Zero to Hero DCO-IDM Guide (v1.1)

Matthew Iverson

1. Introduction

A Security Operations Center (SOC) Analyst is responsible for monitoring, detecting, analyzing, and responding to security incidents and must build both technical expertise and soft skills. This document outlines the critical areas of focus—including gear configurations, troubleshooting, threat intelligence, threat hunting, tool mastery (with Splunk and Security Onion), presentation skills, documentation practices, and the ability to teach others—to transform a novice into a seasoned professional over a three-year period.

Throughout this guide, you will learn to configure and optimize your tools, troubleshoot complex issues, and harness threat intelligence to drive proactive security measures, while mastering industry-leading tools to analyze and correlate vast amounts of data. By following the guidelines and best practices presented here, you will build a robust technical foundation and develop a strategic mindset essential for thriving in today's dynamic security landscape.

Over the next three years, this journey will empower you to become a well-rounded SOC Analyst capable of detecting, mitigating, and leading initiatives to continuously improve your organization's security posture. Embrace this blueprint to transform your skills from zero to hero and become one of the best analysts in the field.

2. Technical Fundamentals

2.1. Configurations of Our Gear

Hardware and Software Setup

Network Devices and Firewalls

- **Cisco Switches**
    - **Basic commands**
    - **VLAN Configuration:**
    - **Static Routes:**
    - **Enable ssh**
- **Palo Alto Firewalls**
    - **NAT Rules:**
        - Configure NAT (Network Address Translation) rules to translate between internal and external IP addresses.
    - **Security Policies:**
        - Create and fine-tune security policies, including application-level controls, URL filtering, and threat prevention.
    - **Monitoring and Logging:**
        - Use built-in logging and reporting tools to monitor traffic and analyze potential security incidents.

Server and Domain Infrastructure

- **Windows Domain Controller (DC)**
    - **Domain Joining:**
        - Ensure that devices are properly joined to the domain, facilitating centralized management and authentication.
    - **Shares and Group Policy Objects (GPO):**
        - Configure file and folder shares with proper permissions. Develop and manage GPOs to enforce security settings and operational policies across the network.
    - **Active Directory Management:**
        - Implement user and computer account management, and understand the role of domain controllers in the security ecosystem.

Virtualization and Hypervisor Management

- **ESXi and vSphere**

- **Hypervisor Configuration:**
  - Deploy and manage ESXi hosts. Use tools like GParted for partitioning and managing disk space on the hypervisor.
- **vSphere Cluster Management:**
  - Configure clusters to combine multiple ESXi hosts for high availability and load balancing.
- **Datastore Management:**
  - Set up and maintain datastore clusters, ensuring proper storage allocation and redundancy.
- **Virtual Machine Management:**
  - Understand best practices for creating, cloning, and managing virtual machines within a clustered environment.

SIEM Solutions and Log Management

Splunk

- **Overview:** Splunk is a widely adopted SIEM solution that collects, indexes, and analyzes machine data from diverse sources.

Infrastructure Components:

- **Search Head:**
  Provides a centralized interface for querying, visualizing, and analyzing data using SPL (Search Processing Language).
- **Indexer:**
  Parses and indexes incoming data with horizontal scalability, supporting high-volume ingestion.
- **Deployer & Manager:**
  - **Deployer:** Manages and distributes configuration files, apps, and dashboards across distributed search heads.
  - **Manager:** Oversees user access, configurations, and overall system health.
- **Forwarders:**
  - **Heavy Forwarder:** For complex data parsing and routing before forwarding data.
  - **Universal Forwarder:** A lightweight agent for efficient log forwarding.
- **Deployment Server:**
  Centralizes the management of forwarder configurations and app deployments across distributed environments.

