5-STEP CHECKLIST FOR SOC ANALYSTS

BLUE TEAM RESOURCES

BLUE TEAM RESOURCES

01 Beginning of Shift

- Check-In
- Shift Handover
- Review Logs
- Update on Threat Landscape

02 Triaging Alerts

- Prioritize Alerts
- Validate Alerts
- Document Alerts

03 Analyzing Alerts

- Investigate Alerts
- Correlate Information
- Determine Impact

04 Responding to Incidents

- Implement Immediate Actions
- Develop Response Plan
- Execute Response Plan

05 End of Shift

- Review and Update Documentation
- Shift Handover
- Check-Out

1) BEGINNING OF SHIFT

BLUE TEAM RESOURCES

Check-In

1. **System Access**: Log into all necessary systems, tools, and platforms that you will be using throughout your shift.
2. **Resource Availability**: Ensure that all the resources you need are available and functioning correctly.
3. **Communication Channels**: Check your email, chat applications, or any other communication channels for any important updates or instructions.

Shift Handover

1. **Incident Status**: Receive a detailed handover from the previous shift. Understand the status of ongoing incidents, including what has been done so far, what needs to be done next, and any issues or challenges encountered.
2. **Outstanding Tasks**: Understand any tasks that have been left incomplete by the previous shift. These could include ongoing investigations, pending reports, or follow-ups with other teams.
3. **Key Events**: Get briefed on any key events that occurred during the previous shift. This could include major incidents, system outages, or significant changes in network traffic patterns.

Review Logs

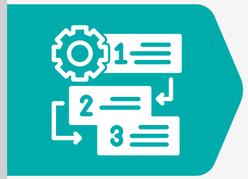
1. **Incident Logs**: Review the logs from the previous shift for any anomalies or incidents that may have occurred. Pay particular attention to high-severity incidents or unusual patterns of activity.
2. **System Logs**: Check the logs of key systems for any errors, warnings, or unusual events. This could include server logs, firewall logs, or application logs.
3. **Network Logs**: Review network logs for any signs of suspicious activity. This could include unusual traffic patterns, attempts to access restricted areas, or signs of a potential DDoS attack.

Update on Threat Landscape

1. **Threat Intelligence Reports**: Review the latest threat intelligence reports from both internal and external sources. Be aware of any new vulnerabilities, attack methods, or threat actors that could potentially impact your organization.
2. **Security News and Updates**: Check reputable cybersecurity news sources for any important updates or developments. This could include new malware strains, major cybersecurity incidents in other organizations, or changes in the tactics and techniques of known threat actors.
3. **Security Advisories**: Review any security advisories or alerts from vendors, industry groups, or government agencies.

BLUE TEAM
RESOURCES

2) TRIAGING ALERTS



Prioritize Alerts

- **Severity Assessment**: Review each alert and assess its severity. This could be based on factors like the potential impact on the organization, the systems or data involved, and the nature of the threat.
- **Impact Analysis**: Analyze the potential impact of each alert. Consider factors like the criticality of the affected systems, the sensitivity of the data involved, and the potential business impact.
- **Urgency Determination**: Determine the urgency of each alert. This could be based on factors like the speed at which the threat is progressing, the potential for harm, and any time-sensitive factors.
- **Alert Prioritization**: Prioritize alerts based on their severity, impact, and urgency. High-priority alerts should be addressed first.

Validate Alerts

- **Alert Verification**: Verify each alert to determine if it's a true positive or a false positive. This could involve cross-referencing with other data sources, checking against known indicators of compromise (IOCs), or using threat intelligence feeds.
- **False Positive Analysis**: If an alert is determined to be a false positive, analyze why it was triggered. This could involve checking the alerting rules, the system configuration, or the behavior of the system or network.
- **False Positive Reporting**: Document and report any false positives to the relevant team or individual. This could help improve the alerting system and reduce the number of false positives in the future.

Document Alerts

- **Alert Details**: For each validated alert, document the details. This should include the time of the alert, the systems involved, the nature of the alert, and any immediate actions taken.
- **Alert Context**: Provide context for the alert. This could include what was happening on the system or network at the time, any relevant events or changes, and any potential triggers for the alert.
- **Alert Classification**: Classify the alert based on its type, severity, and impact. This could help in tracking and reporting, as well as in identifying trends or patterns.
- **Initial Response**: Document any initial response to the alert. This could include isolating affected systems, blocking malicious IP addresses, or initiating an incident response process.

3) ANALYZING ALERTS

BLUE TEAM
RESOURCES

Investigate Alerts

- **Log Analysis**: Conduct a thorough analysis of log files related to the alert. This could involve system logs, application logs, network logs, or security logs. Look for any anomalies, patterns, or indicators of compromise.
- **Network Traffic Analysis**: Analyze network traffic data for any signs of malicious activity. This could involve looking at packet data, connection data, or flow data. Use tools like intrusion detection systems (IDS) or network traffic analysis (NTA) tools to assist in this analysis.
- **System Behavior Analysis**: Examine the behavior of the affected systems. Look for any changes in system performance, unusual processes, or unexpected system calls. Use tools like endpoint detection and response (EDR) solutions to assist in this analysis.

Correlate Information

- **Alert Correlation**: Correlate alerts from different systems to get a complete picture of the incident. This could involve correlating alerts based on time, source, destination, or type of alert.
- **Threat Intelligence Correlation**: Correlate the alert with threat intelligence information. This could involve checking the indicators of compromise (IOCs) against threat intelligence feeds, or comparing the tactics, techniques, and procedures (TTPs) used in the alert with known threat actor profiles.
- **Data Correlation**: Correlate the alert with other data sources. This could involve correlating the alert with user behavior data, system performance data, or business process data.

