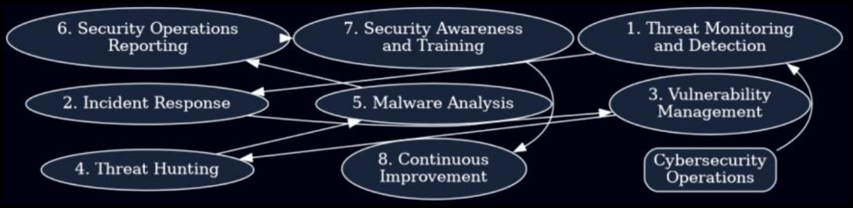
SecOps 101 Cheat sheet

SecOps Vertical


6. Security Operations Reporting
7. Security Awareness and Training
1. Threat Monitoring and Detection
2. Incident Response
5. Malware Analysis
3. Vulnerability Management
4. Threat Hunting
8. Continuous Improvement
Cybersecurity Operations

Major Roles

1 Security Consultant

1. Assess and evaluate the security posture of organizations.
2. Conduct security audits and risk assessments.
3. Develop security strategies and roadmaps.
4. Provide guidance and recommendations for security improvements.
5. Deliver security awareness training and workshops.

2 Security Engineer

1. Design, implement, and maintain security systems and controls.
2. Configure and manage firewalls, intrusion detection/prevention systems, and other security infrastructure.
3. Conduct risk assessments and develop mitigation strategies.
4. Collaborate with cross functional teams to ensure security best practices are followed.
5. Provide technical guidance and support for security related projects.

3 Security Architect

1. Design and plan the overall security architecture of an organization.
2. Develop security frameworks, standards, and guidelines.
3. Evaluate and recommend security technologies and solutions.
4. Conduct security assessments and audits.
5. Collaborate with stakeholders to align security requirements with business goals.

4 Incident Responder

1. Respond to and investigate security incidents, breaches, and threats.
2. Perform analysis of malware, compromised systems, and network traffic.
3. Develop incident response plans and playbooks.
4. Coordinate with internal teams and external stakeholders during incident response.
5. Conduct post incident analysis and implement preventive measures.

5 Threat Intel Analyst

1. Collect and analyze threat intelligence from various sources.
2. Identify emerging threats, vulnerabilities, and attack techniques.
3. Develop and maintain threat profiles and indicators of compromise.
4. Collaborate with other security teams to enhance threat detection and response capabilities.
5. Provide actionable intelligence to support decision making and incident response.

6 Security Analyst

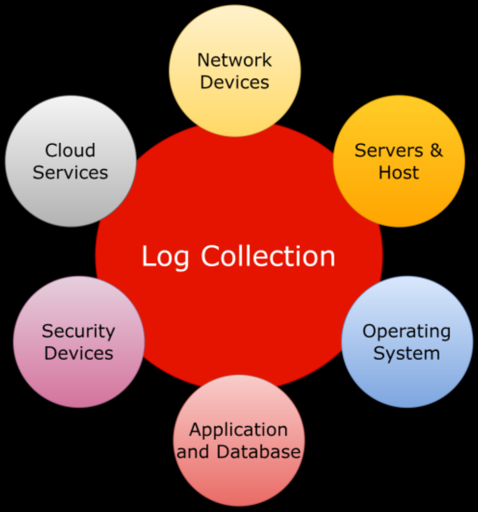
1. Monitor and analyze security events and incidents.
2. Conduct vulnerability assessments and penetration testing.
3. Develop and implement security policies and procedures.
4. Respond to and investigate security breaches or incidents.
5. Stay updated with emerging threats and security trends.

7 Cryptographer

1. Design and develop cryptographic algorithms and protocols.
2. Assess the security of cryptographic systems.
3. Conduct research on encryption, key management, and data protection.
4. Provide cryptographic solutions for secure communication and data storage.
5. Stay updated with advancements in cryptography and cryptographic standards.

