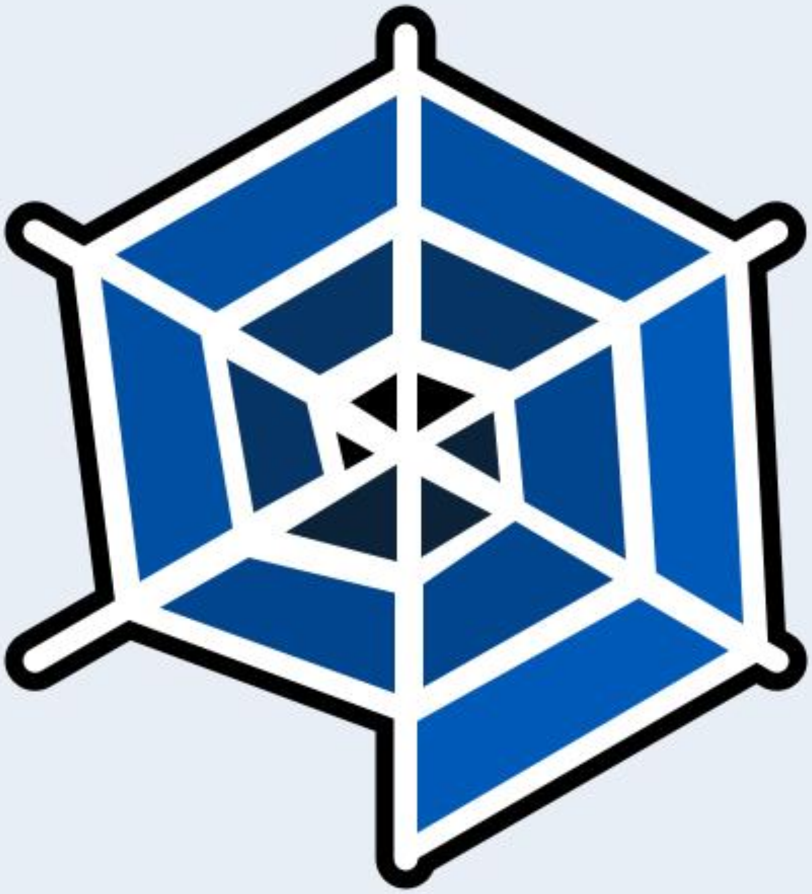

OPERATIONAL DATA TEMPLATE

MITRE | Engage™

This page intentionally left blank

Table of Contents

1 Foreword

The following is a template of the type of information the MITRE Engage™ team captures for a given operation. Adapt and build on this template as needed in your organization.

1.1 A Brief (but important) Note on Operational Security (OPSEC)

When capturing operational data, it is essential to define clear operational security (OPSEC) protocols to protect this data. Adversary engagement operations, by nature, assume a presumption of compromise mentality. Therefore, extra care should be placed to protect sensitive operational details appropriately. At MITRE, we password protect this data, keeping a small list of individuals with need-to-know access to any given operation. Sensitivities will vary across operations, so defining the OPSEC requirements for each operation is essential. For example, unattributed operations run in isolated environments for research purposes may be considered low sensitivity. Alternatively, insider threat operations run in integrated environments on the production network may be considered high sensitivity. High sensitivity data may require offline storage and limited, need-to-know access lists. Defining clear operational protection levels and protocols and ensuring that all parties know which level is assigned to a given operation is essential.

2 Operation Details

This section includes high-level details about the operation.

Operational Partners	Names/contact info for operational partners
Sharing Restrictions	Any sharing restrictions
Rules of Engagement	Link to Rules of Engagement document (this document should include all gating criteria and appropriate response policies)
Engagement Narrative	Description of engagement narrative
Persona(s)	Brief description of persona (may include link to completed Persona Profile worksheet)
Dates	Operation dates
Attribution Information	Is this op attributed to your organization? If not, who is this operation attributed to?
Malware Analysis	Links to any relevant malware analysis

3 Roles

This section includes information about the operators assigned to each role.

Depending on available resources and size of the operation, one person may fill multiple roles. Multiple people can also split a role. However, it is recommended that a primary point-of-contact (POC) is established for each role.

Role	**Responsibilities**	**Name**	**Contact Information**	**Notes**
Op Stakeholders	Any relevant POCs who are not directly on the op team but may be needed for input during the operation (i.e. when a gating criterion is crossed). Examples include legal counsel, CISO, relevant vendor support POC, etc.			
Team Lead	Responsible for decisions that need management approval, require coordination with other entities in the organization, or necessitate visibility across multiple engagement operations			
Op Coordinator	Day-to-day coordination for a single operation to ensure forward progress and clear any roadblocks			
Reverse Engineer	Provide expertise and analysis related to malware introduced into the engagement environment			
Threat Analyst	Gather threat intelligence about the adversary, constructing Persona Profile(s) for the operation, and for attribution analysis of collected data			
Operational User	Engage with the deceptive assets to generate user activity based on Persona Profile(s)			
System Administrator	Test, build, and configure the environment (engagement environment, collection system, and analysis system)			
Blue Team	Analysis of the data obtained from the operation			
Red Team	Test the engagement environment, collection system, and analysis system			

4 Environment

The environment is made up of three systems: the collection system, the engagement environment, and the analysis system. The collection system is the set of systems used to gather artifacts and other data from an operation to monitor the engagement. The engagement environment is the set of carefully tailored, highly instrumented systems designed on an engagement-by-engagement basis as the backdrop to the engagement narrative. It is the actual environment that the adversary will operate in. The analysis system is the set of systems used to review and analyze data collected in the collection system.

