

The Golden Hour of Incident Response

General Information

Incident Number	Date of Incident	Primary Contact

IH&R Team Information

Name	Email Address	Office Contact

Questions that need to be answered

Considering the Golden Hour approach, the organization affected by the incident should answer the following questions:

Who is Responsible for the Incident?	
Which Communication Strategy is Used?	
What are the Actions Taken to Resolve Incident?	
Who will be Affected by the Incident?	

What are the Additional Intelligence Sources Utilized?	
What is the Effect and Impact of Incident?	
What Procedure will be used to Record Log Data?	
What can be Identified by Analyzing the Event logs?	
How are Partners, Customers, and Stakeholders being Notified about the Incident?	

Performing a trial run

Conduct the trial runs for security incidents to establish an opportunity for the IH&R team to practice their actions for the Golden Hour period.

Date:	
Name of the Responder:	
The Purpose of Trail Run:	
Security Errors Fixed:	
Severity of the Incident:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Critical
Previous System Status:	
Current System Status:	
Differences:	
Remarks:	

Practice incident simulation

Practice the opportunity of Golden Hour with a simulation process to help your organization manage a real situation rapidly by limiting damages.

Implementation of Active Monitoring:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Use of Process-Oriented Approach:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Resolved Root Cause of the Incident:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Develop an Awareness Culture Across the Organization:	<input type="checkbox"/> Yes <input type="checkbox"/> No