Information Security

**CSIRT Table Top Exercise After Action Report**

11/02/2017

**Version 1.0**

**Prepared by:**

**Contributors:**

## Document Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Editor** | **Change Description** |
| 11/02/2017 | 1.0 |  | Create document |
| 11/21/2017 | 1.1 |  | Minor adjustments and corrections |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document Revisions 2](#_Toc518561037)

[Exercise Overview 4](#_Toc518561038)

[Exercise Logistics 5](#_Toc518561039)

[Participating Organizations 5](#_Toc518561040)

[Exercise Design Summary 5](#_Toc518561041)

[Exercise Purpose 5](#_Toc518561042)

[Goals and Objectives 6](#_Toc518561043)

[Scenario Summary 6](#_Toc518561044)

[Scenario Timeline 7](#_Toc518561045)

[Inject Observations 7](#_Toc518561046)

[Scenario Timeline with Results 10](#_Toc518561047)

[Hot Wash Feedback 10](#_Toc518561048)

[Survey Feedback 11](#_Toc518561049)

[Lessons Learned 11](#_Toc518561050)

[Appendix A: *Participant Sign in Form* 11](#_Toc518561051)

[Appendix B: *Participant Feedback Summary* 12](#_Toc518561052)

[Appendix C: *Acronyms* 15](#_Toc518561053)

# Exercise Overview

In order to have an effective Computer Security Incident Response Team (CSIRT) capability in any organization a plan must be in place. The plan is only effective if all members of the process are working together and understand their role. One way to ensure this happens is utilizing a table top exercise (TTX). A TTX is designed to incorporate a preplanned and fully scripted set of scenarios’ that test the current people capabilities and process flow. TTX are an easy way to train the entire team that would be involved in a real incident as well as identify areas for improvement.

The TTX was a joint effort between the Crisis Prevention & Management Information Security teams. The ACME team based the TTX off a set of industry best practices. Specifically, The “[Cyber Exercise Playbook](https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf)” by Jason Lick of MITRE. The playbook provides an overview of the cyber exercise process from inception to reporting. Per the playbook the Information Security team chose the Table Top exercise illustrated in the figure below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Style | Description | Complexity | Timing | Resources | Matches |
| Table Top | Paper-driven exercise with injects scripted by exercise planners and delivered via paper (cards/ discussion). | This type of exercise can be planned and executed quickly, depending on the number of organizations involved. | **Planning:** 1–2 months  **Execution:** 1–3 days | Limited resources needed, depending on number of organizations | Organizations new to exercises and to assessing organizational IA objectives.  Organizations that need to validate processes/ train personnel in-between other exercises. |

## Exercise Logistics

* 3-hour session
* Tuesday, October 17, 2017 – Building X 8:00 am – 12:00 pm
* 1 scenario – The scenario will be a choose your own adventure exercise, with rewards (hints) for following the correct processes and procedures. The scenario will be easy at first to get the participants in the correct frame of mind. As the scenario progresses it will start to push the participants and possibly expose gaps in current people, process, and technology.

## Participating Organizations

* Information Security
* Crisis Prevention & Management
* Legal / Privacy
* Internal Audit
* Enterprise Risk Management
* Physical Security
* Strategic Communication
* Marketing
* Infrastructure & Operations

A complete list of all individuals that participated in the TTX can be found in Appendix A: Participant Sign in Form

# Exercise Design Summary

## Exercise Purpose

The purpose of the TTX was to practice incident response procedures related to Information Security in order to identify potential weaknesses in people, process, and technology. Another helpful byproduct of hosting the exercise is to educate and inform departments of the correct incident response procedures.

