==========

==========

CATEGORY: LoggingForensics

==========

==========

Logging and forensic operations are among the most sensitive workflows in any enterprise environment. These SOPs ensure every action performed through RDAM Script Wizard is **controlled**, **auditable**, **forensically sound**, and aligned with **security, compliance, and incident-response standards**.

SOP 1 – Export Event Logs (Filtered)

Script Name: Export Event Logs (Filtered) **Category:** LoggingForensics **Version:** 1.0 **Approved By:** Security Operations / IT Leadership

1. Purpose

This script exports Windows Event Logs based on specific filters (Event ID, time range, provider, severity). It supports forensic investigations, compliance reporting, and incident response by providing a controlled, repeatable method for extracting relevant log data.

2. Scope

- **Systems:** Windows servers and workstations
- **Logs:** System, Application, Security, and custom logs
- **Use Cases:**
    - Incident response
    - Forensic preservation
    - Compliance audits
    - Troubleshooting

3. Definitions

- **Filtered Export:** Exporting only events matching specific criteria.
- **EVTX:** Native Windows event log file format.

4. Preconditions

- Operator must have read access to the target log.
- Export path must be writable.
- Filters must be valid (Event ID numeric, time range logical).
- Export must comply with forensic chain-of-custody requirements.

5. Required Inputs

- Log name
- Filter criteria:
    - Event ID
    - Time range
    - Provider
    - Severity
- Export path

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for log name, filters, and export path.
    - Validate all inputs.
2. **Log Resolution**
    - Confirm log exists on target system.
3. **Filter Construction**
    - Build query using provided criteria.
    - Validate syntax.
4. **Event Retrieval**
    - Query log for matching events.
    - Handle large result sets with pagination.
5. **Export Operation**
    - Write filtered events to EVTX file.
    - Ensure file integrity.
6. **Post-Export Verification**

    - Confirm file exists and is readable.
    - Validate event count > 0 (unless expected).
7. **Logging**
    - Log operator, filters, export path, timestamp.

7. Expected Output

- EVTX file containing filtered events.

8. Post-Execution Validation

- Forensics team may load EVTX into Event Viewer or SIEM.

9. Error Handling

- Invalid filters
- Log not found
- Access denied
- Export path invalid

10. Security Considerations

- Exported logs may contain sensitive data.
- Must be stored securely and handled per chain-of-custody policy.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Export path
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for extracting relevant event logs, supporting investigations, compliance, and operational troubleshooting.

SOP 2 – Search Logon Events

Script Name: Search Logon Events **Category:** LoggingForensics

1. Purpose

This script searches Windows Security logs for logon-related events (e.g., Event IDs 4624, 4625, 4634). It supports authentication analysis, brute-force detection, and forensic investigations.

2. Scope

- **Systems:** Windows servers and workstations
- **Events:** Successful logons, failed logons, logoffs
- **Use Cases:**
    - Security monitoring
    - Incident response
    - Account misuse investigations

3. Definitions

- **Event ID 4624:** Successful logon
- **Event ID 4625:** Failed logon
- **Event ID 4634:** Logoff

4. Preconditions

- Operator must have read access to Security log.
- Log must exist.
- Filters must be valid.

5. Required Inputs

- Event ID(s)
- Optional:
    - Username
    - Time range
    - Logon type

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for Event ID(s) and optional filters.
2. **Log Resolution**

    - Confirm Security log exists.
3. **Query Construction**
    - Build filter for Event ID(s) and optional parameters.
4. **Event Retrieval**
    - Query Security log.
    - Extract relevant fields:
        - Timestamp
        - Username
        - Logon type
        - Source IP
        - Status code
5. **Output Formatting**
    - Present structured results.
    - Highlight failed logons or suspicious patterns.
6. **Logging**
    - Log Event ID(s), filters, operator, timestamp.

7. Expected Output

- List of logon events matching criteria.

8. Post-Execution Validation

- Security team may correlate with SIEM or AD logs.

