Gilbert Collado

01JUL2024

Implementing Detective Controls on the Web Server

Objective:

To implement detective controls on the web server hosting SimCorp's web application to monitor for unauthorized access attempts, data exfiltration, and other malicious activities.

Scope:

This SOP applies to all team members responsible for the security and monitoring of the web server hosting SimCorp's web application.

Steps:

1. **Preparation and Planning:**
    - **Identify Key Assets:**
        - Determine the critical components of the web server and the web application that need monitoring.
        - Identify sensitive data and resources that require protection.
    - **Select Monitoring Tools:**
        - Choose appropriate tools for logging and monitoring (e.g., OSSEC, Wazuh, AWS CloudTrail, Splunk).
2. **Configure Logging and Monitoring:**
    - **Enable System Logging:**
        - Ensure that logging is enabled on the web server at the operating system level.
        - Configure logging for key system activities (e.g., user logins, file access, system changes).
    - **Application Logging:**
        - Enable and configure logging for the web application to capture critical events (e.g., login attempts, data access, transactions).
    - **Network Monitoring:**
        - Implement network monitoring tools to capture network traffic and detect anomalies (e.g., Zeek, Suricata).
        - Configure the tools to monitor for unauthorized access attempts, data exfiltration, and other suspicious activities.
3. **Set Up Alerts:**
    - **Define Alert Criteria:**

        - Establish criteria for generating alerts based on suspicious activities (e.g., multiple failed login attempts, access to sensitive files, unusual network traffic patterns).
        - Prioritize alert criteria based on the potential impact and risk.
    - **Configure Alerts:**
        - Set up alerts in the chosen monitoring tools to notify the security team of suspicious activities.
        - Ensure alerts are actionable and provide sufficient context for investigation.

4. **Implement Additional Detective Controls:**
    - **File Integrity Monitoring:**
        - Implement file integrity monitoring tools to detect unauthorized changes to critical files (e.g., Tripwire, AIDE).
        - Configure the tools to monitor key directories and files on the web server.
    - **User Activity Monitoring:**
        - Deploy tools to monitor user activities, including login attempts, command execution, and access to sensitive data (e.g., auditd, OSSEC).
        - Configure the tools to log and alert on suspicious user activities.
    - **Intrusion Detection Systems (IDS):**
        - Implement IDS solutions to detect potential intrusions and malicious activities (e.g., Snort, Suricata).
        - Configure IDS rules to focus on the web application and server-specific threats.
5. **Test and Validate Controls:**
    - **Conduct Testing:**
        - Perform testing to ensure that the detective controls are functioning correctly.
        - Simulate various attack scenarios to validate the effectiveness of logging, monitoring, and alerting.
    - **Review and Adjust:**
        - Review the test results and make necessary adjustments to the configurations.
        - Fine-tune the alert thresholds and monitoring rules to minimize false positives and negatives.
6. **Documentation and Reporting:**
    - **Document Configurations:**
        - Maintain detailed documentation of the configurations for logging, monitoring, and alerting.
        - Include information on tools used, settings applied, and alert criteria.
    - **Reporting:**
        - Develop a reporting mechanism to summarize the detected activities and incidents.
        - Provide regular reports to the security team and management on the status of the detective controls and any significant findings.

7. **Review and Update:**
    - **Regular Audits:**
        - Schedule regular audits of the detective controls to ensure they remain effective and up-to-date.
        - Adjust configurations based on audit findings and changes in the threat landscape.
    - **Continuous Improvement:**
        - Encourage continuous improvement of the detective controls by incorporating feedback and lessons learned from incidents and audits.
        - Stay updated with the latest security trends and adjust the monitoring strategy accordingly.

Responsibilities:

- **Security Analysts:** Configure and maintain the logging and monitoring tools, respond to alerts, and conduct regular reviews.
- **System Administrators:** Ensure the web server is properly configured for logging and monitoring, assist in implementing detective controls.
- **Application Developers:** Provide insights into application-specific logging requirements and assist in configuring application logs.
- **Stakeholders:** Review reports, provide feedback, and support the continuous improvement of detective controls.

Tools and Resources:

- **Logging and Monitoring Tools:** OSSEC, Wazuh, AWS CloudTrail, Splunk, Zeek, Suricata.
- **File Integrity Monitoring:** Tripwire, AIDE.
- **User Activity Monitoring:** auditd, OSSEC.
- **Intrusion Detection Systems (IDS):** Snort, Suricata.
- **Documentation Platforms:** Confluence, SharePoint, Google Drive.