**金融行业对NGSOC的认知和需求**

**——安全牛CSO高端沙龙内容精选**

**会议主题：**新一代SOC与态势感知

**会议时间：**2017年11月2日 9:30-12:50

银行、保险、证券等金融行业客户的业务、信息资产价值高，是网络攻击的重要目标，因此这些客户对信息安全非常重视，也非常关注安全价值，有意愿选择新技术，是NGSOC的目标客户之一。

在11月2日安全牛组织的CSO沙龙中，有来9位来自银行、证券、投资行业的网络安全主管参会，他们分享了各自对于SOC的理解、实践经验、困惑和需求，在此将他们的发言整理成册，作为参考资料。

**目录**

**行业背景**

基本概念

新一代SOC兴起的四个背景

新一代SOC的特征

**用户认知、实践及需求**

中央国债的安全主管马涛

农信银数据清算中心运维中心负责人杨伟

中信建投信息技术部的姜明元副总裁

嘉实基金的高级安全架构师周明昊

国家电投张萌

农商银行的郭世荣

农业银行的李强

人民银行吕毅

国开行的林东升

**行业背景**

最近一年来，以态势感知和安全运营为核心的新一代SOC成为行业热点，从公安、网信等政府监管部门，很多省市、重要行业、重要企业和机构都在积极筹备或者规划新一代态势感知系统和安全运营平台，很多项目也已经成功设施。

SOC不是一个新东西，国内很多的机构和企业十多年前就曾经尝试了第一代SOC的建设，但是受限于技术的局限、缺乏有效的运营或者与业务场景不匹配等多种原因，传统SOC系统在国内鲜有成功者，所以用户普遍认同传统SOC对于机构和企业是一个大坑。

有了传统SOC建设的教训，对于新一代SOC（态势感知和安全运营平台）的建设相当审慎，一方面基于新的安全运营需求和相关监管需求，新一代SOC建设是一个趋势和方向，但同时用户对于新一代SOC的建设更加务实和理性，从之前的安全管理和合规要求的诉求专项价值诉求，系统通过新一代SOC的建设，构建安全体系，实现安全能力落地，提升安全防御能力和安全管理水平。

**基本概念**

**传统SOC（安全运营中心）**是指以信息资产为核心，通过针对网络、系统、应用、安全设备的日志和报警事件进行监控和分析，建立一套实时的资产风险模型，以安全事件管理为核心流程，协助安全管理员进行事件分析、风险分析、预警和应急响应处理的集中安全管理系统。

传统的SOC 主要采用安全信息和事件管理（SIEM）系统，为防火墙、入侵检测/ 保护系统、漏洞扫描等安全设备提供设备管理和监控服务。——安全牛

**新一代SOC（iSOC、NGSOC,态势感知与安全运营中心）**必须以数据和情报驱动，采用自适应安全架构来进行环境和态势感知，通过自动化或半自动化工具、流程和策略来对抗新一代威胁。新一代SOC 将成为企业安全能力中心，具备安全防御、持续监测、快速响应、溯源取证、风险预警等能力。——安全牛

**新一代SOC兴起的四个背景**

（以下内容来自谷安天下李华的发言）新一代SOC成为行业热点，主要基于以下四个背景:

**一是国家提出态势感知的要求**，从国家层面高度重视，所以各个行业、企业和政府相关部门都在推进；

**二是安全环境发生了巨大的变化**。原来的是一种以防护为核心的体系，现在转向以检测和响应为核心的体系。

随着越来越多的安全事件的发生，安全威胁形势发生了变化，新一代的攻防体系需要转型，从已经发生的很多安全事件看，发生很长时间之后才能够被发现。所以，原来的防御系统正在失效，必然导致机构和企业的安全体系要升级，从重防护转向重监测、快响应，同时对防御做相应的改造。

之前企业和机构买了大量的防御设备，可能没有起到关键的作用。未来可能要在持续监控方面、响应技术方面做大量的投入。

Garner也做过预测，未来50%以上的安全投入是在检测和响应层面的，新一代SOC（态势感知和安全运营平台）正是顺应了这样一种潮流，通过态势感知和安全运营平台的建设，把检测响应体系和能力能够快速地建立起来。

**三是由于大数据技术的成熟**，和开源的技术应用，各个厂家发布了各种各样大数据平台开源的框架，机器学习、深度学习等领域都开源了很多东西。这些东西让大数据、机器学习、深度学习等技术快速地平民化，快速地被各个企业、各个厂商应用，安全领域也得以快速地在应用这些技术，这些技术应用让新一代SOC有了成型的可能。