Determine Impact

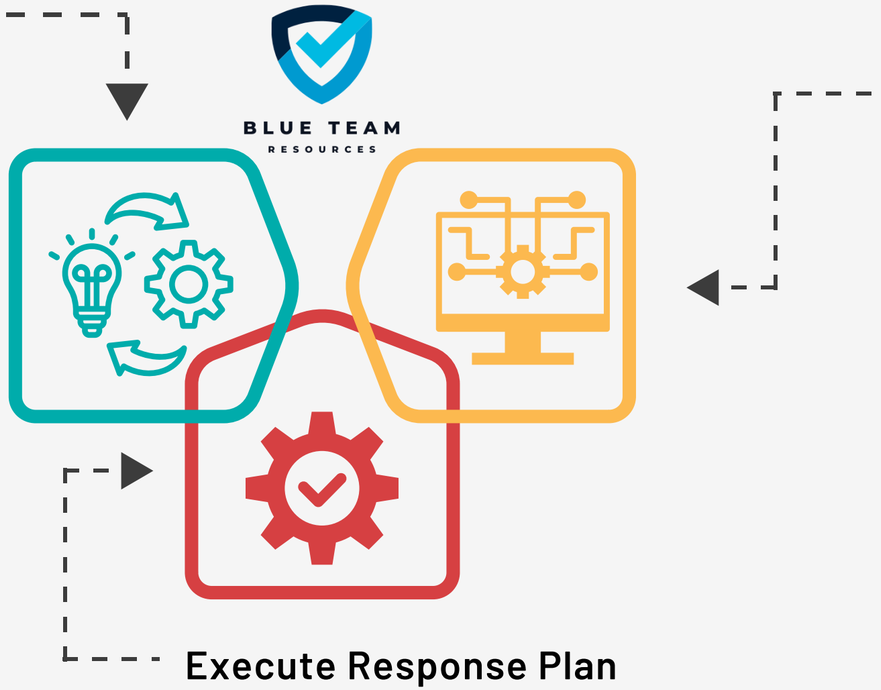
- **Affected Systems Identification**: Identify the systems affected by the incident. This could involve identifying the systems that generated the alert, the systems that were communicating with them, or the systems that are on the same network segment.
- **Affected Data Identification**: Identify the data that could be affected by the incident. This could involve identifying the data stored on the affected systems, the data being processed by the affected systems, or the data being transmitted by the affected systems.
- **Business Impact Assessment**: Assess the potential business impact of the incident by considering the criticality of the affected systems and data.

4) RESPONDING TO INCIDENTS

www.blueteamresources.in

Implement Immediate Actions

- **Containment Actions**: Implement any immediate actions needed to contain the incident. This could involve isolating affected systems to prevent the spread of the threat, blocking malicious IP addresses to stop further intrusion, or disabling compromised user accounts to prevent unauthorized access.
- **Preservation of Evidence**: Preserve any evidence related to the incident. This could involve taking system snapshots, making copies of log files, or documenting the state of the system or network. This evidence could be crucial for a detailed investigation or for legal proceedings.
- **Communication**: Communicate the incident to the relevant stakeholders. This could involve notifying the incident response team, informing management, or alerting other teams that may be affected.



Develop Response Plan

- **Incident Analysis**: Analyze the incident to understand the nature of the threat, the systems and data affected, and the potential impact. Use this analysis to inform your response plan.
- **Response Strategy**: Develop a strategy for responding to the incident. This should include the steps needed to eradicate the threat, recover affected systems and data, and prevent a similar incident in the future.
- **Resource Allocation**: Determine the resources needed to execute the response plan. This could involve personnel, tools, or external support. Ensure that these resources are available and ready to be deployed.

- **Action Execution**: Execute the response plan, following the steps outlined in the plan. This could involve removing malware, patching vulnerabilities, restoring systems from backups, or changing security configurations.
- **Documentation**: Document each step taken and the results. This could involve documenting the actions taken, the systems or data affected, any issues or challenges encountered, and the final outcome.
- **Validation**: Validate that the response plan has been successful. This could involve checking that the threat has been eradicated, that affected systems are functioning normally, and that security controls are effective.
- **Lessons Learned**: After the response, conduct a lessons learned session to identify what went well, what could be improved, and how to prevent similar incidents in the future. Update your incident response plan and procedures based on these lessons.

BLUE TEAM
RESOURCES

5) END OF SHIFT

Review and Update Documentation

- **Documentation Review**: Review all documentation from the shift to ensure it is complete, accurate, and clear. This could involve checking incident reports, alert logs, investigation notes, or any other documentation created during the shift.
- **Incident Ticket Updates**: Update any incident tickets with the latest information. This could involve updating the status of the incident, adding new findings or actions, or updating the impact assessment.
- **Documentation Finalization**: Finalize all documentation for the shift. Ensure that it is saved in the appropriate location, that it is accessible to those who need it, and that it is protected from unauthorized access.

Shift Handover

- **Incident Status Summary**: Prepare a summary of the status of ongoing incidents. This should include what has been done, what needs to be done next, and any challenges or issues encountered.
- **Outstanding Tasks List**: Prepare a list of any tasks that are outstanding. This could involve tasks that were not completed, tasks that need to be started, or tasks that need to be followed up.
- **Key Information Transfer**: Transfer any key information from the shift to the next team. This could involve important findings, key events, or important changes in the threat landscape.

Check-Out

- **System Log-Out**: Log out of all systems and tools. This could involve logging out of the SIEM system, the incident management system, the threat intelligence platform, or any other systems or tools used during the shift.
- **Secure Information**: Ensure that any sensitive information is securely stored or disposed of. This could involve saving sensitive documents in a secure location, encrypting sensitive data, or securely deleting any sensitive information that is no longer needed.

THANK YOU FOR READING!