度过从0到1的阶段，一家安全公司该如何跨越从1到100、从100到1000的复制难题？

在安全市场竞争日益激烈的前提下，这几乎已成行业共同命题。

绿盟科技也正在求索途中。36氪获悉，过去4年，这家成立超20年的安全上市公司一直在推进渠道战略转型，希望通过这一动作探索市场新增量。

“2019年公司制定渠道战略转型时规划了一个远景目标，即在2027年整体业务营收能够达到100亿元。” 绿盟科技副总裁孙冀平介绍。

孙冀平接着表示，为完成整体营收达成百亿的目标，公司制定了渠道业务1.0、2.0、3.0的规划，并规定每三年为一节点，实现渠道业务的迭代。

如今，1.0阶段刚刚过去。孙冀平介绍，在渠道业务1.0阶段，绿盟的目标是筑巢引凤，与合作伙伴形成良好的合作。当前，绿盟正处于2.0阶段，目的是向能力和价值型过渡，为2027年的百亿目标打下基础。

站在2.0的开端总结过去，孙冀平认为，第一个三年，绿盟的渠道成果颇有成效——在这三年里，绿盟与合作伙伴共同服务的客户数量累计突破5万家。同时，公司还与合作伙伴探索面向客户的联合营销、专业产品、解决方案、运营服务，共计9大类70多种300多款安全产品，和覆盖7大行业50多个细分行业的安全解决方案。

"我们渠道的战略是非常明确、非常坚定的。"在孙冀平眼中，绿盟对渠道战略的坚定体现在对合作伙伴的培养，以及从高层到基层的全员投入等方面。

"绿盟对整个合作伙伴的培养纳入到整个公司的渠道政策里。我们也制定了培训的体系和培训的目标。目前通过绿盟培训认证的人员超过五千人。"孙冀平表示。

从组织方面，他介绍，绿盟搭建了公司渠道战略的委员会，去审视每一年渠道工作的进展。同时，与渠道合作的指标已被纳入到一线人员到考核中，"渠道发展的好坏和他们最终的业绩强相关。"孙冀平补充。

而在渠道之外，安全企业也会通过拓展新产品线，并将产品和渠道结合的方式，促进达成整体的业务扩张目标。对此，绿盟科技首席技术官叶晓虎同样对36氪表示，公司当前也在不断探索新场景和新产品，希望满足更多客户和合作伙伴的需求。

他介绍，去年随着数据安全的需求增长，绿盟已和政府、企业等角色合作，从标准制定、方案制定、业务梳理等角度出发，探索数据安全的落地方式。而在产品方面

，绿盟也构建了数据安全平台，推出“数安湖”隐私计算平台，在教育、医疗、金融等行业得到应用。

同时，他还分享了绿盟在AI大模型方面的布局，认为大模型的出现，有助于提升安全业务的研判速度，并对产品研发等方面产生变革作用。

以下是孙冀平、叶晓虎和36氪等媒体的对话部分（经36氪不改变原意的编辑）：

数据安全成业务重心，目前依旧"在路上"

媒体：现在国内在建智慧城市，发现各部门都有大量的海量的数据。在数据安全方面，绿盟有着怎样的经验？

叶晓虎：数据安全目前大家都非常重视。前段时间设立国家数据局的消息，也可以说明整个数字化应用会加速。

数据要素20条里也提到，数据持有者，数据使用者和数据经营者，是整个链条里面的三个主要角色。

目前可能大家更为关心的还是数据持有者。它持有这些数据，需要承担数据安全的责任，需要看对应的场景、技术应该是怎样的。

我们更多还是和一些运营商、金融客户做数据安全方面工作。数据安全确实有点复杂和困难。它和区域IT的成熟度，数据安全的管理制度非常相关。虽然现在有数据安全法、数据20条，但在落地执行层面，当每个区域自身发展的情况、阶段不一样的时候，很难有一套普适性的东西覆盖。

从标准角度，大家都想设立一个通用标准来使数据安全进一步落地，但发现行不通，因为定得太抽象会落不了地，太具体又和各地的情况不匹配。

我们参与了数据安全的地方标准、行业标准以及企业标准相关的制定，盘点了一下去年大概就得一百多项。参与度非常广，但工作压力也挺大。这里面大部分都是地方和团体的一些标准。通过地方、局部的标准实践积累经验，我们希望未来能更好地抽象出模型，进一步去支持工作。

从智慧城市的角度来说，目前智慧城市数据的经营者应该以各地政数局为主。我们去年和不少地方政数局从标准、方案、技术上开展合作。去年下半年，我们发布的

“数安湖”隐私计算平台，可以解决数据共享的“可用不可见”的问题。在这个场景里，政数局需要和很多业务系统做对接，实现数据共享。

另外，我们去年和一个比较大的集团型企业合作。这个企业有中央总部，各地都有分公司，希望能建设从总部到分公司的整体数据安全监控体系。

我们和对方一起从总部到每个省公司的，流量、日志、API这些角度做了一整套设计方案，帮他们发现包括API、数据脱敏、加密等等安全问题。

媒体：绿盟的数据安全平台里面有一个敏感数据流转监控模块，这里的细粒度是怎样的？另外，隐私计算平台的效率达到了怎样的水平？

叶晓虎：数据安全的基础工作是对数据资产做梳理，分类分级，这样才能定义什么是敏感数据。而且，敏感数据在不同企业、不同应用场景的定义都不太一样。所以，我们的产品需要把逻辑设计出来。很多时候，需要我们和客户一起来设计敏感数据规则。