This section includes relevant information for operators to understand the layout of these three deployed systems.

Collection System Diagram	Link to collection system diagram
Engagement Environment Diagram	Link to engagement environment diagram
Analysis System	Description and relevant information regarding accessing analysis system

4.1 Engagement Systems

This section includes relevant information for each machine present in the engagement environment. It may be useful to include similar information for machines in the collection and analytics systems.

Machine	**Type**: **Asset #**: **Deployed Image**:
Networking Information	
Hostname	
Accounts (username/password)	
Custom Software Installations	
Custom Software Modifications	
Instrumentation Software	

5 Operation Events

5.1 Engagement Activities

This section tracks the various deceptive activities the operator deploys and their implementation details.

Engage Activity Name/ID	Implementation Details	Notes

5.2 Adversary Timeline

This section tracks adversary activity in the engagement environment

Datetime (UTC)	Observation Details	How was this observed	ATT&CK Technique

5.3 Malicious Timeline

This section tracks malicious files added to the engagement environment

Datetime (UTC)	Hash	Filename	Location	Notes

5.4 User Activity

This section includes a log of manual or automatic actions that occur in the engagement environment. Logging this activity is essential to maintain operational awareness and consistency throughout an operation.

Date/Time	Operator Name or Automated Tool	Description

6 Analysis

6.1 Useful Commands

This section contains any useful queries used when reviewing operational data in a database.

Query	Description

6.2 Analyst Notes

This section captures important analysis notes.

Date	Time	Analyst	Notes

7 Useful Files

This section contains a list of all specialized files used in the collection system, engagement environment, and analysis system. It is recommended to use source control to manage these files. If using source control, include a link to the specific commit version of the deployed file.

7.1 Configuration Files

This section contains information about deployed configuration files in the engagement environment.

File Link	Deployed Location	Description

7.2 Scripts

This section contains information about useful scripts used either in the analysis or collection environment.

File Link	Description

8 Malware (if applicable)

This section includes information about the malware sample used if this is a self-infection operation

Hash	**Sample hash**
Malware POC	**Who identified the sample? Who conducted initial analysis?**
Malware Origin	**Where was the malware sample obtained?**
Why is this malware interesting to us?	**What about this malware made it interesting enough to run (or was it the campaign/actor behind it that was interesting)?**
Introducing to victim host	**How malware needs to be introduced to the host so it executes properly**
Executing the malware	**How to properly execute malware so it runs**
Persistence	**How the malware persists across logout/reboot (which folder or reg key or however else it does it)**
Expected Behavior	**What we expect to see if the malware runs properly.**
Detecting Proper execution and behavior	**How we know things executed properly without compromising the operation**
Requirements	**Any system or network requirements for the malware to execute properly**

8.1 Capability Tracker (observed during operation)

This section tracks the capabilities of each piece of malware observed during an operation.

Capability	**Confirmed** This capability was seen successfully	**Attempted** This capability wat attempted unsuccessfully	**Denied** This capability was blocked by something in the environment	**Inconclusive** No definite observations	**Risks** List risks this capability poses to maintaining operational safety	**Details** Other notes
C2 Infrastructure Location						
Commonly Available Tools						
Custom Tools						
Disable Endpoint Protection						
Exfiltration						
Host Identifier Tracking						
Keylogging						
Lateral Movement						
Password Dumping						
Persistence						
Privilege Escalation						
Screenshots						

Capability	**Confirmed** This capability was seen successfully	**Attempted** This capability wat attempted unsuccessfully	**Denied** This capability was blocked by something in the environment	**Inconclusive** No definite observations	**Risks** List risks this capability poses to maintaining operational safety	**Details** Other notes
User History Dumping						

9 Miscellaneous

9.1 Lessons Learned

This section contains lessons learned during an operation to inform future activities. These lessons learned can inform future operations or be used to improve a running operation.

Event Description	Mitigation/Action/Refinement
What happened	What could be done differently, better, etc. in the future

9.2 Open Questions

This section contains a list of questions for the team. Tracking these questions, and answers can save time in future operations.

Contact	Target	Question
Who asked this question/ Who can clarify or elaborate on it	Who is this question mainly directed at/ Who might be able to investigate or answer it	