

# Email Security Incident Detection and Analysis

**Note:** Prior to starting the detection and analysis of network security incidents, Section 1 and Section 2 must be filled with required information.

## Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

## Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			
<i>Additional Details (If any):</i>			

### Section 3: Detection of Email Security Incidents

Indications	Type of Email Security Incident	Detected By	System Details

## Section 4: Analysis of Email Server Logs

### ☐ Analyzing Email Logs

#### ☐ Examining System Logs

Technique/tools used:

Results obtained:

#### ☐ Examining Network Equipment Logs

Technique/tools used:

Results obtained:

#### ☐ Examining Linux Email Server Logs

Technique/tools used:

Results obtained:

☐ **Examining Microsoft Exchange Email Server Logs**

Technique/tools used:

Results obtained:

☐ **Analyzing SMTP Logs**

Technique/tools used:

SMTP status code detected:

Results obtained: