Gilbert Collado

01JUL2024

Adversarial Activity Observation

Objective:

To actively observe adversarial actions and collect evidence of scanning activities, TTPs (Tactics, Techniques, and Procedures), and any other indicators of compromise (IOCs) to understand the evolving threat landscape and inform response strategies.

Scope:

This SOP applies to all team members responsible for monitoring and responding to security threats, including security analysts, incident responders, and threat intelligence teams.

Steps:

1. **Preparation and Planning:**
    - **Define Objectives:**
        - Clearly outline the goals of adversarial activity observation.
        - Establish the scope, focusing on key assets and critical systems.
    - **Select Monitoring Tools:**
        - Choose appropriate tools for monitoring and collecting evidence (e.g., SIEM, IDS, EDR).
        - Ensure the tools are capable of detecting scanning activities, TTPs, and IOCs.
2. **Set Up Monitoring and Detection:**
    - **Configure SIEM:**
        - Integrate all relevant data sources into the SIEM (e.g., network logs, system logs, application logs).
        - Configure dashboards and alerts for real-time monitoring of adversarial activities.
    - **Deploy IDS/IPS:**
        - Implement Intrusion Detection/Prevention Systems (e.g., Snort, Suricata) to monitor network traffic.
        - Configure IDS/IPS rules to detect known TTPs and IOCs.
    - **Endpoint Detection and Response (EDR):**
        - Deploy EDR solutions (e.g., CrowdStrike, Carbon Black) on critical endpoints.
        - Configure EDR to capture detailed activity logs and detect suspicious behaviors.

3. **Identify Adversarial Activities:**
    - **Scanning Activities:**
        - Monitor for common scanning activities such as port scans, vulnerability scans, and network sweeps.
        - Configure alerts for unusual scanning patterns and repeated scanning attempts.
    - **Tactics, Techniques, and Procedures (TTPs):**
        - Use threat intelligence feeds to stay updated on the latest TTPs used by adversaries.
        - Configure detection rules in SIEM, IDS/IPS, and EDR to identify known TTPs.
    - **Indicators of Compromise (IOCs):**
        - Integrate IOCs from threat intelligence sources into monitoring tools.
        - Configure alerts for detection of IOCs such as malicious IP addresses, domain names, file hashes, and email addresses.
4. **Collect and Preserve Evidence:**
    - **Logging and Storage:**
        - Ensure all monitoring tools are configured to log relevant data.
        - Store logs securely in a centralized location for future analysis and legal compliance.
    - **Network Traffic Analysis:**
        - Capture and analyze network traffic using tools like Zeek or Wireshark.
        - Store network traffic captures for forensic analysis.
    - **System and Application Logs:**
        - Collect logs from critical systems and applications.
        - Ensure logs are detailed and include timestamps, user actions, and system events.
5. **Analyze and Document Findings:**
    - **Initial Analysis:**
        - Perform initial analysis of detected adversarial activities.
        - Categorize findings based on severity, potential impact, and type of activity.
    - **Detailed Investigation:**
        - Conduct a detailed investigation of significant findings to understand the full scope and impact.
        - Use forensic tools to analyze system images, memory dumps, and other artifacts.
    - **Documentation:**
        - Document all findings in a structured format.
        - Include details such as the nature of the activity, affected systems, evidence collected, and analysis results.
6. **Reporting and Communication:**
    - **Incident Reports:**
        - Generate detailed incident reports for significant adversarial activities.

        - Include an executive summary, detailed analysis, evidence, and recommended actions.
    - **Regular Updates:**
        - Provide regular updates to stakeholders on observed activities and trends.
        - Share relevant findings with the incident response team and other relevant parties.
7. **Review and Improve:**
    - **Regular Reviews:**
        - Schedule regular reviews of the adversarial activity observation process.
        - Update monitoring and detection configurations based on new threats and changing environments.
    - **Continuous Improvement:**
        - Encourage feedback from team members and stakeholders.
        - Implement improvements to enhance detection capabilities and response strategies.

Responsibilities:

- **Security Analysts:** Monitor and analyze adversarial activities, configure detection rules, and collect evidence.
- **Incident Responders:** Investigate significant findings, preserve evidence, and coordinate response actions.
- **Threat Intelligence Team:** Stay updated on the latest TTPs and IOCs, integrate threat intelligence into monitoring tools.
- **Stakeholders:** Review reports, provide feedback, and support continuous improvement efforts.

Tools and Resources:

- **SIEM Solutions:** Splunk, LogRhythm, QRadar.
- **IDS/IPS:** Snort, Suricata.
- **EDR Solutions:** CrowdStrike, Carbon Black.
- **Network Analysis Tools:** Zeek, Wireshark.
- **Forensic Tools:** EnCase, FTK, Volatility.
- **Threat Intelligence Feeds:** AlienVault OTX, ThreatConnect, MISP.
- **Documentation Platforms:** Confluence, SharePoint, Google Drive.