

白皮书
版本 001



生态系统

2017年8月

目录

摘要	1
引言	2
什么是HACKEN生态系统？	3
Hacken如何利用区块链？	5
为什么需要另一个网络安全市场？	6
Hacken代币	7
HKN的销售 7 代币分销 8 里程碑 8 路线图	9
“燃烧”机理	10
第三方托管和审计	11
免责声明	11
HackenProof	12
未报告的零日报酬平台	14
Hacken加速器	15
网络安全分析中心	16
HackIT大会	17
夺旗比赛	17
“黑客之战”	17
网络侦探OSINT挑战赛	17
HackIT杯	17
关于我们	19
此事为何重要？	20
附录。现有的漏洞研究众包业务简析	22

摘要

本白皮书阐释了Hacken生态系统的业务组成部分。它还详细介绍了Hacken代币的销售，其将从2017年10月9日00:00（欧洲东部时间）开始，于2017年11月9日00:00（欧洲东部时间）结束。白皮书还说明了如果代币销售达到其目标里程碑后如何打造Hacken生态系统的后续路线图。

Hacken生态系统是一个社区驱动的业务组织，它因此次代币销售而产生，并且将会融入全球多个司法管辖区。它由HackenProof漏洞悬赏市场、未报告的零日报酬平台、Hacken网络安全初创公司孵化器、网络安全分析中心和HackIT大会而组成。

Hacken（HKN）是一种ERC20代币，它是Hacken生态系统中允许的唯一支付工具。今天立即购买Hacken，能让您在未来以具吸引力的价格获得优质网络安全服务。

请谨记：与此次代币销售有关的所有财务数据和法律文件均可应请求在本白皮书之外单独提供。

引言

2017年，Parity被盗3200万美元，Coindash被盗740万美元；2016年，Bitfinex被盗7200万美元；2015年，Bitstamp被盗510万美元，2014年，Mt. Gox被盗6500万美元。这些是各种加密货币基础架构项目损失给黑客的可怕的法定等价物。

据位于Tulsa的Tandy计算机学院的Tyler Moore研究，自2009年比特币出现至2015年3月，在此期间的所有比特币交易中有约33%被黑客袭击。加密货币当然并不是受到黑客困扰的唯一业务。美国总统唐纳德·特朗普本人最近就陷入网络安全争议，他表示网络偷窃是迄今为止在美国增长最快的犯罪。

随总统的这种担心而来的是一大笔投资。作为2017年联邦预算的一部分，美国将投资190多亿美元在网络安全上。这一数字较奥巴马政府2016年预算的140亿美元有所增加。

不幸的是，并没有足够的人才利用这巨大的财务资源。根据CyberSeek的统计，2017年有超过348,000个网络安全职位空缺，到2022年这一数字将会达到180万个。连同在防火墙的另一侧所雇佣的无法说明的黑帽黑客数量，这些统计数字需要得到快速响应。

直到最近，东欧，特别是乌克兰，已成为各种颇具争议的网上行动的安全港。该国拥有数量庞大的高素质的数学和计算机科学本科毕业生，但是其经济给这些人提供的机会仍然很少。尽管如此，乌克兰创始人藏身于像PayPal、WhatsApp这样的硅谷独角兽，甚至于你现在可能正在使用的WiFi技术之后。

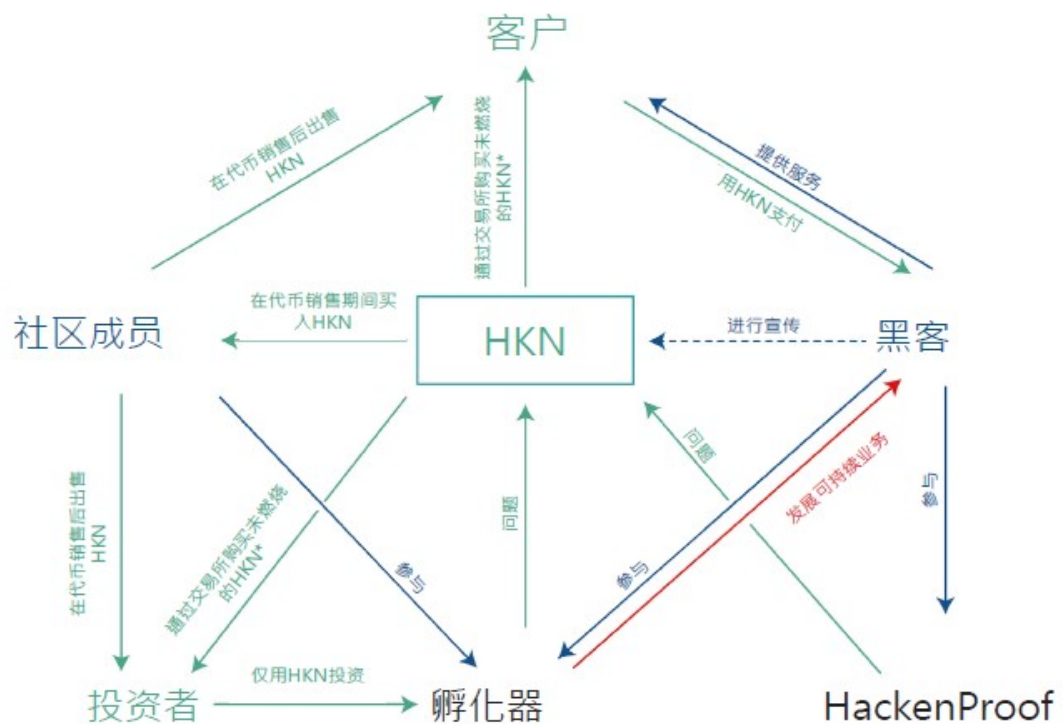
我们认为乌克兰能够成为下一个欧洲网络安全中心。考虑到2015年的强制性电网停电事故Pet ya.A以及必定降临的其他国家网络攻击，大力提升这个领域中的技术专长事关该国存亡。然而，这个蓬勃发展的网络安全产业的兴起应当得到足智多谋、具有道德的专家社群的支持。

我们在Hacken的目标是通过为成员创造稳定的收入手段和经济刺激机制而设立这样一种框架。长期而言，您参与Hacken生态系统将会确保下一代本地计算机天才同你站在防火墙的同一侧。

什么是HACKEN生态系统？

我们的生态系统由一种代币（Hacken）和一系列提供服务的业务组成。这些服务只能通过使用Hacken作为支付工具获得。Hacken的数量是有限的，限定为2000万个代币，这些代币将在预售和主要的代币销售期间进行分发。

组成Hacken生态系统的业务包括HackenProof漏洞悬赏市场、未报告的零日报酬平台、Hacken网络安全初创公司孵化器、网络安全分析中心和HackIT大会。本白皮书有独立章节进一步描述这个生态系统的每个要素。



* 请参阅“燃烧机理”部分

图1 Hacken生态系统

Hacken背后的大创意是将Hacken的每个拥有者转变为社区成员。因为Hacken是一个专业软件实用程序代币，主要针对网络安全专业人士和项目，所以它还能通过他们彼此进行交易，以及对网络安全初创公司进行投资提供奖励，把这些人聚到一起。这些人需要沟通和彼此交流，以便利用他们的Hacken。社区越活跃，它给每位成员带来的价值越多。

尽管我们的生态系统拥有稳健的商业计划和产品路线图，它不只是和商业有关。我们的目的还包括促进HackIT（乌克兰最大的国际网络安全大会）的发展并为其提供支持。网络安全业务事关专门知识、道德伦理和持续培训。通过为HackIT提供支持，我们想要确保回馈给我们的平台提供支持的群体。

Oleksii Matiasevych的故事很好地诠释了我们的核心价值观。他是乌克兰的网络安全专家、Ambisafe的EDCC架构师以及我们此次代币销售的技术顾问。

就在今年夏天，2017年7月19日，Oleksii在Parity以太坊钱包代码中[发现了一个关键漏洞](#)。Oleksii展示的证据表明，黑客持续攻击，导致数百个以太坊钱包受损，根本来不及与其他人进行讨论。他最终将价值1,402,996.09美元的以太币从受损的钱包中转到了他取得并控制的钱包当中。然后Oleksii与白帽黑客组织取得了联系，他们负责搜寻并将全部货币返还给其合法的拥有者。

我们的生态系统的终极目标是造就新一代黑客，对他们来说Oleksii所做的一切是完全正常的，是唯一可以接受的生命场景。

Hacken如何利用区块链？

漏洞检测的证据

在客户签署漏洞悬赏计划协议时，我们的团队会创建一个相关的区块链区块，当中含有关于产品、服务协议条款和时间戳的数据。链的下一个区块专属该客户，将包含在我们的安全研究期间所发现漏洞的相关信息。

在客户解决了在漏洞悬赏研究期间所发现的漏洞之后，HackenProof专家会进行研究后审计。之后，我们会与客户讨论我们的研究结果，并会告知需要采取的任何额外措施。如果审计结果对于我们团队和客户双方来说都令人满意，我们将形成链中的下一个区块，其中包含有关已经解决问题的相关信息。

最后，客户会收到HackenProof漏洞和对策证书，其中包含关于已发现并解决的所有漏洞的报告，并附有每个事件的时间戳。之后，客户可以调整自己的区块链共享偏好，并向公众、客户、投资者或他们指定的人士公布此证书。

