurity Communities

Key Concepts to Learn:

- **Participation in Forums and Meetups:**
  - Join online forums like Reddit's r/cybersecurity, Stack Overflow or Spiceworks to discuss topics with peers and experts.
  - Participate in local or virtual meetups through platforms like Meetup.com, where you can engage in discussions and learn from industry professionals.
  - Example: Participating in an online discussion about the latest vulnerabilities found in a popular software and sharing mitigation strategies.
- **Engaging in Online Communities:**
  - Join cybersecurity-specific communities such as Cybersecurity Professionals on LinkedIn, the OWASP community or Defcon groups. These communities often share useful resources, insights into ongoing threats and professional advice.
  - Example: A LinkedIn group that discusses daily cybersecurity news, tools and industry best practices.

Practical Steps:

- **Community Involvement:**
  Join at least two forums or online groups related to cybersecurity. Regularly participate in discussions, ask questions and contribute your knowledge to help others while expanding your network.
- **Attending Meetups:**
  Look for local or virtual cybersecurity meetups, CTF (Capture the Flag) events or webinars. Attend these to learn from industry experts and stay connected with the community.

Stay Updated on Cybersecurity Trends

Key Concepts to Learn:

- **Following Blogs and News Sites:**

    - Stay up-to-date by following reputable cybersecurity blogs and news sites like Krebs on Security, Dark Reading, Threatpost and the SANS Institute. These platforms provide insights into the latest vulnerabilities, incidents and best practices.
    - Example: Reading an article about a newly discovered zero-day vulnerability and understanding its impact on businesses.
- **Engaging with Forums and Discussions:**
    - Actively participate in forums like the ISC^2 Community, Black Hills Information Security or Malwarebytes Labs to engage in real-time discussions about cybersecurity news.
    - Example: Engaging in a forum discussion about the impact of the latest ransomware attack and how to defend against it.

Practical Steps:

- **Daily or Weekly Reading:**
  Dedicate time each day or week to read cybersecurity blogs or news updates. Subscribe to newsletters like the SANS NewsBites or CyberWire to receive the latest news directly to your inbox.
- **Trend Tracking:**
  Use tools like Feedly to aggregate articles from different cybersecurity blogs into one place, so you can easily track trends, new threats and developments.

Engage in Continuous Learning

Key Concepts to Learn:

- **Taking Online Courses:**
    - Platforms like Coursera, Cybrary, Udemy and edX offer a wide range of courses on specific cybersecurity topics. Explore these to deepen your knowledge in areas like threat hunting, incident response or network security.
    - Example: Enrolling in a course on malware analysis to learn advanced techniques for detecting and mitigating malware.
- **Attending Webinars and Conferences:**
    - Attend webinars, workshops and conferences hosted by industry organisations such as ISACA, (ISC)^2 or SANS. These events provide opportunities to learn from experts and stay informed about cutting-edge research and innovations.

    - Example: Attending a SANS webinar on advanced SOC operations to learn new techniques for optimising detection and response processes.

- **Using LinkedIn Learning:**
    - Leverage LinkedIn Learning for structured courses that cover topics such as cloud security, penetration testing and secure coding practices.
    - Example: Completing a course on cloud security fundamentals to understand the unique challenges and strategies for securing cloud environments.

Practical Steps:

- **Course Enrolment:**
  Set a goal to complete at least one online course per quarter. Choose courses that align with your current role or areas you want to specialise in.
- **Webinar Participation:**
  Register for at least one webinar or online conference each month. Focus on topics that are relevant to your work or personal development goals.
- **LinkedIn Learning Utilisation:**
  Explore the vast library of LinkedIn Learning courses and select those that fit your career objectives. Make a habit of completing courses regularly to stay updated on the latest cybersecurity knowledge.

PATH 2: FOR INDIVIDUALS WITHOUT IT EXPERIENCE

1. Advanced IT Knowledge

Operating Systems

Key Concepts to Learn:

- **Windows System Administration:**
  - Deepen your knowledge of the Windows operating system, including system architecture, file systems and security configurations. Learn how to manage users, control access to resources, configure firewalls and monitor event logs.
  - Example: Configuring Group Policies to enforce security standards across a network of Windows systems.
- **Linux System Administration:**
  - Develop advanced skills in Linux, focusing on shell scripting, package management, file permissions and system security. Linux is widely used in servers and many security tools, making it crucial for your role.
  - Example: Writing a shell script to automate system updates and security patches on Linux servers.
- **Security Settings and Hardening:**
  - Learn how to secure both Windows and Linux systems by disabling unnecessary services, applying security patches and configuring firewalls, SELinux (Linux) or AppLocker (Windows).
  - Example: Implementing firewall rules on a Linux system using iptables or UFW to block unauthorised traffic.