## Goals and Objectives

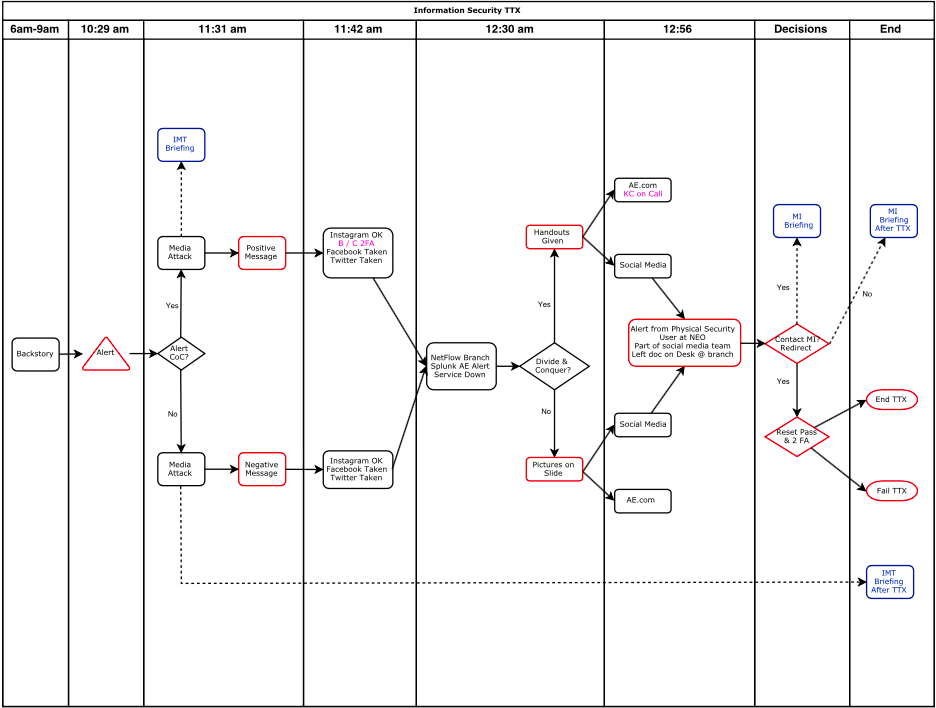
|  |  |
| --- | --- |
| Goal | Establish a baseline for future exercises; raise CSIRT awareness and skill. |
| Objectives | * Expose and correct weaknesses in CSIRT processes and playbooks. * Assess the effectiveness of CSIRT’s incident reporting and communication channels. * Expose any gaps in data sources that could assist in the investigation. * Determine the effectiveness of the various training given to the participants. * Assess the participants’ ability to detect and response to threats during the exercise. * Assess ACME’s guidelines for fixing issues (post-exercise). * Enhance overall Information Security awareness and coordination. |
| Lesson Learned | Focus on what worked well and what requires improvement. |
| Future | Future exercises should enhance training by including live events. |

## Scenario Summary

Following industry best practice (MITRE Cyber Exercise Playbook) Information Security created a scenario with a choose your own adventure style twist. The scenario focused on situations that have happened at ACME in past incidents. Information Security also focused on incidents that have occurred within the past few quarters within the larger Information Industry. These incidents included the following;

* Social media account takeover by miscreants
* External media questioning
* Malware outbreak
* Normal daily alerts
  + Compromised asset
  + Data exfiltration
* Physical security intrusion
* Major service offering outage (Customer Portal)

## Scenario Timeline



# Inject Observations

|  |
| --- |
| Inject Number: 1 Slide 1a |
| Inject Description: [CyberIntel Confidential] ACME theme Loki Malspam |
| Expectation: Check ACME systems for indicators of compromise, recognize this as an incident that has happened in the past with the typo squatting domain, and open a case in the Incident Response Platform (IRP). |
| Outcome Positive:  Outcome Negative: |
| Observation and notes: |

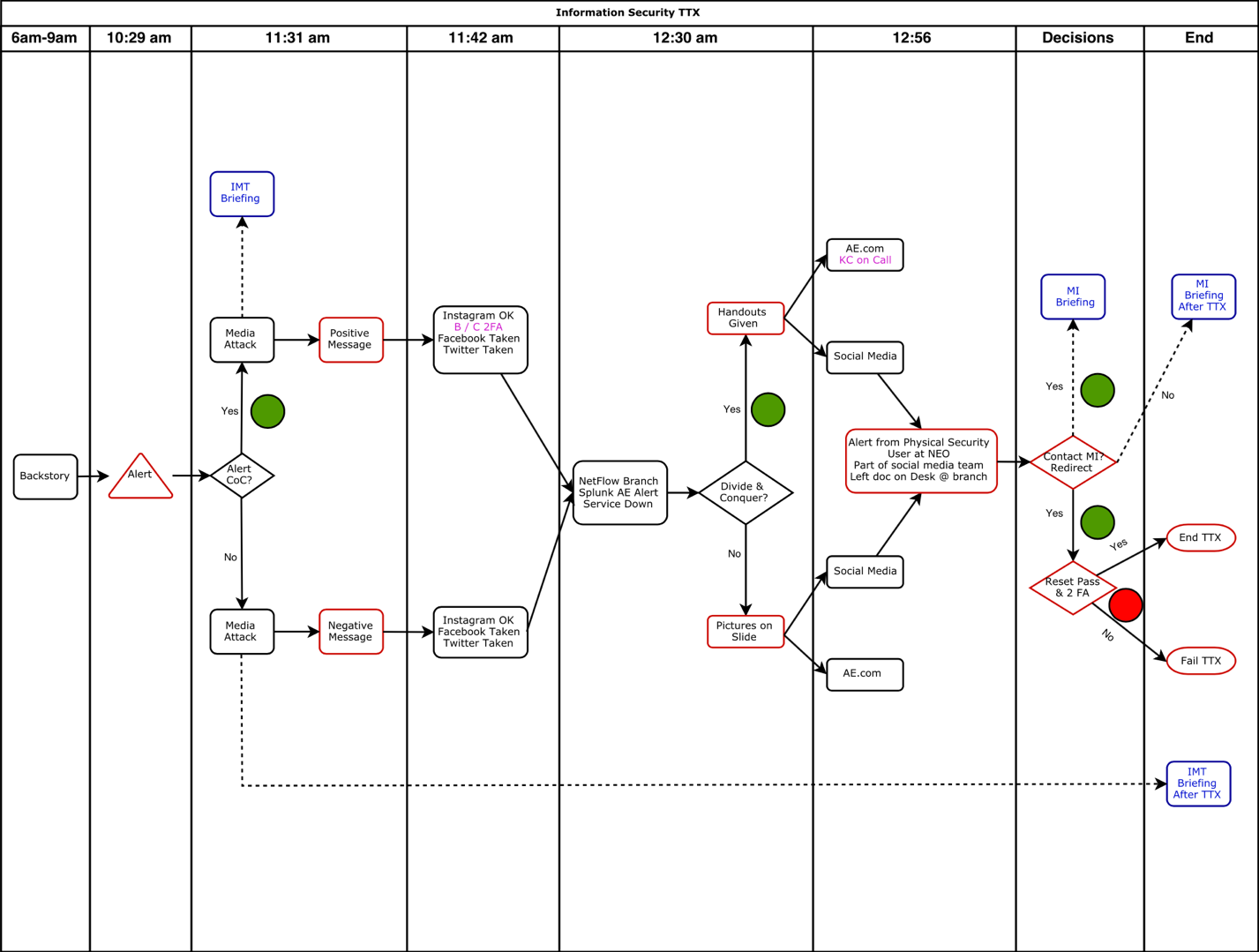
|  |
| --- |
| Inject Number: 2 Slide 4 |
| Inject Description: InfoSec receives notification to investigate |
| Expectation: The InfoSec team should follow the chain of command per the CSIRT Handbook. |
| Outcome Positive:  Outcome Negative: |
| Observation and notes: |

