INSEC WORLD

成都·世界信息安全大会

—— 信息时代，安全发声

2019年10月20-23日

20-23 October, 2019

中国西部国际博览城，成都

Western China International Expo City, Chengdu

会刊

SHOW DIRECTORY

www.insecworld.com

informa markets

大会致辞

我谨代表 Informa Markets 和主办方，诚挚地欢迎各位参与首届 INSEC WORLD 成都·世界信息安全大会！

世界信息安全大会正式落户成都了，非常感谢成都市人民政府的指导；成都市委网信办，成都市经信局，成都市科技局，成都市博览局，四川天府新区成都管委会，成都高新区管委会给予我们各方面的大力支持；软协，大数据联合会等行业协会的协办。在您们的支持与推动下，此次大会最终得以顺利举办。

大会以信息时代、安全发声的理念，广邀全球知名产、学、研安全从业人士及用户企业参与。首届大会总规模达 6000 平米，为期 4 天的大会包含 2 天高阶培训和 2 天主论坛、6 大分论坛，以及信息安全技术展示。大会重磅演讲人包含：2015 年图灵奖获得者、美国国家工程学院院士、斯坦福大学名誉教授 Martin Hellman，奇安信科技集团总裁吴云坤，北京赛博英杰科技有限公司创始人及董事长谭晓生，Palo Alto Networks 亚太区首席安全官 Kevin O' Leary 等近 50 位海内外嘉宾。遵循 Informa 主办的顶级活动如 Black Hat, IoT World 等设立专家顾问团的成功模式，由中国工程院院士、国家科技进步一等奖获得者方滨兴领衔本届大会专家顾问团，为大会量身打造最适合中国的议程。不少专家顾问团成员还依据各自擅长的细分领域，担任出品人为本届大会严选分论坛议题及讲者，其中聂君出任“CSO 论坛”，刘志乐出任“应急响应 / 安全运营论坛”，鲁辉出任“人才培养论坛”，杨卿出任“安全创新论坛”出品人。这 4 位出品人皆为业内知名企业高级管理者，不仅拥有丰富的专业知识，同时对行业需求了如指掌。他们亲力亲为地参与，加上 Informa 作为中立的独立第三方大会平台具备丰富的国内外资源，这样的优势互补、整合首见于国内信息安全圈会议。

成都作为中国西部领导城市，在软件研发、先进制造、智能经济与国际化都市建设方面需求迅猛，政府军工、金融科技、商业零售、医疗健康、信息科技等重点领域，信息安全首当其冲，大会同期推出“蓉安系列计划”，围绕研发、产业、应用、社群、人才，将为成都市建设“中国网络信息安全之城”贡献力量。

借此机会，我也想向我们的合作伙伴、赞助商、参展商、观众和媒体朋友表示由衷的感谢。感谢您们对 INSEC WORLD 成都·世界信息安全大会的鼎力支持，使其成为信息安全领域的优质独立产业平台。

张明
副总裁
Informa Markets China

Welcome Speech

On behalf of Informa Markets and the organizer, I sincerely welcome all guests to attend the inaugural INSEC WORLD · Chengdu!

As INSEC WORLD has officially settled in Chengdu, I would like extend my great gratitude to Chengdu Municipal People's Government for your guidance; Chengdu Municipal Party Committee Network Information Office, Chengdu Municipal Bureau of Economics and Information Technology, Chengdu Science and Technology Bureau, Chengdu Expo Bureau, Chengdu Management Committee of Tianfu New Area and Chengdu Management Committee of Hi-tech Industrial Development Zone for your strong support in all dimensions; Chengdu Software Industry Association, Sichuan Big Data Industry Federation and other industry associations for your co-organization. Thanks to your support and promotion, this conference can be proceeded successfully at last.

The first event with a total scale of 6,000 square meters is driven by the value of "Security Matters" which bringing together InfoSec service providers, researchers, developers and cooperate users around the globe. The 4-day conference includes 2-day advanced trainings, 2-day keynotes, 6 tracks and display of information security technologies. Keynote speakers of this conference include 50 guests from home and abroad, such as Martin Hellman, the winner of 2015 Turing Award, academician of the National Academy of Engineering, also Honorary Professor of Stanford University, Yunkun Wu, Chairman of Qianxin Group, Xiaosheng Tan, President & Founder of Beijing Genius Cyber Tech Co.,Ltd, and Kevin O'Leary, Field Chief Security Officer, APAC, Palo Alto Networks.

Following the successful model of setting up expert advisory boards for top events hosted by Informa, such as Black Hat and IoT World, Binxing Fang, Academician of the Chinese Academy of Engineering and the first prize winner of National Award for Science and Technology Progress, leads the Advisory Board of this conference and customizes the most suited conference agenda for China. Quite a few members of the Board also serve as producers to strictly select topics and speakers for the Tracks according to their specific areas of expertise. Among them, Jun Nie assumes the producer for "CSO Forum", Tony Liu for "Incident Response/Security Operation Forum", Hui Lu for "Talent Development Forum" and Qing Yang for "Security Innovation Forum". The four producers, all of whom are high-level leaders of well-known enterprises in the industry, boast not only a wealth of expertise but also a mastery of industry needs. With their hands-on participation and abundant domestic and foreign resources provided by Informa as a neutral independent third-party conference platform, such strength complementation and integration is unprecedented in a domestic information security conference.

As a leading city in Western China, Chengdu has rapid demand growth in software R&D, advanced manufacturing, intelligent economy and international urban construction, information security becomes the top priority in key fields like government & military industry, fintech, commercial retail, health care and information technology. This conference, therefore, concurrently launches "Chengdu INSEC Plans", which will contribute to the Chengdu's construction of "a cyber information security city in China" by focusing on R&D, industry application, community and talent.

Finally, I would also like to extend my cordial gratitude to our partners, sponsors, exhibitors, attendees and media friends for your strong support to INSEC WORLD · Chengdu and your efforts to build it into a high-quality independent industrial platform in the field of information security.

Warmest,
Bill Zhang
Vice President
Informa Markets China

目录Contents

大会概要
General Information

指导单位：
成都市人民政府

主办单位：
Informa Markets

支持单位：
成都市科技局
成都市博览局
四川天府新区成都管委会
成都高新区管委会

承办单位：
英富曼会展（成都）有限公司
亿百媒会展（上海）有限公司
四川天府国际会展有限公司

协办单位：
中国网络空间安全人才教育联盟
战略网络空间与国际研究中心
云安全联盟大中华区
（ISC）² 国际信息系统安全认证联盟
成都市软件行业协会
四川省大数据产业联合会

Supervising Unit
Chengdu Municipal People’s Government

Organizer
Informa Markets

Supporting Units
Chengdu Science and Technology Bureau
Chengdu Expo Bureau
Chengdu Management Committee of Tianfu New Area
Chengdu Management Committee of Hi-Tech Industrial Development Zone

Executive Undertakers
Informa Markets China (Chengdu) Co., Ltd.
UBM China (Shanghai) Co., Ltd.
Sichuan Tianfu International Conference & Exhibition Co., Ltd.

Co-organizer
The Cyberspace Security Talent Education Alliance of China
Centre for Strategic Cyberspace + International Studies
Cloud Security Alliance Greater China Region
(ISC)² International Information System Security Certification Consortium
Chengdu Software Industry Association
Sichuan Big Data Industry Federation

大会概要
General Information

联系我们 Contact Us

项目合作：
Project Cooperation：

姚慧琳 小姐
Ms. Kelly Yao
T： (86-21) 6157 7209
E： kelly.yao@informa.com

参展及赞助：
Exhibition & Sponsorship：

石黛 小姐
Ms. Shirley Shi
T： (86-21) 6157 7254
E： shirley.shi@informa.com

院校、协会、CXO、新创参会：
Colleges, Associations, CXO, Start-up Inquiry：

施文 小姐
Ms. Ruby Shi
T： (86-28) 8550 0895
E： ruby.shi@informa.com

演讲合作：
Speech Cooperation：

任晓 小姐
Ms. Kathy Ren
T： (86-21) 6157 3911
E： kathy.ren@informa.com

市场合作：
Marketing：

许治平 先生
Mr. Andrew Hsu
T： (86-21) 6157 3913
E： andrew.hsu@informa.com

关注大会微信公众号

观看大会直播相册

专家顾问团

方滨兴
首席顾问
中国工程院院士

陈建
首席信息安全官
平安集团

戴鹏飞
数据安全负责人
美团点评

董贵山
中国电科 首席专家，中国网安 副总工程师
卫士通 总工程师

范渊
董事长
安恒信息

季昕华
CEO
Ucloud

姜开达
副主任
上海交通大学网络信息中心

李雨航
云安全联盟大中华区主席
中国云安全联盟执行理事长

陆光明
COO
亚信安全

鲁辉
秘书长
中国网络空间安全人才教育联盟

马民虎
主任
西安交通大学苏州信息安全法律研究中心

聂君
首席安全官兼网络安全部总经理
奇安信集团

谈剑峰
创始人
众人科技

谭晓生
创始人、董事长
北京赛博英杰科技有限公司

田志宏
院长
广州大学网络空间先进技术研究院

谈剑峰
创始人
众人科技

吴云坤
总裁
奇安信集团

薛锋
创始人兼CEO
微步在线

专家顾问团

杨卿
创始人
独角兽安全团队 (UnicornTeam)

于旸
玄武实验室负责人
腾讯安全

周景平
首席安全官
知道创宇

Meghan Reilly
IT事业部负责人
Informa Tech

Tim Wilson
联合创始人兼主编
Dark Reading

Derek Manky
全球安全战略官
Fortinet

Francis Brown
首席技术官
Bishop Fox

Paul Vixie
董事长、首席执行官、联合创始人
Farsight Security有限公司

Tim Virtue
原安全与风险办公室首席官
Lower Colorado River Authority

Monnappa K A
Black Hat 顾问团成员

Shubham Mittal
Black Hat 顾问团成员

Mika Devonshire
Black Hat 顾问团成员

Aloysius Cheang
董事兼亚太区执行副总裁
战略网络空间与国际研究中心

高阶培训

企业安全建设实践：金融行业安全架构与技术实践

本课程体系重点面向工控安全领域，向信息安全周边范围进行扩散。工控安全领域为信息安全领域的子分支，是信息安全的新兴领域。工控安全领域的安全工程师，不但需要理解工控协议以及工业流程，还需要理解传统信息安全的攻防技术，对工程师要求非常高。本课程体系力求做到设计一个体系框架，从工控安全入门到精通，都需要全部进行涉猎。从理论到实践，再到真实环境的实战渗透，循序渐进，培养一个合格的工控安全工程师。

高阶培训

灯塔实验室：工控安全课程

本课程体系重点面向工控安全领域，向信息安全周边范围进行扩散。工控安全领域为信息安全领域的子分支，是信息安全的新兴领域。工控安全领域的安全工程师，不但需要理解工控协议以及工业流程，还需要理解传统信息安全的攻防技术，对工程师要求非常高。本课程体系力求做到设计一个体系框架，从工控安全入门到精通，都需要全部进行涉猎。从理论到实践，再到真实环境的实战渗透，循序渐进，培养一个合格的工控安全工程师。

高阶培训

安全意识官

安全意识官 (Security Awareness Officer) 培训是由中国网络空间安全人才教育联盟试点推出的、国内首个面向安全意识专业人员的培训课程，旨在帮助企业内负责安全意识与安全文化建设工作的专业人士提升相关专业知识、经验与技能。

易念科技

网络安全文化意识价值传播者

安全意识官培训是由易念科技开发。

Day1 主论坛

公钥密码对信息安全的重要性

Martin Hellman
2015年图灵奖获得者
美国国家工程院院士
斯坦福大学名誉教授

公钥密码学是现代信息安全的核心，每天保护着数千万元的金融交易。虽然这项革命性的技术经常让人们想知道我们是如何看待它的，但在这次演讲之后，你可能会想知道为什么Whit Diffie、Ralph Merkle和我花了这么长时间才发现它。这次演讲也将解释公钥密码学的基本运作，并着重介绍了几位研究人员的重要贡献，他们的贡献并不广为人知。

新技术环境下的“内生安全”能力构建

吴云坤
总裁
奇安信集团

云计算、大数据、物联网、人工智能等新技术的发展和应用，推动了以云计算、大数据为基础设施，以数据共享为目标的等新一代信息化建设，改变了安全环境和安全需求，需要通过全新的安全体系来构建与信息化系统全面覆盖和深度结合的“内生安全”能力来保障信息化投资和业务运行。本专题将从规划、建设和运行三个层面阐述新一代信息化环境下如何构建“内生安全”能力。

从0到1:一个从幕后到董事会的转型路线图

Tim Virtue
原首席安全与风险官
LCRA

演讲将就如何将你的职业生涯提升到一个新的高度展开实际讨论。尽管技术对于职业成功至关重要，但这只是一个开始。
与会者将带着关于职业规划、个人品牌、为企业增加价值的实用技巧和其他一些能够将你的职业提升到下一个层次的策略离开。

CSO论坛

企业安全中台建设探索

陈建
首席信息安全官
平安集团

现今各类中台（技术中台、业务中台和数据中台）概念层出不穷，而安全与业务在中台概念上有许多相似点，可以通过技术沉淀、数据打通和运营框架的不断抽象提炼，以达成更快和更稳定的安全能力交付，支持业务的创新和试错。

全面风险治理

张作裕
钉钉CRO
阿里巴巴

全面风险治理，从CRO视角来看待风险管理。从变换视角以安全价值为导向，设定安全规划与业务发展的平衡目标，利用全面风险治理思路与业务总裁对话。

互联网银行安全建设实践

吴飞飞
高级安全专家
蚂蚁金服/网商银行

作者如何从零到一保护一家公司从创业阶段到纳斯达克上市的全过程安全建设，回过头来看哪些经验是值得被总结分享的?之后加入大型互联网+金融企业负责安全架构，历史的哪些经验可以继续沿用，哪些需要弃用?中小公司和大公司安全建设存在什么区别?有什么可以互相融合借鉴的地方?新型互联网技术和传统金融业务融合的安全该如何做?

大型互联网企业的数据安全攻与防

钱业斐
数据安全负责人
滴滴出行公司

大型互联网企业有着特有的数据安全挑战，即如何在业务迭代快、人员流动性高、数据量巨大、组织变化频繁，信息系统繁多的条件下达成安全、体验与效率的平衡，并最终实现数据安全事件MTTD、MTTR<24小时
常见的数据安全框架和解决方案，是难以实现该目标的。我们将数据安全能力建设融入TOGAF的各个层级架构，通过多个核心抓手并辅以运营实现最终目标，提供大型互联网企业数据安全攻与防的视角和经验。

可信数字身份构筑企业信息安全

谭翔
总经理
上海派拉软件股份有限公司

当下，企业安全措施聚焦在物理安全、网络安全，而对组织内部的权限滥用、内外部人员违规私建账号以及对风险预警和责任追溯等缺失有效的管控手段，导致信息安全事故频发，众多企业及个人数据被批量泄漏。
建立一套现代化、标准灵活、融合各种AI 、大数据 、云端 、物联网等新兴技术的可信数字身份治理体系，直接决定组织是否会成为运用越来越低的成本给客户提供创新服务的企业。

使产品安全而黑客

Craig Smith
安全和研发高级主管
Iconiq Motors
《汽车黑客手册》作者

在汽车工业中，涉及到安全问题，我们往往会从一个极端走向另一个极端。要么我们的车几乎没有安全保障，要么我们试图把车锁死，以至于与第三方合作是一场噩梦。这次演讲将详细介绍如何使产品免受黑客攻击，但仍允许第三方介入。我们将涵盖如何允许修改，并仍然限制滥用。我们还将讨论您是否可以制造一辆可改装的自动驾驶车辆，并且它是否仍然安全？

对机器学习的攻击

David Glance
软件与安全实践中心主任西澳大学

随着越来越多的组织正在利用机器学习以提高效率和执行新功能，针对这些算法的攻击是不可避免的。研究表明，有很多方法可以攻击这些模型，即使它们的工作对象未知（所谓的黑盒模型），攻击者也能够影响这些机器学习模型所做的决策。这可以从改变面部识别软件到识别另一个人，到改变有利于攻击者的业务或合同决策。随着企业开始实施机器学习，从一开始就必须优先考虑安全性。

超级root：ARM设备上强大而隐蔽的root技术

章张锴
博士
北京航空航天大学

Root攻击是一个未经授权的过程，通过利用系统的漏洞获得最高权限。在此之后，攻击者能够完全控制系统并任意访问系统资源，从安全敏感信息到私人个人数据。幸运的是，所有现有的Root技术都是可追踪和可检测的，因为它们不能完全删除指纹，如uid和setuid文件。

我们提出了一种新的强大而隐蔽的Root技术，即Super Root。与传统的获取Root权限的Root技术相比，Super Root试图获得最高的hypervisor/vmm权限。Hypervisor权限允许对手执行传统根目录所做的任何操作，还提供了hypervisor所允许的新的强大功能，例如执行虚拟机自省（vmi）。基于VMI的技术能够完全去除Super Root的指纹，从而使其对现有的所有根检测工具都具有隐蔽性。

我们将在一台树莓型的pi-powered计算机上演示两种超级根攻击。我们使用两个现有的基准工具来度量它们的性能开销，并使用现有的Root检测工具进行安全评估。实验结果表明，超级根的开销可以忽略不计，所有的根检测工具都不能检测到超级根的存在。

最后，我们将讨论超级根的潜在缓解措施，并呼吁越来越多的各方参与这项努力，以加强ARM系统。

漏洞攻防

工控协议非授权入侵

剑思庭
工控安全研究员
破晓安全团队

针对工业常用协议介绍，工业协议的特点和组成部分，阐述对工业协议非授权和未加密的脆弱性分析，通过对Modbus TCP实例化，演示模拟Modbus TCP协议的非授权写入，造成工业设备非正常的动作。

“两字节”攻破Adobe Reader：BOM标记黑魔法揭秘

刘科
高级安全研究员
腾讯安全玄武实验室

本议题将介绍在 Adobe Reader 中发现的多个字符串处理漏洞，其中一个漏洞可以实现信息泄露以绕过 ASLR（该漏洞在 2018 年天府杯比赛中与一个 UAF 漏洞配合使用实现代码执行），另一个漏洞则可以直接实现代码执行。议题将从以下四个方面对该类漏洞进行详细讲解：（1）漏洞本质原理（2）漏洞挖掘方法（3）漏洞利用技巧（4）漏洞修复方案。

Oh! Auth: OAuth 2.0陷阱 & 攻击

Samit Anwer
高级安全工程
Citrix

在提供基于OAuth/Open ID Connect的资产访问的竞争中，授权服务提供商被迫在外发布半成熟的解决方案，因此依赖方和用户面临着大量问题，从授权代码泄露（未经授权的资源访问）到账户接管。向应用程序添加授权或SSO措施的关键是确保安全性与可用性之间的平衡。开发人员在做出关于具体实现的决策时可能会做出权衡——很多决策要做。开发人员仍然希望在安全性上加倍努力以避免2.0中的缺陷，将重点放在会话管理、存储数据和ID的加密/混淆，以及保护应用程序的源代码上。在这项工作中，我们将讨论依赖方开发人员在实现基于OAuth/OpenID的依赖方解决方案时的常见弊端。但是，并不是所有的依赖方开发者都掌握在手中，授权服务提供商也有很大的作用要发挥。典型的OAuth设置主要涉及4个部分，它们是依赖方/客户机、用户/资源所有者、资源提供者、授权服务器。在这项工作中，我们将主要关注授权服务器可能引入的漏洞，讨论每个部分都可能引入的错误。重点-我们介绍了我们对OAuth授权提供者的案例研究，并详细说明了我们在他们的解决方案中发现的问题。这包括Microsoft授权服务器login.windows.net中的漏洞。如PoC视频所示(https://drive.google.com/file/d/1ZFratBPO6qP0hWiCsQH6qJ5fbbx7ghSn/view?usp=sharing)，Auth代码可以重播身份验证代码以生成新的访问令牌和ID令牌。此外，代码验证器没有经过验证，这可能会导致在使用Microsoft标识提供程序login.windows.net的本机应用程序上对访问/ID令牌的危害。漏洞1:Microsoft的IDP服务未能阻止重播的授权代码漏洞2:Microsoft的IDP服务未能验证代码交换验证密钥中使用的代码验证程序（本地应用程序的OAuth 2.0-https://tools.ietf.org/html/rfc8252）。代码验证器保护真实的应用程序不受其他恶意应用程序的攻击，以防其假装真实应用程序的身份并代表它们请求访问/身份令牌。供应商-Microsoft，产品-OAuth的身份提供程序服务，版本-login.windows.net

数据安全与云安全

云环境下数据备份发展趋势分析

胡晓勤
创始人兼CEO
成都云祺科技有限公司

数据保护的重要性毋庸置疑，数据备份是数据安全的最后一道防线，勒索病毒、误操作、软件缺陷、硬件故障、爆恐袭击、地震、洪水等灾难，都能对数据造成毁灭性打击。

在云计算环境下，仍然需要备份技术对数据进行保护，云计算带来了IT基础设施构建方式发生了巨大的变化，从而催生出新的备份技术，无代理备份、瞬时恢复、备份数据管理等技术在云场景下，为客户带来更快的恢复速度、更高效的备份数据利用率、更便宜的异地数据备份，云环境下，备份技术的发展、使用将大有可为。

针对API和微服务的五种最危险数据盗取战术以及缓解措施

董靖
创始人
思睿嘉得

数字经济新基础设施API和微服务带来数据交换快速增长，数据暴露面大幅增加，缺乏风险可见性与检测能力。新部署的微服务在传输敏感数据?哪些URL是潜在攻击面?存在越权使用?恶意员工大量下载数据?程序员偷偷加入隐蔽后门?已废弃API被第三方频繁使用?篡改参数或注入?逻辑绕过业务流程?用丰富实例讲解应对措施。

运用自动化AI技术打击“智能化”网络欺诈

崔宏宇
中国区技术负责人
北京维择科技有限公司

AI技术在赋能各个产业的同时，也被网络黑产所利用，使得黑产攻击更加自动化，更加隐蔽，难于检测。
崔宏宇老师在互联网反欺诈领域研究发现，目前黑产的攻击模型呈现以下趋势:攻击方法多样化而变化快，攻击手段趋于模拟正常用户，攻击账号主要来源由大规模注册渐渐转向ATO账号。传统的规则系统和有监督的模型，由于对欺诈案例以及标签数据的强依赖，往往无法及时应对迅速演化的黑产攻击，在反欺诈中- -直处于被动防守的状态。通过无监督算法全局分析，在高维空间聚类，可以在无标签情况下，自动发现大规模关联欺诈团伙。无监督算法在提前预警以及检测快速演变欺诈模式方面体现了显著的优势。

数据安全与云安全

虚假信息攻击是网络威胁的一种新形式

Roy Zinman
顾问
CrowdSense
顾问
Cybint Solutions
原开源情报分析主管
以色列部队

对虚假信息或网络信息战的感知，和“传统”网络威胁的过程相同。首先，一次大规模、复杂的国家发起的攻击被揭露出来。然后，其他国家参与者、罪犯和商业参与者也效仿并模仿暴露的方法、漏洞和技术。

网络虚假信息攻击在企业界越来越普遍。公司的品牌资产正在受到打击，非法参与者利用社交媒体造假操纵股票价格，以获取攻击的巨大收益。

信息战攻击是通过使用虚假身份和在线资产，在社交媒体、在线交易平台和新闻平台中创建和传播虚假叙述来实施的。这些叙述经过精心设计，对交易员、监管者和公众产生了影响。

这种类型的攻击仍然没有处理，因为组织和技术上的调整还没有进行。目前尚不清楚哪个部门负责防御此类攻击。是CISO吗?市场营销?通信?或者是其他人的问题——社交媒体平台、政府监管机构等。

检测和减轻虚假信息攻击的技术是年轻和复杂的。它需要复杂的人工智能和大量的数据收集和监控。辩护人遇到了巨大的法律和道德困境。例如，“用火灭火”是否合法?我们如何才能减轻虚假信息攻击造成的所有损害?

