УДК 004.056
ББК 16.8
О76

Редактор:
Островская Светлана – ведущий специалист по реагированию на инциденты и компьютерной криминалистике в Group-IB.

Светлана Островская, Олег Скулкин
О76 Криминалистика компьютерной памяти на практике: Как эффективно анализировать оперативную память / авторизован. пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2023. – 256 с.: ил.

ISBN 978-5-93700-157-3

Книга знакомит читателя с современными концепциями активного поиска угроз и исследования передового вредоносного ПО с применением свободно распространяемых инструментов и фреймворков для анализа памяти. В издании принят практический подход, используются образы памяти из реальных инцидентов. Прочтя книгу, вы сможете самостоятельно создавать и анализировать дампы памяти, изучать действия пользователя, искать следы бесфайловых атак и реконструировать действия злоумышленников.

Издание адресовано специалистам по реагированию на инциденты, аналитикам кибербезопасности, системным администраторам, а также может быть полезно студентам вузов и инженерам из смежных областей.

УДК 004.056
ББК 16.8

First published in the English language under the title 'Practical Memory Forensics – (9781801070331)'

ISBN (анг.) 978-1-80107-033-1
ISBN (рус.) 978-5-93700-157-3

ђqdbɣeɤ bɇ dəqɇbɤзə d ɕɑɡɕɑɤ Ɉqdbɣqɣè

Оглавление

ŋqdqуɐʎ bƎ dəqƎbʎзə d єɔɑbɔʎ Ɉqdqʎqʎè