MS-ISAC®

EI-ISAC®

Incident Handling Worksheet

Please fill out the first page of this document as well as the page that corresponds with the type of incident currently affecting your organization. If your incident falls outside of the listed categories, please list a detailed summary on the Other page. Once you have completed this form, please email it back to us at CERT@cisecurity.org.

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Is this elections related?

○ Yes ○ No

Go to:

- Incident Details
- Ransomware
- Suspicious Network Activity
- Malware
- Compromised System
- Other Incident

How was the incident discovered initially?

Other

If other, please describe:

Are you currently working with any 3rd party vendors on this incident?

○ Yes ○ No ○ Unknown

Does your organization currently have cyber insurance?

○ Yes ○ No ○ Unknown

Has any remediation been performed on the affected systems?

○ Yes ○ No ○ Unknown

Have mission critical systems been impacted?

○ Yes ○ No ○ Unknown

Has there been a loss of data?

○ Yes ○ No ○ Unknown

Were you running antivirus software at the time of the incident?

○ Yes ○ No

Is there any known Personally Identifiable (PII) or Personal Health Information (PHI) stored on the affected system(s)?

MS-ISAC®

EI-ISAC®

Incident Handling Worksheet

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Go to:

Incident Details

Ransomware

Suspicious Network Activity

Malware

Compromised System

Other Incident

Ransomware COMPROMISE-SPECIFIC QUESTIONS

Do you know what ransomware variant has infected your systems?

○ Yes ○ No ○ Unknown

How many systems have been affected?

Are systems still actively being encrypted at this time?

The type of system affected:

Desktop

If other, name the system type:

What operating system version(s) are on the affected systems?

Have you identified how the system was infected?

○ Yes ○ No

Have the affected systems been disconnected from the network?

○ Yes ○ No ○ Unknown

Are backups available for the affected systems?

○ Yes ○ No ○ Unknown

Have the integrity of your backups been confirmed?

○ Yes ○ No

Are any network-attached backups currently being separated from the infected network?

○ Yes ○ No

Was the infection limited to a single subnet?

○ Yes ○ No ○ Unknown

MS-ISAC®

EI-ISAC®

Incident Handling Worksheet

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Go to:

Incident Details

Ransomware

Suspicious Network Activity

Malware

Compromised System

Other Incident

Suspicious Network Activity COMPROMISE-SPECIFIC QUESTIONS

Briefly describe the suspicious network activity (300 characters):

Please include a summary of the traffic content/payload included in the suspicious traffic (1,000 characters):

The type of system affected is:

Desktop

If other, name the system type:

Is this activity still occurring?

○ **Yes** ○ **No**

Have any steps been taken to block the suspicious activity?

○ **Yes** ○ **No** ○ **Unknown**

If requested, do you have logs of this activity that you could provide to the MS-ISAC?

○ **Yes** ○ **No**

Were any internal anti-virus or firewall alerts generated from this activity?

○ **Yes** ○ **No** ○ **Unknown**

What destination IP(s) and port(s) were involved in this activity?

MS-ISAC®
EI-ISAC®

Incident Handling Worksheet

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Go to:

- Incident Details
- Ransomware
- Suspicious Network Activity
- Malware
- Compromised System
- Other Incident

Malware COMPROMISE-SPECIFIC QUESTIONS

Have you identified which malware variant this is?

○ Yes ○ No ○ Unknown

Approximately how many systems have been infected by the malware?

Through what method was the malware infection first detected?

The type of system affected is:

Other

If other, name the system type:

What operating system version(s) are on the affected systems?

Was the infection limited to a single subnet?

○ Yes ○ No ○ Unknown

Are any of the systems affected public-facing or have remote-login capabilities?

○ Yes ○ No ○ Unknown

MS-ISAC®

EI-ISAC®

Incident Handling Worksheet

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Go to:

Incident Details

Ransomware

Suspicious Network Activity

Malware

Compromised System

Other Incident

Compromised System COMPROMISE-SPECIFIC QUESTIONS

What date/time was the compromise detected?

The operating system(s) and version(s) installed are:

What user account(s), if any, have been compromised?

What services were running on the compromised system(s)?

Are firewall logs of this activity available for analysis?

○ Yes ○ No ○ Unknown

How often are software and operating system patches deployed to systems in the network?

What method is currently being used to manage credentials for any affected systems? (i.e. "Active Directory")

MS-ISAC®

EI-ISAC®

Incident Handling Worksheet

Incident Details

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

Affected Entity:

Reporting Entity:

Point of Contact information:

NAME

EMAIL

PHONE

ALT. PHONE

Go to:

Incident Details

Ransomware

Suspicious Network Activity

Malware

Compromised System

Other Incident

Other Incidents

If an incident has occurred that falls outside of those listed on the other pages of this document, please fill out this section with a summary of the event while also including the following information: total number of systems and/or users affected and any attempts at remediation that have occurred thus far.

Please be as detailed and concise as possible: