国家信息中心主办
中国科技核心期刊

第8卷 第3期 2022年3月
Vol.8 No.3 Mar. 2022

信息安全研究

Journal of Information Security Research

深度学习安全与对抗专题

面向自然语言处理领域的对抗攻击研究与展望

联邦学习安全威胁综述

人脸深度伪造检测综述

第3期

CN 10-1345/TP
ISSN 2096-1057

9 772096 105228 03>

邮发代号：2-41 定价：38.00元

信息安全研究 第八卷 第三期

Xinxi Anquan Yanjiu

信息安全研究

（月刊　2015 年创刊）

第 8 卷第 3 期（总第 78 期）2022 年 3 月

本刊是中国科技核心期刊，入选 CCF T3 优秀期刊目录，全文被《中国核心期刊（遴选）数据库》《中文科技期刊数据库》《CNKI 中国期刊全文数据库》《超星期刊域出版平台》《博看网》收录。

主管单位　国家发展和改革委员会
主办单位　国家信息中心

出版单位　《信息安全研究》杂志社
地址　北京市西城区三里河路 58 号
邮编　100045
电话　+86(10)68557385
网址　http://www.sicris.cn
电子信箱　ris@cei.cn

社长　李新友
主编　吕　欣
副主编　马修军
融媒体主编　崔传桢

出版日期　每月 5 日
国际标准连续出版物号　ISSN 2096-1057
国内统一连续出版物号　CN 10-1345/TP
广告经营许可证　京西市监广登字 20210016 号
印刷单位　北京博海升彩色印刷有限公司
国内发行　北京市报刊发行局
订购处　全国各地邮电局（所）
邮发代号　2-41
定价　38.00 元

协办单位　亚信安全　龙象之本
合作单位　360 集团　安恒信息
航天云网　恒安嘉新
绿盟科技　蚂蚁集团
明朝万达　奇安信集团
数字认证　青藤云安全
信安世纪　天融信

»深度学习安全与对抗专题

»专家视点

CONTENTS 目次

Issue on Security of Deep Learning in Adversarial Settings

Expert Viewpoint

Journal of Information Security Research

Vol.8 No.3 Mar. 2022

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number: ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Director: Li Xinyou

Editor-in-Chief: Lü Xin

Directed by: National Development and Reform Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security Research

Address: No.58 Sanlihe Road, Xicheng District, Beijing

Zip Code: 100045

Website: http://www.sicris.cn

E-mail: ris@cei.cn

AD Permit: BAIC XBB Ad. No.0410

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 38.00RMB

NSFOCUS绿盟科技

绿盟智能安全运营平台（ISOP）

全场景 | 实战化 | 智能运营

1个中心 · 6大能力 · 3大特点 · 3大价值

辅助决策

- 日志威胁集中管理
- 资产安全管理

管理落地

- 威胁分析与溯源
- 自动化响应流程

运营支撑

- 漏洞生命周期管理
- 可信任运营服务

以“实战化安全运营”为核心，围绕 IPDR 打造纵深能力及安全运营的横向场景化能力，构建“全场景、智能、实战化”的安全运营平台，实现“全面防护，智能分析，自动响应”的防护效果与基于安全治理、等保合规、安全运营的体系化能力，更好地支撑企业常态化安全运营体系建设。

绿盟科技微信公众平台

nsfocus.com

服务热线 400-818-6868