УДК 004.56
ББК 004.56
П32

Эндрю Пиз

П32 Активное выявление угроз с Elastic Stack: Построение надежного стека безопасности: предотвращение, обнаружение и оповещение / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2022. – 326 с.: ил.

ISBN 978-5-93700-116-0

Elastic Stack – мощный инструмент для предотвращения, обнаружения и реагирования на угрозы. Эта книга покажет, как наилучшим образом использовать его для обеспечения оптимальной защиты от киберугроз.

Вы ознакомитесь с основными компонентами Elastic Stack, освоите аналитические модели и методики целенаправленного поиска угроз и научитесь делиться логикой их обнаружения с партнерами и коллегами. Далее вы сможете развернуть Elastic Stack для мониторинга собственной сети и ресурсов, а также использовать панель визуализации данных Kibana для выявления злоумышленников в вашей сети.

Книга предназначена для всех читателей, которые интересуются тематикой активной кибербезопасности.

УДК 004.56
ББК 004.56

First published in the English language under the title «Threat Hunting with Elastic Stack – (9781801073783)»

ISBN (анг.) 978-1-80107-378-3
ISBN (рус.) 978-5-93700-116-0

Оглавление