Practical Steps:

- **System Administration Tasks:**
  Set up a home lab with both Windows and Linux virtual machines. Practice managing user accounts, setting permissions and applying security measures.
- **Hardening Exercises:**
  Use security benchmarks from organisations like CIS (Centre for Internet Security) to guide the hardening of both Windows and Linux systems.

Advanced Networking

Key Concepts to Learn:

- **Networking Protocols and Technologies:**

- Gain a deep understanding of key networking protocols, including TCP/IP, DNS, HTTP/HTTPS, VPNs and VLANs. Learn how IPv6 differs from IPv4 and the implications for network security.
- Example: Setting up a VPN to securely connect remote users to a corporate network.

- **Network Security Measures:**
    - Explore security protocols like SSL/TLS for encrypting traffic and learn how IDS/IPS systems detect and prevent network intrusions. Understand the use of firewalls, segmentation and encryption in protecting networks.
    - Example: Configuring an SSL/TLS certificate on a web server to secure communications.
- **Advanced Network Configurations:**
    - Learn how to set up and manage secure network architectures, including DMZs (Demilitarised Zones), VPN configurations and the implementation of VLANs to segment network traffic.
    - Example: Configuring VLANs to separate sensitive traffic (e.g., HR or finance) from general office traffic on the network.

Practical Steps:

- **Networking Labs:**
  Use tools like Cisco Packet Tracer or GNS3 to simulate network environments. Practice configuring switches, routers, firewalls and VPNs to enhance your understanding of networking.
- **Network Security Simulation:**
  Simulate network attacks in your lab, such as a Man-in-the-Middle (MitM) attack and practice configuring network devices to defend against them.

Virtualisation and Cloud Computing

Key Concepts to Learn:

- **Virtual Environments (VMware, Hyper-V):**
    - Learn the basics of virtualisation, including the creation and management of virtual machines (VMs). Understand how to allocate resources, configure networking for VMs and secure virtual environments.
    - Example: Using VMware or Hyper-V to set up a lab environment with multiple virtual machines for testing security tools.

- **Cloud Security Fundamentals (AWS, Azure):**
    - Familiarise yourself with the fundamentals of cloud computing and the shared responsibility model. Understand how to configure and secure cloud services, including identity and access management (IAM), encryption and security monitoring.
    - Example: Setting up an IAM policy in AWS to ensure that only authorised users have access to critical cloud resources.
- **Security Best Practices for Cloud Environments:**
    - Learn about cloud-specific security challenges, such as securing cloud storage, managing cloud-based workloads and applying security controls for data in transit and at rest.
    - Example: Implementing encryption for data at rest in an Amazon S3 bucket and setting up logging and monitoring for cloud resources.

Practical Steps:

- **Virtual Machine Practice:**
  Install virtualisation software like VMware Workstation, VirtualBox or Hyper-V. Practice creating and managing virtual machines, configuring networks and applying security measures within the virtual environment.
- **Cloud Environment Setup:**
  Use free trials or the free tier in cloud services like AWS or Azure to set up basic cloud environments. Practice securing your instances, setting up monitoring and exploring cloud security tools.

2. Advanced Cybersecurity Knowledge

Advanced Security Concepts

Key Concepts to Learn:

- **Encryption and Secure Communications:**
    - Dive deeper into encryption algorithms (e.g., AES, RSA) and understand their uses in securing data both at rest and in transit. Learn how public key infrastructure (PKI) enables secure communication between parties and protects against interception.
    - Example: Implementing TLS/SSL encryption for a secure web application and using asymmetric encryption (RSA) for secure key exchange.
- **Hashing and Data Integrity:**

