Communications with Stakeholders: A Critical Activity for National CERTs

Cyber Task 1 – Information Sharing

Cyberdrill for Arab Region

Tunisia, May 24, 2016

This session is organized by Intellium and it is structured into three main parts

Cyberdrill Schedule

TIME	ACTIVITY
14:15 – 14:30 (15 minutes)	**Exercise goals and objectives** Introduction to exercises: general instructions and participants ground rules
14:30 – 15:00 (30 minutes)	**Cyber Task 1: ALERT** • Scenario storyline • Exercise
15:00 – 15:15 (15 minutes)	• Key factors for *Alert*

Conductors from Intellium coordinate the drill by providing instructions. Moreover, conductors are available to answer any questions that may arise and will provide final feedback to improve CERT functionalities.

The exercise aims to help the participants improve their communications skills during a cyber crisis

Introduction

Objectives

- Improve the CERT **capability to communicate and coordinate** with relevant stakeholders at national, regional and international level in order to manage cyber emergencies and incidents.
- Explore participants' attitude in understanding how to use **communication and sharing information tools** and **dealing with multiple sources of information** during a cyber crisis.

Format

- Participants will receive **one storyline scenario** designed to simulate the usage of **an ALERT.**
- Exercise activities will be performed in the Survey Monkey platform. Participants are requested to fill in **text boxes** for the exercise.

Assumptions

- CERT has **all communication capabilities and tools** to reach constituency and stakeholders.
- CERT operates in its **typical environment and configuration**, with full access to their typical capabilities, including communication channels to Government, Media, defense, so on.

Context

- This exercise addresses **DO 6 (Information Sharing)**
- Participants are requested to **use real information and/or their professional judgment and knowledge** if the scenario doesn't provide enough information.

After completing the web-based exercise, we will provide specific feedback on how the CERT teams performed

Cyberdrill Format

PARTICIPANTS GROUND RULES

- Participants are divided into **groups** (4-6 members)
- Each **group identifies a team leader and cooperates** to perform exercises
- Participants are requested to **contribute actively** to perform exercises

WEB LINK SCENARIO

- Participants receive **one email from the Survey Monkey Platform** with web link access to the session
- Participants are requested to **submit exercise responses** through the Survey Monkey Platform

WRAP-UP

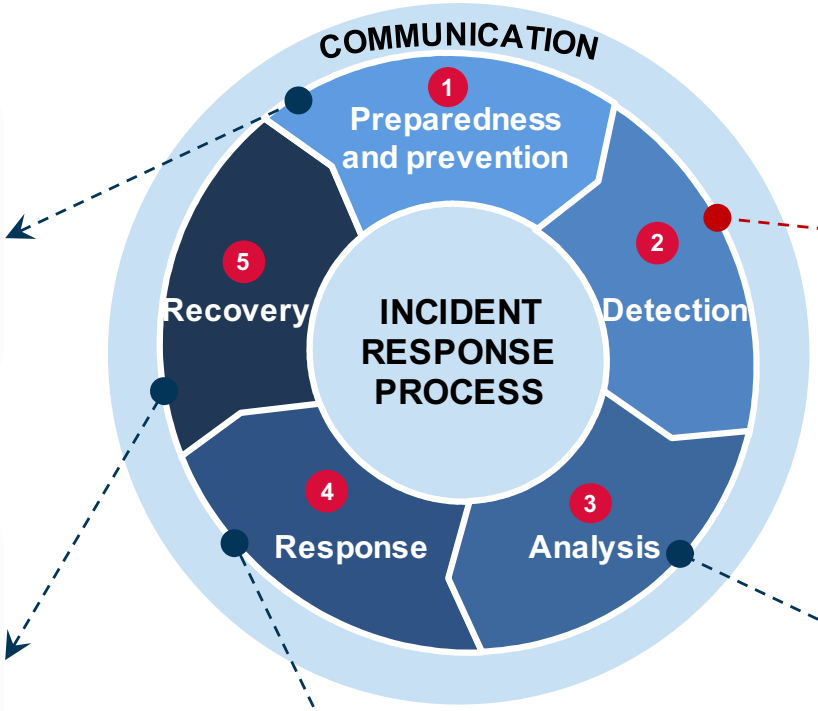
- Outline **key factors** for success in exercises at the end of each exercise
- Feedback and highlights of the **best examples** of the performed exercises as sample for open discussion among participants

There is no single solution and/or answer to the topics and exercise will be discussed. The aim of the exercise is to stimulate participants on identifying several solutions to manage emergencies and crisis.