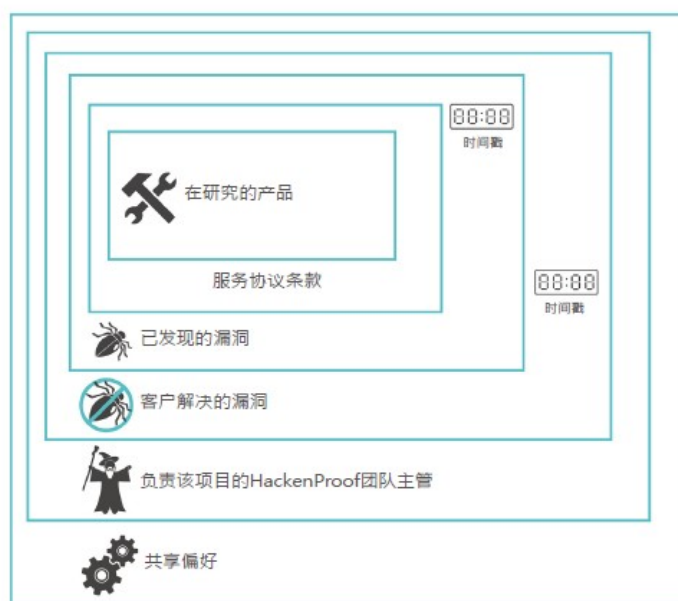


图2 HackenProof漏洞和对策证书

加密货币

除了在网络安全中使用区块链之外，代币销售使用了加密货币领域内的一项有趣金融创新。这就是我们的“燃烧”机理，本书对其作了[单独描述](#)。

为什么需要另一个网络安全市场？

正如本书附录中的[简要市场分析](#)所述，或者通过您自己的观察，目前至少有4个现有漏洞悬赏和侵入测试服务。每一项都有日渐增长的客户群和投资者支持，从几美元到7400万美元不等。因此，显而易见的问题是：真的需要另一个这种市场吗？

我们认为答案是肯定的。原因如下：

1. 目前在侵入测试和漏洞悬赏计划领域，供给无法满足需求。最近，马自达在拉斯维加斯赞助了一场夺旗赛，获胜者荣获一辆卡车。在吉普、特斯拉和尼桑LEAF被黑客入侵之后，汽车行业对高素质的赏金猎人和侵入测试员求贤若渴。在我们看来，这意味着：不，四个现存服务是严重不够的。仍有一片细分市场和通用网络安全社区的蓝海。
2. 为区块链量身打造的网络安全生态系统。作为区块链企业家，我们比目前的大多数网络安全公司更熟悉这项技术，包括它的细微之处、风险和相关群体。在《华尔街日报》上读区块链，作为和同事们茶余饭后的谈资，和投资几千美元比特币来消遣，是一回事。将您整个业务的现金流和核心认证技术建立在区块链基础上完全是另一回事。
3. 我们是否忽略了中小型企业？中小型企业无法负担企业侵入测试和漏洞悬赏计划的好处。这不代表他们不需要该业务。在当前的网络安全环境中，小企业享有的现代计算机安全基础架构福利非常有限。我们将为中小型企业提供简单易行的线上工具，以便让它们组织并运行漏洞悬赏和侵入测试活动。
4. 同一时区，同一文化价值观。Hacken将是欧洲漏洞悬赏市场中的先行者。目前，这一市场由硅谷的供应商主导。这完全可以理解，但是旧金山和湾区并不是世界上唯一能创造出优质软件和硬件项目的地方。世界上其它地区对此类服务仍然有着足够的需求，并且需要物有所值。

Hacken代币

千百年来，金钱是联合人类组织、促进他们随后增长和发展的有效动力，但不是主要的驱动力。Hacken也不例外。这项区块链的分布式性质使我们能够及时创造新的代币，并使其拥有现代货币的最佳品质。智能合约技术使我们能够为Hacken增添一个附加层，为网络安全社区创造经济激励，以道德和正当的方式进行联合与合作。

Hacken是我们生态系统内唯一被接受的货币。任何经由HackenProof、未报告的零日报酬平台、网络安全分析中心下的新订单或是通过Hacken加速器做出的新投资，必须用Hacken币结算。这将会奖励用Hacken币支付的社区成员，为他们提供正向资金流动和低波动性。

请注意：Hacken币无意成为数字货币、商品或任何其它金融工具，不代表任何股份、股权、证券或等价权利，包括但不限于任何接受未来收益股份和知识产权的权利，也不代表任何所有权。

HKN的销售

总供应	2000万Hacken币 130万预售 (100万 + 30% 奖金) 1870万主代币销售	
符号	HKN	
最低卖入	1以太币	
上限	2000万。未来无计划释放	
最初法定等价物	1 HKN = 1美元	
接受的货币	比特币(BTC)、以太币(ETH)、达世币(DASH)、莱特币(LTC)、美元、欧元, TaaS	
代币销售时长	2017年10月9日至2017年11月9日	
第三方保管	平均80%的募集资金将保留在托管账户中	
* 主要代币销售奖金计划	1 — 4小时	25%
	1 — 2天	20%
	3 — 7天	15%
	1 — 2周	10%