  - Understand how hashing algorithms (e.g., SHA-256, MD5) are used to ensure data integrity and authenticate messages. Learn about the importance of avoiding weak hashing algorithms in favour of more secure ones.
  - Example: Using SHA-256 to generate a hash for verifying the integrity of files transmitted across the network.
- **Advanced Threat Types:**
  - **Advanced Persistent Threats (APTs):**
    Learn how APTs are prolonged, targeted attacks carried out by well-funded attackers (often nation-states) to infiltrate networks and maintain a presence. Study the techniques used by APTs, such as social engineering, zero-day exploits and lateral movement within a network.
  - Example: Analysing the tactics of the APT29 (Cozy Bear) group, which was linked to espionage activities targeting governments and industries.
  - **Zero-Day Exploits:**
    Understand what zero-day vulnerabilities are—flaws in software that are unknown to the vendor and have no patch available. Learn how attackers exploit these vulnerabilities and what measures can be taken to mitigate their impact (e.g., patch management, vulnerability scanning).
  - Example: Reviewing a recent zero-day exploit in a popular software and exploring how attackers leveraged it before a patch was released.

Practical Steps:

- **Encryption Labs:**
  Set up a test environment where you can experiment with encryption protocols. Practice configuring encrypted communication channels using TLS/SSL certificates on web servers.
- **Threat Analysis:**
  Use threat intelligence platforms like VirusTotal or OpenCTI to study APT campaigns and analyse how these threats evolve over time. Simulate potential zero-day attack scenarios in your lab and practice detecting indicators of compromise.

Security Policies and Compliance

Key Concepts to Learn:

- **Security Policies and Frameworks:**

  - Expand your knowledge of security policies and how they dictate the behaviour and responsibilities of employees in an organisation. Learn about creating policies for data protection, incident response and access control.
  - Example: Drafting a data classification policy that outlines how sensitive information should be handled and protected across different departments.

- **Compliance Frameworks Relevant to SOC Operations:**
  - **PCI-DSS (Payment Card Industry Data Security Standard):**
    Learn about the PCI-DSS framework, which is designed to protect cardholder data and ensure secure handling of credit card transactions. Understand the 12 core requirements, such as encrypting transmission of cardholder data across open, public networks and regularly testing security systems and processes.
  - Example: Ensuring that a company's SIEM logs all access to cardholder data and triggers alerts for unauthorised access attempts.
  - **HIPAA (Health Insurance Portability and Accountability Act):**
    Study the security and privacy rules of HIPAA, which apply to the protection of health information. Understand the technical safeguards required, including access control, audit controls, integrity and transmission security.
  - Example: Implementing role-based access controls (RBAC) to ensure that only authorised personnel can access electronic protected health information (ePHI).

Practical Steps:

- **Compliance Simulation:**
  In your lab, simulate an organisation preparing for a PCI-DSS audit. Implement the necessary security controls and create detailed audit logs that meet the standard’s requirements.
- **Policy Creation Exercise:**
  Draft a security policy for a hypothetical organisation that includes guidelines for incident handling, data protection and compliance with frameworks such as HIPAA or PCI-DSS. Practice writing this policy with the goal of implementing it in a real-world SOC.

3. SOC-Specific Knowledge (Deeper Focus)

SIEM Mastery

Key Concepts to Learn:

- **Advanced SIEM Features:**
    - **Correlation Searches:** Learn how to build and customise correlation searches to identify specific patterns of malicious behaviour across multiple data sources. Practice creating complex queries that detect unusual activity, such as insider threats or multi-stage attacks.
    - Example: Creating a correlation search that detects lateral movement across the network by correlating login events, file access logs and unusual outbound traffic.
    - **Dashboards and Visualisation:** Become proficient in designing and using SIEM dashboards for real-time monitoring. Learn how to present data in a way that highlights key security metrics, incident trends and potential vulnerabilities.
    - Example: Building a dashboard that tracks the number of failed login attempts across different departments and visualises which endpoints are most at risk.
- **SIEM Integration:**
  Learn how to integrate SIEM with other security tools such as firewalls, IDS/IPS, antivirus and threat intelligence platforms. This enhances the SIEM's ability to collect comprehensive data and generate more accurate alerts.
- Example: Integrating your SIEM with an IDS to automatically trigger alerts when suspicious activity is detected on the network.