我将描述一种基于成熟的网络安全方法的反信息攻击新方法。它是一种全面的方法，包括威胁情报、监测、检测、缓解和事件响应技术，专门针对虚假信息攻击者提出的独特挑战。

个人信息与隐私保护工作中的重点和难点经验分享

叶天斌
网络安全咨询总监
德勤中国

德勤中国网络安全咨询总监叶天斌分享德勤在协助企业在实施数据安全与隐私保护过程中的实战经验，包括PIMS（个人信息管理体系）蓝图、儿童隐私保护关注重点、全球数据跨境流动规则、隐私工程难点、APP及SDK合规针对性的解决方案。

数字科技安全挑战与思考

刘明浩
信息安全团队负责人
京东数字科技

伴随着互联网进入下半场，安全也需求跟随业务进行升级。本次分享主要从京东数科的安全实践经验出发，分析业务所面临的安全挑战，从基础安全到移动安全再到业务安全，全方位介绍分布式安全架构的实践经验。

Day2 主论坛

培养网络空间安全创业者的企业家精神

谭晓生
创始人&董事长
北京赛博英杰科技有限公司

一方面是网络空间安全需要源源不断的创新，一方面是网络安全创新创业公司生存容易发展难，问题的成因相当复杂，问题的求解也需要多管齐下，培养网络安全创业者的企业家精神无疑是必不可少的一步。国内网络安全创业者多是网络安全攻防技术、产品开发背景，对销售体体系设计、公司运营、政府关系、投融资往往缺乏操作经验，在一个企业的发展壮大过程中这些技术之外的能力往往起至关重要的作用，正奇学院安全创业营在网络安全创业者的“企业家精神”培养上做了一些尝试，希望通过创业者企业家精神的提升，提高网络空间安全创业成功率，通过创新技术与产品解决用户的网络安全问题。

基于威胁情报的安全智能化

薛锋
CEO
北京微步在线科技有限公司（ThreatBook）

议题将基于微步在线多年的实践经验，回顾威胁情报这一崭新理念再过去几年的发展壮大，系统阐述威胁情报再国内落地的形式和案例，对于各个行业的安全建设所起到的至关重要的赋能作用。

理解混乱：安全运维的演变

Kevin O’ Leary
亚太首席安全官
Palo Alto Networks

多年来，运营安全已经演变为一种与业务相隔离的追求，只关心保护周边和应用一套既定的规则，而不考虑业务的需要。随着企业的发展和数字转型，云安全运营也需要向机器学习和人工智能的方向发展。

Day2 主论坛

面向未来有效保护，护航企业数字化转型

郝轶
安全业务CTO
深信服科技股份有限公司

当前，以人工智能、机器人技术、虚拟现实等为突破口的第四次工业革命正在全球范围内如火如荼地进行，不断推动着数字化时代的发展。与此同时，伴随着威胁的不断升级、IT系统的不断增加和新技术的不断革新与发展，用户网络空间下的安全建设也提出了更高的要求。在此情况下，如何通过网络安全建设的革新以适应数字化时代的发展，成为不少用户共同关注的话题。在本次演讲中，深信服将分享如何通过“面向未来 有效保护”的安全体系构建，帮助用户抵抗数字世界中的网络安全威胁，护航数字化转型过程中的网络安全。

智慧城市场景下的智能数据安全

刘博
首席科学家
高级副总裁
杭州安恒信息技术股份有限公司

数字经济、智慧城市已成趋势，信息技术与经济社会的交汇融合带来了数据迅猛增长，数据已成为国家基础性战略资源。在数字政府、智慧城市建设推进的同时，还需保障各类数据资源跨层级、跨地域、跨系统、跨部门、跨业务互联互通和协同共享的安全，提升数字经济工作效率，推进了政府数字化转型。

应急响应

工业控制系统网络安全防护的思考

李冰
原副主任
国家信息技术安全研究中心

报告首先从宏观层面给出了工业控制系统当前的安全现状，其次对工业控制系统面临的安全威胁逐一进行分析总结。最后，根据工业控制系统特性和安全防护原则，提出通过体系化的可信技术实现工业控制系统安全保障，并分别从安全防护技术、应急备用和全面安全管理三个层面进行了阐述。

国家级网络安全威胁情报共享的挑战与实践

何能强
高级工程师
国家互联网应急中心

本报告将介绍CNCERT所开展的网络安全威胁信息共享系统的技术架构和共享业务运行机制，并在此基础上构建国家级网络安全威胁信息共享平台和工作体系。

理解与降低企业安全风险

赵阳
总经理
Tenable中国区

企业IT技术日新月异，随着各种新的数字化技术普遍应用各个领域（IOT，SACDA，Cloud，Web，DevOps），企业暴露在外部攻击面的风险也成倍增加。2018全年被公布的漏洞数量超过16,500，相比2017年增加27%。面对如此众多的漏洞问题及各种多样化攻击手段（蠕虫式勒索病毒，ICS攻击，挖矿木马等），安全团队如何能有效的发现企业内部真正的安全风险并及时做出补救?显然，传统的安全技术并不能完全满足新的需求。Tenable将与各位安全专家一起探讨，如何利用最新的Cyber Exposure技术，高效管理和度量企业的资产攻击面，加速理解和减少企业安全风险。

应急响应

打造“无人值守”的安全运营中心

傅奎
CTO
上海雾帜智能科技有限公司

人工智能如何在安全编排、自动化和响应领域，助力企业构建自适应的安全运营体系。通过自动化和可交互性技术链接企业内外部资源，借助人工智能技术打造“无人值守”的安全运营中心，为企业安全运营带来革命化的变革。

基于可信线索挖掘的威胁狩猎

张润滋
高级安全研究员
绿盟科技

我们需要一个统一的、能吞吐海量异构多源数据，快速检测、推理、响应、追踪威胁事件的高度自动化平台及工具链，辅助人进行安全的运营、研究和对抗。议题从实践经验出发，基于对网络安全数据分析中常用数据源的再分类，提出了构建智能安全平台的图模型所需的关键数据图，以支撑“智能化”威胁狩猎、安全研究工作的进一步开展。

数字品牌保护，一种业务安全的主动防御实践

杨大路
CEO
北京天际友盟信息技术有限公司

数字化转型是企业无法回避的命题，企业将越来越难于区分业务安全与网络安全的界限在哪，需要寻找有效的方法来保护数字化资产。

品牌属于企业资产的一种。很多企业运用数字化的力量重新塑造了企业品牌形象；但数据泄露、网络诈骗、网络钓鱼、甚至是网络勒索和胁迫等事件，不仅给各企业带来直接经济损失，也损害了企业品牌和商业形象。

数字品牌保护是一种新的安全实践，抵御各种风险场景，比如网页钓鱼、APP、社交媒体仿冒、威胁误报、供应链安全、品牌侵权等等，帮助企业保护数字品牌和资产。

人才培养

探索政产学研协同育人机制，建设一流网络空间安全学院

刘建伟
院长
北京航空航天大学

北航于2016年获得我国首批网络空间安全一级学科博士学位授权点，2017年正式成立网络空间安全学院，并获批由中央网信办、教育部共同授牌的首批“一流网络安全学院建设示范项目高校”。本讲座首先介绍了北航网络空间安全学院建设的总体目标和建设方针，给出了学科建设的5个发展方向，然后全面介绍了北航网络空间安全学院在本科专业设置、本科生招生及培养、研究生招生规划、科研平台建设、办学基础条件等方面的建设进展情况。本讲座还介绍了北航网络空间安全学院与政府部门、网信企业共同建立校企联合实验室、加强高水平网络安全人才培养的做法，特别总结归纳了一流网络安全学院的建设经验和体会。

网络空间安全人才培养创新模式探索与实践

田志宏
院长
广州大学网络空间先进技术研究院

网络空间安全的需求推动网络空间安全学科的发展，而网络空间安全学科发展的核心任务是高素质专业人才的培养。针对当前网络空间安全人才培养中存在的课程内容分割独立以及学习兴趣不足等问题，基于网络攻防实训演练平台，详细介绍“方滨兴”研究生培养创新班在网络空间安全综合实践分级培养模式方面的探索和实践。

信息安全复合型人才培养经验分享

刘哲理
副院长
南开大学

围绕南开大学“信息安全法学”双学位人才培养，分享课程设置、培养模式方面遇到的问题和举措。

安全人才的人才安全

吴铤
院长
杭州电子科技大学网络空间安全学院

网络空间安全所特有的攻防两面性，使得在网络空间安全人才的培养过程中，不能只是片面强调安全专业知识、技能的学习，而必须把立德树人作为安全人才培养的中心环节，强化安全人才培养的政治红线、法律底线。报告在对全国部分高校网络安全人才培养情况调研的基础上，给出落实安全人才思想政治工作的具体建议以及杭电实践。

网络安全应用型人才培养实践

李洋
360网络安全大学总经理
360

大安全时代下，漏洞无处不在，人是最薄弱的环节。面对网络安全人才严重紧缺的问题，360网络安全大学依托公司十余年在安全技术领域的深耕及人才选拔培养方面的丰富经验，打造出了一整套与行业需求相匹配的人才培养体系。与政府，高校及合作伙伴一起联合培养应用型网络安全人才，为国家网络安全保驾护航。

安全创新

冯继强，总经理，苏州极光无限信息技术有限公司

冯继强
总经理
苏州极光无限信息技术有限公司

我们研究利用图神经网络来快速有效的检测大型代码库中的漏洞，利用RNN和GNN来提取与漏洞存在相关的代码结构和语义特征，将代码分析与离散数学中的图论相结合，用特征学习将已知代码的漏洞转化成量化的指标来进行漏洞的检测，同时建立神经网络来辅助二进制的分析，用开源代码库和CVE作为训练数据建立特征数据库。

新一代高效，精确且能灵活自定义的程序静态应用安全测试技术

刘新铭
首席架构师
鉴释科技发展有限公司

梁宇宁
联合创始人兼首席执行官
鉴释科技发展有限公司

SAST（Static Applications Security Testing）即静态应用安全测试，它是一系列的技术和工具，使程序员获得专业的安全指导，并能够理解和执行。许多SAST工具的误报率非常高，它们显示漏洞的地方实际上根本不存在。这导致开发人员需要花费大量时间进行手动检查。当一个工具试图减少假阳性（误报）时，通常会导致假阴性（漏报）的增加，使得错误被忽略。为了提高准确度，可以使用不同分析方法达到互补的目标。

在本讲座中，我们将使用一些真实示例来演示静态分析工具的挑战和机会，以实现高成本效益。

我们新一代高效，精确且能灵活自定义的程序静态应用安全测试技术包含跨不同语言，不同函数和不同文件，进行四种软件特征，即流敏感、上下文敏感、对象敏感和过程间，这些特征对于SAST工具诊断漏洞和违规行为的有效性至关重要。这四种软件特征无法单独处理，如一个变量可以沿某个执行路径未初始化（流敏感）。该执行路径可以包括函数调用，将该问题变量作为参数传入（过程间）。甚至可能是对同一个函数有多个调用，有一些调用传入有问题的参数，有一些调用没有（上下文敏感）。这四种分析方法必须相互协作，它们不能孤立地进行。此外，分析范围必须尽可能大，同时要考虑内存和计算需求，可能随着分析范围呈指数型增长。减少假阳性（误报）是选择静态分析工具的关键决定因素，这在很大程度上取决于本文探讨的分析准确性。

安全创新

零和博弈-对抗网络犯罪的新战场

张瑞冬
CEO
成都无糖信息技术有限公司

互联网在给我们带来便捷生活的同时，也给不法分子带来了可乘之机。逐步走入日常网络生活的大数据、云计算、AI等技术的发展诱使网络犯罪更趋于多样化和专业化，对抗网络犯罪，是一场网络空间的技术较量，这是没有硝烟的战场，这是一场零和博弈，在残酷的较量中，必须拥有绝对的技术优势才可能取得真正的胜利。

新信息时代下的即时通信

林正显
研发总监
BCM Social Corp

柴坤哲
安全总监
BCM Social Corp

自“棱镜门”监听事件后，用户对平台由完全信任转变为半信半疑，越来越多的用户开始思考厂商究竟是如何使用自己的个人信息与数据，甚至质疑是否有足够安全的即时通信；本议题结合一款安全即时通信软件的开发实践，从一款注重极致安全，高隐私且高效的即时通信软件的架构设计到具体方案落地；关键字：完全端对端加密，全匿名使用，无网络通信。

5G来了 - 不必过于担忧安全

黄琳
360安全研究院高级技术总监
360

5G网络已经在部分城市部署，普通民众能够买到的5G手机终端型号已经越来越多，5G时代已经在慢慢走来。通信网络相关的安全问题是一个长期存在的话题，并不是因为5G新引入的。此议题将介绍，移动通信网过去有哪些影响较大的安全问题；现在的4G网络还存在什么问题；5G相比4G在安全性上有了哪些增强。

演讲嘉宾

Day1 主论坛

谭晓生
创始人、董事长
北京赛博英杰科技有限公司

曾任360集团技术总裁、首席安全官，公安部网络安全保卫局网络安全专家，2018年获中国互联网发展基金会网络安全杰出人才称号，中国计算机学会(CCF)理事、副秘书长，2012年获中关村高端领军人才称号。先后工作于西安交通大学、北大方正，深圳现代、深圳豪信等公司，先后从事过DOS操作系统下反病毒系统研发、磁盘加密系统研发、汉字操作系统开发、大型管理信息系统开发。2003年进入互联网行业，先后任3721技术开发总监、雅虎中国技术开发总监、雅虎中国CTO、MySpace CTO兼任COO。2009年加入奇虎360，云计算基础架构、信息安全、信息检索方面专家。

吴云坤
总裁
奇安信集团

奇安信科技集团总裁。中国信息协会信息化促进工作委员会副会长，中科院大学网络空间学院客座教授，中国互联网金融协会网络与安全专委会副主任委员。
长期从事网络安全领域相关的产品规划、市场品牌和投融资管理。专注于边界安全、大数据安全、云计算安全、大数据威胁情报等多个领域的研究。倡导“数据驱动安全”理念，为国内互联网安全行业的技术发展提供了具有建设性的先进思路。

Martin Hellman
2015年图灵奖获得者
美国国家工程院院士
斯坦福大学名誉教授

Martin Hellman和Diffie和Merkle共同发明了公钥密码学。公钥密码学是一种保护电子商务和每日数万亿美元金融交易的技术。他的荣誉包括计算机科学的最高奖项(图灵奖)和美国国家工程院院士。Martin对技术发展的道德规范有着浓厚的兴趣，并在美国科学家联合会的顾问委员会和验证投票委员会任职。他曾在麻省理工学院(1969-1971)和斯坦福大学(1971-1996)任教，目前是斯坦福大学电气工程荣誉教授。

Tim Virtue
原首席安全与风险官
LCRA

Tim Virtue（CISSP、CFE）是全球网络安全、技术和风险管理的领导者。他在各种类型和规模的上市跨国公司、私营企业、政府机构和非营利组织拥有丰富的工作经验，专注于金融服务、管理咨询和技术。他是业界公认的创新者、屡获殊荣的思想领袖、值得信赖的董事会顾问、演讲者、作者，同时也是新兴和颠覆性技术和商业趋势的早期实践者。

Tim Virtue拥有纽约大学斯特恩商学院的风险管理理学硕士学位、乔治华盛顿大学商学院的信息系统理学硕士学位和刑事司法理学学士学位，以及东北大学刑事司法理学学士。

演讲嘉宾

CSO论坛

金湘宇
Sec-UN网站创始人
威胁情报推进联盟发起人

NUKE，金湘宇，Sec-UN网站创始人、威胁情报推进联盟发起人。前网络安全和信息技术资深咨询顾问，曾就职于启明星辰和埃森哲，分别服务于国家电网、中国移动、中国电信、华为等全球领先用户。曾作为私募基金管理合伙人，主导投资思睿嘉得、图迹科技、神州网云、数字观星、英诺森、嘉韦思等创新公司。

陈建
首席信息安全官
平安集团

陈建，平安集团首席信息安全官，20年左右的信息安全、内控、IT审计和风险管理经验，在反欺诈领域有超过10年的经验。2000-2005年期间在安氏、冠群金辰等安全公司担任资深安全顾问，2005-2015年从零组建携程信息团队，负责整个携程集团的信息安全和业务安全的相关工作，历任携程集团安全中心总监、高级总监、CTO助理，2015年4月加入平安科技，负责集团信息安全工作，2018年被任命为集团首席信息安全官，专注于平安集团信息安全能力建设和为集团专业公司赋能，致力于数据赋能安全和开放API生态能力建设等实践，具备CISSP、CISA、ISO27001、ITIL、Cobit、PMP等多项国际认证。

张作裕
钉钉CRO
阿里巴巴

张作裕，ID:bk7477890。阿里巴巴钉钉安全负责人，曾担任美丽联合集团信息安全总监，负责蘑菇街、美丽说安全体系建设。担任Sobug安全技术总监，负责安全产品设计及研发工作。在《黑客X档案》社区担任技术版主、管理员。创业期间担任多家企业安全顾问，有多年企业风险治理体系建设经验。

吴飞飞
高级安全专家
蚂蚁金服/网商银行

止介（FEEI），Cobra/GSIL作者，蚂蚁金服高级安全专家，网商银行安全架构师。

演讲嘉宾

CSO论坛

钱业斐
数据安全负责人
滴滴出行公司

长期致力于大型企业全球化安全能力建设和运营，探求安全、体验、效率并存的解决方案。
熟悉基础架构安全、数据安全、IT运营和安全审计。目前在滴滴担任数据安全负责人，带领团队致力于保障数据安全工作；曾担任阿里巴巴集团大客户安全运营负责人并负责安全体系能力输出；曾担任华为企业业务安全与运营COE负责人，支持中国企业出海扬帆；曾担任绿盟科技资深安全顾问。

谭翔
总经理
上海派拉软件股份有限公司

在身份安全、数据安全和业务安全领域拥有近20年的实战经验，在IBM、CA有十多年企业软件相关工作经验。
2008年创立派拉软件，深耕企业级信息安全和业务变革，对汽车、制造、医药、零售、地产、金融、教育等行业的信息安全和数字化转型有丰富的行业经验和前瞻洞察。

演讲嘉宾

漏洞攻防

张颖
科技云报道联合创始人&执行主编
希幔传媒副总裁

资深媒体人，前沿科技领域十强精英人物，文章数次被各大科技媒体收录转载。受到政府相关部门与行业高度认可，多次受邀主持工信部可信云大会、全球云计算大会等大型行业会议。曾任联想、网易、奥美等上市集团管理职位，拥有丰富的B2B营销推广实战经验，受邀为众多上市企业及营销学院进行培训。

Craig Smith
安全和研发高级主管
Iconiq Motors
《汽车黑客手册》作者

Craig Smith是艾康尼克汽车的安全和研发高级主管，主要负责产品安全、红蓝团队以及未来产品的研发。他也是Open Garages的创始人，一个由机械师、安全研究人员和艺术家组成的团队。

Craig撰写了《汽车黑客手册》，实际上是《汽车安全指南》。在Rapid7，Craig负责运输业务，专门为运输行业提供战略咨询和深入的技术专长。他的工作包括对汽车工业中正在开发的创新新技术进行广泛的测试。Craig开发了许多免费和开源的工具来帮助别人学习车辆安全。

Craig在安全领域工作了20多年，在过去的8年里，他专注于汽车与其他类型的交通工具。

David Glance
软件与安全实践中心主任
西澳大学

David Glance博士是UWA研究与开发中心软件与安全实践中心的主任。在UWA工作了18年前，Glance博士曾在汇丰、微软、TIBCO和IONA Technologies等公司从事金融和软件行业20多年。UWA CSSP为学生提供培训和研究机会，并在安全、健康和教育部门开发了商业软件。

Glance博士与经合组织就审查国家网络安全战略和评估商业组织的网络安全成熟度进行了协商。他目前正在协助经合组织建立数字安全并促进全球论坛的发展。

Glance博士是一位会经常发表文章的专栏作家，他经常在网络安全、技术和社会的媒体上露面。他是Springer出版的《安全与网络社会》一书的合著者（与Mark Gregory博士合著）。

章张锴
博士
北京航空航天大学

章张凯在北京航空航天大学计算机科学与工程学院获得学士学位和博士学位。他的研究兴趣包括移动安全和虚拟化安全。他的研究成果已发表在CCS、SecureCom、DSC等刊物上。

演讲嘉宾

剑思庭
工控安全研究员
破晓安全团队

复旦大学软件工程硕士，主要从事工控安全渗透和防御，KCon 2018/看雪2019/ISC 2019大会演讲嘉宾，独立开发基于Kali针对工业协议的指纹嗅探工具。

刘科
高级安全研究员
腾讯安全玄武实验室

刘科是腾讯安全玄武实验室的高级安全研究员，他发现并报告了将近400个安全漏洞，这些漏洞影响Adobe、Apple、Google、Microsoft以及部分主流开源软件；2017年获得素有“黑客奥斯卡”之称的Pwnie Awards史诗成就奖提名，同年在黑帽大会（亚洲）和中国网络安全年会发表主题演讲；2018年在天府杯比赛中成功攻破Adobe Reader；2016至2018连续三年位列微软MSRC TOP100榜单。

Samit Anwer
高级安全工程师
Citrix

Samit Anwer是一名网络和移动应用程序安全研究员。2015年，他在印度德里国际信息技术学院（IIIT Delhi）获得移动端和普适计算硕士学位后，不久便加入了Citrix，担任安全工程师。他积极参与网络/移动应用程序中的漏洞研究，并负责揭露了谷歌云打印API、IE 11/MS边缘上的XSS过滤器规避、Microsoft Windows 10上的代码执行、Microsoft的OAuth 2.0实现以及MS边缘/IE 11上的缓冲区溢出等几个安全漏洞。
他是IEEE Bangalore分会的成员，并在以下地点就各种安全主题发表了演讲：
a) DEFCON 中国, 北京 (2018)
b) BlackHat 亚洲, 新加坡 (2018)
c) AppSec 美国, 奥兰多 (2017),
d) CodeBlue, 东京 (2017),
e) c0c0n X, 喀拉拉邦(2017)
f) Null meets (2015, 2016, 2017, 2018)
他的技术兴趣在于使用静态程序分析技术来缓解移动和网络应用程序上的安全和性能问题，以及身份验证和授权机制的研究。

演讲嘉宾

数据安全及云安全

顾伟
日本及亚太地区业务信息安全官
安进生物技术

顾伟先生目前就职于安进生物，担任日本及亚太地区业务信息安全官一职，负责日本及亚太地区所有业务部门相关联的信息安全，风险管理和合规隐私，并且向全球信息安全官汇报。顾伟先生有超过14年的信息安全领域工作经验，在多个世界500强跨国外企中担任过信息安全架构和信息安全管理等工作。尤其在制药行业，信息安全和隐私经验非常丰富。

顾伟先生获得CCSF 2017和 CCSF 2018两届优秀首席信息安全官大奖，2017年度(ISC)^{2}亚太信息安全领袖称号，信息安全专业人士提名大奖，并且是来自中国大陆的唯一获奖者。

胡晓勤
创始人兼CEO
成都云祺科技有限公司

胡晓勤，博士，副教授，成都高新区高层次人才，成都云祺科技有限公司创始人，专注云计算及安全方向，云备份、云容灾方向的工程研究，获2006年度、2008年度四川省科技进步一等奖，获2010年度军队科技进步一等奖，授予国家发明专利及国防专利5项。

董靖
创始人
思睿嘉得

董靖先生是思睿嘉得创始人，致力于将机器学习、自然语言处理、和行为分析技术，应用于文本分析、数据安全、威胁检测响应等领域；其自主研发的轻量化人工智能引擎，适用多种安全和业务场景，可部署于云平台或边缘计算节点，被众多云和安全厂商青睐并内置；其标准产品也在各行业财富500强公司创造巨大价值。

崔宏宇
中国区技术负责人
北京维择科技有限公司

崔宏宇，现任DataVisor维择科技中国区技术负责人，自2015年起，在DataVisor开发使用分布式无监督机器学习算法进行反欺诈检测。负责过如Pinterest、Yelp、阿里巴巴和猎豹移动等大型互联网企业的机器注册、虚假评论、垃圾邮件、欺诈交易和虚假应用安装等场景的反欺诈建模 。在模型调优、特征工程和算法开发等领域都有着丰富的经验。

演讲嘉宾

Roy Zinman
顾问，CrowdSense
顾问，Cybint Solutions
原开源情报分析主管
以色列部队

Roy Zinman作为情报官员和创新领袖，在以色列国防军精英情报部门工作了25年，参与了几个具有国家安全战略意义的开创性项目。在上一份工作中，Roy Zinman带领IDF开源情报部门，并对其进行了重建，以应对现代社交媒体和大数据分析带来的挑战。
2017年年初，Roy Zinman从IDF退休后便加入了Recongate有限公司，这是一家专注于中国市场的线上数据分析的高科技企业。如今，他活跃于几家专注于信息战的网络安全和社交媒体数据分析初创企业。

叶天斌
网络安全咨询总监
德勤中国

叶天斌，现任德勤风险咨询总监，长期专注于安全技术架构、网络安全治理、数据安全与隐私合规业务领域，协助高科技、互联网用户应对数据安全与网络安全风险。

刘明浩
信息安全团队负责人
京东数字科技

十余年安全行业从业经验，在安全领域有丰富的实战经验。目前负责京东数字科技整体安全能力建设，主要包括自主安全产品开发与架构设计、业务安全、基础安全、安全运营、安全合规以及金融科技安全能力输出等。

Day2 主论坛

Sara Peters
资深编辑
Dark Reading

Sara Peters是Dark Reading专题“The Edge”的主编，负责对网络安全问题进行深入报道。她还经常担任美国及国际安全活动的主席、发言人和主持人，包括“Interop中国站”、“印度网络安全对话”、“Black Hat亚洲”、“Interop拉斯维加斯站”和“RSA”。就在2005年ChoicePoint数据泄露几个月后，Sara开始涉及该领域，那时候甚至大多数人还没有听说“数据泄露”这个词。

薛锋
CEO
北京微步在线科技有限公司（ThreatBook）

薛锋此前担任亚马逊(中国)首席信息安全官(CISO),负责亚马逊中国企业及客户信息安全。加入亚马逊前，薛锋任微软公司互联网安全战略总监，负责制定微软的中国互联网安全战略。薛锋是国际顶级黑帽子(Blackhat)欧洲安全大会和微软Bluehat安全大会上第一位来自中国的演讲者。2018年底，薛锋获《中国信息安全》杂志社主办中国信息安全产业“双推”活动年度领军人物奖项，2019年4月，薛锋获动点科技主办ChinaBang Awards年度创始人奖项。

Kevin O’ Leary
亚太首席安全官
Palo Alto Networks

Kevin O 'Leary是一名资深IT安全专家，在亚太和欧洲的公共机构、私营企业和大型跨国公司拥有20多年的管理、工程和咨询经验。他曾在多个商业垂直领域(特别是ICT、制药、金融、航空和制造业)担任首席安全官和首席安全架构师。Kevin在亚太地区拥有丰富的经验，在加入Palo Alto networks之前，Kevin曾担任通用电气大中华区副总裁和首席信息安全官。在这个职位上，Kevin为全球和当地的领导层提供安全与风险方面的建议，这些建议与中国和全球其他增长地区的商业战略相一致。在此之前，Kevin是惠普交付的亚太及日本地区 CISO。

演讲嘉宾

郝轶
安全业务CTO
深信服科技股份有限公司

深信服安全业务CTO，14年网络安全行业从业经验。长期从事于网络安全行业态势跟踪、趋势洞察、方法总结、架构设计、规划咨询等工作。
对网络安全等级保护、NIST CSF、ISO27001/20000/22301有一定了解。

刘博
首席科学家
高级副总裁
杭州安恒信息技术股份有限公司

刘博，杭州安恒信息首席科学家（高级副总裁），美国马里兰大学计算机博士，曾在美国Facebook和Square担任大数据和机器学习科学家职位，2017年回国后入选浙江省千人计划专家，中国软协2017年优秀CTO，主导省级、国家级重大科研项目3项。在大数据，机器学习和人工智能领域研究10余年，发表多篇英文文章，国际总引用5000多次。完成智能威胁检测、AI异常分析、UEBA、网络安全威胁智能推理等50余项技术发明专利。担任大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心副主任。

应急响应

刘志乐
首席安全官、高级副总裁
杭州安恒信息技术股份有限公司

刘志乐，现任杭州安恒信息技术股份有限公司（以下简称：“安恒信息”）高级副总裁兼首席安全官，北京大学光华管理学院EMBA硕士学位。同时担任中国计算机学会青年计算机科技论坛（CCF YOCSEF）杭州分论坛副主席（2016-2017届,2017-2018届）、中国网络空间安全协会竞评演练工作委员会委员、中国网络空间安全协会应急工作委员会委员（筹）、中国网络安全产业联盟常务理事、中国通信学会网络空间安全战略与法律委员会第一届委员、首届网络安全人才发展工作组副组长、云安全联盟（CSA）杭州分会负责人、OWASP中国分会委员、浙江省计算机信息系统安全协会安全技术专业委员会副主任、浙江师范大学特聘教授、浙江工业大学计算机科学与技术学院/软件学院校企合作委员会专业建设咨询委员会专家、广东外语外贸大学特聘教授、广州大学网络空间先进技术研究院企业导师等职务。

长期致力于网络安全方面的研究，并始终保持着对信息安全前沿技术的敏锐把握。在安恒信息工作期间先后参与和主持了智慧城市安全、大数据安全和态势感知等信息安全创新领域的研究和开拓，主要研究方向有：1、安全形势的严峻与安全技术的发展趋势 2、云计算和大数据的安全挑战与机遇 3、云计算安全模式的实践 4、基于大数据的态势感知实践。

李冰
原副主任
国家信息技术安全研究中心

国家信息技术安全研究中心原副主任，长期从事网络安全研究工作，先后主持或参加完成了多项重大网络安全专项科研项目，获科技进步奖十多项。

何能强
高级工程师
国家互联网应急中心

何博士毕业于清华大学电子工程系，2012年7月进入国家互联网应急中心（CNCERT/CC）工作，现任高级工程师，长期从事国家级网络安全应急响应工作，包括移动恶意程序逆向分析、移动应用程序安全检测及相关威胁情报提取分析等技术研究和系统研发工作，完成十余项移动互联网安全的国家标准、行业标准，以一作形式获得国家发明专利授权3项，组织出版移动互联网安全年度报告3本，发表SCI、EI等学术论文十余篇，承担中国反网络病毒联盟（ANVA）、中国互联网网络安全威胁治理联盟（CCTGA）等行业自律组织主要工作。

演讲嘉宾

赵阳
总经理
Tenable中国区

现任Tenable中国区总经理，超过20年的IT领域技术与管理从业经验，有着丰富的网络及安全技术背景，曾先后就职于Nortel，Aruba等多家IT知名厂商，了解国内外最新的安全技术动态，也曾参与国内多家大型金融机构及企业的态势感知，资产与风险管理平台项目建设。

张润滋
高级安全研究员
绿盟科技

张润滋，中国科学院大学博士，博士主要研究方向为网络安全数据采集与分析。2018年加入绿盟科技，现任绿盟科技创新中心高级安全研究员，研究领域涉及威胁检测与威胁狩猎、安全知识图谱等。参与用户实体行为分析、威胁狩猎、威胁情报分析等创新项目的孵化工作，主持北京博士后资助项目《基于数据分析方法的网络威胁狩猎研究》。

傅奎
CTO
上海雾帜智能科技有限公司

信息安全领域十三年以上从业经验，曾服务于华为、唯品会等公司。前千寻位置信息安全负责人，阿里云MVP项目成员，掌握极其丰富的云上企业安全最佳实践。目前正担任上海雾帜智能科技有限公司CTO，为企业锻造革命化的安全运营利器。

杨大路
CEO
北京天际友盟信息技术有限公司

杨大路，天际友盟创始人&CEO，烽火台安全威胁情报联盟联合创始人，中国科学院西安光机所大数据应用工程中心副主任。曾任前全球最大公用事业公司安全运营中心负责人，具备多年的超大型企业信息安全运营实践经验，在态势感知、威胁情报、安全监测、安全攻防、模拟仿真、大数据分析等领域有丰富的实践经验和独到的技术见解。

演讲嘉宾

人才培养

鲁辉
秘书长
中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟秘书长，广州大学网络空间先进技术研究院方滨兴班主任，中国网络空间安全协会竞评演练工作委员会竞演办主任，广东省计算机学会第十一届竞赛委员会常务委员。广州大学“百人计划”引进人才，深圳平安金融研究院专家委员，中国网络空间安全协会大数据安全人才培养基地技术委员会委员。主要研究方向包括网络自动化攻防、人工智能安全等工作。筹划组织了“XP靶场挑战赛”、“特定音视频分析系统评测资格大赛”、“强网杯”网络安全挑战赛等全国网络安全赛事，并指导极棒嘉年华，XCTF全国联赛，参与筹划落实“网安中国行”全国多站活动。

刘建伟
院长
北京航空航天大学

刘建伟，教授、博导，北京航空航天大学网络空间安全学院院长。现任中国密码学会理事、教育部高等学校网络空间安全专业教学指导委员会委员。获得国家技术发明一等奖、国防技术发明一等奖、山东省计算机应用新成果二等奖、山东省科技进步三等奖、北京市教学成果二等奖；出版教材5部、专著1部、译著1部，获得全国普通高校优秀教材一等奖、国家网络安全优秀教材奖、国家精品教材、第四届中国科普作家协会优秀科普作品金奖、第十一届“文津图书奖”、全国优秀科普作品奖。荣获国家网络安全优秀教师、北京教学名师、北京市优秀教师、北航教学名师称号。享受国务院政府特殊津贴。

田志宏
院长
广州大学网络空间先进技术研究院

博士，教授，博士生导师，广州大学网络空间先进技术研究院院长，中国网络空间安全协会竞评演练工作委员会秘书长。岭南英杰工程后备人才，广州大学“百人计划”引进学科带头人，广州市优秀专家，曾任哈尔滨工业大学计算机网络与信息安全技术研究中心（北京）主任。长期致力于网络靶场、网络攻防、网络取证等网络空间安全热点领域研究工作。作为课题负责人先后主持了多项国家自然科学基金、国家重点研发计划课题、国家863课题、中央网信办课题，研究成果获钱伟长中文信息处理科学技术一等奖一项，黑龙江省科技进步二等奖一项，黑龙江省高校科技进步二等奖一项，多次获得中央网信办、国家计算机网络与信息安全管理中心、中国网络空间安全协会嘉奖及感谢信。在IEEE Network、TII、TVT、IoTJ、GLOBECOM、WWW等国内外期刊与会议共计发表论文140余篇，专利20余项。

演讲嘉宾

刘哲理
副院长
南开大学

刘哲理，博士（后），南开大学计算机学院副院长、网络空间安全学院副院长，南开大学百名青年学科带头人、天津市千人计划入选者，副教授，博士生导师。主要研究方向为基于密码学的数据隐私保护、密文数据库、密文集合运算等，有5篇论文进入ESI高被引前1%，是腾讯广告、华为数据库的紧密合作伙伴。

吴铤
院长
杭州电子科技大学网络空间安全学院

吴铤，博士，教授，博士生导师，主要从事信息安全与保密研究，先后主持或参与了国家863计划、973计划、国家自然科学基金、浙江省重点研发项目等研究工作。现为杭州电子科技大学网络空间安全学院院长、教育部保密管理专业教学指导分委员会委员。2016年获浙江省保密工作二等功，2017年获中国电子学会科学技术二等奖。

李洋
360网络安全大学总经理
360

360网络安全大学总经理，曾任360校园关系负责人，人人网校园关系负责人，洋葱投CEO等。人力资源管理学士，计算机技术硕士，国际心理咨询师。工作10多年以来一直从事与高校相关的工作，如校园招聘，校园活动，校园营销，校园粉丝团，校园俱乐部，校企合作，协同育人，产学研等业务，并兼任多所高校的创业辅导，人才培养，职业生涯规划等课外导师。在网络安全人才的选拔，职业教育培训，企业内部安全人才的培养方面有着丰富的经验。

李洪伟
副院长
电子科技大学网络空间安全研究院

李洪伟，电子科技大学教授，博士生导师，网络空间安全研究院副院长。IEEE Vehicular Technology Society Distinguished Lecturer，《IEEE Internet of Things Journal》（中科院JCR-1区）Associate Editor。承担1项国家重点研发计划项目（项目总经费1590万元，项目牵头单位总体负责人），发表学术论文100余篇，其中中科院JCR-1区/CCF-A类论文25篇，获IEEE MASS 2018和IEEE Healthcom 2015的唯一最佳论文奖。研究成果已应用于具有百万量级客户量的成都市农商银行的业务系统，该成果的应用成功获得了2017年中国银行业信息科技风险管理课题成果奖。基于以上荣誉与成果，荣获2018中国网络安全与信息产业“金智奖-十大人物奖”。

演讲嘉宾

安全创新

杨卿
创始人
独角兽安全团队(UnicornTeam)

黑客&安全专家，全球黑帽大会Blackhat&黑客大会DEFCON技术演讲者，知名安全团队独角兽(UnicornTeam)的建立者，HACKNOWN黑客创新文化的创始人。研究成果入选特斯拉、GSMA等安全研究名人堂，曾获全球Pwnie Awards黑客奥斯卡”最具创新研究奖”及2018中国网络安全十大影响力人物”真观奖”提名。51CTO俱乐部讲师，央视《315》《汽车百年II》等节目出镜安全专家。世界黑客大会DEFCON China Art Contest Winners获胜作品人物原型，也是公安文学作品《东方黑客》的故事人物原型，以及国内首部黑客微电影《I’ m Here》的男主角。著有《无线电》《硬件》《智能汽车》安全攻防大揭秘”技术三部曲”及Springer《Inside Radio: An Attack and Defense Guide》英文技术专著，安全技术成果曾被福布斯、福克斯新闻、WIRED连线、美国国家地理、CNET、IEEE Comsoc、《芭莎男士》等媒体报道。

冯继强
总经理
苏州极光无限信息技术有限公司

冯继强 网名风宁，国内资深安全专家，COG信息安全专业委员会委员、SACC中国架构师大会顾问组专家成员。
现任极光无限总经理，负责公司漏洞研究实验室、红蓝对抗高级攻防及金融行业安全运营中心工作，曾主导建设多个大型企业网络安全纵深防御体系并担任技术顾问。

刘新铭
首席架构师
鉴释科技发展有限公司

刘新铭先生是国际上少数精通编译器技术的计算机科学家之一，他在计算机语言设计和高级编译器优化技术方面具有深入的实践经验。
在30余年的职业生涯中，刘新铭先生在建立和领导系统软件组织的大型研发团队方面具有丰富经验，同时针对不同的客户群需求研发出极具竞争力的产品。他曾担任惠普Java编译器技术实验室主任，领导基于惠普安腾处理器的编译器开发工作。
迄今为止，刘新铭先生在程序分析和优化领域获得了十余项技术专利，而且在多个核心技术期刊上发表了多篇重量级论文。
刘新铭先生毕业于犹他州立大学，并获得了计算机科学硕士学位

演讲嘉宾

梁宇宁
联合创始人兼首席执行官
鉴释科技发展有限公司

梁宇宁先生是鉴释的联合创始人兼首席执行官，管理公司的战略发展、技术研发和市场增长。他的技术背景包括嵌入式系统、平台APIs和计算机视觉(人工智能领域)等。作为一名技术精湛又脚踏实地的技术专家，梁宇宁先生一直希望可以在亚洲创建一家利用编译器技术提高代码质量的科技公司。得益于在中国广泛的联系，他和几位志同道合的好友共同创立了鉴释，将新一代的静态代码分析技术应用到软件开发中。他是一个终身学习者，并不断进步严以律己，这也植根于鉴释的发展使命中——鉴释始终致力于帮助开发者构建和部署安全可靠的代码。

在创立鉴释前，梁宇宁先生在世界500强企业（包括三星、诺基亚、华为）和初创科技公司领导软件开发工作，他拥有超过二十年的软件开发和管理经验。在他的职业生涯中，他曾在中国、韩国和欧洲多个国家的国际性企业就职，对全球的科技和软件安全行业有深刻的行业洞见。

梁宇宁先生毕业于南洋理工大学，并获得工程硕士学位。

张瑞冬
CEO
成都无糖信息技术有限公司

张瑞冬，Only_guest，现任成都无糖信息技术有限公司CEO，四川大学特聘网络安全专家，知名安全团队PKAV负责人，国内最有影响力的白帽子之一。在WEB安全、漏洞挖掘、网络攻防等研究领域具备卓越的技术实力和丰富的实战经验，目前致力于反网络犯罪领域的安全技术研究与产品研发，为国家及各省市公安机关在反网络犯罪领域做出了积极的贡献。

柴坤哲
安全总监
BCM Social Corp

柴坤哲，BCM Social Corp安全总监，八年安全领域从业经验，国内首个无线安全防御产品标准制定者，伪基站防御技术发明者，知名无线安全工具MDK作者之一，获得无线通信防御专利30余个；带领团队在国内外各大安全会议BlackHat、DEFCON、HackInTheBox、POC、Codeblue等分享研究成果。

演讲嘉宾

林正显
研发总监
BCM Social Corp

林正显，BCM Social Corp研发总监，二十年通信及互联网研发从业经验，对通信及其安全有浓厚的兴趣；荣获过省级优秀专利奖及多项公司技术大奖，拥有多项发明专利。

黄琳
360安全研究院高级技术总监
360

黄琳，360公司安全研究院高级安全研究员，无线安全专家，北京邮电大学博士。360公司3GPP标准组织SA3参会代表。北京邮电大学硕士研究生企业导师。擅长无线信号分析和逆向，移动通信安全。

赞助商

黄金合作方

深信服科技股份有限公司
Sangfor Technologies

深信服科技股份有限公司是一家专注于企业级安全、云计算及基础架构的产品和服务供应商，拥有智安全、云计算和新IT三大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让用户的IT更简单、更安全、更有价值。经过十九年的发展，公司先后被评为国家级高新技术企业、下一代互联网信息安全技术国家地方联合工程实验室、广东省智能云计算工程技术研究中心等。目前在全球设有50余个分支机构，员工规模超过5000名。

360网络安全大学
360 CYBER SECURITY UNIVERSITY

360公司是中国最大的互联网和移动安全产品及服务提供商。360网络安全大学是中国最大、最专业的网络安全教育服务提供商。360网络安全大学前身是360网络安全学院，成立于2017年，周鸿祎先生任荣誉校长。专注于网络安全教育及网络安全产业相关领域，为政府企业培养网络安全人才，为国家网络安全保驾护航！

赞助商

黄金赞助商

AURORA极光无限

苏州极光无限信息技术有限公司
AURORA INFINITY INFORMATION TECHNOLOGY CO.,LTD.