图3 代币销售详情

代币分销

公开销售	80%
团队薪酬	10%
代币销售奖励·其中：	3%
博客帖子	1.2%
BitcoinTalk签名	0.45%
BitcoinTalk翻译	0.45%
BitcoinTalk跟帖	0.3%
Tweeter帖子	0.3%
Facebook帖子	0.3%

图4 代币分销表

里程碑

承诺	最低里程碑	限定量里程碑	目标里程碑	高级里程碑	最大里程碑
已售代币	150万	400万	1000万	1800万	2000万
HackIT大会	15%	15%	15%	10%	10%
HackenProof市场	85%	60%	40%	30%	25%
Hacken加速器	—	25%	45%	30%	25%
零日平台	—	—	—	30%	30%
分析中心	—	—	—	—	10%

图5 里程碑

路线图

该承诺路线图适用于最大里程碑。该资源分布同样适用于其他里程碑的每个承诺项目。

粗体和突出显示表示产品发布期间。

项目 / 资源分布	2017年 第4季度	2018年 第1季度	2018年 第2季度	2018年 第3季度	2018年 第4季度	2019年	2020年
HackIT大会	—	—	—	35%	—	33%	32%
HackenProof市场	10%	20%	10%	10%	10%	25%	15%
Hacken加速器	5%	5%	10%	10%	15%	30%	25%
零日平台	5%	5%	10%	15%	15%	25%	25%
分析中心	2.5%	5%	5%	7.5%	7.5%	37.5%	35%

图6 路线图

发布期间：

HackenProof市场——2017年第4季度

分析中心——2018年第1季度

Hacken加速器——2017年第4季度

零日平台——2018年第3季度

HackIT大会——2018年第3季度 · Hacken将支持2018年HackIT大会的新竞赛和演讲组

“燃烧”机理

出于监管原因，我们为此次代币销售发明了“燃烧”机理，否则将会导致居住在某些行政辖区的客户无法参与其中。我们也相信“燃烧”机理将会促进Hacken的流动性增长，减少波动性风险。Hacken的所有者需理解“燃烧”机理仅仅影响平台费用，从而减少了我们（平台的创始人而非顾客或客户）拥有的Hacken数额。这一点非常重要。

项目	“燃烧”机理	通知	时机
HackenProof	每笔交易，50%的平台服务保证金。目前，预计HackenProof服务的平均保证金是每笔交易30%，这意味着涉及HackenProof服务的每笔交易金额的15%将被“烧掉”。	燃烧前24小时	每天12:00 PM（欧洲东部时间）
加速器	在初创公司退出期间，加速器保证金的50%。显然，目前难以估计确切的退出保证金。我们期待投资复制因子会在10倍或更高的范围内。		
零日平台	Hacken从管理两项业务的公司中所实现的年利润的50%。利润金额将根据知名国际审计师所审计的财务报告计算得出。	燃烧之前的日历周	每年，财务报表审计之后
分析中心			

图7 “燃烧”机理

我们服务保证金没有被燃烧的另外50%会怎么样？Hacken生态系统的管理公司将会收集这些Hacken币，直到其金额达到Hacken币流通总金额的1%。

在此次活动中，我们将会24小时发布公告，然后通过主要的加密货币交易所出售在活动时所累积金额的1%（即活动那一刻Hacken币总金额的0.01%）。销售将在公告发布之后第二天的14:00（欧洲东部时间）开始。交易所名单将在发生第一笔此类销售时提供给公众。我们保留将来修改交易所名单的权利。

“燃烧”将会改变Hacken币兑其他加密货币或法定货币的结算汇率。我们需要借此保持漏洞搜索服务有合理的价格，吸引更多黑客到平台，以及确保对生态系统进行稳定高效的维护。所有燃烧数据将通过我们的网站公开、透明地提供给公众。

第三方托管和审计

托管代理参与对投资者资产的监管过程。他们的功能是根据本文描述的路线图来监督筹措资金的使用。托管代理可以通过对项目的HKN钱包（用来积累投资者资金）使用密钥来禁止交易。

托管账户供应商将为Juscutum以及通过Hacken生态系统公共理事会招标选定的四大审计公司之一。Juscutum是一家位于乌克兰首都基辅的律师事务所，为区块链业务提供法律支持。对HackenProof和HackIT大会来说，70%筹集到的资金将会以托管形式进行保管。我们将为零日平台，Hacken加速器 and 网络安全分析中心建立一个托管账户，将其预算的研发成本100%纳入其中。

对Hacken生态系统法人实体的财务报表的年度审计将由国际知名的审计机构进行，该机构将由通过Hacken生态系统公共理事会所管理的招标选定。

免责声明

本文件以及所提供的任何其他文件或资料不构成出售股份或证券的要约或招揽。所呈列的信息均不拟作为且不应被视作任何投资决策的依据。

Hacken生态系统不提供任何证券投资建议、咨询或招揽，且不得以此方式进行诠释。本文件不构成且不得被诠释为任何证券或其它金融工具的要素，不应被理解为任何出售或认购、或是任何购买或认购的邀请。