从敏感数据流转的角度来说，需要在每个部署节点上，根据分类分级的定义识别出它是不是敏感数据，是谁在访问它，哪个系统在通过什么样的API去调用它。这样，整个过程可以画出一个比较完整的图，发现敏感数据流转背后所产生的安全隐患的问题。和其他很多数据安全问题一样，这部分比较难的原因是，它和很多业务逻辑的设计有关。它最终呈现的结果是数据安全问题，实际上和很多业务逻辑的设计是有关联的。

隐私计算的效率不好，主要还是针对同态加密等一些加密算法。我们更多还是从数据可用不可见的视角去看，实际上利用多方计算来实现一些业务目标。当然这本身也要做很多系统性能优化的底层工作，有些技术壁垒确实是需要突破的。

媒体：绿盟在数据安全方面，有着怎样的核心竞争力？

叶晓虎：数据安全不能把它割裂来看，其实如果参考OSI网络模型来说，网络应用、数据、业务这是一个栈。铺天盖地的数据泄漏，很多都是由一些相对比较底层的安全问题引发的。数据安全问题这两年被重视以后，大家会单点关注。但我觉得发展趋势时一定要融合的，我们做网络安全工作也是为了保护数据，所以要把网络安全、数据安全融合。

当然数据安全有特殊性。数据要流动，实际上是大家最关心，也是在技术上比较有难度的一个方向，需要很多技术突破。从网络安全、数据安全融合的角度来说，过去在网络安全积累的经验，其实可以形成我们在数据安全领域的一些优势。

另外我们看到，这两年出现很多数据安全的创业公司。目前从技术创新的成熟度角度来看，还有很长的路要走，大家基本上处在同一起跑线。

信创是必要场景，AI带来想象空间

媒体：你在演讲中提到，绿盟正在做关于大模型的研究，这方面的具体情况是？

叶晓虎：我们目前进行类GPT产品的设计。现在叫智能安全客服机器人，也可以叫在线知识问答系统。其实我们团队对ChatGPT做了很多分析，研究怎么把它应用在安全产品方案里。安全现场的运维工作其实存在一些问题，首先是工作量很大，因为它涉及的系统非常多。另外，不同人员的安全技能和效率差别非常大。以一个刚毕业的应届生为例，至少需要六个月实践才基本能满足高水平的现场服务要求。

我们多年的安全研究和实践中产生很多数据，包括各种不同类型的安全日志、系统日志以及其他日志，以及威胁情报生产和分析过程收集到的数据，开源情报和安全技术报告、APT报告等。我们基于这些数据的积累，进行数据融合，在AI智能化方面展开了研究，形成一系列实战化攻防模型以及安全知识图谱。

我们的判断是，可以利用类似ChatGPT的大语言模型去对这些知识做进一步加工，形成自己在安全专业领域里面的类GPT的应用，即知识问答系统。希望达到的效果是，在现场工作的同事碰到问题时，比如说发现漏洞或者异常现象，马上可以把所有相关的知识以及应对措施都列举出来，让现场同事得到非常好的输入支撑。

另外，如果在安全事件应急响应处置的时候，这个系统如果可以给你一个比较好的响应处置的建议的话，那出错的概率和处置的水平就可以得到相应的保障。

第三个应用就是安全工作人员很头疼的事情，分析研判。海量日志来了以后，到底是不是误报，到底意味着什么，这其实是非常复杂的一件事情。我们可以把现场日志脱敏，看ChatGPT能输出什么，辅助我们进行判断。我觉得ChatGPT的技术，有些亮点是特别值得我们去参考的。当然ChatGPT使用的是通用语言模型，我们也在研究在安全领域的专用语言模型，可以更好地来为现场安全事件的分析研判提供强有力的支撑。

还有一个可能会更复杂一些。我们觉得大语言模型，会改变以后安全产品开发的底层逻辑。

如果我们能把大语言模型梳理好，安全智能推理、智能决策就会有更好的支撑。以前，我们团队也在做AI的研究，智能推理和智能决策，但从模型支撑的角度来讲，我觉得是不太够的。如果我们能把这条路走通，可能未来智能对抗可以更进一步。

另外，我们用ChatGPT来辅助写代码，结果非常不错，比应届生入职那几个月写的代码质量高很多。我们现在也推荐在产品开发当中去用ChatGPT，相信将来安全产品研发的效率和质量也会进一步提升。

