

**SOC - INCIDENT REPORT**

**INCIDENT REPORT**

**\*\* 1288479 \*\***

## Overview

Quick Summary.

### Incident details

ATTRIBUTE	VALUE
TYPE	case
LABEL	manual_incident
ID	1288479
NAME	Test Events
DESCRIPTION	This is a test container (used for phantom_report.py script).
OWNER	Julien Bernard
CLOSING OWNER	Julien Bernard
SEVERITY	high
SENSITIVITY	amber
CURRENT PHASE	Step #1: Incident Response Start (L1)
STATUS	closed
FINAL STATUS	N/A
ARTIFACTS	0
CREATED	2018-05-28T13:06:59.927359Z
CLOSED	2018-05-28T13:11:08.472503Z
UPDATED	2018-05-28T13:11:08.465828Z

## Details

Quick Summary.

### Activity timeline

↪ 2018-05-28 @ 13:07:44	Julien Bernard	COMMENT
This is a comment added in the "COMMENT" field (Activity TAB)		
↪ 2018-05-28 @ 13:08:17	Julien Bernard	NOTE
Phase: → Step #1: Incident Response Start (L1)		
First NOTE		
This note has been added in the NOTE section (Artifacts / Notes)		
↪ 2018-05-28 @ 13:09:06	Julien Bernard	PHASE
Phase: → Step #2: Initial Investigation (L1)		
Task: → #2.2 - Identify Business Unit and Business Group		
Second NOTE		
This NOTE has been added from the Case Template / Tasks section		
↪ 2018-05-28 @ 13:09:27	Julien Bernard	PHASE
Phase: → Step #2: Initial Investigation (L1)		
Task: → #2.2 - Identify Business Unit and Business Group		
3rd Note		
Another note added for the same TASK.		
↪ 2018-05-28 @ 13:09:44	Julien Bernard	PHASE
Phase: → Step #2: Initial Investigation (L1)		
Task: → #2.2 - Identify Business Unit and Business Group		
Closing TASK		
Note added for the task closure.		
↪ 2018-05-28 @ 13:10:00	Julien Bernard	PHASE

Phase: → Step #2: Initial Investigation (L1)  
Task: → #2.3 - Identify Asset(s)

Another NOTE

Another NOTE added in a case/task

→ 2018-05-28 @ 13:10:14 Julien Bernard COMMENT

New COMMENT added (comment section)

→ 2018-05-28 @ 13:10:20 Julien Bernard COMMENT

Another comment!

→ 2018-05-28 @ 13:10:45 Julien Bernard NOTE

Phase: → Step #3: Incident Handling (L2)

Note

Another NOTE added in the NOTES section (not in the case/tasks)