HackenProof

HackenProof是一个由白帽黑客和区块链社区基于公平分配的原则建立的漏洞悬赏市场平台。这里是两个社区可以合作与互相支持的地方。该合作的目的是产生高品质的侵入测试和漏洞报告，提交报告的社区成员将获得高额报酬。

它是如何运行的？

1. 客户报名参加赏金狩猎计划，选择一个已确定的程序策略，选定邀请和奖金，并设置奖金支付级别。
2. 我们的专家会帮助客户建立并自定义程序，如有需要还可以对它进行管理。
3. 确立安全评估范围之后，我们的团队将邀请Hacken社区来参与评估。数百名白帽黑客会评估客户的代码查找漏洞和臭虫。
4. 社区成员会提交漏洞并按照优先次序对其进行处理。专家将就其报告的相关性和独创性进行检查。
5. 如社区成员发现有价值的漏洞，他们将得到一笔费用。
6. 如果需要，客户可以向Hacken安全解决方案架构团队订购额外建议来制订应对措施。
7. 客户将得到一份漏洞证书，以证明其软件通过了Hacken社区的检测。另外一种方式是，在证书中单独设应对措施一节，列出所有客户发现并补救的问题。

关键特征

- 仅限邀请或公开——漏洞悬赏计划的公共可见性级别可以根据您的目标进行配置。
- 自我管理或专用——您的程序可根据您的预算和专业知识水平进行定制。
- 高度灵活的客户自助服务门户。您可以运行向导来定义和启动您的程序，然后，机器人将检查报告并消除重复。然后，您可以调整付款来为那些最有价值的发现提供奖金。
- 由VDI、VPN和PAM解决方案提供技术支持的可定制、密封的测试环境，能使参与该活动的研究人员更好地了解客户的基础架构，而不会造成任何伤害或意外。

未报告的零日报酬平台

我们将为未报告的零日漏洞创建一个报酬基金。Hacken会资助聪明的技术专家，在经济上奖励他们进行原创、之前未曾披露的零日研究。

我们理解所涉及的法律和道德风险，但我们坚信零日发现必须拥有透明且公开合理的报酬渠道，否则他们会落入不法之徒之手。目前的主要风险是，自发的零日研究方法的许多要素在许多司法区域被视为非法。这种监管态度阻滞了所验证的报酬渠道和零日研究本身的发展。

监管不一致会让为了人类利益而公开从事研究的白帽专家面临刑事起诉的风险，而黑帽黑客通常却会逃避处罚，为非法集团或流氓国家从事违法工作。究其原因，是当地执法机构缺乏有效的数字发现和证据收集机制，或者在国家支持的非法黑客攻击下，政府直接支持并资助黑帽黑客行动。

我们将为富有才华的零日漏洞研究人员建立符合道德的匿名业务流程。该计划将在此次代币销售期间筹集的资金大量投入研究主要司法管辖区，特别是欧洲的监管和立法框架上。最终目标是在我们的基金开始运作前为其营造一个透明的监管环境。

我们希望为我们的社区成员提供特别折扣，让他们成为我们零日平台的用户。然而，Hacken社区成员需要明白，出于道德和监管的原因，

他们参与此次代币销售并不会自动授予他们访问零日平台的权限，这点很重要。

零日报酬平台公共理事会将草拟访问规则并执行筛选程序。如果我们达到启动零日报酬平台的里程碑，该理事会将在代币销售后一年内成立。请参阅Hacken代币一节了解更多细节。理事会将由我们社区中最受尊敬且经验最丰富的成员组成。

Hacken加速器

如果您的员工决定自己创业，那非常好。这表明他们现在的工作内容丰富、令人鼓舞并且具有力量。在本世纪初谷歌开始鼓励员工“搞副业”开发自己的项目和产品。最近，它导致了谷歌创投的出现，这是世界上最受尊敬和最具有创新的风险资本基金之一。

作为网络安全领域的商业拥有者，我们看到了东欧网络安全市场的巨大开放性和潜力。坦白地说，它需要更多的高质量用户和更创新的商业模式。

目前最大的问题是缺乏吸引可靠投资者的能力，以及在决定创建自己的网络安全业务的东欧人之间建立一个透明的公司结构。这导致我们地区的实质性交易量有限。没有大交易，少有天使基金准备支持早期初创公司。随之而来的是，早先犯下的错误和造成的失败会使年轻创始人受到创伤，使他们摒弃自主创业的想法。

我们相信Hacken可以打破这个恶性循环，在投资者和企业主之间建立良好的声誉，为我们社区中最好和最可靠的成员提供支持。然后，我们不仅能从他们的融资书和Linkedin简介中，而且从他们在现实生活中的日常压力和业务关键绩效指标中知道他们是谁。