**第四是威胁情报技术的成熟**。在国内经过最近两三年的推广，威胁情报概念和相应的技术已经逐渐开始落地，威胁情报技术成为新一代SOC一个非常重要的技术特点。

**新一代SOC的特征**

新一代SOC，我们叫做iSOC，情报驱动或者叫智能驱动，我们更愿意把它叫智能驱动的SOC，原来我们叫情报驱动，情报驱动有点窄了，现在我们更愿意把它叫智能驱动。这里要体现一些安全智能的思维，未来整个SOC不能仅仅靠传统的人或者是我们利用已有的工具模型或者是已有的模式去处理，要通过大数据技术，通过机器学习技术，通过一些新的安全技术去把它进行一些带有一些智能性的特点，这是它一个非常重要的特点，它一定是基于大数据平台的。我们第一代SOC，常用的SOC追根溯源，处理能量是有限的，进来也是有限的。大数据平台本身的性能也好，包括处理能力，包括它自我的学习能力各方面会有一个比较大的提升。

第一、威胁情报在新一代的SOC里是非常非常重要的，我们希望今天就这些问题来讨论。有了这些威胁情报的存在，可以让我们的响应包括检测的快速，包括联动，很多东西能够起到更快的作用。新一代的安全体系下，它会发挥比较大的作用。这也是现在全球威胁情报的厂商、用户，大家都利用威胁情报在做驱动，驱动整个运营，安全运营方面会有一个比较大的升级。

具体到落地层面，其实我们还有一个非常重要的观点，一定要记住，SOC不是一个产品能够搞得定的，SOC绝对不是一个产品能够搞得定的。

十几年前我们在做第一代SOC建设的时候，实际上大家要做的，都是上一套产品来解决问题。但实际上产品是不能完全解决问题，要以人为核心，我们提出来人在整个安全运行当中是逐渐成为一个核心。新一代SOC体系，我们可以认为它是一个体系，不是一个平台。既然它是一个体系，就涉及到所有我们的用户要想清楚这个SOC将来怎么去用，我们内部的场景是什么，SOC用在什么地方，什么样的部门，提供什么样的服务，我们的帐户，我们的人员，我们的内部流通怎么去打通。比如说安全动态，最外面的攻防层面，运维是一个场景，它还有可能支撑我们的业务，它有可能做我们业务风险的管理，它在每一个场景下，整个人员也好，体系也好，流程也好，都是不一样的。可能我们在座的一些甲方单位也已经做了类似的尝试建设，可能有一些经验，这里必然要有一个体系的构建过程，我们的流程体系、人员、技术体系的融合都不太一样。

第二、厂商相关的一些技术的完善，也正在完善当中，各个厂商都有各自的特点，厂商会在技术层面，完成整个体系当中的点，而且这些点更多跟以前不一样，以前是以防御为核心，现在是以检测为核心。

第三，在运营体系当中人的作用。以前我们很多时候建完SOC之后就是一个系统自己在那儿跑。但是实际上在新一代SOC当中，特别是运维人员能力的提升可能是一个比较重要的点。因为SOC将来是要靠持续运营的，在运营里边，运维人员应该掌握什么样的技能，在这个体系当中发挥什么样的作用，厂商之间怎么去协作，面对威胁情况专家之间协同，可能很多方面都需要做改进。这个实际上也是在我们新一代体系当中，在落地当中要注意的几个点。我们在报告里面也有相应的体现。

从市场层面分析，因为在座的大部分都是我们的一些客户、老朋友，我们发现几乎所有的客户都在关注一个点。从我们今天的会可以看到，各方面都有，有金融，有能源，有交通，主要的行业都在关注我们这样一个点。所以，未来的两三年应该是一个大规模建设的过程。通过我们跟各个厂家的调研，初步的调研情况，都反馈出这个特点。但是我们在研究当中还是发现有不少难点，尤其是在各个企业碰到的情况还不太一样。

我们认为其实每一个企业的SOC可能都是一个不同的SOC，当然每个行业可能有一些借鉴复制的作用，但是每个企业由于它的应用场景不一样，包括内部的资源环境不一样，包括人员的能力、结构不一样，每一个SOC可能都是跟自己很相关的不一样的SOC，很独特的一个SOC。而且SOC的投入，态势感知的投入都比较大，企业上千万的投入，投入规模很大。所以，在做整个规划的同时，用户要深入地了解自己，对自己的情况很了解，再结合各个厂商的一些能力，才能够真正把这个事情做好。

