Threat Hunting and Incident Response Playbook

Redback Operations

Version	Modified By	Approver	Date	Changes made
0.1	Devika Sivakumar		08 August 2024	Created the initial draft of the Threat-Hunting Playbook. Established the structure and content outline, including sections on roles, incident response workflow, and detailed frameworks. Integrated key tools like Wazuh and VirusTotal for threat detection and response processes. Drafted the Incident Response and Threat Hunting frameworks.
1.0	Devika Sivakumar		31 August 2024	Reviewed and refined the content for clarity, accuracy, and completeness. Added an Incident Response Workflow section, including a detailed activity diagram. Expanded the Incident Response Framework with additional details on containment, eradication, and recovery processes. Incorporated specific Redback Operations tools like Nagios and Suricata into the playbook. Finalized the terminology section to ensure consistent understanding across the team. Included the flowchart for incident response stages, enhancing visual representation and understanding.

Contents

1. Introduction

Overview

This playbook lays out the practical steps we will take to hunt for threats and respond to incidents within Redback Operations. The approach is built on real-world scenarios we have encountered and is designed to be used by all members of our cybersecurity teams.

Context

Our operations are based in virtual environments, with VMs provided through Deakin University's VPN. We have integrated tools like SIEM, Suricata, Wazuh, Nagios, and now VirusTotal within Wazuh, which gives us a strong base for both initiative-taking threat hunting and reactive incident response.

2. Purpose and Scope

Purpose

This playbook is intended to guide us through identifying and mitigating threats as efficiently as possible. By following these steps, we aim to minimize the impact of security incidents and keep our systems—and by extension, our projects—secure.

Scope

Everyone in the cybersecurity teams at Redback Operations—SecDevOps, GRC, Blue Team, Red Team, Infrastructure Team—is expected to follow this playbook. It applies across all our digital workspaces, particularly the VMs we use daily.

3. Roles and Responsibilities

Threat Hunting Team

- **Lead Threat Hunter**

Responsibilities: Oversee threat hunting, decide which threats to prioritize, and ensure hunts are well-documented.

- **Threat Hunters**

Responsibilities: Carry out the hunting process, using tools like Wazuh (with VirusTotal integration) to analyze data for signs of compromise.

- **Tool Specialists**

Responsibilities: Keep tools like SIEM, Suricata, Wazuh, and Nagios running smoothly and optimally configured.

Incident Response Team

- **Incident Response Lead (IRL)**

Responsibilities: Lead the response to incidents, coordinating all actions to resolve the issue efficiently.

- **Incident Responders**

Responsibilities: Handle the containment, eradication, and recovery phases of incidents.

- **Forensics Analysts**

Responsibilities: Analyze compromised systems to understand the scope and impact of an incident.

- **Communications Officer**

Responsibilities: Manage all communication during an incident, ensuring information is clear and accurate.

Support Teams

- **IT Support**

Responsibilities: Assist in system restoration and ensure infrastructure is secure post-incident.

- **Legal and Compliance**

Responsibilities: Ensure our incident response is compliant with all legal and regulatory requirements.