Practical Steps:

- **SIEM Labs:**
  In your lab, practice configuring correlation rules, dashboards and custom alerts. Experiment with integrating external tools (e.g., firewalls, threat intelligence feeds) into your SIEM environment.
- **Scenario-Based Drills:**
  Simulate advanced attack scenarios like data exfiltration or insider threats and practice using SIEM to detect and respond to these incidents.

Advanced Incident Response

Key Concepts to Learn:

- **Advanced Incident Response Scenarios:**
  Practice responding to advanced threat scenarios, such as targeted attacks, data breaches and ransomware outbreaks. Learn to follow a structured approach—detection, containment, eradication, recovery and lessons learned.
- Example: Responding to a spear-phishing attack that led to a compromised endpoint, isolating the affected system and eradicating malware from the network.
- **Forensic Analysis Basics:**
  Understand the basics of forensic analysis, including disk and memory forensics, to investigate the root cause of incidents. Learn about tools like Autopsy, Volatility and FTK Imager for collecting and analysing digital evidence.
- Example: Analysing memory dumps to identify the presence of malware or investigating deleted files during an incident response.

Practical Steps:

- **Incident Response Playbooks:**
  Develop detailed playbooks for various incident types (e.g., malware infection, insider threat) and practice using them in simulated environments.
- **Forensics Practice:**
  Set up a test environment where you can practice capturing and analysing forensic data, such as retrieving logs, recovering deleted files and analysing network traffic.

Advanced IDS/IPS Management

Key Concepts to Learn:

- **Tuning IDS/IPS:**
  Learn how to fine-tune IDS/IPS configurations to minimise false positives while maintaining high detection accuracy. This involves tailoring rules to your specific network environment and adjusting thresholds based on normal traffic patterns.
- Example: Adjusting IPS rules to better distinguish between legitimate high-traffic events (e.g., backups) and potential DDoS attacks.
- **Integration with SIEM and Other Tools:**
  Understand how to integrate IDS/IPS with your SIEM to automate the detection and response process. Learn how to feed IDS/IPS alerts into your SIEM and set up rules that trigger actions based on the severity of the threat.
- Example: Configuring your SIEM to automatically block an IP address after a certain number of failed IDS alerts, indicating a brute-force attack.

Practical Steps:

- **IDS/IPS Labs:**
  In your home lab, set up IDS/IPS solutions (e.g., Snort, Suricata) and practice fine-tuning rules and alerts. Simulate different types of attacks to test the effectiveness of your configurations.
- **SIEM Integration Practice:**
  Work on integrating IDS/IPS with your SIEM and other security tools. Practice creating workflows where your SIEM automatically responds to alerts generated by IDS/IPS systems.

4. Developing Advanced Analytical and Monitoring Skills

Advanced Alert Analysis

Key Concepts to Learn:

- **Pattern and Behaviour Recognition:**
  Learn how to identify recurring patterns in alerts, such as those indicating stealthy attacks like lateral movement or data exfiltration. Study common techniques used by attackers, such as persistence mechanisms and privilege escalation and how they manifest in network logs and alerts.
- Example: Recognising a series of low-severity alerts that, when analysed together, indicate a slow-moving APT (Advanced Persistent Threat) attempting to establish persistence within the network.
- **Threat Hunting Techniques:**
  Develop proactive threat-hunting skills by leveraging both internal data (e.g., logs, network traffic) and external intelligence (e.g., threat feeds) to identify indicators of compromise (IOCs) that may not have triggered traditional alerts. Threat hunting involves actively searching for hidden threats using a hypothesis-driven approach.
- Example: Hunting for traces of known malware variants in network traffic that bypassed the detection system but exhibited unusual behaviour patterns.

Practical Steps:

- **Advanced Labs:**
  Set up scenarios in your lab where you must analyse multiple, seemingly unrelated alerts to uncover the root cause of an attack. Use real-world case studies of advanced threats as a reference to recreate similar environments for hands-on practice.

- **Threat Hunting Exercises:**
  Engage in threat hunting by using tools like ELK stack, Splunk or QRadar to search for IOCs. Create hypotheses based on recent threat trends and use network data, logs and endpoint activity to confirm or refute your hypotheses.

