INCIDENT SUMMARY CHECKLIST

# INITIAL QUESTIONS

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

When was the incident reported?

When was the incident detected?

Who is documenting this checklist?

Who reported the incident? (Contact details)

Who detected the incident? (Contact details)

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

What was the type and number of resources affected?

What tool, process or scan identified the incident?

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

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

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)

# DETECTION

Was the detection through a manual or automated process?

What information was apart of the initial detection?

Has someone validated the data to ensure confidence it is an incident?

# SYSTEM DETAILS

*Recommend gathering details in a spreadsheet or similar report to handle multiple systems*

Physical Location

Asset Tag

Make and Model

OS Installed

Primary function

Responsible administrator and/or user

IP address

Hostname/Domain

Critical information on the system

Backups available?

Still connected to the network?

Significant alerts?

Remediation already done?

# NETWORK

Suspicious IP’s or domains identified?

Availability of network monitoring?

Remediation steps already taken? (Block listing, firewall changes)

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?

## REFERENCES

Anson, S. (2020). *Applied Incident Response*. Wiley & Sons Canada, Limited, John.

Luttgens, J. T., Pepe, M., & Mandia, K. (2014). *Incident Response & Computer Forensics* (3rd ed.). McGraw-Hill Education.