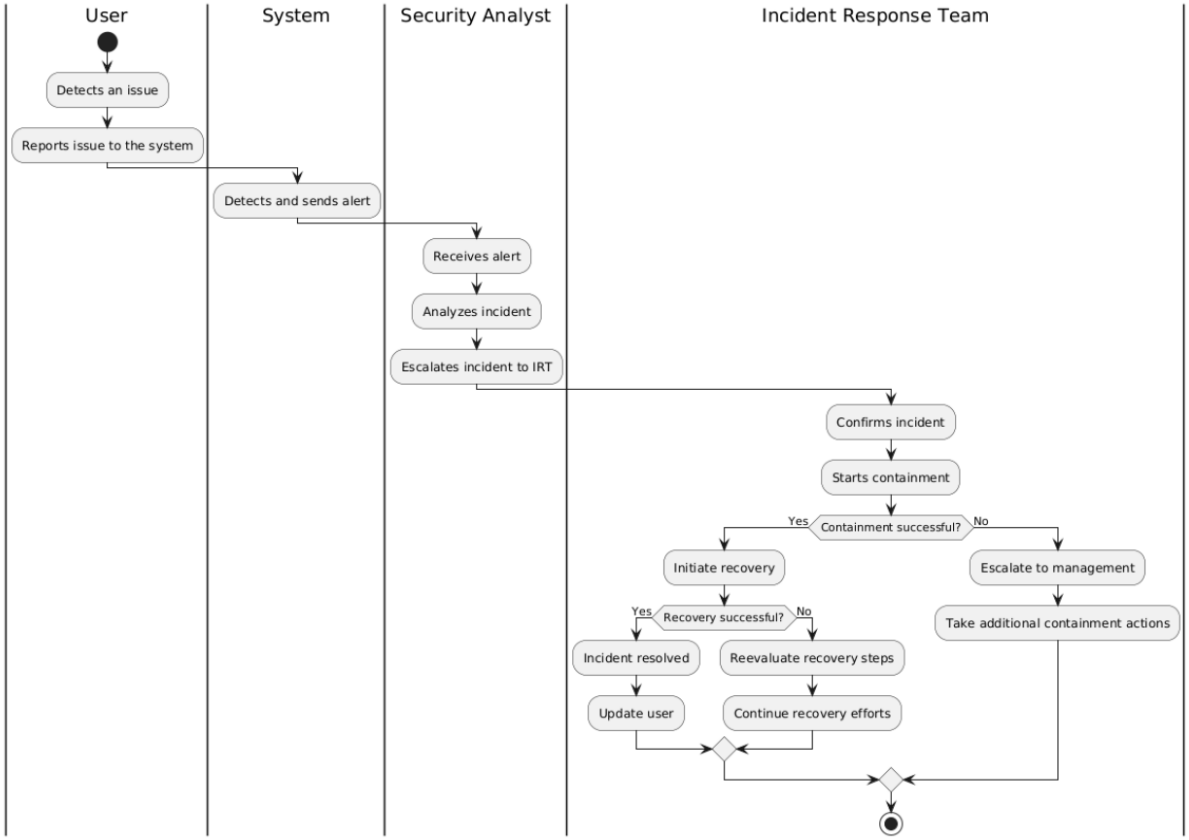
- **Management**

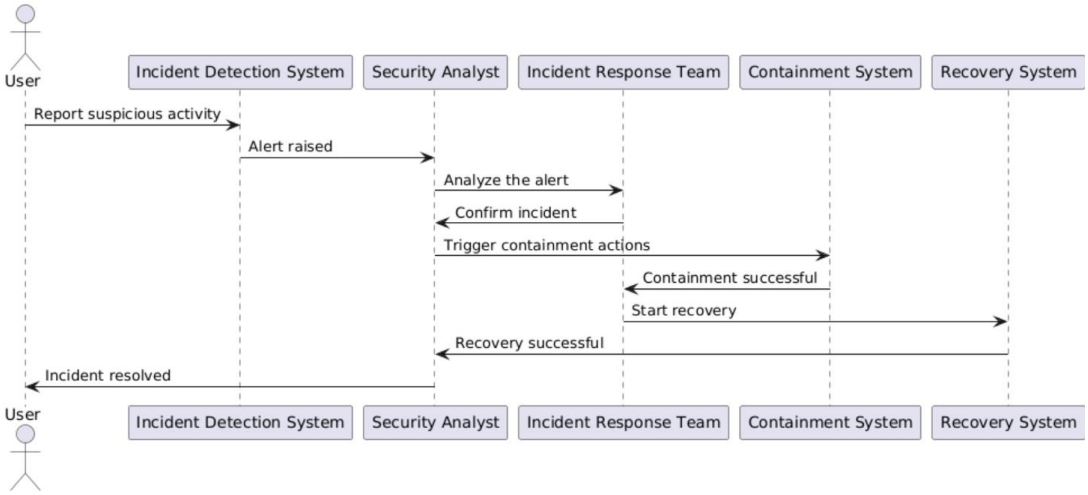
Responsibilities: Provide necessary oversight and resources to support effective threat hunting and incident response.

4. Incident Response Workflow

The incident response process at Redback Operations involves several key stages:

- Detection of the issue, either by the system or reported by a user.
- Analysis and escalation by the Security Analyst.
- Confirmation of the incident and initiation of containment by the Incident Response Team.
- Containment and, if successful, moving onto recovery efforts.
- Post-incident review and documentation of lessons learned.





Explanation:

Actors and Participants:

- **User** (U): Represents the end-user who detects an issue.
- **System** (Sys): The system that detects and sends alerts.
- **Security Analyst** (SA): The security professional who escalates the incident.
- **Incident Response Team** (IRT): The team responsible for managing the incident.

Flow:

- The user detects an issue, and the system sends an alert.
- The security analyst escalates the incident to the incident response team.
- The team confirms the incident, starts containment, and initiates recovery.
- Once recovery is successful, the incident is resolved, and the user is updated.