|  |
| --- |
| Inject Number: 3 Slide 8 |
| Inject Description: NetFlow, SIEM, website down alerts |
| Expectation: The InfoSec team should divide and conquer the alerts for investigation. |
| Outcome Positive:  Outcome Negative: |
| Observation and notes: |

|  |
| --- |
| Inject Number: 4 Slide Social A |
| Inject Description: Physical security alerts and Norman Shady information |
| Expectation: The InfoSec team should invoke the Incident Management Team (IMT). |
| Outcome Positive:  Outcome Negative: |
| Observation and notes: |

|  |
| --- |
| Inject Number: 5 Slide Social Debrief |
| Inject Description: Did the InfoSec team reset the password and enable 2FA? |
| Expectation: The InfoSec team should not only reset the social media account passwords but also enable two factor authentication for the accounts. |
| Outcome Positive:  Outcome Negative: |
| Observation and notes: |

## Scenario Timeline with Results



# Hot Wash Feedback

|  |
| --- |
| Hot Wash Questions |
| Any concerns for ACME as a whole? |
| Any issues with procedures / documentation? |
| In what ways did the involvement of the media change the dynamics of the incident? |
| How would the media have gotten involved? |
| General Feedback |

# Survey Feedback

|  |
| --- |
| Survey Questions |
| What should a future TTX look like or any other improvements? |
| What did you like about the TTX? |
| Any other comments? |

# Lessons Learned

Information Security has compiled the following list of recommended action items to help improve future table top exercises:

# Appendix A: *Participant Sign in Form*

# Appendix B: *Participant Feedback Summary*

1. The objectives of the TTX, as started at the beginning of the training, were accomplished.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The TTX scenario was plausable and realistic.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The TTX material (i.e., WebApp presentation, handouts, etc.) were useful for the TTX discussions.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The facilitator(s) was knowledgable about the material, kept the exercise on target, and was sensitive to the group dynamics.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. There were enough activities/issues for the froup to work on during the TTX.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. Participation in the exercise was appropriate for someone in my position.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The participants included the right people in temrs of level and mix of disciplines.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The TTX contributed to my understanding of ACME’s CSIRT proces and my role on the team.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. The room layout was conducive for the TTX.

* Strongly agree
* Somewhat agree
* Neither agree nor disagree
* Somewhat disagree
* Strongly disagree

1. What should a future TTX look like or any other improvements?

1. What did you like about the TTX?

1. Any other comments?

# Appendix C: *Acronyms*

|  |  |
| --- | --- |
| Acronym | Meaning |
| TTX | Table Top Exercise |
| CSIRT | Computer Security Incident Response Team |
| IRP | Incident Response Platform |
| InfoSec | Information Security |
| IMT | Incident Management Team |
| AAR | After Action Report |
| 2FA | Two Factor Authentication |
| C&C | Command and Control |
| PCAP | Packet Capture |
| SSO | Single Sign-On |