# **Cyber Simulation Exercise Report Sample**

## Executive Summary

Describe the exercise and activity at a high level, along with a brief summary of the findings to enable a quick read with details below for those interested in reading further…

## Simulation Exercise Details

**Exercise Objective**

Simulation exercise object goes here

**Exercise Lead and Team**

This exercise was led by <name of exercise lead, title, department>

The exercise team consisted of:

<name of team member, title, department>

<name of team member, title, department>

<name of team member, title, department>

…

**Exercise Scenario**

Simulation exercise scenario goes here

**Inject Development Details**

Discuss the development of the events/injects

For example:

Developed injects based on detailed descriptions of organizational processes utilizing input from exercise team members regarding their functional areas and processes

* <SPECIFIC NUMBER> of independent injects used for the simulation
* Each inject consisted of multiple parts
* Simulated injects sent from Exercise Lead/ Planner
* Meant to mimic real breach scenarios
* Injects clearly marked EXERCISE, so recipients would not be confused

**Exercise Execution**

Discuss the start and end time of the exercise

Detail the kick-off inject

For example:

The exercise began 9am on Monday 9-5-19 with INJ-01-01

* INJ-01-01 - is a complaint from customer XYZ regarding a malfunctioning product ABC
* The exercise continued over a 3-day period, ending on Thursday 9-8-19
* Additional details regarding exercise execution

**Process Issues/Gaps Identified**

Discuss the results of the exercise in terms of process gaps identified (use charts/graphs when possible)

A picture containing screenshot

Description automatically generatedFor example:

* Formal process gap in the communication of security incidents from receivers (customer-facing organizational functions) to internal cybersecurity team for further investigation
  + No formal method to discern security incidents from general customer complaints

**Summary/Next Steps**

Summarize the exercise and discuss the plan to address the gaps from the previous section. Can be modified depending on the audience being addressed.

***Ken Zalevsky***

*CEO, Vigilant Ops*

*Former Head of Medical Device Cybersecurity, Bayer*

*Founded in 2019, Vigilant Ops is an innovator in the medical device cybersecurity industry. Led by seasoned medical device cybersecurity experts with more than forty years of combined experience, Vigilant Ops provides medical device manufacturers and hospitals with unprecedented insight into device risk profiles, enabling proactive management of threats before they impact the quality of patient care.*

For more information about Vigilant Ops or the InSight Platform, please visit our website at [www.vigilant-ops.com](http://www.vigilant-ops.com)

Or drop us an email at: [inquiries@vigilant-ops.com](mailto:inquiries@vigilant-ops.com)