INCIDENT RESPONSE SCOPING

# INITIAL QUESTIONS

#### Organization and key members?

#### When was the incident reported?

#### Who is assigned to the engagement?

#### Who reported the incident? (Contact details)

#### Who is aware of the incident?

#### Is the incident ongoing?

#### Are there “need-to-know” requirements needed for the incident? (Legal privilege, limit public knowledge)

#### What are the objectives?

# DETECTION

*Try to convert all times into UTC or at the very least state specific time zones*

#### When was the incident detected

#### Who detected the incident? (Contact details)

#### How would you categorize the detection? (mass malware, phishing, failed login, etc.)

#### What tool, process or scan identified the incident?

#### Was the detection through a manual or automated process?

#### What information was part of the initial detection?

# IMPACT

#### What was the type and number of resources affected?

#### Is there a unique identifier for the affected resources? (Host naming, asset tag, static IP or range)

## System Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hostname/Domain** | **Location** | **OS** | **Function** | **IP address** | **User/Admin** | **Backups?** | **Isolated?** | **Alerts** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# ACTIONS

#### Who has accessed the systems since detection? What was done?

#### Any remediation already done? (Block listing, firewall changes)

# ENVIRONMENT

#### How many endpoints in the organization? (Servers, Workstations)

#### How many users?

#### Capabilities of the security/response team?

#### Toolset

* Network/Firewall
* EDR/AV
* DNS
* SIEM/Central Logging
* Asset Management
* DLP
* Mail Protection

# NETWORK

#### Suspicious IP’s or domains identified?

#### Availability of network monitoring?

#### Remediation steps already taken?

#### Network logs being preserved? (SIEM, Console retention)

#### Network diagrams or documented configurations?

# MALWARE

#### Date/Time of detection

#### How malware was detected

#### List of systems where it was found

#### Name of the file and file path

#### Is the malware currently active or showing active connections?

#### Has malware been quarantined or separately preserved?

#### Status of analysis at this time?

# NEXT STEPS