The exercises are focused on three communications tools related to different step of the incident response process

Communication Tools

NOT EXHAUSTIVE



1
- ARTICLES
- NEWSLETTER
- PERIODIC REPORT
- …

Cyber Task 1 - Today's session

2
- EARLY WARNINGS
- ALERT
- BULLETIN

5
- RECOVERY REPORT
- LESSONS LEARNED
- PRESS RELEASE
- …

3
- INCIDENT ANALYSIS
- VULNERABILITY REPORT
- THREAT REPORT
- …

4
- REPORT
- BULLETIN
- ACTION PLAN
- …

Cyber Task 1: ALERT (30 minutes)

Cyber Task 1: Storyline

During the daily morning review of social media sources the **National CERT** discovers a post on Twitter saying that the **global hacktivist group Synonymous** has posted **data and e-mail traffic from the employees of CREDIT Bank of Salama.**

Information has been posted on the "Synonymous.onion" address on the dark web and a link to their website has been provided.

Rapidly, information on the dark website is **published on the web**. Social media and News broadcasters are **propagating the information to the world** in almost real time.

As the news broadcasters are reporting the Synonymous web posts, the Synomous sends out its first direct **threat and claim** to the Salama government, "*National bank deserves to be punished*".

https://www.surveymonkey.com/r/IntelliumCyberTask1

Cyber Task 1: Exercise

Task description

You as a CERT have to report this threat through an ALERT in order to:

- **Notify stakeholders on the current threat**
- **Suggest actions to prevent potential cyber attacks**

Topics to be addressed

- Stakeholders to be notified
- Format to report the information
- How to handle this threat

https://www.surveymonkey.com/r/IntelliumCyberTask1

Wrap up session - Cyber Task 1: ALERT

Alert

Key factors

1. Classify the information according to the **Information Sharing Protocol** (e.g. for TLP, color)
2. State clearly the **subject (title) of the alert**
3. Identify the **distribution list** that has to be contacted
4. Include **reference number, date and time** including time zone
5. Summarize the **event**, including all **details** that have **to be shared**
6. Suggest **solution** and **course of action**
7. Include **CERT contact information** to request more information

Examples from current exercise

Team 1

Dear CREDIT Bank of Salama,

This is a notification from National CERTos SALAMA, During our Regular Analysis we discovers a post on Twitter belongs to your organization contains sensitive information about your organization.
Analysis:
Ticket Number: ABCD00001
Incident Classification: High
Category: Information Leakage
During our Regular Analysis we discovers a post on Twitter belongs to your organization contains data and e-mail traffic from the employees of CREDIT Bank of Salama.
Impact:
This Leaked data is online and anyone can reach them which may impact your organization and discolse sensitive information against your clients.

Recommendation:
- review all leaked information if it is real data leaked from your organization.
- please change any disclosed credentials.
- block any disclosed Credit cards.
- Do your investigation on how this data leaked.

For any assistance please contact us immediately .
Regards,,
National CERT of SALAMA.
+123 123456789

https://www.surveymonkey.com/r/IntelliumCyberTask1

Please feel free to contact us directly for any further questions or information requests

Francesco Tozzi

Associate

- Mr. Tozzi is an Associate at Intellium and has 10 years' experience in governance and security consulting. His background encompasses ICT and ICS Cyber Security strategies, Security assessment in ICT and ICS environments, strategies for SOC development, compliance evaluation against the international Security standards ISO/IEC 27001, ISO/IEC 22301, NIST 800-53 and NIST 800-82.
- Main areas of expertise include: Cyber Security Strategy and Governance, SOC, Identity and Access Management, Business Continuity and ICS Security.

+39 334 6541428

francesco.tozzi@intelliumgroup.com

Valeria Risuglia

Senior Consultant

- Mrs. Risuglia is a Senior Consultant at Intellium and has 6 years' experience in information security, military, and defence sectors. Her background encompasses ICT Security Governance, ICS Security, National Cybersecurity Strategy, SOC (Security Operations Center) and Security Incident Handling.
- Her experience includes also exercises with the ITU and Italian Armed Forces. She worked as Project Manager for European R&D projects on ICT Security and since May 2014 she is Expert Evaluator for the European Commission.

+39 349 9243403

valeria.risuglia@intelliumgroup.com

INTELLIUM

Focusing on cyber security for critical infrastructures.

Intellium LTD | Charles House, 108-110, Finchley Road - NW3 5JJ LONDON | Tel: +44 20 3290 4911 - E-mail: contact@intelliumgroup.com