8 Security Manager

1. Oversee and manage the overall security program of an organization.
2. Develop and implement security policies, procedures, and guidelines.
3. Ensure compliance


Log Collection

Network Devices

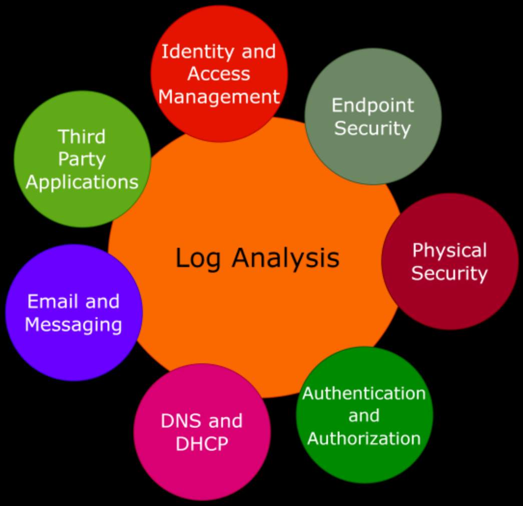
Servers & Host

Operating System

Application and Database

Security Devices

Cloud Services


Log Analysis

Identity and Access Management

Endpoint Security

Physical Security

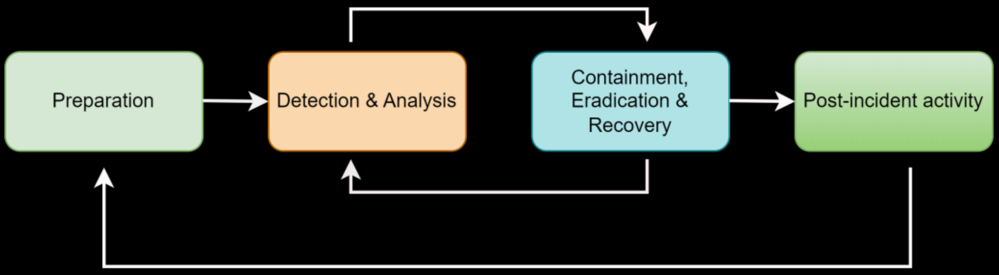
Authentication and Authorization

DNS and DHCP

Email and Messaging

Third Party Applications

Incident Response Life Cycle


Preparation

Detection & Analysis

Containment, Eradication & Recovery

Post-incident activity

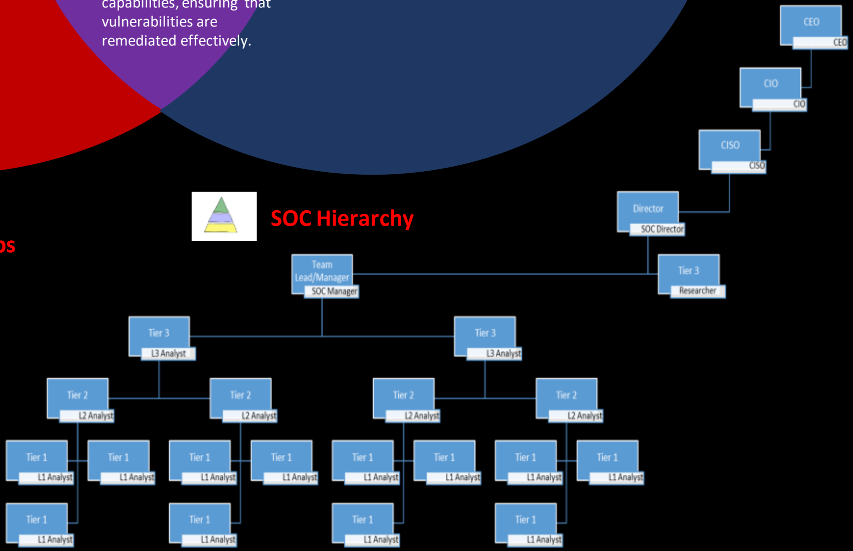
Red VS Purple VS Blue Teams

- Simulate real world attacks
- Perform PT operation on applications, and assets
- Identify Vulnerabilities and provide measures
- Establish processes and programs which investigate cyber security efforts of an organization and apply technical expertise in executing covert system operations.
- All offensive efforts, such as measuring performance quality, establishing goals, and planning resources fall under the Red Team Operations Lead.
- Identify bypass mechanism to help to create defensive strategy