- **Monitoring Console:**
  Provides system health monitoring, performance metrics, and capacity planning for the Splunk environment.
- **Enterprise Apps:**
  - **Splunk Enterprise Security (ES):** Enhances Splunk with advanced security analytics, threat detection, and incident response capabilities.
  - **Splunk IT Service Intelligence (ITSI):** Offers real-time monitoring, analytics, and service-level management for IT operations.
- **Data Handling:**
  - **Searching:** Utilizes SPL for efficient and flexible querying of indexed data.
  - **Data Models and Indexes:**
    Customizes design and management of data models, indexes, and sourcetypes to optimize performance and accuracy.
  - **Search Time vs. Index Time:**
    Balances parsing during indexing for speed versus at search time for flexibility based on organizational needs.

Security Onion

- **Overview:** Security Onion is an open-source SIEM platform that integrates multiple tools to provide comprehensive intrusion detection, network monitoring, and log management.
- **Components and Tools:**
  - **Logstash:** Sets up pipelines to collect and process diverse log data.
  - **Strelka:** Performs file analysis and threat detection.
  - **Kibana:** Provides data visualization and dashboarding to analyze log data.
  - **Stenographer:** Captures high-speed network traffic metadata to reveal hidden or obfuscated data.
  - **Suricata & Zeek:**
    - **Suricata:** Offers high-performance network IDS/IPS capabilities, including signature-based detection and protocol analysis.
    - **Zeek (formerly Bro):** Analyzes network traffic for anomalies and generates detailed logs for security monitoring.
- **Deployment Modes:**

- **Distributed:** Offers scalability and centralized management for larger environments with multiple sensors.
- **Standalone:** Simplifies management for smaller setups while still providing key intrusion detection capabilities.

2.2. Troubleshooting

1. **Layer 1 / Physical Connection:** Confirm the device is properly connected and powered on.
2. **Logs:** Review logs for errors or unusual activity related to the issue.
3. **Permissions:** Ensure file or resource ownership is correct using commands like **`chown` or `chmod`.**
4. **Firewall:** Check if the firewall is blocking the connection or necessary ports.
5. **Password:** Verify credentials are correct and have not expired or been mistyped.
6. **IP/Domain Configuration:** Check if the device has the correct IP configuration and is joined to the appropriate domain. know the OSI model.
7. **NAT Issue:** Investigate if network address translation is causing connectivity problems.
8. **DNS Resolution:** Ensure the domain name resolves correctly to the intended IP address.
9. **Service Status:** Verify the required services or processes are running.
10. **Updates:** Confirm the system, software, or firmware is updated to the latest version.

2.3. Baselining

- **Definition and Importance:**
  - Understand the concept of baselining: establishing normal activity patterns for systems, networks, and applications.
- **Establishing Baselines:**
  - Learn how to collect and analyze baseline data using SIEM tools.
  - Monitor deviations from the baseline to identify anomalies.

3. Threat Intelligence & Threat Hunting

3.1. Threat Intelligence (Threat Intel)

- **Understanding Threat Intel:**
    - Familiarize yourself with different types of threat intelligence (strategic, tactical, operational, and technical).
    - Learn about threat feeds, open-source intelligence (OSINT), and commercial threat intel services.
- **Analyzing Threat Data:**
    - Understand the process of correlating threat intel with internal logs and alerts.
    - Use threat intel platforms to monitor emerging threats and vulnerabilities.
- Know where to look
    - Commafeed
        - Cisco talos
        - Cyber security news
        - Bleeping computer
        - Cisa blog
        - Black hills information security
        - The hacker news

3.2. Threat Hunting

- **Threat Hunting Methodologies:**
    - Learn proactive threat hunting techniques to identify and mitigate threats before they escalate.
    - Understand the use of hypotheses based on known attack vectors and adversary behaviors.
- **Tools and Techniques:**
    - Use SIEM (Splunk, Security Onion) for hunting anomalies and correlating events.
    - Develop skills in using scripting and automation to assist in threat hunting.