极光无限，坐落于苏州金鸡湖畔的5A级写字楼苏州中心D座，是一家以安全技术为核心、AI技术为驱动的信息安全科技公司，由十多位来自国内外顶尖安全公司的资深安全专家及数位从事AI及信息安全领域研究的教授、博士进行技术领携。依托最前沿的图神经网络理论，公司致力于打造国际一流的AI自动化漏洞挖掘及APT自动攻防产品；公司将重点组建全球顶级的红蓝对抗及漏洞挖掘研究团队，以辅助和完善AI自动化安全产品研发。

派拉软件 PARAVIEW SOFTWARE

上海派拉软件股份有限公司
Shanghai Paraview Software Co., Ltd.

上海派拉软件股份有限公司（简称：派拉软件）是中国领先的新一代信息安全技术公司，数据定义，AI驱动，智能算法，场景分析，以科技驱动，为企业和机构提供信息安全产品、咨询和实施服务，业务覆盖身份安全、业务安全、数据安全三大领域，涉及企业身份安全、客户身份管理、特权身份管理、多因子安全认证、用户行为分析、API安全管理平台、技术中台、数据湖、数据中台等，已成功为汽车、制造、金融、地产、家居、零售、教育、医药、政府等500多家大中型企业和单位提供了信息安全服务。目前，派拉软件在上海、北京、广州、长春、武汉、成都、深圳设有服务机构。是经政府认定的高新技术企业、软件企业、企业研发机构、专精特新中小企业和上海市科技小巨人企业，通过了ISO9001、ISO27001、CMMI三级、信息系统安全集成服务资质等，拥有多项公安部安全产品销售许可和50多项知识产权。

赞助商

黄金合作方

TENABLE

作为 Nessus 技术的首创者，Tenable 将其在资产发现及漏洞合规管理方面的专业技能扩展到 Cyber Exposure Platform，提供多维度、全方位的持续风险可视解决方案，帮助安全管理者了解安全态势，　提升信息安全应急响应能力。今天，我们与全球各地 27000 家企业和政府机构合作，帮助它们获得其所面临的整个现代网络攻击面的可见性，认识到自身面临的风险，以及该如何集中精力解决那些商业风险最高的问题。目前企业首席信息安全官已将网络风险作为其在战略决策过程中的关键风险指标，这与他们利用客户关系管理系统 (CRM) 预测销售或利用企业资源规划系统 (ERP) 预测供应链趋势是一脉相承的。

Chengdu NoSugar Information Technology Co., Ltd.

成都无糖信息技术有限公司（简称无糖信息）是以国内知名安全团队PKAV为核心的自主创新型企业，致力于反网络犯罪领域的安全技术研究与产品研发，包括电信诈骗、网络诈骗、网络传销、网络色情、网络赌博等。为国家及各省市公安机关提供高效专业的反网络犯罪情报分析服务和实战解决方案。

无糖信息已与180余家公安机关开展合作，项目涉及反电信网络诈骗预警反制平台、反涉众型经济犯罪预警反制平台等相关自动化实战平台建设，并与相关部局建立联合实验室，进行相关领域技术研究。

网络流量分析 NTA 加速利器

GS7000 系列

NTA加速利器

GE/10GE/40GE/100GE

155M/622M/2.5G/10G POS

汇聚、分流、复制、过滤、截断、去重样样精通。

应用于DPI、APM、NPM、大数据分析、
网络安全等领域。

MIPS/FPGA智能网卡

支持2/4个10G 光口

8/16核处理器、8/16/32G内存

采集、过滤、会话管理、POS协议转换、时间戳样样都行。

应用于高性能流量采集、关键字匹配，
卸载服务器压力。

致力于为网络大流量分析 NTA 提供硬件级网络加速解决方案

方案特点:

- 提供高性能网络捕包、DPI和会话管理能力，卸载主机业务，提升总体性能；
- 支持155M/622M/2.5G/10G SDH/POS信号转换，串接/并接采集分流解决方案；
- 开放硬件平台基于可编程FPGA/NP架构，灵活定制；
- 提供国产自主可控产品定制；

湖南有马信息技术有限公司
www.uucode.com.cn

赞助商

展位赞助商

亚数信息科技(上海)有限公司
TRUSTASIA TECHNOLOGIES, INC.

亚洲诚信是亚数信息科技（上海）有限公司应用于信息安全领域的品牌，专业为各行业提供国际知名品牌数字证书及网络信息安全管理解决方案。旗下TrustAsia品牌SSL证书市场占有率在国内保持领先地位。客户覆盖电子商务　　、互联网金融、银行及政府机构、保险证券、医疗机构、系统与软件开发商等各个领域。亚洲诚信是网络信息安全领域深受认可和值得信赖的品牌！

奇安信科技集团股份有限公司
QI AN XIN TECHNOLOGY GROUP INCORPORATION

奇安信集团是专门为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，相关产品和服务已覆盖90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展了安全业务。

微步在线科技有限公司
THREATBOOK

微步在线是专注威胁情报能力输出的安全企业，国内威胁情报领军品牌，提供专业的威胁检测产品与服务。公司主要成员来自于亚马逊、微软、BAT、美团等科技公司。微步在线从成立初始便专注于威胁情报领域，积累了深厚的威胁分析能力，已将情报数据能力和分析能力以专业的威胁检测/情报管理产品等方式赋能给客户，帮助客户落地威胁情报能力、建立全方位的威胁监控体系。2017-2018年多次入选全球网络安全500(CyberSecurity 500)，并在2017、2019年连续两次成为唯一入选Gartner全球威胁情报市场指南的中国公司。

成都云祺科技有限公司
Chengdu Vinchin Technology Co.,Ltd

成都云祺科技有限公司，专业的云计算容灾备份解决方案提供商，专注于虚拟机备份与恢复。其产品云祺虚拟机备份与恢复系统（Vinchin Backup & Recovery）,属于云计算安全产品,该产品主要完成在虚拟化环境下，对虚拟机进行备份、恢复、迁移、灾难恢复，实现数据的容灾，防止由于人为误操作、病毒、攻击、自然灾害、战争等对数据的毁灭性破坏。目标用户群体为政府、军队、医院、学校、研究所、设计院、军工、大型企业、国有企业等企业级用户。

赞助商

展位赞助商

OPPO安全应急响应中心
OPPO Security Response Center

OPPO安全应急响应中心（OPPOSecurity Response Center，以下简称OSRC），是致力于保障OPPO用户、业务和产品等安全，促进与安全专家的合作与交流，而建立的漏洞收集及响应平台。OPPO互联网安全团队主要负责OPPO互联网安全体系建设，包括攻击对抗平台、业务安全风控平台、安全预警平台、数据安全技术平台，入侵防御平台等；安全技术攻防对抗，包括Web攻防、Linux攻防、移动应用攻防、物联网攻防；大数据安全和人工智能安全平台建设；安全标准体系建设等。

北京天际友盟信息技术有限公司
TIANJI PARTNERS CO., LTD.

北京天际友盟信息技术有限公司，成立于2015年，总部设在北京。一直以来，天际友盟秉承“创造安全价值”的品牌理念，以安全能力出发，致力于为客户解决实际业务风险，让安全解决方案为客户带去真正的价值。天际友盟在北京、西安、石家庄三地设有研发中心，在上海、深圳、西安、长春、长沙、重庆、银川、石家庄八地设有办事处，为全国20余家合作伙伴和近百家客户提供高效、优质的服务。目前，天际友盟旗下有两大类业务：安全情报应用和数字品牌保护。

赞助商

展位赞助商

成都世纪顶点科技有限公司
Chengdu Global Capsheaf Solution Co.,Ltd

成都世纪顶点科技有限公司成立于2012年，是一家专业从事网络安全、容灾抗毁、云计算产品研发、生产及销售的供应商，是国家高新技术企业、国家商用密码生产定点单位、信息安全重点培育企业、软件企业、保密协会理事单位.公司取得国家发明专利19项、计算机软件著作权60多项，先后获得四川省科技进步一等奖、成都市科技进步一等奖；产品通过了公安部、国家保密局、中国信息安全认证中心认证，是国家保密局推荐产品、四川省地方名优产品、成都市首版次产品，产品已经广泛应用于政府、医疗、教育、企业、能源等2000多家单位。

湖南有马信息技术有限公司
Hunan UUCODE Information Technology CO.,LTD

有马信息专注网络安全领域、网络协议分析领域的大数据接入、汇聚、筛选、分发、预处理、DPI前端技术和产品。致力于为网络流量分析（NTA）领域提供硬件加速和业务卸载解决方案。
自主产品:
GE/10GE/40GE/100GE可视化交换机、智能加速卡、开放网络通信硬件平台和网络流量采集方案。
产品特点:
提供高性能网络捕包、DPI和会话管理能力，卸载主机业务，提升总体性能；
支持155M/622M/2.5G/10G SDH/POS信号转换，串接/并接采集分流解决方案；
开放硬件平台基于可编程FPGA/NP架构，灵活定制。

赞助商

展位赞助商

维择科技
DataVisor

DataVisor致力于建立与保护终端用户对在线服务的信任。DataVisor携手世界上最大的金融公司和互联网产业，保护他们免受欺诈，虚假推广、和洗钱在内的一系列攻击。DataVisor的无监督机器学习是反欺诈领域的最前沿技术，其检测解决方案无需训练数据，即可自动检测各类攻击，并且能做到提前预警。

DataVisor由从事大数据分析和机器学习各方面的世界级专家组成。并协作构建了世界上最先进的算法，以应对最复杂的在线攻击。

智联招聘
BEIJING ZHAOPIN.COM COMPANY LIMITED

智联招聘，成立于1994年，深耕人力资源服务市场25年。目前已拥有39家分公司，业务遍及200多个城市，已累计为456万家以上企业提供了人力资源服务。同时，也成为1.8亿职场人信任的职业发展平台。智联招聘数据报告拥有25年数据积累，覆盖中国地区全行业的调研范围，全方位展示国内职场动态，被众多国内外权威媒体誉为“中国职场风向标”，为政府的宏观调控、企业的微观决策和劳动者个人的选择起到指引作用。

上海易念信息科技有限公司
Shanghai Yinian Information Technology Co., Ltd.

上海易念信息科技有限公司（易念科技）是中国网络安全意识教育的领导企业，公司秉承教育改变认知、意识决定安全的核心理念，面向企业提供教学内容、工具平台、运营服务等配套解决方案，致力成为网络空间安全人脑防火墙缔造者。

烽台科技（北京）有限公司
FENG TAI TECHNOLOGY(BEIJING) CO,LTD

烽台科技专注于工控安全领域，主要提供专业化、标准化工控安全咨询、评估服务，保障工业关键信息基础设施信息安全，完善安全防护解决方案。主要服务于政府、行业客户、设计院／所、科研院／所、集成商及软硬件厂商，通过可视化、流程化、定制化的工具和方法，协助用户进行有效的风险管理与可靠的运营支撑。

赞助商

展位赞助商

BCM MESSENGER

BCM是一支由追求极致与创新的世界知名研发人员和黑客组成的团队。他们设计了一款高度安全的即时通信平台，其每一条信息都经过严格加密，没有任何第三方可以解密其内容；他们的自研算法可组成多跳ad hoc网络，即不依赖运营商网络即可与附近的人进行通信的新型技术； 他们将始终如一地致力于隐私保护和通信互联，努力构建一个可靠、安全的万物互联网络。现在，由BCM重新定义一个新的信息时代。

北京赛博英杰科技有限公司
BEIJING GENIUS CYBERTECH CO.,LTD

中国第一家为网络安全公司提供全生命周期服务的顾问公司，为客户提供定制化商业建议并协助客户管理增长。本公司由原360集团技术总裁谭晓生先生创建，连同行业众多专家共同为中国网络安全企业服务，连接资本与行业，满足创业者、CEO、董事会和投资人的独特需求。专门为网络安全行业量身定制的创新咨询模式，在企业生命周期中为其提供卓越运营、企业融资、战略规划、退出规划和并购等服务。

中国网络空间安全人才教育联盟
THE CYBERSPACE SECURITY TALENT EDUCATION ALLIANCE OF CHINA

中国网络空间安全人才教育联盟（The Cyberspace Security Talent Education Alliance of China，简称为：CEAC）是在中国产学研合作促进会的指导下，由从事网络空间安全相关教育、科研、产业、应用的高校、科研学术机构、企业单位、社会团体、事业单位，以及热衷于网络空间安全人才教育的个人共同自愿结成的全国性、行业性、非营利性、创新性组织。

赞助商

合作单位

Inspiring a Safe and Secure Cyber World

(ISC)²

(ISC)² （国际信息系统安全认证联盟）是一个国际非营利会员组织，专注于启迪构建一个安全可靠的网络世界。因其广受好评的信息系统安全认证专家(CISSP®)认证而最为人熟知，(ISC)² 提供全方位、程序化的安全解决方案认证组合。我们的全球会员人数已经超过140,000，由经过认证的网络、信息、软件和基础设施安全专家组成，志在为行业发展带来改变并协助其进步。我们以慈善基金——网络安全和教育中心TM对教育和普及大众的承诺而践行我们的愿景。

CDSIA 成都市软件行业协会

成都市软件行业协会
Chengdu Software Industry Association

成都市软件行业协会是国家5A级社会组织，由成都从事软件研究、开发、生产、销售，计算机系统集成、信息技术服务及信息化系统应用，计算机教育和管理工作的单位、个人自愿组成，是成都市民政局核准登记的非营利性组织。协会以服务企业、整合资源、共享信息、树立品牌为宗旨，面向政府、企业与社会，发挥政府与企业间的桥梁与纽带作用，成为成都市软件和信息技术服务行业的信息交流中心、政策研究中心、经营指导中心、技术培训中心、科技服务中心。

BigData 四川省大数据产业联合会 Sichuan Big Data Industry Federation

四川省大数据产业联合会
Sichuan Big Data Industry Federation

四川省大数据产业联合会是在四川省经信委的指导下，由省内多家企业和高校联合发起成立的行业性社团组织，致力推动省内云计算大数据产业的发展。联合会以促进省内云计算大数据企业互动、聚力产业发展为指导方针，落实四川省大数据产业发展和应用的具体工作要求，围绕大数据技术链、产业价值链，实现产学研用等机构在战略层面的有效结合，通过资源共享、协同行动和集成发展等市场化运作，形成产业核心竞争力，创新四川省大数据应用水平，促进数据驱动的产业变革和模式创新。

无糖信息

致力于反网络犯罪领域的安全技术研究与产品研发

向网络犯罪开炮

反电信网络诈骗

反网络传销

反网络赌博

反网络黑灰产

新型网络违法犯罪

反网络色情

51CTO | AI·X

AI·X人工智能社区

直播
【大咖来了】AI大咖定期直播

资讯
人工智能热门资讯

博客
畅意分享您的工作生活

社群
随时随地交流 AI·X大咖来了交流群

公众号
有趣有料的 AIX人工智能前沿

直播栏目 大咖来了

大咖来了第一期

杨海明
原京东集团技术发展部负责人
新零售时代的智慧中台

大咖来了第二期

胡显波
快狗打车订单策略负责人
快狗打车智能化演进之路

更多精彩 等待您来

http://aix.51cto.com

加我进群 了解更多

合作媒体

核心合作媒体

FreeBuf
www.freebuf.com

国内最早、知名度和活跃度最高的安全技术交流平台，汇集全球最新安全资讯、深度报告，是安全技术人员交流、分享、学习和成长最佳的平台。

51CTO
www.51cto.com

51cto.com是中国IT及互联网领域领先的专业垂直技术媒体，拥有1700万注册用户，覆盖了中国主流城市大多数IT从业人群，致力于促进IT技术领域知识传播与服务创新。平台汇聚超过10000名技术专家，在人工智能、云计算、开发、物联网、大数据等多个技术领域产出80W篇文章及1万多个专题，与包括IBM、微软、戴尔、华为、腾讯、阿里巴巴、百度等20000多家国内外企业成为合作伙伴，与上百家网络媒体、平面媒体、广电媒体、移动媒体等保持良好的密切合作关系。

至顶网
www.zdnet.com.cn

至顶网，前身ZDNet China于1997年在北京成立，是国内最早的科技网络媒体，见证了中国IT产业和互联网的成长历程。同时，至顶网是CBS美国哥伦比亚广播公司的在华独家科技内容战略合作伙伴，拥有后者全球12个国家或地区的内容资源，品牌和相关创新产品的使用权。
近年来，至顶网在基于原有IT应用与业界新趋势的报道与分析上，不断强化在业界的领导地位，并不断延伸自身业务发展，尤其强调信息技术和传统行业的结合。

科技行者
http://www.cnetnews.com.cn/

科技行者是一个集合了科技行者网站、APP、新媒体等平台资源的媒体矩阵，为用户提供人工智能、区块链等新技术的的信息服务平台，致力于记录并推动人工智能和区块链的行业应用、产业发展、技术创新。

合作媒体

合作媒体

Dark Reading
www.darkreading.com

是全球最大的网络安全信息平台之一，提供最新的网络威胁，漏洞和趋势提供情报跟踪。同时由行业分析师，技术专家编辑来运维的13大社区版块，与会员分享实时的文章和交流讨论，在全球安全圈享誉盛名。

Information Week
www.informationweek.com

定义数字化商业时代科技技术的价值。作为全球最可信的商业技术资源，InformationWeek提供独道的见解和意见帮助当下技术领袖探索快速变化的技术市场以及挖掘推动企业向前发展的最佳策略和工具。

Network Computing
www.networkcomputing.com

IT专业人士依靠Network Computing及其附属会议Interop向读者展示下一代网络、数据中心、存储系统、通信和云架构背后的方式和原因。interop是it社群的线下会议，而网络计算为it从业人员提供了在线体验。

安全牛
www.aqniu.com

安全牛是国内目前影响力最大的安全行业媒体和调研机构，其核心为对网络安全行业的调查与研究，如每年的网络安全100强报告、安全行业细分领域矩阵图，以及反映整个产业的网络安全行业全景图等。同时，撰写和发布相关领域的技术指南与应用指南白皮书。

安全牛以“媒体即服务”为运营理念，为政府、企业、安全公司及相关机构，提供新闻报道、会议沙龙、调查报告、咨询智库、创业孵化、资源对接等服务，实现安全知识及经验的传递与分享。

合作媒体

合作媒体

OWASP中国
www.owasp.org.cn

OWASP安全组织是一个免受商业压力的社区,能够提供有关应用程序安全性的公正、实用、经济高效的信息。OWASP安全组织不隶属于任何技术公司，尽管我们支持在知情的情况下使用商业安全技术。与许多开源软件项目类似，OWASP安全组织以协作和开放的方式生产多种类型的材料。OWASP中国是OWASP安全组织在中国区域的分部。开展有关互联网安全技术的研究和推广工作。

C114通信网
www.c114.com.cn

C114通信网创立于1999年，运营至今，影响力广泛覆盖通信及ICT领域， C114拥有海量原创资讯和读者、商业价值深受客户认可和信赖，成为国内通信及ICT领域决策者优先选择的网站。伴随着中国通信产业链的高速崛起，C114持之以恒为整个行业提供包括资讯、论坛、会展、公关等多元化服务； C114拥有手机网页版、微博、微信公众号、客户端APP等多种移动端呈现形式；满足广大用户对浏览学习、交流互动、分享表达等多元化与个性化的诉求。

E安全
www.easyaq.com

E安全创办于2014年，是北京易安乾坤信息科技有限公司旗下的一款内容分享平台，主要受中群体为信息安全行业内人员。
目前，E安全运营着E安全app、E安全门户网站（www.easyaq.com）以及E安全官方微信公众号（EAQapp）三大内容平台，并与搜狐、网易、新浪、腾讯、凤凰、今日头条、一点资讯、百度百家展开合作，年度总阅读量突破9000万，月均受众突破600万。

安全内参
https://www.secrss.com/

《安全内参》是专注于网络安全产业发展和行业应用的高端智库平台，依托于专业的安全团队和数千位国内外顶级的产业和行业智库和专家团队，为网络安全相关政府主管、行业、企业和机构的管理者、决策者和从业者提供全球视野、高价值的安全知识和安全智慧，致力于成为网络安全首席知识官。

合作媒体

合作媒体

极客网-科技使能新商业
www.FromGeek.com

极客网创办于2012年，早期是一个由技术爱好者组成的极客（Geek）社区，后尊崇“科学技术是第一生产力”实现商业化运作，旨在探索科技创新在新商业变革中的角色和能量。

亿邦动力
www.ebrun.com

亿邦动力是目前国内最具影响力的电商知识平台，立足电商，覆盖了2000余万国内外电商经理人，在零售、大宗、农业、跨境、大健康、汽车、电商服务、国际电商等诸多重点电商领域与方向上建立了广泛的影响力。

畅享网
www.vsharing.com

畅享网是第三方IT服务平台模式的创立者。至今，畅享网积累了400余万实名制会员用户，会员主体为企事业单位信息化管理者和决策者。畅享网聚焦信息化，面向大型企事业单位，提供媒体服务和 IT 服务。媒体服务包括：创新解决方案及技术研讨、第三方研究、专业活动等。IT服务包括：信息化规划、原型设计及概念验证、软件创新开发、项目监理、费用及绩效评估、服务外包等。

网络安全和信息化
www.365master.com

IT运维网是《网络安全和信息化》杂志官方网站，杂志原名《网管员世界》《网络运维与管理》，是由工业和信息化部主管，中国电子信息产业发展研究院（暨赛迪集团)主办的信息安全技术类杂志，杂志内容以网络安全、运维、云计算、大数据、人工智能、物联网、软件、虚拟化、服务器、数据中心等为主，读者面向企事业单位CIO、CTO等网络管理人员和技术人员，是一本实用性强的信息安全类杂志。

合作媒体

合作媒体

中国电子银行网
www.cebnet.com.cn

FreeBuf
www.freebuf.com

国内最早、知名度和活跃度最高的安全技术交流平台，汇集全球最新安全资讯、深度报告，是安全技术人员交流、分享、学习和成长最佳的平台。

OFweek | smartcity.ofweek.com
智慧城市网
中国智慧城市行业门户

OFweek智慧城市网
ofweek.com/smartcity

OFweek智慧城市网是智慧城市行业门户网站，为城市管理者和信息化厂商机构提供及时、全面的智慧城市业界新闻、顶层设计、软/硬件、网络通信、物联网、云计算、数据中心、系统集成，以及运营服务等新闻报道。
OFweek智慧城市网秉承“专业、思想、价值”的服务理念，致力于推动智慧城市、智慧产业、智慧民生等产业的发展，促进新一代信息技术、智慧应用项目及智慧城市建设。

安全牛
AQNIU.COM

调查报告

市场指南

☑中国网络安全100强企业　☑中国网络安全行业全景图　☑中国网络安全细分领域矩阵图

技术指南

移动业务安全

反欺诈　威胁情报

新一代SOC　工控态势感知

应用指南

- 数据库安全
- 视频监控安全
- UEBA
- 数字品牌保护
- 数据防泄密
- 在线交互安全
- 信息资产风险与合规管理

媒体服务

安全牛拥有微信公众号（aqniu-wx）、网站（www.aqniu.com）、牛聘（job.aqniu.com）、今日头条、搜狐、腾讯企鹅号、阿里大鱼号、百度百家等内容传播平台。

- 行业资讯整理
- 专业文章撰写
- 会议活动报道
- 人物专访

会议活动

安全牛长期举办网络安全会议，已成功举办十几场CS系列解决方案大会，同时与国家部委、地方政府、安全厂商、展会公司等共同合作举办行业大会。会议内容包括解决方案、技术趋势、产业分析、政策宣贯等。

智库服务

安全牛为政府、监管单位、投融资及相关研究机构提供行业咨询及智库咨询服务。

C114.COM.CN

推动智能 连接世界

C114 官方APP

C114 微信公众号

通信人家园

C114 微博

通信人说

物联网杂谈

5G观察家

光通信观察

量子大观

运营商招标

网址：www.c114.com.cn / 地址：上海市徐汇区桂平路418号1104/1105室

极客网

FROMGEEK.COM

科技使能新商业

极客网创办于2012年，早期是一个由技术爱好者组成的极客（Geek）社区，后尊崇“科学技术是第一生产力”实现商业化运作，旨在探索科技创新在新商业变革中的角色和能量。

极客网的极客不是狭义上的极客，而是广义上的极客精神——崇尚科技、自由与创造。极客网以推动极客精神为己任，极致报道、客观记录科技创新引领商业变革的轨迹。

极客网以“极客观察”、“极客访谈”、“极客评测”、“极客图说”、“锐话题”、“大事件”、“极品”等匠心内容连接优质读者；覆盖IT网络通信、智能硬件、人工智能、汽车科技、金融科技、新零售、大文娱等领域；另有“自明星”和“极客大奖”汇聚、联接产业创新者与行业观察者。

极客网拥有一支跨界融通的原创报道团队，骨干成员有来自新浪科技、21世纪经济报道、易观国际等机构的传媒、研究人员，也有来自华为、德州仪器（TI）等企业的技术、营销人士。跨行业、跨工种的融会贯通，让我们的报道更专业、更深刻、更接地气。

极客网的读者受众是中国新兴的创业创新、年轻白领一代，他/她们崇尚科技和自由，尊重努力与创新，正在成长为中国的“新中产阶级”。

展望未来，未来已来。极客网与您一起成长！

网址：http://www.fromgeek.com

微信公众号：fromgeek_com

QQ：1811731053

关于畅享网

ABOUT VSHARING

成立于2006年，是第三方IT服务平台模式的创立者，被公认为企业级信息技术领域最具影响力的第三方IT服务平台，畅享网是上海市“专精特新企业“、上海市和浦东新区的中小企业共服务机构，获得高新技术企业认定，拥有国家级信息系统监理资质曾多次获得国家和市级的资金支持及荣誉称号。至今，畅享网积累了400万余实名制会员用户，会员主体为企事业单位信息化管理者和决策者。畅享网为会员提供每日海量信息化资讯、230万篇专业的文档下载、每年超过20场的线上线下主主题活动，及为高端会员搭建的社区平台，畅享网一直专注专业。

核心业务

媒体服务

1. 深度内容：通过网站及微信服务号，提供创新解决方案及技术的新闻、案例、观点等。
2. 第三方研究：以第三方视角，对行业、专业领域、用户、产品、厂商、政府政策等进行研究。
3. 创新方案：通过活动、网站、服务号等，进行创新方案及技术推广。
4. 品牌活动：聚焦企事业单位信息化，为CIO举办多种形式、创新主题的研讨会、论坛、参观和培训。

IT服务

1. 信息化咨询：主要是信息化规划、原型设计及概念验证、专项咨询等。
2. 第三方IT治理：信息系统工程监理、IT费用评估、IT绩效评估、软件测试、安全测评等。
3. 创新方案开发：创新设计研讨会、场景设计、交互开发、运营改造。
4. 服务外包：信息系统运维外包、网络运维外包、微信运营外包。

投资服务

以伟众投资为载体，向具有核心能力的企业级IT企业以及利用互联网进行转型的企业进行股权投资，注入技术、行业、人力、政策等资源，帮助其健康成长。

专家顾问团 2019 Advisory Board

总部地址：上海市浦东新区浦建路 145 号强生大厦 2303 室
电话：021-5109-6826
联系邮箱：frances.zhou@vsharing.com

订阅

网络安全和信息化

Security & Informatization

订阅杂志送

50元京东E卡

2020全年300元

邮发代号2-99

咨询电话:010-88558703

邮局订阅:11185(全年360元,含APP)

微店订阅

注：赠京东E卡活动仅限在杂志社订阅全年杂志用户享有！

中国电子银行网

www.cebnet.com.cn

专业领先的新金融平台

中国电子银行网（www.cebnet.com.cn）是由中国金融认证中心（CFCA）联合近百家成员银行创建的电子银行业垂直网站，是目前金融领域极具权威性和专业度的行业平台。网站主要下设金融科技、名家专栏、银行动态、信息安全、Bank帮等频道，内容汇聚重要行业政策解读、重磅专家观点分享、行业热点评论、前沿资讯以及权威研究数据发布等。网站始终聚焦于电子银行、互联网金融、金融科技等前沿领域，为金融行业尤其银行业提供专业化的信息服务。我们致力于将网站打造成集前沿资讯和综合服务于**一体的新金融平台。**

中国电子银行网官方微信

400-880-9888

北京市西城区菜市口南大街平原里20-3

媒体合作联系方式：
电话: 010-80864579 电子邮箱: yuanyuan@cfca.com.cn

商务合作联系方式：
电话: 010-80864578 电子邮箱: ffzhang@cfca.com.cn

合作媒体

自媒体伙伴

科技云报道
www.itcloudbd.com

科技云报道——前沿企业级IT领域Top10媒体之一。获工信部权威认可，可信云、全球云计算大会官方指定传播媒体。成立5年来以原创优质的新闻报道吸引了超过500万次的阅读。

2019 Advisory Board

Binxing Fang
Chief Advisor, Academician, Chinese Academy of Engineering

Jian Chen
CSO
Ping An Group

Pengfei Dai
Leader of Data Security Department, Meituan-Dianping

Guishan Tung
CISO,CETC, Deputy Chief Engineer
CETC / Chief Engineer, Westone

Yuan Fan
President
Das-Security

Xinhua Ji
CEO
Ucloud

Kaida Jiang
Deputy Director
Network Information Center
Shanghai Jiao Tong University

Yale Li
Chairman of CSA GCR
Executive Chairman of C-CSA

Guangming Lu
COO
AsiaInfo

Hui Lu
General Secretary
The Cyberspace Security Talent Education Alliance of China

Minhu Ma
Chairman,Suzhou Information Security Law Research Center, Xi'an Jiaotong University

Jun Nie
Chief Security Officer and General Manager of Network Security Department
Qianxin Group

Jianfeng Tan
Founder
Shanghai PeopleNet Security-Technology Co., Ltd.

Xiaosheng Tan
Founder and President
Cyber Hero Pte.Ltd.

Zhihong Tian
President, Cyberspace Institute of Advacned Technology, Guangzhou Univeristy

Huaibin Wang(Content Advisor)
CEO
Neural Flex

Yunkun Wu
Chairman
Qianxin Group

Feng Xue
Founder and CEO
ThreatBook

2019 Advisory Board

Qing Yang
Founder
UnicornTeam

Yang Yu
Head of Xuanwu Lab
Tencent Security

Jingping Chou
CSO
Knownsec

Meghan Reilly
Group Director
IT Portfolio, Informa Tech

Tim Wilson
Co-founder and Editor-in-Chief
Dark Reading

Derek Manky
Chief, Security Insights & Global
Threat Alliances, Fortinet

Francis Brown
Chief Technology Officer
Bishop Fox

Paul Vixie
Chairman
CEO & Cofounder, Farsight Security, Inc.

Tim Virtue
Former Chief Security & Risk Office
Lower Colorado River Authority

Monnappa K A
Black Hat Review Board

Shubham Mittal
Black Hat Review Board

Mika Devonshire
Black Hat Review Board

Aloysius Cheang
Board Director and Executive Vice
President Asia Pacific
Centre for Strategic

Advanced Training

Effective Cybersecurity Practices: Architecture and Technology for Financial Institutions

Course Outline:

It is mainly divided into two parts: Security Architecture and Security Technology Practice.

Part I: Security Architecture

This paper mainly introduces the fields involved in enterprise security construction, the main points of financial industry security construction, several key security management fields such as internal control compliance, outsourcing management, etc. It elaborates on security team building, security training, security assessment, security budget and so on, which is helpful to understand the perspective of enterprise security from the perspective of enterprise security builders and to solve problems. This part includes the introduction of enterprise information security construction, financial industry information security, security planning, internal control compliance management, security team building, security training, outsourcing security, security assessment, security certification and others, and other aspects include security budget, vendor management, security summary and security reporting.

Part II: Security Technology Practice

This paper mainly introduces the application practice of security technology in enterprise security construction, including application security, intranet security, data security and business security. It elaborates on some key protection points such as mail, activity catalogue, patch management, anti-DDoS attack, and makes some open discussions on security operation, emergency response and security trend as well as the future of practitioners. These are helpful for enterprise security managers to better grasp the overall situation and act in accordance with the situation.

Beacon Lab: Industrial Control Security

This course system focuses on the field of industrial control security, and spread to the periphery of information security. Industrial control security is a sub-branch of information security and a new field of information security. Safety engineers in the field of industrial control security need to understand not only the industrial control protocol and industrial process, but also the attack and defense technology of traditional information security, which requires very high requirements for engineers. This course system strives to design a system framework, from the introduction of industrial control safety to proficiency, all need to be involved. From theory to practice, and then to the actual penetration of the real environment, step by step, to train a qualified industrial control safety engineer.

Advanced Training

Security Awareness Officer

SAO Training is the first and the only course in China coaching security awareness professions organized by The Cyberspace Security Talent Education Alliance of China. The program aims to support the key person who is responsible for building security awareness and culture within the cooperation by enhancing relative knowledge, experience, and skill.

易念科技
网络安全文化意识价值传播者

SAO Training is developed by Shanghai Yinian Information Technology Co.,Ltd.

Day1 Keynotes

Importance of Public Key Cryptography to Information Security

Martin Hellman
Turing Award Winner 2015
Member of the National Academy of Engineering
Professor Emeritus of Electrical Engineering
Stanford University

Public key cryptography is at the heart of modern information security and protects tens of millions of millions of yuan in financial transactions every day. While this revolutionary technology often leads people to wonder how we thought of it, after this talk you might wonder why it took Whit Diffie, Ralph Merkle and me so long to discover it. The talk also explains the basic operation of public key cryptography as well as highlighting the important contributions of several researchers whose contributions are not widely known.

Achieve Build-in Security in New Technology-System

Yunkun Wu
President
Qi AnXin Group

New generation of information technology such as cloud computing, big data, IoT, MI and AI, has promoted the new generation of information and business system construction based on cloud and big data infrastructure. The new systems need "build-in security" to realize the real safeguard of information investment and business operation.

This topic Focus on how to planning, building and operationing a security system to Achieve "build-in security" in new generation of information and business system.

One's & Zeroes Were Just the Beginning: A Transformational Roadmap for the Backroom to Boardroom

Tim Virtue
Former Chief Security & Risk Officer
LCRA

Join a veteran CSO/CISO for a practical discussion on taking your career to the next level. While technical expertise and a commitment to technology is essential for career success, it is just the beginning.

Attendees will walk away with practical tips on career planning, personal branding, adding value to the business and several other strategies to take your career to the next level.

CSO

Exploration on the Construction of Enterprise Security Mid-platform

Jian Chen
CSO
Ping An Group

Nowadays all kinds of mid-platform (Technology Mid-platform, Business Mid- mid- platform and Data Mid-platform) concepts keep coming up. Security and business have many similarities with the concept of Mid-platform, which can be achieved through continuous abstraction of technology precipitation, data penetration and operational framework for faster and more stable security capability delivery, supporting business innovation and trial and error.

Overall Risk Management

Zuoyu Zhang
DingTalk CRO
Alibaba Group

Overall Risk Management, discussing the risk management from a CRO perspective. Setting balanced objectives for security planning and business development from a transpositional perspective with the guidance of security value and using overall risk management ideas to communicate with business executives.

Internet Bank Security Construction Practice

Feifei Wu
Senior Security Specialist
Ant Financial/ MyBank

How does the author protect the whole process security construction of a company from the start-up stage to NASDAQ listing from zero to one? What experiences are worth summarizing and sharing in retrospect? After that, he joined a large Internet + financial enterprise to take charge of the security architecture. Which historical experience can be followed and which should be discarded? What are the differences between small and medium-sized companies and large companies in security construction? What can we learn from each other? How to protect the security of New Internet technology and traditional financial business integration?

Data Security for Large Internet Companies

Yefei Qian
Head of Data Security
Didi Chuxing

This talk will provide a unique for security perspective and experience from large Internet companies. Large Internet companies have unique data security challenges, namely fast business iteration, high employee turnover, large data volume, frequent organizational changes, and a wide range of information systems. How to achieve a balance of security, experience and efficiency under these conditions, and ultimately bring security incident MTTD and MTTR to under 24 hours?

These problems are difficult to solve under traditional data security frameworks and solutions. Therefore, we integrate data security capabilities into all levels of TOGAF architecture, and achieve security through multiple key objectives supplemented by operational processes.

Trustworthy, Controllable, and Manageable - Identity Security in Digital Transformation

Tony Tan
CEO
Shanghai Paraview Software Co., Ltd.

At present, corporate security focuses on physical security and network security, while there are no effective control means for the abuse of authority within the organization, the illegal establishment of private account number by internal and external personnel, and risk warning and responsibility traceability, leading to frequent information security incidents and mass leakage of many corporate and personal data.

The establishment of a modern, flexible standard and trusted digital identity governance system that integrates various emerging technologies such as AI, big data, cloud and IOT directly determines whether an organization will become an enterprise that provides innovative services to customers with lower costs.

Vulnerability A&D

Making Products Secure yet Intentionally Hackable

Craig Smith
Senior Director of Security and R&D
Iconiq Motors
Author of "Car Hacker's Handbook"

In the automotive industry, when it comes to security, we tend to go from one extreme to the other. Either we have little to no security in our vehicles or we try to lock the vehicle down so much that working with 3rd parties is a nightmare. This talk goes into details on how to make a product that is secure from hackers but still allows for 3rd party repairs, end of warranty aftermarket support and consumer modifications. We will cover how to allow modifications and still limit abuse such as insurance fraud. We will also discuss if you can you make a modifiable self driving vehicle and still have it be safe?

Adverserial Attacks on Machine Learning

David Glance
Director
UWA Centre for Software and Security Practice

As more organisations are deploying machine learning to gain efficiencies and perform new functions, attacks targeting these algorithms are inevitable. Research is showing that there are many ways to attack these models, even if who they work is unknown (so-called black box models), giving attackers the ability to influence the decisions that these machine learning models take. This can range from fooling facial recognition software to identifying another person, to changing a business or contractual decision in the attackers favour. As businesses move to implementing machine learning, security must be a priority from the very start.

Super Root: A New Powerful and Stealthy Rooting Technique to Hacking ARM Devices

Zhangkai Zhan
Ph.D. Student
Beihang University

Root attack is an unauthorized process of gaining the highest privilege by exploiting vulnerabilities of a system. After that, attackers are able to fully control the system and arbitrarily access system resources, from security sensitive information to private personal data. Fortunately, ALL existing rooting techniques are traceable and detectable as they cannot completely remove the fingerprints, such as UID and setuid files.

We propose a new powerful and stealthy rooting technique, named super root. Comparing to traditional rooting techniques that obtain root privilege, the super root attempts to get the HIGHEST HYPERVISOR/VMM privilege. The hypervisor privilege allows the adversary to do whatever traditional root does, and also provides a new powerful capability that is allowed by the hypervisor, e.g., doing Virtual Machine Introspection (VMI). The VMI-based technique is able to completely remove the fingerprints of the super root, and thus make it stealthy to all existing root-detection tools.

We will demonstrate two super root exploits on Pi-top a Raspberry pi powered computer.

We measure their performance overhead using two existing benchmark tools, and do the security evaluations using existing root-detection tools. The experiment results show that the overhead of super root is negligible, and all root-detection tools can NOT detect the existence of our super root.

At last, we will discuss potential mitigations for super root, and call for more and more parties to join in this effort to harden the commodity ARM systems.

Vulnerability A&D

Unauthorized Exploit of Industrial Control Protocol

Siting Jian
Industrial Security Researcher
Pox Team

Aiming at the introduction of common industrial protocols, the characteristics and components of industrial protocols, explains the vulnerability analysis of unauthorized and unencrypted industrial protocols, and demonstrates the simulation of unauthorized writing of Modbus TCP protocol by instantiating Modbus TCP protocol, causing abnormal actions of industrial equipment.

Two Bytes to Pwn Adobe Reader: The Black Magic Behind the Byte Order Mark

Ke Liu
Senior Security Researcher
Tencent Security Xuanwu Lab

This presentation will talk about some interesting string-related vulnerabilities which were discovered in Adobe Reader. One of them could be used to leak sensitive information to bypass ASLR, and it was used with another Use-After-Free vulnerability to pwn Adobe Reader at Tianfu Cup 2018. Another one could be used to achieve remote code execution directly. The following four topics will be discussed in this presentation: (1) Root cause analysis (2) Finding methods (3) Exploiting tricks (4) Patching suggestions

Oh! Auth: Pitfalls of OAuth 2.0 & attacking the fallen

Samit Anwer
Senior Security Engineer
Citrix

In the race of providing OAuth/ Open ID Connect based access to assets, authorization service providers have been forced to release half-baked solutions in the wild because of which relying parties and users face myriad of issues ranging from authorization code compromise (unauthorized resource access) to account takeovers.

The key to adding authorization or SSO measures to your app is to ensure you are balancing security with usability. Developers likely make trade-offs when making decisions about specific implementation - and there are a lot of decisions to make. Developers still want to double down on security to avoid flaws in 2.0, paying attention to things like session management, encryption/obfuscation of stored data and IDs, and securing the source code of an app.

In this work we will discuss common malpractices that relying party devs perform when implementing OAuth/ OpenID based relying party solutions. However, all is not in the hands of relying party developers, the authorization service providers have a big role to play as well.

There are mainly 4 entities involved in a typical OAuth setup, they are – relying party/client, user/resource owner, resource provider, authorization server. In this work, we discuss the goof-ups that each of these entities can introduce with special focus on vulnerabilities that the authorization server can introduce.

The highlight - We present our case study on OAuth authorization providers and detail the issues we found in their solutions. This includes vulnerability in Microsoft's authorization server - login.windows.net. As can be seen in the PoC video (https://drive.google.com/file/d/1ZFratBPO6qP0hWiCsQH6qJ5fbbx7ghSn/view?usp=sharing) the auth code can be replayed to generate fresh access tokens and id tokens. Moreover, the code verifier is not being validated which can lead to a compromise of the access/id tokens on native apps which use Microsoft's identity provider - login.windows.net.

Vulnerability 1: Microsoft's IdP service failed to block replayed authorization codes

Vulnerability 2: Microsoft's IdP service failed to validate code_verifier which is used in Proof Key for Code Exchange (OAuth 2.0 for Native Apps - https://tools.ietf.org/html/rfc8252). The code_verifier protects a genuine app against other malicious apps from assuming identity of the genuine app and requesting access/identity tokens on behalf of them.

Vendor - Microsoft, Product - Identity Provider Service for OAuth, Version - login.windows.net

Data Security & Cloud Security

Data Backup Development Trend Analysis Under Cloud Environment

Xiaoqin Hu
Founder and CEO
Chengdu Vinchin Technology Co., Ltd.

There is no doubt about the importance of data protection. Data backup is the last line of defense for data security. Rankware virus, misoperation, software defects, hardware failures, terrorist attacks, earthquakes, floods and other disasters can all cause devastating impact on data.

Under cloud computing environment, it is still necessary to protect data backup technology, cloud computing has brought the great changes of IT infrastructure build way, which leads to create a new backup technology, no agent transient recovery, instantaneous recovery, backup data management technology in cloud scenarios, bringing customers recover faster, cheaper and more efficient utilization rate of the backup data of different data backup, the use of backup technology development will be promising under a cloud environment.

Five Most Dangerous Data Theft Tactics and Mitigations in APIs & Microservices

Jing Dong
Founder
Cirrusgate

New infrastructure API and micro-services for the digital economy have led to rapid growth in data exchange, data exposure has increased dramatically, and lacks of risk visibility and detection capabilities. Do newly deployed micro-services transmit sensitive data? Which URL is potential attacked surface and has excessive use? Malicious employees download massive amounts of data? Programmers sneak in hidden backdoors? Are deprecated API frequently used by third parties? Tamper with parameters or inject? Logic bypasses the business process? Explain countermeasures with plenty of examples.

Data Security & Cloud Security

How to Fight Advanced "AI" Fraud Attacks with Unsupervised Learning

Hongyu Cui
Technical Leader of China Region
DataVisor

AI technology is used by network hackers while it empowers various industries, making the attacks more automatic, more covert and difficult to detect.

Hongyu Cui found that, in the field of Internet anti-fraud research, the current attack model of dark industry shows the following trend: the attack methods diversifiy and change quickly, attack means tend to simulate normal users, the main source of the attack account from large-scale registration gradually shifted to ATO account. Traditional rule systems and supervised models, due to their strong dependence on fraud cases and tag data, are often unable to respond to the rapidly evolving dark industry attacks in a timely manner and are always in a passive defensive state in the anti-fraud. Through global analysis of unsupervised algorithm, clustering in high-dimensional space can automatically discover large-scale connected fraud rings without labels. Unsupervised algorithms have significant advantages in early warning and detecting rapidly evolving fraud patterns.

Disinformation Attacks as an Emerging Form of Cyber Threat

Roy Zinman
Advisor for CrowdSense
Advisor for Cybint Solutions
Former Intelligence Officer and Innovation Leader
Israeli Defense Forces
Elite Intel ligence Unit

The perception of Disinformation, or Cyber Information Warfare, have traced the same course of the "conventional" cyber threat. First, a large scale and sophisticated state sponsored attack is revealed. Then, other state players, criminal and commercial players follow suit and mimic the methods, vulnerabilities and techniques that were exposed.

Cyber disinformation attacks are becoming more and more prevalent in the corporate world. Companies brand equity is being hit, and illicit players manipulate stock prices with social media disinformation for enormous gains in "pump and dump" or "short and distort" attacks.

Information warfare attacks are performed by creating and disseminating false narratives in social media, online trading platforms and news platforms by using false identities and online assets. These narratives are sophisticatedly designed to create an impact on traders, regulators and the general public.

This type of attack remains unhandled because the organizational and technological adaptations have not been made yet. It is unclear which department is responsible for defending against such attack. Is it the CISO? Marketing? Communications? Or is it someone else' s problem – social media platforms, government regulators etc.

The technology for detecting and mitigating disinformation attacks is young and complex. It requires sophisticated AI and massive data collection and monitoring. There are great legal and ethical dilemmas encountered by the defenders. For example, is it legitimate to "fight fire with fire"? And how can we mitigate at all the damage inflicted by disinformation attacks?

I will describe a new approach to combat disinformation attacks based on proven cybersecurity methodology. It is a holistic approach that encompasses threat intelligence, monitoring, detection, mitigation and incident response techniques tailored to the unique challenges posed by disinformation attackers.

Data Security & Cloud Security

Key and Difficult Points in Personal Information and Privacy Protection

Tianbin Ye
Director of Cyber Security Consulting
Deloitte China

Mr. Ye, cyber security consulting director of Deloitte China, will share experience of Deloitte helping enterprises in the implementation of data security and privacy protection in the process of actual combat, including PIMS (Personal Information Management System) blueprint, children's privacy concerns, cross-border flow rule, global data privacy engineering difficulties, APP and SDK compliance targeted solutions.

Digital Technology Security Challenge and Thinking

Minghao Liu
Information Security Team Leader
JD Digits

With the Internet into the second half, security needs to follow the business upgrade. This sharing mainly starts from the security practice experience of Jingdong Science and Technology Department, analyzes the security challenges faced by the business, from fundamental security to mobile security to business security, and comprehensively introduces the practical experience of distributed security architecture.

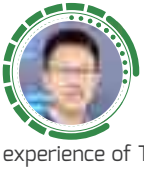
Day2 Keynotes

Title: Cultivate the Entrepreneurship of Security Entrepreneurs in Cyberspace

Xiaosheng Tan
Founder and President
BEIJING GENIUS CY-BERTECH CO.,LTD

On the one hand, cyber space security needs continuous innovation; on the other hand, cyber security innovation startups are easy to survive and difficult to develop. The cause of the problem is quite complex, and the solution of the problem also needs multi-pronged approach. Therefore, cultivating entrepreneurship of cyber security entrepreneurs is undoubtedly an indispensable step. Domestic network security entrepreneurs mostly are network security attack and defense technology, product development background, often lacking of operating experience of the sales system design, operations, government relations, investment and financing. In the process of the development of an enterprise ability outside of these technologies are often vital role, Zhengqi College Security Entrepreneurship Camp has made some attempts on the cultivation of "entrepreneurship" of network security entrepreneurs, hoping to improve the success rate of network space security entrepreneurship and solve users' network security problems through innovative technologies and products.

Intelligent Security Powered by Threat Intelligence



Feng Xue
Founder and CEO
ThreatBook

Based on the practical experience of ThreatBook for many years, this speech will review the development and growth of the new concept of Threat Intelligence in the past few years, and systematically elaborate the forms and cases of Threat Intelligence landing in China, which play a vital role in the security construction of various industries.

Making Sense of Chaos: The Evolution of Operational Security

Kevin O'Leary
Field Chief Security Officer
APAC
Palo Alto Networks

Over the years operational security has evolved from a pursuit isolated from the business, concerned only with protecting the perimeter and applying a prescribed set of rules regardless of the needs of the business. As businesses have evolved and embraced digital transformation and cloud security operations also needs to evolve towards machine learning and AI

Day2 Keynotes

Effective Protection for the Future to Escort Digital Transformation for Enterprises

Yi Hao
Security Business CTO
Sangfor Technologies Co., LTD

At present, the fourth industrial revolution, with artificial intelligence, robot technology and virtual reality as the breakthrough points, is being carried out in full swing all over the world, constantly promoting the development of the digital era. At the same time, with the constant upgrading of threats, the continuous increase of IT systems and the continuous innovation and development of new technologies, the security construction of user network space has put forward higher requirements. In this case, how to adapt to the development of the digital era through the innovation of network security construction has become a common concern of many users. In this speech, Sangfor will share how to build a security system of "future-oriented effective protection" to help users resist network security threats in the digital world and escort network security in the process of digital transformation.

Intelligent Data Security in Smart City

Bo Liu
Chief Scientist
Senior Vice President
Das-Security

Digital economy and smart city have become a trend. The convergence of information technology and economic society has brought rapid growth of data, and data has become the basic strategic resources of the country. While promoting the construction of digital government and smart city, it is also necessary to ensure the security of interconnection and collaborative sharing of various data resources across levels, regions, systems, departments and businesses to improve the efficiency of digital economy, and promote the digital transformation of government.

Incident Response/Security Operation

Consideration on Network Security Protection of Industrial Control System

Bing Li
Former Deputy Director-National Research Center for Information Technology Security

The speech begins with the current security status of Industrial Control System from the macro level, and then analyzes and summarizes the security threats faced by Industrial Control System. Finally, according to the characteristics of Industrial Control System and the principle of security protection, proposes to realize the security protection of Industrial Control System through systematic credible technology, and expounds the three aspects of security protection technology, emergency standby and comprehensive security management respectively.

The Challenge and Practice of National Cyber Threat Intelligence

Nengqiang He
Senior Engineer
CNCERT/CC

This speech will introduce the technical architecture and operation mechanism of CNCERT's Network Security Threat Information Sharing System, and build a national network security threat information sharing platform and working system on this basis.

Understanding and Reducing the Enterprise Security Risks

Yang Zhao
General Manager
Tenable China Region

With the rapid development of enterprise IT technology, as a variety of new digital technologies are widely applied in various fields (IOT, SACDA, Cloud, Web, DevOps), the risk of enterprises' exposure to external attacks also increases exponentially. More than 16,500 vulnerabilities were reported in 2018, a 27 percent increase from 2017. Facing so many vulnerabilities and a variety of attack means (worm ransomware, ICS attack, mining Trojan, etc.), how can the security team effectively find the real security risks within the enterprise and make timely remedies? Obviously, the traditional security technology can not fully meet the new requirements. Tenable would discuss with security experts that how to make use of the latest Cyber Exposure technology, efficient management and measure enterprise assets attack surface to accelerate the understanding and reduce enterprise security risk.

Incident Response/Security Operation

Creating an "Unattended" Security Operation Center

Kui Fu
CTO
Shanghai Flagify Intelligent Technology CO., LTD

How AI can help enterprises build adaptive safe operation systems in the field of security choreography, automation and response. By linking internal and external resources of enterprises through automation and interactive technology, and by means of artificial intelligence technology to build "unattended" safe operation center, it brings revolutionary changes to the safe operation of enterprises.

Threat Hunting Based on Trusted Clue Mining

Runzi Zhang
Senior Security Researcher
NSFOCUS

We need a unified, highly automated platform and tool chain that can handle massive heterogeneous multi-source data, quickly detect, reason, respond and track threat events, and assist people in safe operation, research and countermeasures. Starting from practical experience and based on the reclassification of common data sources in network security data analysis, the topic proposes the key data graphs needed to build the graph model of intelligent security platform, to support the further development of "intelligent" threat hunting and security research.

Digital Brand Protection, an Active Defense Practice of Business Security

Dalu Yang
CEO
Tianji Partners Co., Ltd.

Digital Transformation is an inevitable proposition for enterprises. It will be increasingly difficult for enterprises to distinguish the boundary between business security and network security, and they need to find effective ways to protect digital assets.

Brand is a kind of enterprise asset. Many enterprises use the power of digitization to rebuild their brand image. However, data leakage, online fraud, phishing, and even cyber blackmail and coercion have not only brought direct economic losses to enterprises, but also damaged their brand and business image.

Digital brand protection is a new security practice that helps companies to protect their digital brands and assets against various risk scenarios, such as phishing, APP, social media phishing, threat false positives, supply chain security, brand infringement, and so on.

Talent Development

Exploring the mechanism of collaborative education between government, industry, University and research institutes to build a first-class cybersecurity school

Liu Jianwei
Dean
Beihang University

Beijing University was awarded the first batch of first-level doctoral degree programs of cyberspace security in China in 2016. In 2017, Beihang School of Cyber Science and Technology was formally established, and was awarded the first batch of "First-Class Demonstration Project Cybersecurity School Academy Construction" jointly awarded by cyberspace administration of the CPC Central Committee and the Ministry of Education. This lecture firstly introduces the overall goal and construction policy of Beihang Cybersecurity School, and gives five development directions of the discipline construction, and then this paper introduces the its institute for network security in the undergraduate specialties, undergraduate students and training, planning, scientific research platform construction, the school of graduate student recruit students for the construction of the basic conditions and so on. This lecture also introduces the practice of establishing school-enterprise joint laboratory together with government departments and network information enterprises, and strengthening the training of high-level network security talents. In particular, it summarizes the construction experience and experience of first-class cybersecurity school.

Exploration and Practice of Innovative Mode for Training Cybersecurity Talents

Zhihong Tian
Dean Cyberspace Institute of Advanced Technology-Guangzhou University

The demand of cyberspace security promotes the development of cyberspace security, and the core task is the cultivation of high-quality professionals. Aiming at the problems existing in the current training of cyber space security talents, such as the separation of course content and the lack of learning interest, based on the network attack and defense training platform, this speech introduces in detail the exploration and practice of " Binxing Fang" graduate training innovation class in the classified training mode of comprehensive practice of cyber space security.

Information Security Compound Talent Training Experience Sharing

Zheli Liu
Deputy Dean
Nankai University

Information Security Compound Talent Training Experience Sharing

Talent Development

Talent Safety for Security Talents

Ting Wu
Dean
School Of Cyberspace Security, Hangzhou Dianzi University

Due to the unique attack and defense duality of cyber space security, the training of cyber space security talents should not only emphasize the learning of security professional knowledge and skills, but also take the cultivation of moral education as the central link of the training of security talents and strengthen the political red line and legal bottom line of the training of security talents. On the basis of the research on the training of network security talents in some universities in China, the report gives the concrete suggestions on the implementation of the ideological and political work of security talents and the practice of Hangzhou Dianzi University.

Network Security Application-oriented Talent Training Practice

Yang Li
General Manager of 360 Cyber Security University
360

In the era of macro security, vulnerabilities are everywhere and people are the weakest segment. Faced with the serious shortage of network security talents, 360 Network Security University has created a set of talent training system that matches the needs of the industry, relying on the company's more than 10 years of deep cultivation in the field of security technology and rich experience in talent selection and training. 360 Network Security University, together with the government, universities and partners, jointly cultivates application-oriented network security personnel for the national network security escort.

Application of Graph Neural Network (GNN) in Vulnerability Discovery

Jiqiang Feng
General Manager
Aurora Infinity Information Technology Co.,Ltd

Our research is about using graph neural network to quickly and effectively detect vulnerabilities in large code bases, using RNN and GNN to extract code structure and semantic features related to vulnerabilities, and combining code analysis with graph theory in discrete mathematics. We also use feature learning to convert known code vulnerabilities into quantitative indicators to detect vulnerabilities, while establishing neural networks to assist binary analysis, and using open source code base and CVE as training data to build feature databases.

The New Generation of High Efficiency, Precision and Flexibility Program Static Applications Security Testing

Xinming Liu
Chief Architect
Xcalibyte

Yuning Liang
Co-founder and CEO
Xcalibyte

SAST (Static Application Security Testing) is a series of technologies and tools that enable programmers to obtain professional security guidance, understand and execute it. Many SAST tools have such a high rate of false positives that they show vulnerabilities where they don't actually exist. This causes developers to spend a lot of time doing manual checks. When a tool tries to reduce false positives, it usually leads to an increase in false negatives, making errors ignored. In order to improve accuracy, different analytical methods can be used to achieve complementary goals.

In this lecture, we will use some real examples to demonstrate the challenges and opportunities of static analysis tools to achieve high cost-effectiveness.

Our new generation of high efficient, precise and flexible customization of the static program application security testing techniques include across different languages, different functions and different files, four software characteristics, namely the flow between acute, context, objects and processes, these features in the diagnosis of SAST tools loopholes and the effectiveness of irregularities is crucial. These four software characteristics cannot be handled separately, such as a variable that can be uninitialized along an execution path (stream sensitive). The execution path can include function calls that pass in the problem variable as a parameter (between procedures). It may even be that there are multiple calls to the same function, with some passing in problematic parameters and some not (context-sensitive). These four analytical methods must work together and cannot be carried out in isolation. In addition, the scope of the analysis must be as large as possible, taking into account memory and computing requirements that may grow exponentially with the scope of the analysis. Reducing false positives is a key determinant in choosing a static analysis tool, which largely depends on the accuracy of the analysis discussed here.

Security Innovation

Zero-Sum Game - A New Battleground against Cybercrime

Ruidong Zhang
CEO
NoSugarTech

While the Internet brings convenience for us, it brings opportunities for criminals as well. With the development of big data, cloud computing and AI technology, cybercrime tends to be more diversified and specialized. Fighting cybercrime is a technological contest in cyberspace, which is a battlefield without smoke of gunpowder, also a zero-sum game. In the cruel competition, only the absolute technical advantages can achieve the final win.

Instant Communication in the New Information Era

Zhengxian Lin
R&D Director
BCM Social Corp

Kunzhe Chai
Security Director
BCM Social Corp

Since the news of PRISM users' trust in the platform has changed from complete trust to doubt. More and more users start to think about how manufacturers use their personal information and data, and even question whether there is enough secure instant communication. This topic combines the development practice of a secure instant messaging software, from the architectural design of an extremely safe, highly private and efficient instant messaging software to the implementation of specific plans; Key words: complete end-to-end encryption, fully anonymous use, no network communication.

5G Is Coming - Don't Worry about Security

Lin Huang
Director
360 Research Institute
360 Technology

5G networks have been deployed in some cities, and the 5G era is slowly coming as more and more mobile phone terminal models are available to ordinary people. Security issues related to communication networks are a long-standing topic, not because of the new introduction of 5G. This topic will introduce the past big security issues caused by mobile communication networks; What's wrong with 4G? What security enhancements does 5G have compared to 4G?

Speakers

Day1 Keynote

Xiaosheng Tan
Founder and President
BEIJING GENIUS CY-BERTECH CO.,LTD

Tan was the former CIO and CSO of 360 Group and the network security expert of the Network Security Bureau of the Ministry of Public Security. In 2018, he was awarded as the outstanding network security talent of the China Internet Development Foundation, elected as the board member and deputy secretary general of the China Computer Society (CCF). And Tan was the high-end leader of Zhongguancun in 2012.

He had worked in Xi'an Jiao Tong University, Peking University Founder, Shenzhen Hyundai, Haoxin Shenzhen and more. He has been engaged in research and development of an anti-virus system under the DOS operating system, disk encryption system, Chinese operating system and large-scale information management system. In 2003, he entered the Internet industry and served as 3721 Director of Technology Development, Yahoo China Director of Technology Development, Yahoo China CTO, MySpace CTO and COO. In 2009, Tan joined Qihu 360 as an expert in cloud computing infrastructure, information security and information index.

Martin Hellman
Turing Award Winner 2015
Member of the National Academy of Engineering
Professor Emeritus of Electrical Engineering
Stanford University

Martin Hellman is co-inventor, with Diffie and Merkle, of public key cryptography, the technology that secures e-commerce and protects trillions of dollars per day in financial transactions. His many honors include the top prize in computer science (the million dollar ACM Turing Award) and election to the National Academy of Engineering. Hellman has a deep interest in the ethics of technological development and serves on the Advisory Boards at the Federation of American Scientists and Verified Voting. He was on the faculty at MIT (1969-1971) and Stanford University (1971-1996), where he is now Professor Emeritus of Electrical Engineering.

Speakers

Yunkun Wu
President
Qi AnXin Group

President of Qi AnXin Group, deputy head of the Information Technology Promotion Working Committee of China Information Industry Association, deputy head of the Cyberspace and Security Committee, National Internet Finance Association of China.

Mr. WU is a veteran in the cybersecurity business, especially in areas of product planning, branding, financing and investment. He directs his research interests to perimeter security, big data security, cloud computing security and big-data-derived threat intelligence.An advocator of "data-driven security", Mr. WU is acclaimed for his constructive, advanced suggestions and ideas to advance the development of cybersecurity technology in China.

Tim Virtue
Former Chief Security & Risk Officer
LCRA

Tim Virtue, CISSP, CFE is a global cybersecurity, technology, and risk management leader. He has extensive experience with publicly traded multinational corporations, privately held businesses, government agencies, and non-profit organizations of all types and sizes with a focus in Financial Services, Management Consulting, and Technology. He is an industry recognized innovator, award winning thought leader, trusted board advisor, speaker, author of several books & articles and an early adopter of emerging & disruptive technology and business trends.

Mr. Virtue holds an Executive Master of Science Degree in Risk Management from New York University, Stern School of Business, an Executive Master of Science Degree in Information Systems from George Washington University School of Business and a Bachelor of Science Degree in Criminal Justice with a concentration in Security Management from Northeastern University.

Speakers

CSO

Xiangyu Jin
Founder of the Sec-UN Website
Founder of the Threat Intelligence Advance Alliance

NUKE, Xiangyu Jin, Founder of the Sec-UN Website、Founder of the Threat Intelligence Advance Alliance. Former senior consultant of network security and information technology, worked in Venustech and Accenture, respectively provided service for State Grid, China Mobile, China Telecom, Huawei and other world-leading users. As a managing partner of private equity fund, he led the investment in innovative companies such as Cirrusgate, Togeek, Secksky, Data Star Observatory, Inossem, and Jiaweisi etc.

Jian Chen
CSO
Ping An Group

Jian Chen, Chief Security Officer of Ping An Group, has about 20 years of experience in information security, internal control, IT audit and risk management, and more than 10 years of experience in the field of anti-fraud. From 2000 to 2005, he served as a senior security consultant in security companies such as Anshi Group and CA Jinchen Group. From 2005 to 2015, he established Ctrip information team and took charge of information security and business security related work of the whole Ctrip Group. He successively served as Director, Senior Director and CTO Assistant of Ctrip Group's security center. In 2018, he was appointed as the Chief Information Security Officer of the group, focusing on the information security capacity building of Ping An Group and empowering the group's professional companies. He is committed to the practice of data enabling security and open API ecological capacity building, and has several international certifications including CISSP, CISA, ISO27001, ITIL, Cobit and PMP.

Speakers

Zuoyu Zhang
DingTalk CRO
Alibaba Group

Zuoyu Zhang, ID:bk7477890. Alibaba DingTalk CRO, once served as MEILI United Group information security director, responsible for the Mogujie, Meilishuo security system construction. He is the security technical director of Sobug and responsible for security product design and development. He is the technical moderator and administrator in the "Hacker X Files" community. During the period of entrepreneurship as security consultants, he has many years of enterprise risk management system construction experiences.

Feifei Wu
Senior Security Specialist
Ant Financial/ MyBank

FEEI, the author of Cobra /GSIL, Senior Security Specialist of Ant Financial, Security Architect of MyBank.

Speakers

Yefei Qian
Head of Data Security
Didi Chuxing

A long career in the construction and operation of global security capabilities for large enterprises, specialize in solutions that combine security, experience and efficiency.
Expert in IT infrastructure security, data security, IT operations, and security auditing. Currently heads the Data Security Department at Didi Chuxing. Previously was the leader of Major Customers Security Operations at Alibaba Group, COE leader of Huawei's business security and operations division, and served as senior security consultants for NSFOCUS.

Tony Tan
CEO
Shanghai Paraview Software Co., Ltd.

20 years' experience in identity security, data security and business security.
More than 10 years' experience in enterprise software in IBM and CA.
Tan Xiang established Paraview Software in 2008. He focuses on enterprise information security and business transformation, and has extensive industry experience and forward-looking insights in information security and digital transformation in the fields of automotive, manufacturing, pharmaceutical, retail, real estate, finance, and education.

Speakers

Vulnerability A&D

Lisa Zhang
Co-founder and Executive Editor of ITCloud Report
Vice President of Heman Media

Senior media personnel, top 10 leading figures in the frontier of IT field, whose in-depth articles have been cited by several times by major media. Highly recognized by relevant government departments and industries, and invited to host many large-scale industry conferences including Trusted Cloud Summit, Cloud Connect. Has been in the management positions of listed groups including Lenovo, Netease, Ogilvy. Owned rich practical experience in B2B marketing promotion and has been invited to provide trainning to many listed companies and marketing institutes.

Craig Smith
Senior Director of Security and R&D, Iconiq Motors
Author of "Car Hacker's Handbook"

Craig Smith is the Senior Director of Security and R&D at Iconiq Motors, where he leads the product security, red and blue teams and future research and development. He is also the founder of Open Garages, a distributed collective of performance tuners, mechanics, security researchers and artists.

Craig authored the "Car Hacker's Handbook", the de facto guide to automotive security. At Rapid7, Craig runs the Transportation Practice, which specializes in providing strategic consultancy and deep technical expertise to the transport industries. His work includes extensive testing for innovative new technologies being developed in the automotive industry. Craig has developed many free and open source tools to help teach others about vehicle security.

Craig has worked in security for over 20 years, with a focus on automotive and other types of transport for the last 8 years.

Speakers

David Glance
Director
UWA Centre for Software and Security Practice

Dr David Glance is Director of the UWA Centre for Software and Security Practice, a UWA research and development centre. Dr Glance worked in the finance and software industry for over 20 years at companies such as HSBC, Microsoft, Tibco and IONA Technologies before spending the last 18 years at UWA. The UWA CSSP provides training and research opportunities for students and has developed commercial software in the security, health and education sectors.

Dr Glance has consulted with the OECD on reviewing national cybersecurity strategies, and assessments of cybersecurity maturity in business organisations. He is currently assisting the OECD in establishing the Global Forum on Digital Security for Prosperity.

Dr Glance is a widely published columnist at The Conversation making regular media appearances on cybersecurity, technology and society. He is a co-author (with Dr Mark Gregory) of the book Security and the Networked Society published by Springer.

Zhangkai Zhang
Ph.D. Student
Beihang University

Zhangkai Zhang received his bachelor degree and Ph.D. degree in the School of Computer Science and Engineering, both from Beihang University. His research interests include mobile security and virtualization security. His research work has been published in CCS, SecureCom, DSC etc.

Speakers

Siting Jian
Industrial Security Researcher
Pox Team

Master of software engineering in Fudan University, mainly engaged in industrial control security infiltration and defense, KCon 2018/ SDC 2019/ISC 2019 conference speaker, independently developed fingerprint sniffing tool based on Kali for industrial protocol.

Ke Liu
Senior Security Researcher
Tencent Security Xuanwu Lab

Ke Liu is a senior security researcher of Tencent Security Xuanwu Lab. He found and reported nearly 400 vulnerabilities which affect Adobe, Apple, Google, Microsoft, and some popular open source projects. He was one of the nominees of Pwnie Awards 2017 (Epic Achievement). He once spoke at Black Hat Asia 2017 and CNCERT Annual Conference 2017. He successfully pwned Adobe Reader at Tianfu Cup 2018. He's also in MSRC top 100 list in 2016, 2017, and 2018.

Samit Anwer
Senior Security Engineer
Citrix

Samit Anwer is a Web and Mobile Application security researcher. He joined Citrix as Security Engineer soon after completing his Master's degree from IIIT Delhi in Mobile and Ubiquitous Computing in 2015. He is actively involved with vulnerability research in Web/Mobile apps and has responsibly disclosed several security vulnerabilities with Google Cloud Print API, XSS filter evasion on IE 11/MS Edge, code execution on Microsoft Windows 10, Microsoft's OAuth 2.0 implementation and buffer overflows on MS Edge/IE 11.

He is an active member of the Null Bangalore Chapter, IEEE community and has spoken on various security topics at the following venues:

a) DEFCON China, Beijing (2018)
b) BlackHat Asia, Singapore (2018)
c) AppSec USA, Orlando (2017),
d) CodeBlue, Tokyo (2017),
e) c0c0n X, Kerala (2017) and
f) Null meets (2015, 2016, 2017, 2018)

His technical interests lie in using static program analysis techniques to mitigate security and performance issues on mobile/web apps, breaking web/mobile apps, and researching on cutting edge authentication and authorization mechanisms.

Data Security & Cloud Security

Wei Gu
Business Information Security Officer for Japan and Asia Pacific Region
Amgen Biotechnology

Mr. Wei Gu is currently working for Amgen as the Business Information Security Officer in Japan and the Asia Pacific region. He is responsible for the Information Security, Risk Management and Compliance Privacy related to all business departments in Japan and the Asia Pacific region, and reports to the Global Information Security Officer. Mr. Wei Gu has more than 14 years of work experience in the field of Information Security, and responsible for Information Security Architecture and Information Security Management in several world's top 500 multinational companies. Especially in the pharmaceutical industry, he has rich experience of information security and privacy.

Mr. Wei Gu won CCSF 2017 and CCSF 2018 Excellent Chief Information Security Officer Awards, 2017 $(ISC)^2$ Asia-Pacific Information Security Leader Title, Information Security Professionals Nomination Award, and is the only winner from mainland China.

Xiaoqin Hu
Founder and CEO
Chengdu Vinchin Technology Co., Ltd.

Xiaoqin Hu, PhD, associate professor, Chengdu high-tech zone high-level talents, the founder of chengdu Vinchin Technology co., LTD., focuses on cloud computing and security direction, cloud backup, cloud disaster recovery direction of engineering research, won the 2006 and 2008 Sichuan Science and Technology Progress Award, won the 2010 Military Science and Technology Progress Award, awarded five national invention patents and national defense patents.

Speakers

Jing Dong
Founder
Cirrusgate

Mr. Dong is the founder of Cirrusgate. He is committed to applying machine learning, natural language processing, and behavioral analysis technologies to the fields of text analysis, data security, threat detection and response. His independently developed lightweight artificial intelligence engine, suitable for a variety of security and business scenarios, can be deployed in the cloud platform or edge computing node, is favored by many cloud and security manufacturers and built in; Its standard products also create great value for fortune 500 companies in various industries.

Hongyu Cui
Technical Leader of China Region
DataVisor

Hongyu Cui is currently the technical leader in China region of DataVisor, and has been developing and using distributed unsupervised machine learning algorithm for anti-fraud detection in DataVisor since 2015. She used to be responsible for anti-fraud modeling of machine registration, fake reviews, spam, fraudulent transactions and fake application installation of large Internet enterprises such as Pinterest, Yelp, Alibaba and Cheetah Mobile. She has rich experience in model tuning, feature engineering and algorithm development.

Roy Zinman
Advisor for CrowdSense
Advisor for Cybint Solutions; Former Intelligence Officer and Innovation Leader
Israeli Defense Forces Elite Intelligence Unit

Mr. Roy Zinman has served for 25 years in the Israeli defense forces elite intelligence unit, as an intelligence officer and innovation leader. He took part in several groundbreaking projects with strategic national security implications. In his last role, Mr. Zinman commanded the IDF open source intelligence unit and rebuilt it to match the modern challenges of social media and big data analysis. In the beginning of 2017, after his retirement from the IDF, Mr. Zinman has joined Recongate Ltd., a high-tech company that specializes in online data analysis in the Chinese market. Nowadays he is active in several cybersecurity and social media data analysis start-ups focused on information warfare.

Speakers

Tianbin Ye
Director of Cyber Security Consulting
Deloitte China

Tianbin Ye, director of risk consulting at Deloitte, has long been focusing on Security Technology Architecture, Network Security Governance, Data Security and Privacy Compliance Business fields, helping high-tech and Internet users deal with data security and network security risks.

Minghao Liu
Information Security Team Leader
JD Digits

He works in the security industry for more than ten years and has rich practical experience in the field of security. At present, he is responsible for the overall security capacity building of JD Digits, including Independent Security Product Development and Architecture Design, Business Security, Basic Security, Security Operation, Security Compliance and Financial Science and Technology Security Capability Output.

Speakers

Day2 Keynote

Sara Peters
Senior Editor
Dark Reading

Sara Peters is the lead editor for Dark Reading's feature section The Edge, directing all in-depth coverage of cybersecurity issues. She also regularly serves as track chair, speaker and moderator at security events in the US and internationally, including Interop China, the India Cyber Security Dialogue, Black Hat Asia, Interop Las Vegas and RSA. Sara first began covering the field in 2005, just a few months after the ChoicePoint data breach, before most people had even heard the term "data breach."

Feng Xue
Founder and CEO
ThreatBook

Xue Feng, founder and CEO of ThreatBook, previously served as the Chief Information Security Officer (CISO) of Amazon (China), he used to be responsible for the information security of Amazon enterprises and customers in China. Before joining Amazon, Xue was the Director of Internet Security Strategy in Microsoft, responsible for formulating Microsoft's Internet Security Strategy in China. Xue was the first Chinese speaker at the International BlackHat European Security Conference and Microsoft BlueHat Security Conference. At the end of 2018, Xue won the annual leader award of "Double Push" in Chinese information security industry which was sponsored by "China Information Security". In April 2019, Xue was awarded the Founder of China Bang Awards sponsored by Technode.

Speakers

Kevin O'Leary
Field Chief Security Officer
APAC, Palo Alto Networks

Kevin O'Leary is a senior IT Security professional with over 20 years of experience working for public institutions, private companies and large multinationals across Asia Pacific and Europe in a variety of management, engineering and advisory roles. He has worked both as a Chief Security Officer and Principal Security Architect across a range of business verticals (ICT, Pharma, Finance, Aviation and Manufacturing in particular). Kevin has extensive experience within the Asia Pacific region, prior to joining Palo Alto networks as their Field Chief Security Officer, APAC, Kevin served as the VP and Chief Information Security Officer, GE Regions and Greater China. In this role Kevin advised the global and local leadership on Security and Risk aligned to business strategy within China and other growth regions globally. Prior to this role Kevin was the APJ CISO for HP Delivery based in Singapore, where he is still based.

Yi Hao
Security Business CTO
Sangfor Technologies Co., LTD

He is CTO of the Sangfor Technologies Security Business, and has 14 years of experience in network security industry. He engages in network security industry situation tracking, trend insight, method summary, architecture design, planning consulting and other work for a long time.
He has a certain understanding of network security level protection, NIST CSF, ISO27001/2000/22301.

Speakers

Bo Liu, Chief Scientist, Senior Vice President, Das-Security

Bo Liu, Chief Scientist of Hangzhou Das-Security(Senior Vice President), A Ph.D. in computer science at the university of Maryland and a former big data and machine learning scientist at Facebook and Square. After back to China in 2017, he was selected as an expert of the thousand talents plan of Zhejiang province, and he was also an outstanding CTO of China software association in 2017, leading three major scientific research projects at provincial and national level. He has been working in the field of big data, machine learning and artificial intelligence for more than 10 years and has published many articles in English, and cited over 5,000 times in the world. He has completed more than 50 technology invention patents including intelligent threat detection, AI anomaly analysis, UEBA and intelligent reasoning of network security threats, and served as the deputy director of the national and local joint engineering research center of big data network security situational awareness and intelligent prevention and control technology.

Incident Response/Security Operation

Tony Liu
CSO and Senior Vice President
Das-Security

Liu Zhile is currently CSO and CEO of Das-Security and holds a master's degree in EMBA from Guanghua School of Management, Peking University. At the same time, he served as the vice chairman of the China Computer Federation Young Computer Scientists & Engineers Forum (CCF YOCSEF) Hangzhou track (2016-2017, 2017-2018), member of the China Cyberspace Security Association Competition Review Working Committee, China Cyberspace Security Association Emergency Work Committee (funding), and executive director of China Cyber Security Industry Alliance. Liu was also the first member of China Cyber Association Cyberspace Security Strategy and Law Committee, deputy head of the first network security talent development working group, head of cloud security alliance (CSA) Hangzhou branch, member of OWASP China Branch, deputy director of Safety Technology Professional Committee of Zhejiang Computer Information System Security Association, distinguished professor of Zhejiang Normal University, College of Computer Science and Technology of Zhejiang University of Technology/Professional Construction Advisory Committee of Software College and Enterprise Cooperation Committee, Guangdong University of Foreign Studies Distinguished professor, corporate tutor of the Institute of Cyberspace Advanced Technology of Guangzhou University.

He has long been committed to research in cybersecurity and has always maintained a keen grasp of cutting-edge technologies in information security. During the work at Das-Security, he participated in the research and development of information security innovation in smart city security, big data security and situational awareness. The main research directions are: 1. The security situation and the development trend of security technology. 2. Security challenges and opportunities for computing and big data. 3. Practices for cloud computing security models 4. Situation-aware practices based on big data.

Speakers

Bing Li, Former Deputy Director, National Research Center for Information Technology Security

Former Deputy Director of National Research Center for Information Technology Security, he has engaged in network security research for a long time, and has presided over or participated in the completion of a number of major network security special research projects, won more than 10 Science and Technology Progress Awards.

Nengqiang He Senior Engineer CNCERT/CC

Dr. He graduated from Tsinghua University Electrical Engineering Department. He entered CNCERT/CC from July 2012, and currently is the senior engineer. He has been engaged in the national network security emergency response work for a long time, including the reverse analysis of mobile malicious programs, security detection of mobile applications and the extraction and analysis of related threat intelligence and other technical research and system development and finished about 10 mobile Internet security national standards, industry standards, with a form to obtain authorization 3 national invention patents, published three copies of mobile Internet security annual report, published SCI, EI, such as more than 10 papers. He is responsible for the main work of China Anti-Network Virus Alliance (ANVA), China Internet Network Security Threat Management Alliance (CCTGA) and other industry self-regulatory organizations.

Speakers

Yang Zhao
General Manager
Tenable China Region

The general manager of Tenable in China, has more than 20 years' experience of IT technology and management, and has a wealth of network security and technical background. He formerly worked at Nortel, Aruba, and other well-known IT manufacturers, understanding the latest security technology developments at home and abroad, and also participated in several large domestic financial institutions and the situational awareness of the enterprise, assets and risk management platform project construction.

Runzi Zhang
Senior Security Researcher
NSFOCUS

Runzi Zhang is a Ph.D. from the University of Chinese Academy of Sciences. In 2018, he joined NSFOCUS and is now a senior security researcher at NSFOCUS Innovation Center. His research fields include threat detection, threat hunting and security knowledge mapping. He participated in the incubation of innovative projects such as user entity behavior analysis, threat hunting and threat intelligence analysis, and hosted the Beijing postdoctoral research project "Research on Network Threat Hunting Based on Data Analysis Method".

Kui Fu
CTO
Shanghai Flagify Intelligent Technology CO., LTD

More than 13 years of working experience in the field of information security, and he used to serve Huawei, VIPS and other companies. He is the Former Qianxun SI Information Security leader, Ali Cloud MVP project member, and masters a wealth of enterprise security best practices on the cloud. At present, he is serving as the CTO of Shanghai Flagify Intelligent Technology co., LTD., forging revolutionary safe operation weapon for the enterprise.

Dalu Yang
CEO
Tianji Partners Co., Ltd.

Dalu Yang, founder & CEO of Tianji Partner, co-founder of FengHuoTai CTI Alliance, Deputy Director of Big Data Application Engineering Center of XI 'AN Institute of Optics and Precision Mechanics of CAS. As the former head of the security operation center of the world's largest utility company, he has many years of practical experience in information security operation of super-large enterprises, and has rich practical experience and unique technical insights in the fields of situational awareness, threat intelligence, security monitoring, security attack and defense, simulation and big data analysis.

Speakers

Talent Development

Hui Lu
General Secretary
The Cyberspace Security Talent Education Alliance of China

Lu Hui is the Secretary General of China Cyberspace Security Talent Education Alliance, director of Fang Binxing, Guangzhou University's Cyberspace Advanced Technology Research Institute, director of the competition committee of the China Cyberspace Security Association, and standing member of the 11th competition committee of the Guangdong Computer Society. He is also an introducing talent of Guangzhou University ""100-person plan"", the member of Shenzhen Ping An Financial Research Institute expert and China Cyberspace Security Association big data security personnel training base technical committee.

His main research topics include network automation attack and defence, artificial intelligence security and other work. He has planned and organized the ""XP Range Challenge"", ""specific audio and video analysis system evaluation qualification contest"", ""Strong Network Cup"" network security challenge and other national network security events, and has guided the excellent carnival, XCTF National League. He has participated in the planning and implementation of the "China Network Security" national multi-station activities as well.

Liu Jianwei
Dean
Beihang University

Dr. Jianwei Liu received his Ph.D. in communication engineering from Xidian University, China in 1998, and his B.S. and M.S. degrees in electronic engineering from Shandong University, China in 1985 and 1988. He is currently a professor and dean of School of Cyber Science and Technology, Beihang University. His current research interests include cryptographic protocol design, wireless and mobile network security, space-air-ground integrated network security, and 5G network security. He has published 6 books and nearly 200 papers in his research fields. He is a senior member of the Chinese Institute of Electronics and director of the Chinese Association for Cryptologic Research. He has been awarded the first prize of technological invention of China.

Speakers

Zhihong Tian
Dean
Cyberspace Institute of Advanced Technology-Guangzhou University

Zhihong Tian is Ph.D., Professor, Ph.D. Supervisor, President of Guangzhou University's Cyberspace Institute of Advanced Technology, General Secretary of The Cyberspace Security Talent Education Alliance of China's Competition Committee. He is Ling-Nan Talents Reserve Project Candidate, Guangzhou University "Hundred People Project" Academic Leader, Guangzhou Outstanding Expert. Tian was the Supervisor of the Harbin Institute of Technology's Computer Network and Information Security Research Center (Beijing). He has focused on Cyber Security issues research, such as Cyberspace Range, Cyberspace Attack & Defense, Cyber Forensic and more. Being as the project manager, he has led several projects of the National Natural Science Foundation of China, the National Key Research and Development Project, the National 863 Project, the Central Cyberspace Administration Project. And his research has been awarded by Qian Wei Chang Chinese Information Processing Technology Primary Award, Heilongjiang Province Technology Progression Second Prize, Heilongjiang Province High School Technology Progression Second Prize, and he has awarded several letters of thanks or awards by Central Cyberspace Administration, National Computer Networking and Information Security Management Center and Cybersecurity Association of China. Finally, Tian has published more than 140 essays, 20 patents through the domestic and overseas journals and conferences including IEEE Network, TII, TVT, IoTJ, INS, FGCS, T-SUSC, ISCC, GLOBECOM, WWW.

Zheli Liu
Deputy Dean
Nankai University

Zheli Liu, Postdoctor, deputy president of school of computer science, deputy president of school of cyberspace security, academic leader of One Hundred Young People at Nankai University; Selected Member Of Tianjin Thousand Talents Program, associate professor, doctoral supervisor. The main research direction is data privacy protection based on cryptography, ciphertext database, ciphertext collection operation, etc. Five papers have been listed in the top 1% of ESI with high citation, and he is the close partner of Tencent advertising and Huawei database.

Speakers

Ting Wu
Dean
School Of Cyberspace Security
Hangzhou Dianzi University

Ting Wu, Ph.D., professor, Doctoral Supervisor, mainly engaged in information security and security research, and has participated in the National 863 Program, 973 Program, National Natural Science Foundation, Zhejiang Province Key Research and Development Projects and other research work. He is currently the president of the school of cyberspace security of Hangzhou Dianzi University and a member of the teaching guidance sub-committee of the Confidentiality Management Major of The Ministry of Education. In 2016, he won the second prize of Zhejiang Province's Security Work, and in 2017, he won the second prize of Science and Technology of Chinese Society of Electronics.

Yang Li
General Manager of 360 Cyber Security University
360

General manager of 360 Network Security University, former head of 360 campus relations, head of Renren campus relations, CEO of Yangcongtou, etc., with bachelor of human resource management, master of computer technology, international psychological consultant. She has been engaged in the work related to colleges and universities for more than 10 years, such as campus recruitment, campus activities, campus marketing, campus fan group, campus club, school-enterprise cooperation, collaborative education, industry-university-research and other businesses, and concurrently served as the entrepreneurship guidance, talent training, career planning and other tutors of many colleges and universities. She has rich experience of the network security personnel selection, vocational education and training, enterprise internal security personnel training.

Hongwei Li
Deputy President
School of Cyberspace Security
University of Electronic Science and Technology of China

Hongwei Li, Professor of University of Electronic Science and Technology of China, Doctoral Supervisor, Deputy Director of The School of Cyberspace Security. IEEE Vehicular Technology Society Distinguished Lecturer，《IEEE Internet of Things Journal》(CAS JCR-1 area) Associate Editor. He undertook a national key research and development program project (with a total project budget of 15.9 million yuan, and he is the overall leader of the project leading unit), and published more than 100 academic papers, 25 of which were in the JCR-1 area/ CCF-A category of the Chinese Academy of Sciences, and won the Single Best Paper Award of IEEE MASS 2018 and IEEE Healthcom 2015. The research results have been applied to the business system of Chengdu Rural Commercial Bank with millions of customers, and the successful application of the results has won the 2017 China Banking Information Technology Risk Management Project Achievement Award. Based on the above honors and achievements,he won the "Golden Wisdom Award - Top Ten People Award" of China's network security and information industry in 2018.

Speakers

Security innovation

Qing Yang
Founder
UnicornTeam

Hacker and Security Expert who has been the technical speaker on Black Hat and DEFCON, founder of the well-known security team UnicornTeam and the founder of the hacker innovating culture- HACKNOWN. His researches have been collected into Tesla and GSMA's Security Hall of Fame, awarded as Top Innovation Award of "Pwnie Awards" which is the Oscar Award in the hacker community, and has been nominated as the top 10 influencers of Chinese internet security "True Views Award" in 2018. Yang is the 51 CTO lecturer, security expert on CNTV's 《315》 and 《The Century With Cars II》, and the original role of DEFCON China Art Contest Winners and Public Security's lecture story 《Oriental Hacker》, as well as the male chief actor of China's first hacker microfilm 《I'm Here》. He is the writer of 《Radio》, 《Hardware》, 《Intelligence Car》, 《Revealing Security Attach and Defence Technology III》, and the English technical book 《Inside Radio: An Attack and Defence Guide》. His security abilities has been reported by Fox, Fox News, WIRED, National Geography, CNET, IEEE Comsoc, BAZAAR Men's Style and more.

Jiqiang Feng
General Manager
Aurora Infinity Information Technology Co.,Ltd

Mr. Jiqiang Feng, also known as Fengning, is a domestic senior security expert, the member of COG Information Security Professional Committee and the member of SACC China Architects Conference Advisory Board.

He is currently the general manager of Aurora Infinity, responsible for the vulnerability research lab, A&D advanced attack and defense and security operations center for financial industry. Mr. Feng has also led the construction for several large enterprises cyber security defense system and served as a technical consultant.

Speakers

Xinming Liu
Chief Architect
Xcalibyte

Mr. Xinming Liu is one of the few international computer scientists who are proficient in compiler technology. He has deep practical experience in computer language design and advanced compiler optimization technology.

In his career for more than 30 years, Mr. Xinming Liu has rich experience in building and leading large research and development teams of system software organizations, and has developed highly competitive products according to different customer needs. He served as a HP Java compiler technology lab, director of leadership based on Itanium processor compiler development work.