在选择了这些将来的企业家后，我们将会加强他们的知识。通过邀请那些已经拥有自己企业的最佳客户和社区成员，他们将受到启发并成长为下一代网络安全领导者。

投资者利益

1. 我们会联合资助项目，并与投资者分享风险。Hacken将投资高达25%的股权加盟初创公司。
2. Hacken营销平台和我们的营销团队将对加速器参与者进行培训，共同制定市场进入战略并帮助他们成功执行。
3. [Hacken分析中心](#)将帮助加速程序参与者研究竞争和相关的客户细分市场，并形成独特的客户价值主张。

网络安全分析中心

我们将创建一个分析师团队，他们将进行网络安全基础研究，以及监控和审核现有的和即将推出的网络安全产品。然后，我们的团队将提供员工外派企业网络安全研究，专业清理并且对产品进行自主研究和比较。

该中心的基本通讯将可通过Hacken网站和社交媒体公开查阅。所有深度分析将可通过订阅以及直接购买获得。

研究领域

- 区块链安全、漏洞和对策；
- 网络安全产品的分类、比较和市场调研；
- 密码技术、安全通信和数据保护；
- 网络安全中的大数据分析和可视化。

团队

该中心将由著名的CTF组织及其国际顾问而领导。其首要任务是开发一个用于分析和研究30多种不同类型的网络安全产品的基础架构和框架。

我们还计划与该中心建立一个乌克兰和国外学生永久实习项目。人才来源最有可能是HackIT大会的入围者和获奖者。

HackIT大会

HackIT是在乌克兰哈尔科夫市举办的年度网络安全国际论坛。第一届HackIT大会聚集了来自两个国家的450位参与者，第二届有来自六个国家的650名参与者。除了有本地和国际专家参加的传统演讲环节，HackIT还举办了许多专门的网络安全比赛，所有人都可免费参与。

夺旗比赛

HackIT

CTF

将于今年8月25日至27日举行。黑客们将在8个类别展开竞争：网络、混合赛、娱乐赛、加密、PW N、反向、辩论、Stego。2016年，来自93个国家的1062个团队的5000多名参与者在线参与了比赛。根据CTF Time的排名，

“黑客之战”

比赛的选拔环节在大会上半场进行，决赛在下半场进行。在选拔环节，每位参与者有30分钟解决网络安全任务并得分。得分最高者进入决赛，之后决赛选手将登台进行实时的网络安全问题解决。观众可以看到他们的电脑屏幕，网络竞技主播将现场直播他们的表现。

网络侦探OSINT挑战赛

这一比赛将通过专门的网站进行，于大会前几周开始。参赛者会接收到一系列要求其在最流行的社交网络、聊天应用程序和搜索引擎中执行在线开源信息研究的问题。获奖者可获得纪念品和大会免费入场券。

HackIT杯

来自世界各地的30名最聪明的黑客将参加该比赛，他们是HackIT CTF获胜者。参赛的同行们将提高他们的技能，将他们的组织发展的更加强大。他们还将有机会参与一个即时付款的私人漏洞悬赏计划。今年，漏洞报告将在全世界最大的飞机安225米莉亚上呈现给客户。