5. Threat Hunting Framework

5.1. Preparation Phase

- **Establish Baselines**: We need to understand what normal operations look like across our VMs, including typical network traffic and system processes.
- **Tool Configuration**: Verify that all tools, especially Wazuh with VirusTotal integration and Nagios, are configured to provide actionable data with minimal false positives.
- **Hypothesis Development**: Based on recent threat intelligence and known vulnerabilities, create specific hypotheses to guide our threat hunting efforts.

5.2. Hunting Phase

- **Data Collection**: Gather data from our tools—SIEM for event correlation, Suricata for network traffic, Wazuh for endpoint monitoring, and Nagios for system performance.
- **Hypothesis Testing**: Analyze the collected data to validate or disprove the hypotheses, focusing on any anomalies identified by VirusTotal scans within Wazuh.

5.3. Analysis Phase

- **Pattern Recognition**: Look for patterns in the data that suggest malicious activity, such as unusual traffic or system performance issues flagged by Nagios.
- **Behavioral Analysis**: Dive deeper into any suspicious activity, correlating it across multiple data sources to see if it fits the profile of a known threat.
- **Threat Attribution**: If a threat is detected, use available threat intelligence to determine its origin and actors.

5.4. Discovery Phase

- **IOC Identification**: Document any Indicators of Compromise (IOCs) discovered during analysis, such as malicious IPs or file hashes flagged by VirusTotal.
- **Threat Validation**: Confirm that the threat is real and not a false positive by performing further checks, involving sandboxing or deeper forensics.
- **Threat Reporting**: Compile a report detailing the findings and share it with the Incident Response Team for further action.

5.5. Reporting Phase

- **Threat Report Compilation**: Summarize the key findings in a clear and actionable report that includes technical analysis and recommended next steps.
- **Dissemination**: Distribute the report to all relevant stakeholders, ensuring that everyone is aware of the findings and the required response actions.

6. Incident Response Framework

6.1. Identification Phase

- **Alert Triage**: Monitor alerts from SIEM, Suricata, Wazuh (with VirusTotal), and Nagios. Prioritize based on severity and potential impact on our systems.
- **Incident Classification**: Classify the incident to determine the appropriate response strategy, considering the specific tools and systems affected.

6.2. Containment Phase

- **Immediate Containment**: Isolate affected VMs or systems from the network to prevent further spread of the threat.
- **Short-Term Containment**: Apply temporary fixes, like blocking IPs or disabling compromised accounts, to keep the threat under control.
- **Long-Term Containment**: Implement more permanent solutions, such as patching vulnerabilities or improving access controls.

6.3. Eradication Phase

- **Root Cause Analysis**: Investigate the root cause of the incident, identifying how the threat entered the environment.
- **Threat Removal**: Remove the threat entirely, whether it involves deleting malware, reconfiguring systems, or resetting compromised accounts.
- **Validation of Eradication**: Ensure that the threat has been fully eradicated by performing follow-up scans and monitoring.

6.4. Recovery Phase

- **System Restoration**: Restore systems to normal operation, ensuring they are secure before reconnecting to the network.
- **Verification of Integrity**: Verify that all systems are functioning properly and that no residual issues remain from the incident.
- **Post-Recovery Monitoring**: Keep a close watch on recovered systems to detect any signs of residual threats or reinfection.

6.5. Lessons Learned Phase

- **Post-Incident Review (PIR)**: After resolving the incident, review the response process to identify strengths and areas for improvement.
- **Root Cause Documentation**: Document the root cause and response actions taken, using this information to update our procedures and tools.
- **Process Improvement**: Update the playbook based on lessons learned, ensuring that we continually improve our threat hunting and incident response capabilities.

7. Communication and Escalation Procedures

Internal Communication

- **Incident Notification**: Notify key stakeholders as soon as an incident is detected.
- **Status Updates**: Provide regular updates throughout the incident response process to keep everyone informed.
- **Escalation Protocols**: Know when to escalate incidents to higher management or involve external partners.

External Communication

- **Customer and Partner Notification**: If necessary, inform external parties of the incident, following legal and compliance guidelines.
- **Media Relations**: Handle media inquiries carefully, ensuring that all information shared is accurate and controlled.
- **Regulatory Notification**: Notify regulatory bodies if required, adhering to legal requirements for incident reporting.

8. Tools, Technologies, and Techniques

SIEM (Security Information and Event Management)

- **Role**: Centralizes and correlates security data from various sources, providing real-time alerts and insights.
- **Key Functions**: Monitoring, event correlation, alerting.