9. Error Handling

- Access denied
- Invalid Event ID
- Log not found

10. Security Considerations

- Logon data is highly sensitive.
- Must be handled per security policy.

11. Audit Logging Requirements

- Operator ID
- Event ID(s)
- Filter parameters
- Timestamp

12. Organizational Benefit Statement

This script provides a precise, auditable method for analyzing authentication activity, supporting threat detection and forensic investigations.

SOP 3 – Monitor File System Changes

Script Name: Monitor File System Changes **Category:** LoggingForensics

1. Purpose

This script monitors a specified folder for real-time file system changes (create, modify, delete, rename). It supports forensic monitoring, malware detection, and operational troubleshooting.

2. Scope

- **Systems:** Windows servers and workstations
- **Targets:** Folders and subfolders
- **Use Cases:**
    - Ransomware detection
    - Suspicious activity monitoring
    - Application troubleshooting

3. Definitions

- **FileSystemWatcher:** Windows API for monitoring file system events.

4. Preconditions

- Operator must have read access to target folder.
- Folder must exist.
- Monitoring must be authorized.

5. Required Inputs

- Folder path
- Optional:
    - Include subfolders
    - Filter (e.g., *.log, *.exe)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for folder path and options.
2. **Folder Validation**
    - Confirm folder exists.
3. **Watcher Initialization**
    - Configure FileSystemWatcher with filters.
    - Enable event handlers.
4. **Monitoring Operation**
    - Capture events:
        - Created
        - Modified
        - Deleted
        - Renamed
    - Timestamp each event.
5. **Output Formatting**
    - Display events in real time.
6. **Logging**
    - Log monitoring start/stop, folder, operator.

7. Expected Output

- Real-time stream of file system events.

8. Post-Execution Validation

- Operator may test by creating or modifying files.

9. Error Handling

- Access denied
- Folder not found
- Watcher overflow

10. Security Considerations

- Monitoring sensitive folders must follow policy.
- Output may reveal confidential data.

11. Audit Logging Requirements

- Operator ID
- Folder monitored
- Monitoring duration
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for monitoring file system activity, supporting threat detection and operational troubleshooting.

SOP 4 – Collect Diagnostics Bundle

Script Name: Collect Diagnostics Bundle **Category:** LoggingForensics

1. Purpose

This script collects a comprehensive diagnostics bundle from a system, including logs, configuration data, and system state information. It supports incident response, troubleshooting, and forensic preservation.

2. Scope

- **Systems:** Windows servers and workstations
- **Data Types:**
    - Event logs
    - System info
    - Network config
    - Running processes

        - Services
        - Installed software
        - Registry snapshots

3. Definitions

- **Diagnostics Bundle:** A packaged set of system data for analysis.

4. Preconditions

- Operator must have administrative rights.
- Sufficient disk space must be available.
- Export path must be writable.
- Collection must be authorized.

5. Required Inputs

- Output folder path
- Optional: Include memory snapshot

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for output path and options.
2. **Environment Validation**
    - Confirm path exists or can be created.
    - Validate disk space.
3. **Data Collection**
    - Gather:
        - System info
        - Network config
        - Running processes
        - Services
        - Installed software
        - Event logs
        - Registry exports

    - Optional: Memory snapshot
4. **Bundle Packaging**
    - Compress collected data into a single archive.
5. **Post-Collection Verification**
    - Confirm archive exists and is readable.
6. **Logging**
    - Log operator, output path, timestamp.

7. Expected Output

- A compressed diagnostics bundle.

8. Post-Execution Validation

- IR or engineering teams may review bundle contents.

9. Error Handling

- Access denied
- Insufficient disk space
- Missing components

10. Security Considerations

- Bundle may contain highly sensitive data.
- Must be stored and transmitted securely.
- Must follow chain-of-custody procedures.

11. Audit Logging Requirements

- Operator ID
- Output path
- Bundle size
- Timestamp

12. Organizational Benefit Statement

This script provides a comprehensive, auditable method for collecting system diagnostics, supporting rapid incident response and deep forensic analysis.