**用户认知、实践和需求**

**中央国债的安全主管马涛**

我们在实际做SOC的过程中，其实更多思考的问题，是安全运营的问题。一个企业的运营实际是都是执行ISO，作为ISO的框架体系，要遵循这个框架。

我们前面提到安全营运，我们既要做到7×24小时的安全监控、安全快速响应，同时又要保证资源高效和最大化利用，我们希望获得一些经验，怎么在快速安全响应和一线监控，把职责分得更清晰，使我们的安全员更有效地发挥价值。

**农信银数据清算中心运维中心负责人杨伟**

我们目前主要是建设SOC，主要关心如何融入新一代SOC？如何在新一代SOC上做好逐步升级？新一代SOC在建设上可否做的更细致些？新一代SOC的坑有哪些，遇到过哪些坑，如何避免？

**中信建投信息技术部的姜明元副总裁**

**(惟一一个成功建设了SOC平台（瀚思合作），分享经验)**

我这边正好分享一下我们**中信建投的SOC平台**，我们是把这个叫做安全运营中心，介绍一下心得。

我们是从2015年开始就在做相关的调研，调研以后，我们其实考虑的方向，刚才各位专家也提到了，就是人、技术、运营这三方面，觉得运营SOC会面临很大的一些困难。我们人员的储备问题，券商普遍来说安全团队的架构不是很大，我们现在的人员也就是7个人的规模。所以，去做安全运营的事情，我们的压力非常大，这是我们当时考虑的一个很主要的原因。第二，技术。之前很多老一代的SOC，进入中国很长时间，不过特别是在券商我们了解到的所有案例当中，真的没有哪个券商能够用起来。其中一个很大的原因，当然也有人的问题，还有技术上落地的问题。**我说的落地是，实际我们的工作场景是不是能够融合，是不是能够真正解决我们的痛点。**

我们2015年调研以后，之所以决定做这个事情，也是觉得现在有一些新的技术出来了，一些大数据、机器学习、人工智能这一类新的技术出来以后，**我们看到了一些希望，觉得新的SOC的东西确确实实能够给我们解决一些技术上的难点或者是我们不足的地方。**

**运营当中的问题，最大的考量是我们的知识储备，包括后期流程上。SOC建起来，我们是不是能够围绕着它进行快速的运营，有响应的过程，有一个快速分析的过程，包括我们后期的持续性，作为甲方来讲，去运营一个实验室的架构，选SOC直接输出这个知识是不现实的，因为一个是我们的实验场景不够丰富，人也不多，不够专业。**

这三方面是我们当时去考量SOC的时候面临的问题。

2016年开始，我们通过半年的评估和调研，2016年下半年正式开始实施这个SOC，也是跟瀚思合作。我们现在运营的状况，现在走了半年左右的时间，我们最开始其实挺彷徨的，很担心我们走的路不正确，或者是不是走弯路。不过万幸，刚才听我们专家介绍PPOR的模型，当然我们之前确实没了解真的实施或者是落地的场景，PPOR这个场景。不过很幸运，我们现在实施的路径是按照专家说的路子走的。

第一，人员的情况，我们现在设了一个安全分析的岗位，专门做这部分数据的分析跟收集。当然这部分我们不仅仅是依靠我们的人，我们得依靠厂商的人员。**我们现在对于所有的安全设备和平台进来的时候，我会跟他们额外要一个服务，就是安全分析服务。**你给我上了IDS，你给我一个定期的升级。你给我上WAP，就得有一个定级的升级。你给我一个分析，我的目的没有别的，就是看怎么在我自己的系统上落地，有没有能够优化我内部规则的空间。**这是我给厂商提的要求，目的就是去弥补我们安全分析人员能力不足的问题。这是我们对于人员的控制。**

刚才提到事件岗位，我们现在是由问题岗位的人兼任这个岗位，**不过这方面在应急后续的支持上，一线的人员不足，这应该都是大家普遍面临的问题，一线真正处置的时候人手不足，可能有些事件处置起来，响应的时间不够。这是人员（问题）。**

