Sinopsis

Digital Forensic and Incident Response

Penulis Buku : Gerald Johansen

Pemahaman tentang bagaimana forensik digital terintegrasi dengan respons keseluruhan terhadap insiden keamanan siber adalah kunci untuk mengamankan infrastruktur organisasi Anda dari serangan. Edisi kedua yang diperbarui ini akan membantu Anda menjalankan aktivitas forensik digital dan respons insiden yang mutakhir.Setelah berfokus pada dasar-dasar respons insiden yang penting bagi tim keamanan informasi mana pun, Anda akan melanjutkan untuk menjelajahi kerangka respons insiden. Dari memahami pentingnya hal tersebut hingga menciptakan respons yang cepat dan efektif terhadap insiden keamanan, buku ini akan memandu Anda dengan bantuan contoh-contoh yang bermanfaat. Nantinya, Anda akan memahami teknik forensik digital, mulai dari memperoleh bukti dan memeriksa memori volatil hingga pemeriksaan hard drive dan bukti berbasis jaringan.

Seiring kemajuan Anda, Anda akan menemukan peran yang dimainkan oleh intelijen ancaman dalam proses respons insiden. Anda juga akan mempelajari cara menyiapkan laporan respons insiden yang mendokumentasikan temuan analisis Anda. Terakhir, selain berbagai aktivitas respons insiden, buku ini akan membahas analisis malware, dan menunjukkan bagaimana Anda dapat secara proaktif menggunakan keterampilan forensik digital Anda dalam perburuan ancaman. Di akhir buku ini, Anda akan mempelajari cara menyelidiki dan melaporkan pelanggaran keamanan dan insiden yang tidak diinginkan secara efisien di organisasi Anda.

Apa yang akan Anda pelajari Membuat dan menerapkan kemampuan respons insiden di dalam organisasi Anda sendiriMelakukan akuisisi dan penanganan bukti yang tepatMenganalisis bukti yang dikumpulkan dan menentukan akar penyebab insiden keamananMenguasai analisis memori dan logMengintegrasikan teknik dan prosedur forensik digital ke dalam keseluruhan proses respons insidenMemahami berbagai teknik untuk perburuan ancaman.

Menulis laporan insiden yang efektif yang mendokumentasikan temuan utama analisis AndaUntuk siapa buku iniBuku ini ditujukan untuk para profesional keamanan siber dan keamanan informasi yang ingin menerapkan forensik digital dan respons insiden di organisasi mereka. Anda juga akan merasa buku ini bermanfaat jika Anda baru mengenal konsep forensik digital dan ingin memulai dengan dasar-dasarnya. Pemahaman dasar tentang sistem operasi dan beberapa pengetahuan tentang dasar-dasar jaringan diperlukan untuk memulai buku ini.

ACHMAD KOLBINUS, S.T., M.T., M.Sc.
Serdik SPPK I T.A. 2024
No. serdik 202409002002