媒体：现在信创的进展是？

叶晓虎：信创实际上第一步解决了供应链相关的安全问题，但是信创并不意味着就安全了，反而可能会更不安全，从逻辑上来说肯定是这样。

现在Windows、苹果这些操作系统，再想找到比较严重的漏洞已经非常非常难。这么多人在用它，天天给你反馈问题，这么多年的积累已经很完善了，在这么多工作基础之上，它的安全性才能有足够的保障。

今天信创这个事情会面临更多这样的挑战。系统，比如说数据库、操作系统，还有很多我们不知道的应用系统，安全性都需要确定。

我们虽然也参与了很多信创适配的工作，但还是觉得只看到冰山一角。各种系统的安全漏洞还是非常不够。

现在，我们基本上所有主流的产品都已经在信创的环境下做了适配。而且，未来我们所有的新产品、新型号都会按照对应的信创适配要求去开展。现在主要希望有一些制度和机制上的突破和创新，能让大家参与进更开放的环境里。

战略目标：2027年达成百亿

媒体：今年其实是绿盟转型渠道战略的第五年，绿盟是怎么一步步来构建自己的渠道生态的？

孙冀平：在2019年做渠道战略转型的时候，这是公司管理层统一的认知，这个事情才能推得下去。

为什么要做渠道战略的转型？第一，不同类型的客户，没有任何一个厂商/企业能够独自做完这个工作。这需要广大的合作伙伴，大家一起去面对这个事情构建各自的能力，形成这种合作。在这个点上，绿盟在管理层是达到了非常好的共识。

第二，我们从公司组织和架构上去做推进。公司的组织是推进这个工作的基础，同时，我们有公司渠道战略的委员会，去审视每一年渠道工作的进展。董事会、管理层会去看渠道业务进展是不是达到预期，看有什么问题，需要做哪些改进。

我们会把整个渠道合作的指标，纳入到一线主管的考核里。他们是有渠道合作分数的，渠道发展的好坏实际上和他最终的业绩是强相关的。做完这几个以后，公司内部的战略、组织、目标、分工以及整个考核上，我们认为能够做拉通的，能够保障我们对整个这项工作的共识。这是我们做一切工作的基础。

另外，我们整个政策上，是对合作伙伴的收益有保障的。在日常中，很多时候政策也有了，但大家的磨合和信任还是非常关键的。我们定位全员渠道，每一个角色都有明确的要求，要求大家和渠道合作伙伴去形成良好的互动信任。我们希望通过这种方式，在实际落地过程中形成组织对组织，人对人的相互信任，有了这种信任以后，能够更好地开展工作。

媒体：渠道战略2.0的进展情况可以介绍一下吗？

孙冀平：2019年做渠道战略的时候，我们规划了一个远景目标，在2027年希望能够达到100亿。分三个步骤，渠道1.0、2.0、3.0。

1.0更多的是说我们要搭好我们的平台，筑巢引凤。第一步，我们在几个重要的领域上还是取得了比较好的进展。我们有2500家合资渠道，渠道占比超过70%，这些年累计和合作伙伴共同服务了超过五万家客户，1.0阶段的任务我们认为还是达成了。

2.0我们给自己提出了更高的目标，一方面围绕100亿目标，会有相关的任务和目标。第二，我们在做这个规划的时候就重点提了2.0，希望向能力和价值型去发展和过渡。

我们渠道的战略是非常明确、非常坚定的。我们对整个合作伙伴的培养是纳入到整个公司的渠道政策里面去的。我们也制定了培训的体系和培训的目标。通过绿盟培训认证的人员有超过五千人。

媒体：3.0打算什么时候进入？

孙冀平：我们初步按照时间做了计划，以三年为一个节点，完成1.0、2.0和3.0。九年下来，2027年的时候，我们希望能够在渠道的助推下达到百亿业务规模。

媒体：安全厂商做渠道的时候，总会提到安全和云结合的厂商经验。也请你总结一下，绿盟做了五年之后，一些可以代表自己的渠道经验。

孙冀平：大家都在去提渠道战略或者渠道转型，我想可能大家的出发点或者战略上的规划设计不同。这里面不太好去评价别人怎么做，因为每个企业有自身发展的背景。我想对于绿盟，有几个方面可以概括。

第一，我们一直是全渠道战略，意味着我们会开放全部的这些业务的能力。这是绿盟渠道战略能够取得进展和成功的重要基础。

第二，任何事情要去长期推进，一定是能够真正形成公司层面的战略。我认为在渠道战略上，绿盟做得非常坚决。

第三，当然在这过程中也会碰到很多问题，比如说生态的问题、渠道的冲突等，绿盟在内部有相关的组织，负责对接渠道伙伴的各种问题并负责解决、闭环。我们不是把维护秩序、维护良好的生态和环境停留在口头上。

策略也好、方法也好，其实大家有可能是大同小异的。事实上比到最后就是看谁有更好的战略定力、谁有更好的执行力、谁有更好的自我优化的能力。绿盟有这个基因。