==========

==========

CATEGORY: IncidentResponse

==========

==========

Incident Response (IR) scripts must be treated as **high-sensitivity**, **high-impact**, and **high-auditability** tools. These SOPs ensure every IR action performed through RDAM Script Wizard is controlled, logged, and aligned with enterprise security and forensic standards.

SOP 1 – Network Connections with Process Mapping

Script Name: Network Connections with Process Mapping **Category:** IncidentResponse **Version:** 1.0 **Approved By:** Security Operations / Incident Response Leadership

1. Purpose

This script enumerates active network connections on a system and maps each connection to the owning process. It supports threat hunting, malware analysis, and incident triage by identifying suspicious outbound or listening connections.

2. Scope

- **Systems:** Windows servers and workstations
- **Use Cases:** IR triage, malware investigation, lateral movement detection
- **Authorized Personnel:**
    - Security analysts
    - Incident responders
    - Forensic investigators
    - Tier-3 system administrators

3. Definitions

- Network Connection**:** Active TCP/UDP communication endpoint.

- Process Mapping**:** Identifying which executable owns a connection.
- Listening Port**:** Port awaiting inbound connections.

4. Preconditions

- Local admin rights required to enumerate all processes.
- System must be reachable.
- Script must run under a trusted security context.

5. Required Inputs

- Optional:
    - Filter by port
    - Filter by process name
    - Filter by remote IP

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for optional filters.
    - Validate filter formats.
2. **Connection Enumeration**
    - Retrieve all TCP/UDP connections.
    - Include:
        - Local address/port
        - Remote address/port
        - State (Established, Listening, etc.)
3. **Process Mapping**
    - Map each connection to owning PID.
    - Retrieve process name, path, and command line.
4. **Suspicious Pattern Detection**
    - Highlight:
        - Unknown processes
        - Connections to foreign IPs
        - Unusual listening ports

5. **Output Formatting**
    - Present structured table with connection → process mapping.
6. **Logging**
    - Log filters, operator, timestamp.

7. Expected Output

- Full list of network connections with associated processes.

8. Post-Execution Validation

- IR team may correlate with firewall logs, SIEM, or threat intel.

9. Error Handling

- Access denied
- Process terminated during enumeration
- Network stack unavailable

10. Security Considerations

- Output may reveal sensitive system activity.
- Must be restricted to IR personnel.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Result count
- Timestamp

12. Organizational Benefit Statement

This script provides a rapid, auditable method for identifying suspicious network activity, accelerating incident triage and reducing dwell time.

SOP 2 – Search for Known IOCs

Script Name: Search for Known IOCs **Category:** IncidentResponse

1. Purpose

This script searches a system for known Indicators of Compromise (IOCs), including file hashes, malicious domains, IP addresses, and registry artifacts. It supports threat hunting and incident containment.

2. Scope

- **IOC Types:**
    - File hashes
    - Filenames/paths
    - Registry keys
    - Domains
    - IP addresses
- Used by IR and security teams.

3. Definitions

- IOC**:** Observable artifact indicating malicious activity.
- Hash**:** Unique identifier for a file’s contents.

4. Preconditions

- Operator must have read access to file system and registry.
- IOC list must be validated and approved by IR leadership.

5. Required Inputs

- IOC list (hashes, domains, IPs, registry paths)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for IOC list.
2. **IOC Categorization**
    - Separate IOCs by type.
3. **Search Operations**
    - Hash search: compute file hashes and compare.
    - Domain/IP search: inspect DNS cache, logs, and connections.

    - Registry search: enumerate keys and values.
4. **Match Identification**
    - Flag any IOC matches.
    - Include file paths, timestamps, and process associations.
5. **Output Formatting**
    - Present matches with severity indicators.
6. **Logging**
    - Log IOC count, matches, operator.

7. Expected Output

- List of matched IOCs with context.

8. Post-Execution Validation

- IR team may escalate to containment or eradication.

9. Error Handling

- Invalid IOC format
- Access denied
- Large directory scan timeout

10. Security Considerations

- IOC lists may contain sensitive threat intel.
- Results must be handled securely.

11. Audit Logging Requirements

- Operator ID
- IOC count
- Match count
- Timestamp

12. Organizational Benefit Statement

This script accelerates threat detection by providing a fast, auditable method for identifying known malicious artifacts.

SOP 3 – Dump Process Memory

Script Name: Dump Process Memory **Category:** IncidentResponse

1. Purpose

This script captures the memory of a running process for forensic analysis. It supports malware investigation, credential theft detection, and advanced IR workflows.

