TANGGAP DARURAT MALWARE

Gregorius Hendita AK,S.Si.,M.Cs

ACAD-CSIRT

arthacool@gmail.com

OUTLINE

- Insident Malware
- Tujuan Insiden
- Metodologi
- Penutup

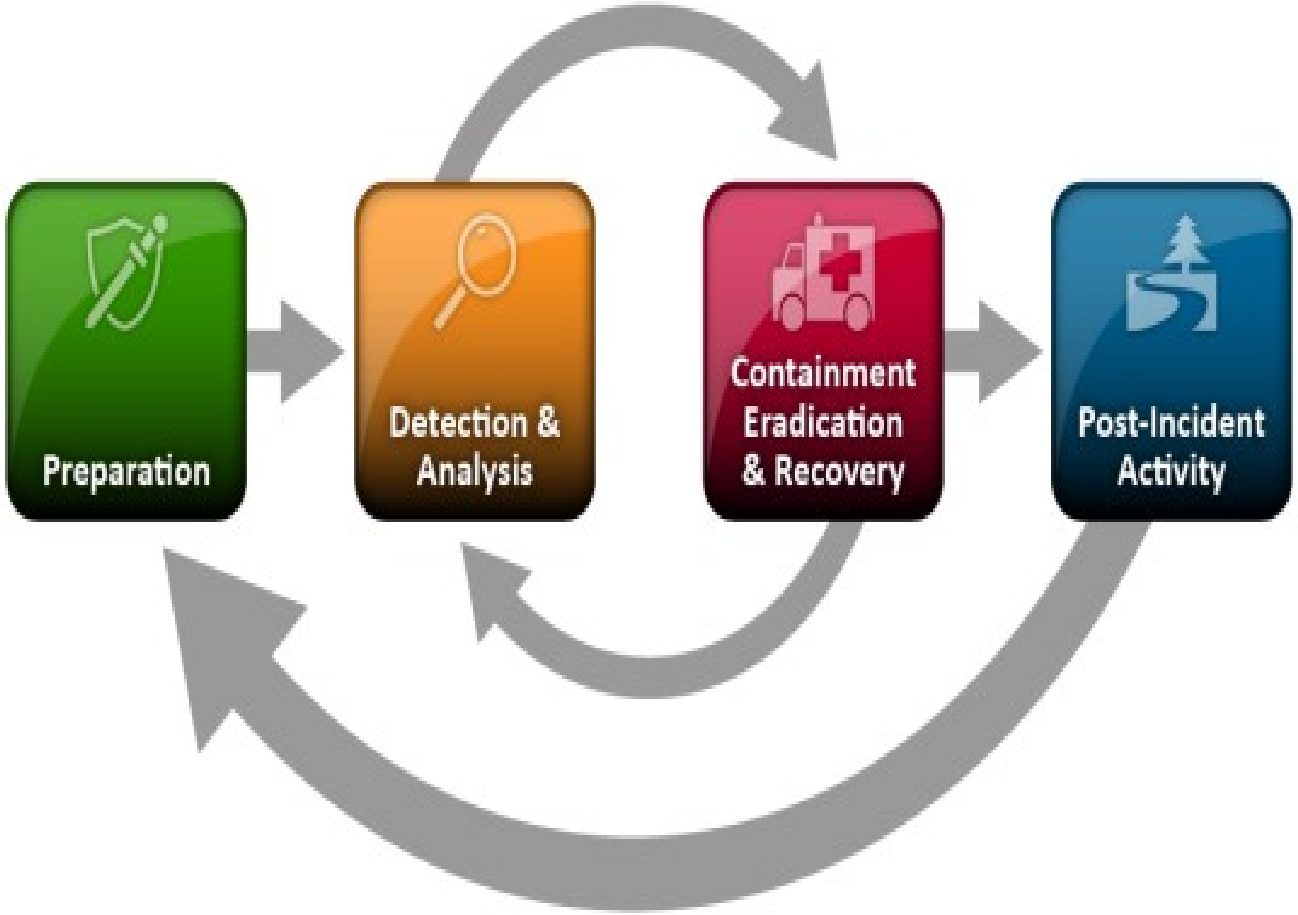
Insident Malware

- Virus
- SpamMail
- Previloge attack, rootkit, intrusion
- Dos Attack
- Unauthorized Access

Tujuan Insiden

- Check Kondisi Komputer
- Data dan informasi yang tepat & akurat
- Meminimalkan attacker pada sebuah operasi sistem.
- Membuat laporan yang akurat beserta rekomendasi insiden.

Metodologi


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Preparation

Persiapan terhadap insiden yang mungkin terjadi dengan berkoordinasi serta berkomunikasi dalam membuat peraturan dan sanksi terhadapnya.

- Skill
- Tools
- Resources
- Technologi

Detection and Analysis

- Melakukan inisialisasi awal bagaimana dalam mendeteksi insiden serta karakteristik malware
- Identifikasi terinfeksi Hosts
- Identifikasi dengan Forensic
- Active Identification
- Manual Identification

Detection and Analysis

- Tahap awal dalam melakukan penanganan
- awal (rekomendasi penanganan insiden) supaya bukti tidak hilang
- Pengaturan stategi terhadap insiden yang terjadi
- Memilih Prioritas untuk Insident Handling Malware
- Analisis Malware

Containment

- Izin/pemberitahuan untuk melakukan Containment
- Isolasi sistem
- Memeriksa gejala kemiripan
- Melihat insiden yang pernah ada (Basis Pengetahuan)
- Melakukan backup semua data pengguna

Eradication

- Memeriksa Integritas Sistem file
- Mengidentifikasi file baru
- Identifikasi gejala lain
- Menganalisis file
- Memeriksa Jaringan
- Memeriksa Backup
- Menemukan Penyebab
- Meningkatkan Pertahanan

Recovery and Lesson Learned

- Validasi sistem
- Pemulihan Operasi
- Pemantauan Sistem
- Tindakan lanjut yang akan diambil
- Penambahan pengetahuan dasar tentang penangan insiden
- Penciptaan signature dan inklusi anti malware

Recovery and Lesson Learned

- Pelatihan untuk tim penanganan insiden
- Memperbarui aturan penyaringan
- Pendidikan bagi penggunan dalam identifikasi Malware
- Peningkatan Pertahanan

Penutup

Terima Kasih

arthacool@gmail.com