HackIT大会快览

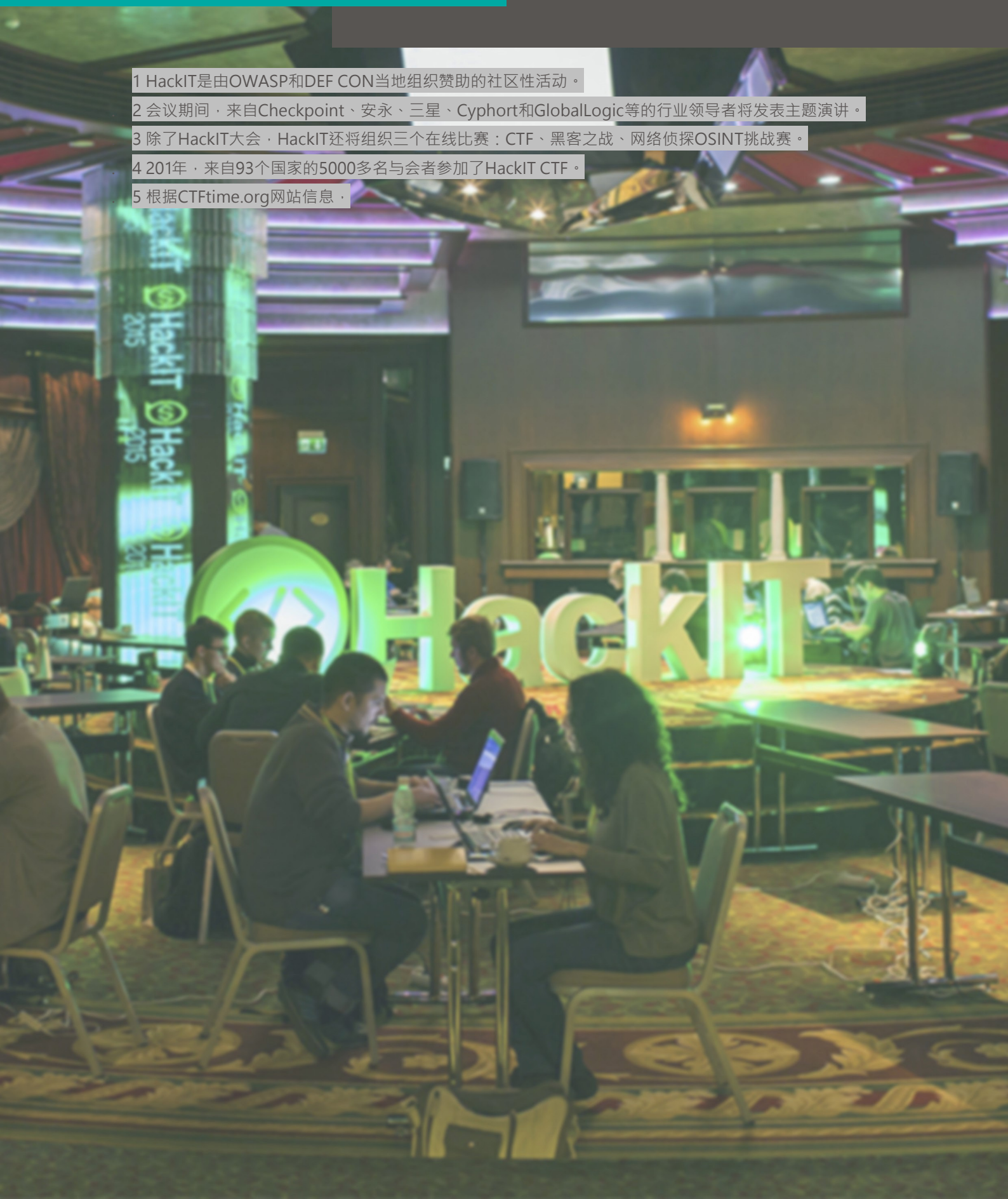
1 HackIT是由OWASP和DEF CON当地组织赞助的社区性活动。

2 会议期间，来自Checkpoint、安永、三星、Cyphort和GlobalLogic等的行业领导者将发表主题演讲。

3 除了HackIT大会，HackIT还将组织三个在线比赛：CTF、黑客之战、网络侦探OSINT挑战赛。

4 2011年，来自93个国家的5000多名与会者参加了HackIT CTF。

5 根据CTFtime.org网站信息，



我们职业生涯的大多数时间致力于各种网络安全项目。我们早就认为乌克兰是一个在网络安全领域具有巨大潜力的国家。最近由国家发起的针对国家基础设施的网络攻击使我们相信我们的时代已经到来。



Dmytro Budorin

是Hacken的首席财务官和牵头经理。Dmytro是ACCA成员，他在Deloitte会计师事务所工作了8年，担任过各种会计、审计和项目管理职位。目前，他是乌克兰军事国防工业的高管之一。在2014-2015年政府发起大规模改革后，他一直担任这一职位。在Deloitte期间，Dmytro通过对大数据SAP解决方案进行审计成为Deloitte独联体审计挑战的获胜者，该解决方案在独联体办事处广泛实施，并且大大提高了项目效率。



Mykyta Knysh

是Hacken的社区总监。Mykyta专门从事针对乌克兰各政府机构的网络安全培训。他在ProtectMaster担任首席执行官，该公司是乌克兰历史最悠久，最有声望的网络安全公司之一。Mykyta是乌克兰总统行政部门的网络安全顾问，也是HackIT大会的联合创始人。



Yegor Aushev

博士是Hacken的首席运营官。Yegor拥有汉堡DESY高能物理学系的博士学位。他在该领域著有22篇科学论文。自2015年以来，Yegor就是信息安全集团的首席执行官。信息安全集团是一家提供侵入测试、数据保护服务和信息安全审计的网络安全公司。



Andrii Matiukhin

是Hacken的首席技术官。Andrii在网络安全方面有13年的成功职业生涯。他为企业客户、集成商工作，成功地为数十个国家的公司、政府机构、银行甚至国际奥委会的十几个项目提供了复杂的技术解决方案。他是许多技术公司，包括CheckPoint、Cisco和Juniper网络等厂商的认证专家。他在项目中承担技术领导的角色，开发，整合Hacken平台并为其提供支持。

此事为何重要？

目前网络安全很热门，加密数字货币也很热门，这都已经不是新闻。东欧已经成为国家赞助的网络战的测试区也不再让世人感到惊讶。现在，乌克兰已成为传统机构不能保护他们本应保护的东西的一个案例，声名狼藉。部分借口是我们的后苏维埃心态尚未改变，对于扁平化的世界的巨大数字威胁尚未做好准备。

与此同时，在最近的动荡时期里我们观察到一个对这个世界来说的全新现象——公民网络活动。普通人：大学教授、商业顾问、律师和银行家一起努力建设国家的共同网络防御体系。三年前，乌克兰在真实空间发生军事冲突之后，我们已经看到了这一点。