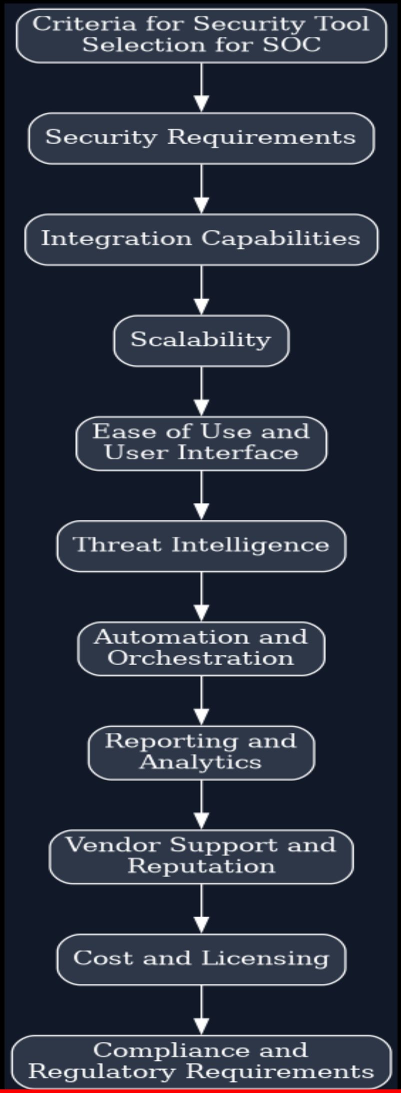
- Collaborative engagement to improve security posture
- It's not a separate entity or Team as such, but people from both team create a program to work on a same goal.
- Red Team conducts simulated attacks and shares their techniques and findings with the Blue Team
- The Blue Team, in turn, utilizes this information to enhance their defensive capabilities, ensuring that vulnerabilities are remediated effectively.

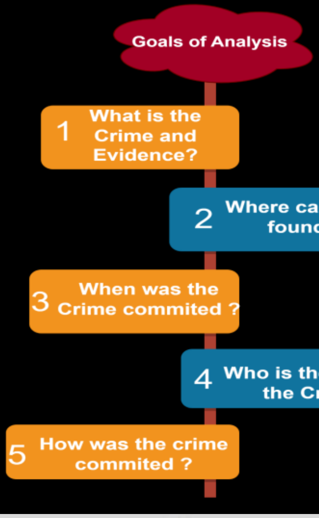
- Defender Team
- Incident Response, Detection & Monitoring, Analyze logs, Monitor network traffic, Implement security controls, and conduct regular security assessments.
- Perform Forensics Investigation
- Engage with Red Team to remediate the gaps identified by Red Team operations

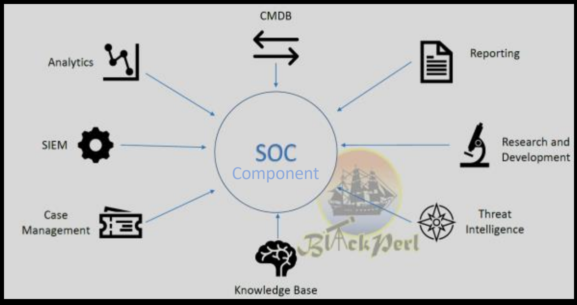
SOC Hierarchy



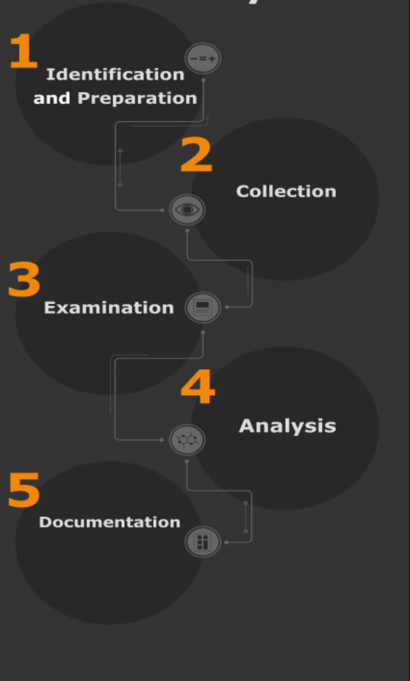
Criteria to Choose Tools for SecOps


Criteria for Security Tool Selection for SOC
Security Requirements
Integration Capabilities
Scalability
Ease of Use and User Interface
Threat Intelligence
Automation and Orchestration
Reporting and Analytics
Vendor Support and Reputation
Cost and Licensing
Compliance and Regulatory Requirements


Goals of Analysis
1 What is the Crime and Evidence?
2 Where can it be found?
3 When was the Crime commited ?
4 Who is the culpit of the Crime ?
5 How was the crime commited ?



Forensics Investigation Lifecycle


1 Identification and Preparation
2 Collection
3 Examination
4 Analysis
5 Documentation