Suricata

- **Role**: Monitors network traffic for suspicious activity, acting as an IDS/IPS.
- **Key Functions**: Network traffic analysis, anomaly detection.

Wazuh (with VirusTotal Integration)

- **Role**: Monitors endpoints for security issues and integrates with VirusTotal to provide additional malware detection capabilities.
- **Key Functions**: Log analysis, file integrity monitoring, real-time malware scanning via VirusTotal.

Nagios

- **Role**: Monitors the performance and availability of systems, alerting us to any issues that might indicate a security problem.
- **Key Functions**: System performance monitoring, alerting on failures or anomalies.

OpenCTI (if implemented)

- **Role**: Provides a centralized platform for managing threat intelligence, helping us stay informed about emerging threats.
- **Key Functions**: Threat intelligence aggregation, analysis, and integration with other tools.

MQTT

- **Role**: Used for secure messaging in IoT projects, requiring careful monitoring for anomalies.
- **Key Functions**: Secure messaging, real-time monitoring of IoT communications.

9. Post-Incident Activities and Continuous Improvement

1. Documentation

- **Incident Documentation**: Keep detailed records of every incident, including timelines, actions taken, and outcomes. This helps us learn and improve.
- **Lessons Learned Reports**: After each incident, write up what we learned and how we can do better next time.

2. Process Improvement

- **Process Audits**: Regularly audit our threat hunting and incident response processes to make sure they are still effective and up to date.
- **Policy Updates**: Based on lessons learned, update our policies and procedures to prevent future incidents.
- **Technology Evaluation**: Periodically evaluate our tools to ensure they are still meeting our needs and keeping pace with new threats.

3. Training and Drills

- **Refresher Training**: Regularly train our team on the playbook, focusing on any areas where we identified gaps during incidents.
- **Scenario-Based Drills**: Conduct drills to practice our response to different types of incidents. Use these exercises to refine our processes.

10. Playbook Maintenance and Review Cycle

Review Frequency

- **Quarterly Review**: Every three months, review the playbook to ensure it reflects the current threat landscape and our operational environment.
- **Post-Incident Review**: After every significant incident, review the playbook to see if any changes are needed based on what we learned.
- **Annual Audit**: Once a year, conduct a thorough audit of the playbook to ensure it aligns with industry best practices and any regulatory requirements.

Version Control

- **Document Versions**: Each time the playbook is updated, assign a new version number (e.g., v1.1, v2.0) and keep a detailed change log.
- **Change Log**: Maintain a record of all changes, including what was updated, why, and who approved the changes.
- **Approval Process**: All updates to the playbook must be approved by the Incident Response Lead and other relevant stakeholders.

Feedback Mechanisms

- **Internal Feedback Loop**: Regularly gather feedback from team members to identify areas where the playbook can be improved.
- **External Feedback and Peer Review**: Engage with external experts to get an outside perspective on our playbook and processes.
- **Continuous Improvement**: Use the feedback to continuously refine and improve the playbook, keeping it relevant and effective.

11. Appendices

Appendix A: Threat Intelligence Sources

- **External Sources**: Include details on threat intelligence feeds we use, such as STIX/TAXII feeds, government advisories, and industry-specific intel.
- **Internal Sources**: Outline our internal sources, like SIEM logs and incident reports, which help inform our threat hunting.

Appendix B: Incident Response Contact List

- **Incident Response Team**: List contact information for key personnel, including the Incident Response Lead, Threat Hunters, Forensics Analysts, and Communications Officer.
- **Support Teams**: Include contact details for IT Support, Legal, and Management.
- **Escalation Contacts**: Provide escalation contacts, including university security team and external partners.

Appendix C: Threat Hunting Checklist

- **Preparation**: Confirm that baselines are up-to-date, and tools are correctly configured.
- **Hunting**: Collect and analyze data, testing hypotheses as you go.
- **Reporting**: Document findings and share them with the necessary teams.

Appendix D: Incident Response Checklist

- **Identification**: Triage alerts and classify the incident.
- **Containment**: Quickly isolate and contain the threat.
- **Eradication and Recovery**: Remove the threat and restore systems, verifying integrity before reconnecting to the network.
- **Lessons Learned**: Conduct a review and document what was learned.

Appendix E: Legal and Compliance Considerations

- **Data Breach Notification**: Summarize the legal requirements for notifying affected parties and authorities in the event of a data breach.
- **Internal Policies**: List internal policies related to data handling and incident response.
- **International Considerations**: If applicable, include guidelines for complying with international data protection laws.