So far, Mr. Xinming Liu has obtained more than ten technology patents in the field of program analysis and optimization, and has published many heavyweight papers in several core technology journals.

Mr. Xinming Liu graduated from Utah State University with a master's degree in computer science

Yuning Liang
Co-founder and CEO
Xcalibyte

Mr. Yuning Liang is the co-founder and CEO of Xcalibyte, managing the company's strategic development, technology development and market growth. His technical background includes embedded systems, platform APIs, and computer vision (the field of artificial intelligence). A skilled and down-to-earth technologist, Mr. Liang has always wanted to build a technology company in Asia that using compiler technique to improve code quality. Thanks to his extensive contacts in China, he and a few like-minded friends created a new generation of static code analysis techniques for software development. He is a lifelong learner and a disciplinarian, rooted in the development mission of Xcalibyte, which is dedicated to helping developers build and deploy secure and reliable code.

Prior to his founding, Mr. Liang led software development at fortune 500 companies (including Samsung, Nokia, Huawei) and start-up technology companies. He has more than 20 years of software development and management experience. During his career, he has worked for international companies in China, South Korea and several European countries and has profound industry insights into the global technology and software security industries.

Mr. Yuning Liang graduated from Nanyang technological university with a master's degree in engineering.

Speakers

Ruidong Zhang
CEO
NoSugarTech

Ruidong Zhang, known as Only-guest, currently the CEO of NoSugarTech, the special network security expert of Sichuan University, head of PKAV (a well-known security team), one of the most influential white hats in China. Mr. Zhang has strong technical background and rich practical experience in the field of WEB security, vulnerability mining, network attack and defence and other research areas. He is currently committed to the field of anti-cybercrime security technology and product research and development. He has made huge positive contributions for the national, provincial and municipal public security organs in the field of anti-cybercrime.

Kunzhe Chai
Security Director
BCM Social Corp

Kunzhe Chai, the security director of BCM Social Corp, eight years of experience in the security field, the first domestic wireless security defense product standard setter, the inventor of pseudo-base station defense technology, one of the well-known wireless security tools MDK developer, obtained more than 30 wireless communication defense patents; leads the team to share research results in various security conferences at home and abroad, such as BlackHat, DEFCON, HackInTheBox, POC, Codeblue, etc.

Zhengxian Lin
R&D Director
BCM Social Corp

Zhengxian Lin, the R&D Director of BCM Social Corp, 20 years of experience in communication and Internet research and development, strong interest in communication and security; won provincial excellent patent award and several company technical awards, has a number of invention patents.

Lin Huang
Director
360 Research Institute
360 Technology

Lin HUANG is a senior manager and wireless security expert, from 360 Research Institute, 360 Technology. She is the 360 Technology's 3GPP standard SA3 delegate. She received Ph.D degree from BUPT. Her interests include security issues in wireless communication, especially cellular network security. She was a speaker at BlackHat, DEFCON, and HITB security conferences etc.

Sponsors

Gold Partner

Sangfor Technologies
https://www.sangfor.com/

Sangfor Technologies is a leading global vendor of IT infrastructure solutions, specializing in Cloud Computing & Network Security with a wide range of products including: Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Internet Access Management, WAN Optimization, SD-WAN and many others.

360 CYBER SECURITY UNIVERSITY

Sponsors

Gold Sponsor

AURORA极光无限

AURORA INFINITY INFORMATION TECHNOLOGY CO.,LTD.

Aurora Infinity,relying on the cutting-edge Graph Neural Network Theory, applies ourselves to build the world-class AI automation vulnerability mining and APT automatic products with offensive and defensive integration; we focus on organizing the world's top red-blue confrontation exercises and vulnerability mining research team to assist and improve the level of AI automation security products.

派拉软件 PARAVIEW SOFTWARE

Shanghai Paraview Software Co., Ltd.

www.paraview.cn

Shanghai Paraview Software Co., Ltd. (Hereinafter referred to as Paraview) is a leading information security technology company in China. Data Definition, AI Driven, Intelligent Algorithm, Scenario Analysis, driven by technology, Paraview provides information security products, consulting and implementation services, our business covers identity security, business security and data security, involving enterprise identity management, customer identity management, privileged identity management, multifactor-factor authentication, user behavior analysis, API security management platform and data lake. It has successfully provided information security services for more than 500 large and medium-sized enterprises and units such as automobile, manufacturing, finance, real estate, home furnishing, retail, education, medicine and government. At present, Paraview has established agencies in Shanghai, Beijing, Guangzhou, Changchun, Wuhan Shenzhen and Chengdu. Paraview is certified by the government with the certifications of High & New Technological Enterprise, software enterprise, enterprise R&D institution, specialized and emerging minor enterprise and target enterprise of cultivation by Shanghai little giant of science and technology. Besides, Paraview has been awarded the ISO 9001 Quality System Certification and CMMI L3 Certification, and obtained sale licenses for safety products issued by the Ministry of Public Security and more than 50 intellectual property rights.

Sponsors

Gold Sponsor

TENABLE
www.tenable.com

Tenable®, Inc. is the provider of Cyber Exposure solutions, empowering organizations to manage and measure cybersecurity risk in the digital era. As the creator of Nessus® and pioneer of the vulnerability assessment market, Tenable is building on its deep technology expertise to deliver the world's first platform to secure any digital asset on any computing platform, providing broad visibility across the modern attack surface. Over 27,000 organizations including more than 50 percent of the Fortune 500 around the globe rely on Tenable to understand and reduce cyber risks.

Chengdu NoSugar Information Technology Co., Ltd.

Chengdu NoSugar Information Technology Co., Ltd. (NoSugar Tech) is the leader of anti cybercrime solution provider,committed to anti cybercrime security technology research and product development.Focus on fighting telecom scams,internet fraud,-combating economic crimes involving the mass participation, etc. Providing efficient and professional services to government and public security organization.

Sponsors

Exhibitor

TRUSTASIA TECHNOLOGIES, INC.

TrustAsia is a professional network security service provider, specializing in providing a series of network security management solutions, such as SSL certificate of international famous brand, SSL certificate of TrustAsia® independent brand, SSL certificate management of independent intellectual property rights, SSL protocol level monitoring and certificate risk evaluation, etc for industries. It provides enterprises and individuals with secure and reliable encrypted data transmission and authentication services. TrustAsia is a well-recognized and trusted brand in the field of network security!

THREATBOOK

www.threatbook.cn

ThreatBook is Threat Detection and Response Expert from China, listed by Gartner. We are empowering hundreds of organizations by delivering professional threat detection and intelligence management products and cloud-based DNS Service to help our customers enhance all aspects of network threat monitoring management.

QI AN XIN TECHNOLOGY GROUP INCORPORATION

QI AN XIN TECHNOLOGY GROUP INCORPORATION

Qi An Xin Group is leading security provider dedicated in protecting critical and valuable internet assets in a wide range of areas including Government, Finance, Energy, Telecom etc. We are the fastest growing company in the Chinese security market with over 90% consecutive compound annual growth rate since 2015. Under hard work of 6000+ professionals, our technologies have been adopted in 90% of government departments, state-owned companies, and large banks. We start our international development in 2019 and extend our global business in Indonesia, Singapore, Canada, Hong Kong, Macao etc.

Exhibitor

vinchin

Chengdu Vinchin Technology Co.,Ltd.
www.vinchin.com/en

Founded in 2015 with headquarter in Chengdu, Vinchin is an innovative VM backup solution provider concentrating on researching and developing a series of flexible, reliable and easy-to-use data protection solutions such as VM backup, VM recovery and data disaster recovery across different hypervisors based virtualization environments. Our mission is to help customers to protect their OS, data and applications running on virtual machines from being destroyed due to human error, viruses & attacks, hardware failure or any irresistible disaster.

OPPO 安全应急响应中心
OPPO Security Response Center

OPPO Security Response Center
security.oppo.com

The OPPO Security Response Center (OSRC)is a platform of identifying security vulnerabilities and responding to security threats of OPPO business. We are dedicated to protecting security of OPPO's users, products and services, promoting cooperation and communications among security experts.

天际友盟
TianJi Partners

TIANJI PARTNERS CO., LTD.
www.tj-un.com/en/index.html

Tianji Partners, founded in June 2015, is a leading Security Intelligence solution vendor located in Beijing. Tianji Partners provides professional security services and comprehensive security intelligence solution for enterprise customers, domestically and globally. Globally , Tianji solutions complied with OASIS STIX/TAXII standard and is publicly recognized. Locally, Tianji has paticipated in the process of China Threat Intelligence GB Standard, from drafting to finalization. Enabled by Security Intelligence technology, solve real security issues for customers, is Tianji' s business target.

Sponsors

Exhibitor

Chengdu Global Capsheaf Solution Co.,Ltd

Capsheaf is a product supplier specializing in network security, backup & disaster recovery and cloud computing. It has now obtained 19 national invention patents and more than 60 computer software copyrights. Products have been widely used in more than 2,000 companies and institutions such as government, medical, education, enterprises and some critical infrastructure organizations.

Hunan UUCODE Information Technology CO.,LTD

UUCODE is a rapidly growing technology company focussing on network traffic access, aggregation, filtering, load balancing, deduplication and DPI (deep packet inspection) technologies.provide high-performance application acceleration and offload solutions for Network Traffic Analysis.

Exhibitor

DataVisor

DataVisor's mission is to build and restore trust online. It partners with the largest financial and internet properties in the world to protect them from a wide array of attacks, including fraud, abuse, and money laundering. An industry leader in unsupervised machine learning, DataVisor's Detection Solution detects attackers without needing training data, and often before they can do damage. DataVisor is made up of a team of world-class experts in big data infrastructure and machine learning. It builds the world's most advanced algorithms to fight the world's most sophisticated online attackers.

Shanghai Yinian Information Technology Co., Ltd.

https://www.xianganquan.com

Shanghai Yinian Information Technology Co., Ltd. , the leader company in awareness of Cyber Security in China. Adhering to the core concept of education changing cognition and consciousness deciding security, the company provides teaching content, tool platform, operation services and other supporting solutions for enterprises. The company upholds idea to the new changes of education cognition, conciseness making safety core idea, devote oneself to "" build the safe human firewall of network space"

BEIJING ZHAOPIN.COM COMPANY LIMITED

www.zhaopin.com

Established in 1994, Zhaopin.com has 25 years' experience in the human resource industry. With 39 branches, crossing over 200 cities, Zhaopin.com has already provided over 4,560,000+ enterprise partners with human resource services. Meanwhile, Zhaopin.com is a career development platform trusted by 180 million employees. With 25 years of research experience, Data Report of Zhaopin.com is rated as "an indication of career trends in China" by authoritative media at home and abroad.

FENG TAI TECHNOLOGY(BEIJING) CO,LTD

Sponsors

Exhibitor

BCM MESSENGER
SECURITY, PRIVACY, BLOCKCHAIN.

BCM MESSENGER
https://bcm.social/

BCM Messenger stands for security and privacy, which is built by a tiny team of world-renowned developers and hackers. They design and develop a highly secure instant messaging, each message is strictly encrypted and no one can decrypt the content, and release
a new communication technology without using the internet.
A new era of messaging allows BCM to redefine.

BEIJING GENIUS CYBERTECH CO.,LTD
http://www.geniuscybertech.com

The first cybersecurity consulting company in China that provides lifecycle services to security companies, offering customized business advice and assisting customers in managing business growth. The company was founded by Mr. Tan Xiaosheng, the former CTO of the 360 Group. Together with many experts in the industry, the company mainly serves the Chinese cybersecurity enterprises, connecting capital and industry to meet the unique needs of entrepreneurs, CEOs, boards of directors and investors.

An innovative consulting model tailored specifically for the cybersecurity industry to provide operational excellence, capital raising, strategic planning, exit financing and M&A services throughout the enterprise lifecycle

THE CYBERSPACE SECURITY TALENT EDUCATION ALLIANCE OF CHINA

Sponsors

Partner

(ISC)²
https://www.isc2.org

(ISC)2 is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

Chengdu Software Industry Association
http://www.cdsia.org.cn/

Chengdu Software Industry Association is a nonprofit institution registered with the approval of Chengdu Civil Affair Bureau, and it consists of the units and individuals in the field of software R&D, sales, computer system integration, IT service, application of information system, computer education and management.
CDSIA serve as a bridge and bond between the government and enterprises, enterprises and society, and an information exchange center, policy research center, business direction center, technology training center and scientific service center for Chengdu software and IT service industry.

Sichuan Big Data Industry Federation
http://www.scbigdata.org/

Media Partners

PREMIER MEDIA PARTNERS

FreeBuf
www.freebuf.com

FreeBuf is the earliest, well-known and most active domestic security technology exchange platform bringing together the latest safety information and in-depth reports in the world. This is the best platform for communication, sharing, learning and growth of security technicians.

51CTO
www.51cto.com

Established in 2005, 51CTO is a multiple-dimension platform that focuses on IT tech innovation and development. With over 10 million professional members, 51CTO covers most the IT practitioners from all major cities in China. 51CTO has been a one-stop tech supplying and other requirements , which serves to help IT practitioners for knowledge spreading, experience sharing, technical communicating, career developing, product promoting and other purposes.

ZDNet China
www.zdnet.com.cn

ZDNet China was officially founded in 1997 and was the first Chinese business website and IT portal focused on enterprise. ZDNet provides the most authoritative IT news, most professional IT solutions evaluation system, the most updated SNS interactive system and the most practical CIO professional experiences. ZDNet leads the reporting and analyzing of cloud computing to further strengthen its industry leading position.

Media Partners

MEDIA PARTNERS

Dark Reading
www.darkreading.com

Dark Reading encompasses 13 communities and each community is led by editors and subject matter experts who collaborate with security researchers, technology specialists, industry analysts and other Dark Reading members to provide timely, accurate and informative articles that lead to spirited discussions.

Information Week
www.informationweek.com

InformationWeek defines the value of technology in the age of digital business. As the world's most trusted business technology resource, InformationWeek offers independent insight and advice to help today's IT leaders navigate the fast-changing technology landscape and identify the best strategies and tools to drive their organizations forward.

Network Computing
www.networkcomputing.com

IT professionals count on Network Computing and its affiliated conference, Interop, to show them the how and why behind next-generation networks, data centers, storage systems, communications, and cloud architectures. Interop is the live event for the IT community, while Network Computing provides IT practitioners with an online experience.

AQNIU
www.aqniu.com

AQNIU is the most influential cybersecurity media and research organization in China.Its core is the investigation and research of the cybersecurity industry. For example,the annual Top100 Cybersecurity Report,the matrix diagram of the cybersecurity segmentation area, the "Cybersecurity Full View Graph" that reflects the entire industry.With the concept of "Media As A Service", AQNIU provides news reports,conference salons, survey reports, publish white-book,consulting think tanks,and other services for government, enterprises.

Media Partners

MEDIA PARTNERS

OWASP中国
www.owasp.org.cn

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP CHINA is the OWASP Chapters located in China, which helps to foster local discussion of application security.

E security
www.easyaq.com

E security was established in 2014, and now operating E security app, E security web portal, and E security wechat official account. Moreover, E security is cooperating with Sohu, Netease, Sina, Tencent, Phoenix New Media, Toutiao.com and Baidu Baijia.
At this moment, E security has over 90 million hits annually. For each month, there are more than 6 million people who learn cybersecurity news from E security platform.
E security aims to be the leader of cybersecurity media!

C114（C114 Communication Network）
www.c114.com.cn

C114 Communication Network was established in 1999, a pioneer and leader of Chinese web portal focused on information and communications technology or (ICT) industry, an integrated online media platform provides authoritative industry information, business information and value-added services.C114 Communication Network represents its official brand, also called C114. C114 has the longest history, biggest scale, most extensive coverage, largest page view, most subscribers and longest time viewed for a site.

Cybersecurity Insight
https://www.secrss.com/

Cybersecurity Insight (secrss.com) is a think tank platform focusing on the industry development and best practices of cyber security.

MEDIA PARTNERS

Geek net - technology enables new businesses.
www.FromGeek.com

Founded in 2012, fromgeek.com is a Geek community of technophiles, who later reveres the commercial operation of “ science and technology as the first productivity “ in order to explore the role and energy of technological innovation in the new business revolution.

Ebrun
www.ebrun.com

Ebrun is the most influential e-commerce knowledge platform in China. Focusing on e-commerce, Ebrun has reached more than 20 million e-commerce managers around the world and established an extensive influence on retailing, agriculture, cross-border e-commerce, health, automobile, e-commerce service, international e-commerce, etc.

Vsharing
www.vsharing.com

Founded in 2006, Shanghai Vsharing Technology Co., Ltd. (www.vsharing.com) is a Shanghai SME public service agency and acquires identification of high-tech enterprises. Vsharing now has 4,000,000 real-name system member users. Vsharing provides members with daily mass digital information, 2,300,000+ documents, more than 50 online and offline theme activities. The main cores of the company are media business, IT services and investment services.

Security and Informatization
www.365master.com

Security and Informationization is an information security magazine sponsored by China Center for Information Industry Development (CCID) and headed by the Ministry of Industry and Information Technology. The contents of the magazine are network security and DevOps, Cloud computing, big data, AI, IOT, data centers, etc. Readers are oriented to network managers and technicians such as CIO and CTO of enterprises and institutions. It is a practical information security magazine.

Media Partners

MEDIA PARTNERS

中国电子银行网
www.cebnet.com.cn

FreeBuf
www.freebuf.com

China e-bank website is founded by CFCA(China Financial Certification Authority), and cooperated with nearly 100 commercial banks, which is considered as one of the most authoritative and professional business information platform in the field of electronic banking vertical portals. The website consists of FINTECH, SPECIAL COLUMN, BANKING NEWS, INFORMATION SECURITY, and BANK BANG as a series of channels, and includes policy interpretation, experts' viewpoints, hot comments and updated information. China e-bank website has been concentrating on e-banking, ITFIN, Fintech and research frontiers, and it offers a specialized information service for financial industry especially banks. China e-bank builds a new financial media which combines updated information with integrated service.

OFweek | smartcity.ofweek.com
智慧城市网
中国智慧城市行业门户

ofweek.com/smartcity
ofweek.com/smartcity

ofweek.com/smartcity is a portal of the smart city industry, committed to providing news and information, concept as well as solutions for the smart city industry, driving the development of smart community and smart industry.

Media Partners

self media partner

ITCLOUD REPORT
www.itcloudbd.com

ITCLOUD REPORT -- One of the Top10 leading enterprise IT media in China. Recognized by MIIT and has been official media of several conferences such as Trusted Cloud Summit, Cloud Connect and so on. In the past five years, it has attracted more than 5 million readers with original and high-quality news reports.

展位:A05

AURORA极光无限

AURORA INFINITY 极光无限

300万年薪

对比 阿里P9 腾讯 4.3

RED TEAM负责人

苏州极光无限信息技术有限公司【简称：极光无限】，坐落于苏州金鸡湖畔的5A级写字楼苏州中心D座，是一家以安全技术为核心、AI技术为驱动的信息安全科技公司，由十多位来自国内外顶尖安全公司的资深安全专家及数位从事AI及信息安全领域研究的教授、博士进行技术领携。

依托最前沿的图神经网络理论，公司将致力于打造国际一流的AI自动化漏洞挖掘及APT自动攻防产品，公司将重点组建全球顶级的红蓝对抗及漏洞挖掘研究团队，以辅助和完善AI自动化安全产品研发。

10月23日13:30-14:00安全创新分论坛

演讲嘉宾：风宁

图神经网络(GNN)在漏洞发现中的应用

国内资深安全专家，CDG信息安全专业委员会委员，SACC中国架构师大会顾问指专家成员。现任极光无限总经理，负责公司漏洞研究实验室、红蓝对抗高级攻防及金融行业安全运营中心工作。曾主导建设多个大型企业网络安全纵深防御体系并担任技术顾问。

投递邮箱：hr@secwx.com

扫一扫

关注公众号

团队介绍
Team Introduction

AURORA极光无限

展位:A05

Web安全负责人—余弦

知名黑客，区块链安全公司慢雾科技创始人，红队安全公司 Joinsec 创始人，曾组织打造出了知名黑客大会 “漏洞交易平台 Seebug，网络空间搜索引擎 ZoomEye，中国计算机学会计算机安全专委会委员，中国电子学会电子对抗分会委员，安全领域畅销书《Web前端黑客技术揭秘》作者。

漏洞研究负责人—仙果

十余年致力于网络攻防对抗研究，曾任国内安全公司首席安全官（CSO），网络攻防对抗领域多年漏洞挖掘、攻防对抗实战经验，2011年至今在国内最大软件安全论坛担任看雪论坛漏洞分析版块版主；2015年在i春秋网络安全培训平台开设“软件漏洞分析”基础课程；电子科技大学特聘专家。

热招中

- 高级渗透测试工程师
- 渗透测试工程师
- 高级漏洞挖掘工程师
- 漏洞挖掘工程师

人员需求

苏州200人，成都50-60人

办公地点

优先：苏州

待选：厦门、成都

入职后，表现优秀有机会短期派往莫斯科，和众多国际顶级安全专家、国际CTF战队核心成员、IMO金牌 以及 顶尖从事数学、人工智能领域研究的教授、博士交流学习。

投递邮箱：hr@secwx.com

扫一扫
关注公众号

360 360网络安全大学

360网络安全大学

360网络安全大学是中国最大、最专业的网络安全教育服务提供商。

360网络安全大学前身是360网络安全学院，成立于2017年，周鸿祎先生任荣誉校长。专注于网络安全教育及网络安全产业相关领域，为政府和企业培养网络安全人才，为国家网络安全保驾护航！

360网络安全职业认证

认证安全运维工程师（CSOR）
认证安全服务工程师（CSAA）

网络安全就业培训

线上线下培训相结合
专业系统化的就业培训

校企合作

共建网络安全实训环境
共建网络安全人才基地
共建网络空间安全专业
共建网络空间安全学院

政企培训

为各行业提供定制化阶梯式安全培训课程 内容包括安全意识、安全技术、安全管理等各个方面

网络安全青少年科普基地

科普网络安全知识和技术
互动体验 闯关游戏 寓教于乐

比赛平台

职业技能赛 CTF夺旗赛
红蓝对抗赛 靶场攻防赛

4000-555-360 https://university.360.cn/ university@360.cn