Threat Intelligence Application

Key Concepts to Learn:

- **Deep Understanding of Threat Intelligence Platforms:**
  Explore the workings of threat intelligence platforms (TIPs) such as ThreatConnect, Anomaly or MISP (Malware Information Sharing Platform). Learn how these platforms aggregate, curate and distribute threat intelligence and how to leverage them to improve situational awareness in your SOC.
- Example: Using a TIP to automatically enrich alerts with contextual information about an IOC, such as associated malware families, known threat actors or targeted industries.
- **Improving SOC Detection Capabilities:**
  Practice incorporating threat intelligence into your SOC's detection mechanisms. This includes integrating external intelligence feeds into your SIEM and configuring your tools to trigger alerts when IOCs from these feeds are detected in your network traffic or logs.
- Example: Setting up automatic correlation rules that trigger high-priority alerts when network traffic involves IPs or domains associated with known malicious actors.

Practical Steps:

- **Threat Intelligence Integration:**
  In your lab, integrate a threat intelligence feed with your SIEM and practice configuring your SIEM to use this information to generate actionable alerts. Experiment with different TIPs and understand how to fine-tune their integration for optimal detection.
- **Threat Intelligence Exercises:**
  Create scenarios where you simulate the use of threat intelligence to detect and mitigate emerging threats. Practice identifying how threat actors operate and use this knowledge to predict their next move, allowing for a more proactive defence.

5. **Advanced Hands-On Practice**

Advanced Home Lab Setup

Key Concepts to Learn:

- **Complex Lab Environments:**
  Build a lab environment that includes multiple network segments, servers, firewalls and other security devices. This setup should mimic a small-to-medium-sized enterprise network, allowing for advanced simulation of lateral movement, data exfiltration and attack vectors across different parts of the network.
- Example: Create isolated VLANs for different departments, each with its own servers and workstations. Implement firewalls between VLANs to simulate a segmented network with different security rules.
- **Real-World Incident Response:**
  Practice responding to incidents by introducing advanced attacks into your lab environment, such as APTs or multi-vector attacks. Document each step of your response, from detection to containment and remediation.
- Example: Simulate a spear-phishing attack that leads to an APT establishing persistence on your network, then practice incident response procedures to detect and remove the threat.

Practical Steps:

- **Lab Expansion:**
  Add layers to your existing lab by incorporating more complex network topologies, integrating SIEM, IDS/IPS and setting up multiple firewalls. Use virtualisation software (e.g., VMware or VirtualBox) to host your machines and networks.
- **Realistic Scenarios:**
  Use attack simulation tools (e.g., Caldera or Atomic Red Team) to recreate real-world attack scenarios. Test your incident response playbooks and use your SIEM to monitor for and respond to these threats.

Documentation and Reporting

Key Concepts to Learn:

- **Detailed Incident Analysis:**
  Learn how to perform deep-dive analyses of incidents, focusing on the attack vector, techniques used and their impact on the network. Your analysis should identify how the attacker moved within the network and what vulnerabilities were exploited.
- Example: A report that explains how an attacker used lateral movement to spread malware from one compromised machine to others, along with detailed logs and evidence of the activities.

- **Actionable Remediation Steps:**
  Practice developing remediation steps that not only fix the immediate issue but also strengthen the overall security posture of the network. This could include recommendations for patching, user training or changes in security architecture.
- Example: Recommending specific firewall rule changes and endpoint security updates to prevent a similar attack from happening again.

Practical Steps:

- **Write Advanced Reports:**
  After each incident response exercise, write a comprehensive report that includes a timeline of events, technical analysis and remediation recommendations. Share these reports with peers for feedback or use them as part of a portfolio.

6. Continuous Learning

Engage in Advanced Learning

Key Concepts to Learn:

- **Capture the Flag (CTF) Competitions:**
  Participate in CTFs that focus on advanced topics like reverse engineering, cryptography, network security and web application security. These competitions test both your offensive and defensive skills, providing a well-rounded challenge.
- Example: Competing in DEF CON CTF to solve complex challenges related to vulnerability exploitation and incident response.

Practical Steps:

- **Join CTF Competitions:**
  Regularly participate in online CTF competitions or in-person cybersecurity contests. Platforms like Hack The Box, TryHackMe or OverTheWire offer both beginner and advanced challenges that keep your skills sharp.
- **Expand Skill Set:**
  Focus on improving your skills in areas where you're less experienced, such as cryptography or malware analysis, by seeking out specialised CTFs or training sessions in those areas.