**第二，我们的平台。建SOC的一个主要的目的，我们是梳理我们的资产，也是梳理我们的攻击面。**通过大数据融合以后，我们希望真正了解到我们自己内部有什么东西，这些东西在跑什么业务，跑什么端口。因为也是针对我们真正的痛点，不知道是不是共性的一个痛点。因为实际上我们公司成立的时间较长，系统比较老旧，经过很多交接或者是交割以后，很多人或者是技术负责人都不知道自己手里到底有多少服务器，这是最可悲的一件事情。到时候就会面临一个什么问题？安全人员说有一个紧急漏洞要打，我说我打了10台，其实还有另外10台，但我就不知道这个设备存在。我们的要求很简单，第一年的目标就是把我们自己的家底摸清楚，我到底有什么东西，有什么东西是没意识到的。

**还有一个部分是情报的部分。**刚才一直在提外部情报，我觉得内部情报的掌握跟攻击面的掌握，这是同样重要的。特别是在安全分析的时候，我不清楚我自己的情况下，外部的情报可能分析不全，有些潜在的威胁是发现不了的。这是我们对于平台搭建和数据梳理的过程。

第二，场景。我们对于平台和资产处理完之后，我们发现基于资产的数据，到开始做一些场景，就会非常有意思。**当然不同的行业有不同的方式，不同的企业有不同的运营模式。建一个SOC，企业用起来可能都是五花八门。**我们现在用的，最通用的一个可能就是DNS的解析，跟威胁情报关联以后，能发现一些攻击（音）的情况，这时非常常用的一个场景。对于这次像“永恒之蓝”的监测非常有效。除了这个以外，我们在另外一个场景上发现另外一个动作。比如外部人员接入到我们企业网的时候，他们DNS认证我们是拿不到的。我们用了一个变通的方法，在互联网的防火墙做关联以后，我去监测哪些设备在批量地对外访问的URL,这是另外的一个思路去做一个直接的告警。我们直接就发现了有四台机器做到了，它在1分钟之内可能好几个IP都在向包括国外、国内的IP在访问，但是机器本身没有任何感知，因为现在我们的开发已经关闭了，只是在发报文，尝试在感染别的机器。通过这个，我们非常准确地定位了四台外部人员访客的机器，直接就阻止，直接就把网络切断了，我们说你不要再接入我们企业网，从此以后我们不给你接外网。

这是基于我们的场景几的一个小例子。

为什么我把它称作安全运营中心？因为我们不仅仅是打算用这个做安全事件的分析，像一些合规性的分析，我们也正在往上布一些规则。比如说绕过堡垒机登录3189端口的这种策略，我们可以报过来，我们的策略往上加。还有一些离职人员app的帐号，是不是在所有的日志里，是不是有相关帐号的登录日志，这样去梳理我们的交投帐号也是非常有效的。也是类似的，企业自己的需求出来以后，就会发现能够实现我们场景分析，玩法非常多，效果也非常好。

这是基于我们的场景逐步在做的一个事情。

最后，应急流程和处置的流程。因为我们实施半年已经开始有一部分的功能起来了，我们做的事件分级分类都落地。以前这是一个非常空的东西，国家有标准，有国标的情况下，你想达到什么样的情况，特别重大的应用。在我们企业来说没法落地，因为落地的价值不大。我们现在的做法就是在运营中心里所有的规则我们都给它定义一个紧急度，我按照紧急度去处理，这个紧急度在多长时间里处理掉。因为之前，这部分的处理信心不大，因为觉得事件发生以后，各个系统组可能对于自己不敢去做，也是“永恒之蓝”这个事情发生之后，发现我们企业的潜能是巨大的。大家一直都不敢打这个补丁，打一个补丁大家都退三阻四。那天我们所有部门集体紧急加班，当天晚上就把所有策略处理报告都打完了。很多动作确实需要安全组去推，而且把事件的严重程度给展示出来。现在我只是告诉有这么一个可疑的事件，他觉得这种攻击我看不到，我自己意识不到。当然“永恒之蓝”这类高危的，或者说其它攻击，直接影响到我的业务，影响业务就是影响核心，马上就给我处置，五分钟之内给我处置掉，必须有处置的动作。我们要把事件跟case的规则挂钩之后，然后再做一个不同级别的应对策略。当然这个应对策略，我们后续还要做一个动作，希望它跟我们的防护策略进行联动，这是我们尽可能希望达到的。这个防护联动我们也在做逐步的尝试跟应用，因为我们觉得很多应用级的响应动作耗费我们的人力是不可想象的，这也是我们在下一步做的应急方面的工作。