---

4. Mastering SOC Tools

4.1. Splunk

- **Splunk Fundamentals:**
    - Understand Splunk architecture, data ingestion, and indexing.
    - Learn to create and manage dashboards, alerts, and reports.
- **Query Building:**
    - Develop proficiency in SPL (Search Processing Language) for effective log analysis.
    - Practice writing and refining queries to search through vast amounts of data.
- **Advanced Features:**
    - Learn about Splunk Enterprise Security for threat detection and incident response.
    - Explore integrations and custom app development within Splunk.

4.2. Security Onion

- **Introduction to Security Onion:**
    - Understand the components of Security Onion, including its integrated tools for intrusion detection and log analysis.
- **Using Queries and Dashboards:**
    - Learn to navigate the Security Onion interface (Kibana, Squert, etc.).
    - Practice building queries to analyze network traffic and detect suspicious activities.
- **Log Management:**
    - Understand the process of log collection, storage, and analysis within Security Onion.
    - Develop skills in correlating logs with other sources of data for incident response.

5. Soft Skills & Documentation

5.1. Presentation Ability

- **Effective Communication:**
    - Develop clear and concise communication skills for presenting technical information.
    - Practice creating and delivering presentations to both technical and non-technical audiences.
- **Visualization Tools:**
    - Learn to use visualization tools (e.g., PowerPoint, Tableau) to illustrate findings and trends.
    - Develop skills in creating compelling data visualizations.

5.2. Documentation and Lessons Learned

- **Incident Documentation:**
    - Create comprehensive incident reports detailing what happened, how it was handled, and the steps for remediation.
    - Develop templates and checklists for consistent documentation practices.
- **Post-Incident Analysis:**
    - Learn to conduct post-incident reviews and document lessons learned.
    - Ensure that documentation leads to actionable improvements in processes and configurations.

5.3. Teaching and Mentoring Others

- **Knowledge Sharing:**
    - Develop the ability to explain complex technical concepts in an accessible manner.
    - Practice mentoring junior analysts and conducting training sessions.
- **Creating Training Materials:**
    - Document standard operating procedures (SOPs), best practices, and case studies.
    - Contribute to a knowledge base that can be used by the entire SOC team.

---

6. Training Plan & Resources

6.1. Structured Learning

- **Certifications:**
    - Consider certifications such as CompTIA Security+, CEH (Certified Ethical Hacker), GIAC, or Splunk Certified User/Power User.
    - Explore vendor-specific certifications related to Security Onion and other security tools.
- **Online Courses & Workshops:**
    - Enroll in online courses (e.g., Coursera, Udemy, Cybrary) focusing on SIEM tools, threat hunting, and incident response.
    - Attend workshops and webinars that focus on the latest threat intelligence trends and SOC operations.

6.2. Hands-On Labs & Simulations

- **Lab Environments:**
    - Set up lab environments using virtual machines to practice gear configurations, Splunk queries, and Security Onion deployments.
    - Participate in capture-the-flag (CTF) challenges and simulated attack scenarios.

6.3. Continuous Improvement

- **Community Engagement:**
    - Join professional communities and forums (e.g., Reddit r/cybersecurity, ISACA, local security groups) to stay updated with industry trends.
- **Mentorship and Peer Reviews:**
    - Engage with peers for regular knowledge sharing
    - Schedule periodic training sessions and reviews to assess skill development.

---

7. Properly Leading your team

- **Setting up proper training**
    - Once a week defensive ctfs to hunt threats
    - Once a week setting up your infrastructure and tearing it down
    - Have individuals give one tip or trick about their tool they specialize in
    - Review latest trends going on
    -

8. Conclusion

Becoming an effective SOC Analyst involves mastering both technical tools and soft skills. By following this guide, you will develop a comprehensive understanding of gear configuration, troubleshooting, threat intelligence, and threat hunting. Additionally, honing your skills in Splunk and Security Onion, along with strong documentation and presentation abilities, will empower you to contribute effectively to your SOC team and help mentor others.
Use this guide as a roadmap for your learning journey and continuously update your knowledge to keep pace with evolving cyber threats and technological advancements.
This document is a living resource and should be reviewed and updated regularly to incorporate new tools, techniques, and industry best practices.