2. Scope

- **Targets:** Suspicious or compromised processes
- **Use Cases:**
    - Malware analysis
    - Credential theft investigation
    - Memory forensics

3. Definitions

- Memory Dump**:** Snapshot of a process's memory space.
- PID**:** Process identifier.

4. Preconditions

- Local admin rights required.
- Dumping must be authorized by IR leadership.
- Sufficient disk space must be available.

5. Required Inputs

- PID or process name
- Dump file output path

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for PID and output path.
2. **Process Resolution**
    - Confirm process exists and is accessible.
3. **Dump Initialization**

- Prepare dump writer with appropriate flags.

4. **Memory Dump Operation**
    - Capture full memory or minidump depending on configuration.
5. **Post-Dump Verification**
    - Confirm dump file exists and is readable.
6. **Logging**
    - Log PID, dump path, operator.

7. Expected Output

- Confirmation of successful memory dump.

8. Post-Execution Validation

- Forensics team may load dump into analysis tools.

9. Error Handling

- Access denied
- Process terminated
- Insufficient disk space

10. Security Considerations

- Memory dumps may contain credentials or sensitive data.
- Must be stored and transmitted securely.

11. Audit Logging Requirements

- Operator ID
- PID
- Dump path
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for capturing process memory, supporting advanced forensic investigations.

SOP 4 – Enumerate Persistence Mechanisms

Script Name: Enumerate Persistence Mechanisms **Category:** IncidentResponse

1. Purpose

This script identifies common persistence mechanisms used by malware or threat actors to maintain access on a system.

2. Scope

- **Persistence Types:**
    - Registry Run keys
    - Scheduled tasks
    - Services
    - Startup folders
    - WMI subscriptions

3. Definitions

- Persistence**:** Techniques used to survive reboots or logoffs.

4. Preconditions

- Local admin rights required.
- System must be reachable.

5. Required Inputs

- None (full scan)

6. Procedure Steps

1. **Registry Enumeration**
    - Inspect Run/RunOnce keys.
2. **Scheduled Task Enumeration**
    - List tasks with suspicious triggers.
3. **Service Enumeration**
    - Identify auto-start services with unusual paths.
4. **Startup Folder Inspection**

    - Check user and system startup folders.
5. **WMI Subscription Enumeration**
    - Identify permanent event consumers.
6. **Output Formatting**
    - Present findings with severity indicators.
7. **Logging**
    - Log count of suspicious entries.

7. Expected Output

- List of potential persistence mechanisms.

8. Post-Execution Validation

- IR team may escalate to containment.

9. Error Handling

- Access denied
- Corrupted registry keys

10. Security Considerations

- Results may reveal sensitive system configuration.
- Must be restricted to IR personnel.

11. Audit Logging Requirements

- Operator ID
- Count of findings
- Timestamp

12. Organizational Benefit Statement

This script accelerates detection of malicious persistence, reducing attacker dwell time and improving system integrity.

SOP 5 – Quick Triage Summary

Script Name: Quick Triage Summary **Category:** IncidentResponse

1. Purpose

This script performs a rapid triage of a system, collecting key indicators of compromise and system health to support fast decision-making during an incident.

2. Scope

- Windows servers and workstations
- Used during early IR phases

3. Definitions

- Triage**:** Rapid assessment of system state.

4. Preconditions

- Local admin rights recommended.
- System must be reachable.

5. Required Inputs

- None (full triage)

6. Procedure Steps

1. **System Info Collection**
    - OS version, uptime, logged-in users.
2. **Process Snapshot**
    - List running processes with command lines.
3. **Network Snapshot**
    - Active connections and listening ports.
4. **Service Snapshot**
    - Auto-start services.
5. **Event Log Summary**
    - Recent critical and error events.
6. **Suspicious Artifact Detection**
    - Flag anomalies.
7. **Output Formatting**
    - Present structured triage report.

8. **Logging**
    - Log operator and timestamp.

7. Expected Output

- A comprehensive triage summary.

8. Post-Execution Validation

- IR team may escalate to deeper analysis.

9. Error Handling

- Access denied
- Missing components
- Partial data retrieval

10. Security Considerations

- Triage data may contain sensitive information.
- Must be handled securely.

11. Audit Logging Requirements

- Operator ID
- Summary metadata
- Timestamp

12. Organizational Benefit Statement

This script provides a rapid, auditable snapshot of system health and potential compromise indicators, accelerating IR decision-making.