# NAMA: Wiraswanti Rismanda Putri

# NO: 20

# KELAS: SIB-4C

# Lab - Incident Handling

## Objectives

Apply your knowledge of security incident handling procedures to formulate questions about given incident scenarios.

## Background / Scenario

Computer security incident response has become a vital part of any organization. The process for handling a security incident can be complicated and involve many different groups. An organization must have standards for responding to incidents in the form of policies, procedures, and checklists. To properly respond to a security incident, the security analyst must be trained to understand what to do and must also follow all of the guidelines outlined by the organization. There are many resources available to help organizations create and maintain a computer incident response handling policy. The NIST Special Publication 800-61r2 is specifically cited in the Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam topics.

## Instructions

### Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Study the following scenario and discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a small, family-owned investment firm. The organization has only one location and less than 100 employees. On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. It was several hours after the worm started to spread before antivirus signatures became available. The organization had already incurred widespread infections.

The investment firm has hired a small team of security experts who often use the diamond model of security incident handling.

**Preparation:**

Answer:

- **Apakah organisasi akan menganggap aktivitas ini sebagai insiden?**
- **Jika iya, kebijakan organisasi apa yang dilanggar oleh aktivitas tersebut?**
- **Tindakan apa saja yang diambil untuk mencegah insiden serupa terjadi lagi atau membatasi dampaknya?**

**Detection and Analysis:**

Answer:

- **Tanda-tanda insiden apa saja yang mungkin dapat diidentifikasi oleh organisasi?**
- **Apakah ada indikator yang membuat organisasi bertindak sebelum insiden benar-benar terjadi?**
- **Indikator apa yang dapat menunjukkan bahwa suatu insiden mungkin sudah terjadi?**
- **Alat tambahan apa yang mungkin diperlukan untuk mendeteksi insiden khusus ini?**
- **Bagaimana tim memprioritaskan respons terhadap insiden ini?**

**Containment, Eradication, and Recovery:**

Answer:

- **Strategi apa yang perlu diambil organisasi untuk mengendalikan insiden ini? Mengapa strategi ini lebih disukai dibandingkan yang lain?**
- **Alat tambahan apa yang mungkin diperlukan untuk menangani insiden tertentu ini?**
- **Siapa saja personel yang akan dilibatkan dalam proses penanggulangan, pemberantasan, atau pemulihan?**
- **Sumber bukti apa, jika ada, yang perlu diperoleh oleh organisasi? Bagaimana cara mendapatkan bukti tersebut? Di mana bukti akan disimpan dan berapa lama harus disimpan?**

**Post-Incident Activity:**

Answer:

- **Bagaimana cara mencegah kejadian serupa terjadi lagi di masa depan?**
- **Apa yang bisa dilakukan untuk meningkatkan deteksi terhadap insiden serupa?**

## Scenario 2: Unauthorized Access to Payroll Records

Study the following scenario. Discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a mid-sized hospital with multiple satellite offices and medical services. The organization has dozens of locations employing more than 5000 employees. Because of the size of the organization, they have adopted a CSIRC model with distributed incident response teams. They also have a coordinating team that watches over the security operations team and helps them to communicate with each other.

On a Wednesday evening, the organization’s physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The security teams practice the kill chain model and they understand how to use the VERIS database. For an extra layer of protection, they have partially outsourced staffing to an MSSP for 24/7 monitoring.

**Preparation:**

Answer:

- **Apakah organisasi akan menganggap aktivitas ini sebagai sebuah insiden? Jika iya, kebijakan organisasi mana yang dilanggar oleh aktivitas ini?**
- **Tindakan pencegahan apa yang telah diterapkan untuk mencegah jenis insiden ini terjadi atau untuk membatasi dampaknya?**

**Detection and Analysis:**

Answer:

- **Apakah ada pendahulu dari insiden ini yang bisa dideteksi oleh organisasi? Adakah pendahulu yang cukup signifikan sehingga menyebabkan organisasi bertindak sebelum insiden terjadi?**
- **Alat tambahan apa yang mungkin diperlukan untuk mendeteksi insiden khusus ini?**
- **Indikator apa saja yang bisa dideteksi oleh organisasi terkait insiden tersebut? Indikator mana yang dapat menimbulkan pemikiran bahwa insiden mungkin telah terjadi?**
- **Bagaimana tim akan menentukan prioritas dalam menangani insiden ini?**

**Containment, Eradication, and Recovery:**

Answer:

- **Strategi apa yang perlu diambil oleh organisasi untuk mengendalikan insiden ini, dan mengapa strategi tersebut lebih unggul dibandingkan pilihan lainnya?**
- **Alat tambahan apa saja yang mungkin dibutuhkan untuk menangani insiden khusus ini?**
- **Personel mana yang akan terlibat dalam proses pengendalian, pemusnahan, dan/atau pemulihan?**
- **Bukti apa yang perlu diperoleh oleh organisasi, jika ada, dan bagaimana bukti tersebut sebaiknya diambil? Di mana bukti itu akan disimpan, dan berapa lama sebaiknya disimpan?**

**Post-Incident Activity:**

Answer:

- **Apa yang dapat dilakukan untuk mencegah kejadian serupa terjadi di masa depan?**
- **Apa yang bisa dilakukan untuk meningkatkan deteksi terhadap kejadian serupa?**