这种基层行动不仅提供了希望，也可能导致许多成功的商业案例。毕竟，尽管有更好的制度文化、完善的培训体系、以及最重要的、东欧无法比肩的国防预算，西方的防火墙在2015-2017年期间也仍然失败了。

加密货币在促使个人支持者形成庞大的、分布式的、透明的网络防范预算方面发挥了至关重要的作用。它们可以绕过传统的机构网络，而后者在达到目标时可能已为时太晚。

这样的代币销售如果成功，将使我们不仅可以建立一个健全的区域网络防御系统，而且还可以自我调整以适应未来十年无疑会出现的挑战。这也可能发起一场运动，这一运动几年后将成为阻止和打击国际网络犯罪，包括国家支持的网络犯罪活动的重要因素。

我们在Hacken的实验从明显的商业模式开始：一个漏洞悬赏和众包侵入测试平台。虽然已经存在一些类似的平台，但我们认为广阔天地大有作为，如我们在本文的[单独章节](#)中所解释的那样。

之后，我们计划将生态系统展开，开展最具风险的两项活动：用于从灰色市场购买关键漏洞的**零日基金**，和用于网络安全初创公司的**加速器**。目前，太多的初创公司的融资演讲稿中含有“网络”这个词。在这种情况下，不要考虑商业投机者，而是要考虑自学成才的地方工程师，他们英语水平有限（目前如此），但头脑中充满了好点子，可能会带来下一个WiFi或PayPal。我们知道这样的人就在我们身边。我们认识一些导师，这些导师将帮助他们把想法提升到商业水平。

零日基金最初可能似乎与加速器无关，但绝对是有关系的。为了使聪明的东欧人远离可疑的收入来源，首先我们将获取他们发现的漏洞，确保这些漏洞被披露给合法的相关方，主要是供应商，从而使其工作合法化。然后，我们将提供一个可行的黑客攻击替代方案，这种做法会变得越来越不起眼。我们提倡的另一种方式是开展合法业务，停止依赖那些为了蝇头小利出钱的人。

最后，从现有生态系统中获得最好人才的同时，我们想确保有所回馈。这项工作是我们对**Hack IT大会**和创建**网络安全分析中心**的支持。

HackIT已经成为该行业的门面。它是未来一代的灵感，也是已成名和雄心勃勃的网络安全专业人士之间的知识交流场地。然后，中心将雇用那些不想创业而是更倾向于学术和研究并推动网络安全基础科学的人，并为他们提供支持。

将来还有更多项目，他们已经出现在我们的路线图和雷达中。不过，我们意识到现有的里程碑已经雄心勃勃，至少需要我们几年的全身心投入。所以我们最好做必须先做的事情，然后如乌克兰俗语所言，“我们将边走边看”。

我们希望本文提供了扎实的论据和详细信息，最终将使您参与我们的Hacken销售。如果如此，欢迎加入Hacken生态系统，我们希望很快看到您成为尊敬的社区成员和客户。如果不是的话，我们将很乐意通过[[email](#)]或通过我们的Twitter[[账户名称](#)]为您提供更多的帮助和细节。

我们希望本文提供了扎实的论据和详细信息，最终将使您参与我们的Hacken销售。如果如此，欢迎加入Hacken生态系统，我们希望很快看到您成为尊敬的社区成员和客户。如果不是的话，我们很乐意通过info@hacken.io或Twitter@[Hacken_Mrktplc](#)为您提供更多帮助和细节。

附录。现有漏洞研究众包业务简析

特点	Bugcrowd	HackerOne	Synack	Cobalt	HackenProof
1. 国家	美国	美国 / 荷兰	美国	美国	爱沙尼亚 / 乌克兰
2. 市场细分	大众市场	大众市场	企业	企业	混合
3. 侵入测试计划	否	否	是	是	是
3.1 订阅模式	否	否	是	是	是
4. 咨询 ¹	是	是	是	是	是
5. 私人漏洞悬赏	是	是	否	否	是
5.1 顶级研究人员名单 ²	是	是	否	否	是
5.2 亲自进行漏洞悬赏计划的制定 ³	是	是	否	否	是
5.3 受管理的平台 ⁴	是	是	否	否	是

¹ 高接触特点，包括专家就可利用的严重漏洞提供汇报。

² 研究人员可以接触到私人漏洞悬赏计划。

³ 除了托管管理客户程序的平台之外。

⁴ 在资源有限的环境中，客户可能希望将部分程序外包。

6. 基于时间的漏洞悬赏 (按需) ⁵	是	是	否	否	是
7. 公开漏洞悬赏	是	是	否	否	是
8. 退款	否	否	否	否	是

图9 现有漏洞众包业务

图表列表

1. Hacken生态系统
2. HackenProof漏洞和对策证书
3. 代币销售详情
4. 代币分销表
5. 里程碑
6. 路线图
7. “燃烧”机理
8. HackIT大会：快览
9. 现有的悬赏计划