**嘉实基金的高级安全架构师周明昊**

我是来自公募基金行业。这个行业跟在座的许多同仁，包括银行、央企、券商相比，相当于是一个比较年轻的行业，公募基金的历史只是十几年。我们的安全也起步时间比较晚，我们遇到的问题，可能在座的厂商的安全专家，包括我们的各位同仁可能都碰到过。我这边有两个问题，希望大家给我相关的建议。

第一，现在很多外部的调研中发现，我们企业面临安全入侵平均检测的时间是一个月以上，这个时间由于过长，会导致攻击者有时间在网络内学习到你的业务模式，从而造成一些真正对你业务有影响的攻击。比如说之前的\*\*被盗，其实后来分析那个木马，其实发现它其中包括对你评估录象和分析的能力。

我们现在自己内部的要求，我们要求自己在一天以内能够发现内部的安全事件。我们在十九大安保期间，我们按照这个模式来做，发现要投入的东西还是比较大的，因为我们其实内部已经做了相关的入侵检测也好，基于网络的，基于主机的都有，包括在边界上的检测也好，我们发现我们看到攻击事件以后，我们要确定这个攻击事件真正有没有影响，可能要花两三个小时的时间。由于大家其实平时可能都会有各种会议要参加，还有很多建设的工作要做，这个时间我觉得是非常之长的。我看了我们《安全牛》的这本书中也提到，CSO需要有一个驾驶舱，飞行员在驾驶舱中到底看到飞机有故障的时候，你可能一眼有应该能看到这个故障。如果你需要花两个小时才能看仪表盘，才能看出问题来的话，这个飞机可能早就已经掉下来了。我想通过这个概念，把我们的话题框死，我是希望我们能够在15分钟之内能够看到我们现在的网络内到底有没有异常的发生。

为什么需要两个小时呢？我举个例子，我们看到入侵检测设备上看到外部对你的网站有攻击，我们也看到入侵检测设备把这个攻击拦掉了，但实际上入侵检测设备不会告诉你有没有攻击漏过去，或者说一个漏过去的攻击，有没有实际攻击成功。大多数的入侵检测设备都不会告诉你这一点。

我们内网看到的是入侵内网的IP的行为，大家可以看到，内网系统中有一些设计开发的有问题的系统会产生大量的告警，其实我是很想有一个东西，能够把外部的攻击和内部的异常串起来，能够看到某一个攻击，比如说外部对你网站的扫描也好，员工的电脑感染，恶意情趣也好，跟你内部的内网异常的事件之间到底有什么样的关联？是不是一个攻击从外部进来开始，到你内部实际已经发生后果了。

我相信要做到这一点，需要你的资产跟你的安全的这些事件有很好的关联，刚才中信建投的张总也提到，你要安全防守，首先要把你的资产梳理清楚。我们需要对资产有多么的了解，包括外网IP对你的内网IP，包括对于你的什么业务，你的业务上有什么样的应用，我相信是很丰富的信息。我们现在如果说去做这么一个事情，有没有好的经验、案例，能够把我们的一些资产很好地跟安全的告警做相关的结合。

第二个问题，跟威胁情报、态势感知相关的。其实刚一听到这个词的时候，我想象的是什么样子？当我们看到一个漏洞，比如说永恒之蓝的漏洞出来以后，我们到底有哪些已经是攻击成功的。现在我可能想知道这些信息，可能要通过媒体，通过《安全牛》看一些文章，是不是国内以后出现什么攻击的案例了。包括问我们的安全厂商，现在到底要抬到什么级别，我们一个AA级的漏洞到底要抬到什么级别？有没有实际发生的攻击已经造成影响了？其实都得不到准确的信息。

我接触一家国外的厂商，他们其实有一点做得很好，他们把整个行业异常文件的样本做了一些收集，按行业做了一些分类。但其实这家国外的厂商本身有很强的入侵网络危险检测能力，但是它没有把相关的前项的东西跟后项的关联起来，因为实际用户可能是后项的，在用户之前可能已经有其它一些异常行为产生了。现在我就比较想知道，当你看到比如10月份20多个不同安全事件的漏洞暴露出来以后，哪些漏洞是真正对你造成可能是比较大威胁的，在行业中已经有一些人受到攻击或者已经攻击成功的。这个事情最好由政府部门来牵头，当然厂商和政府合作也是个很好的模式，因为大家私底下都不会跟你说，这个人到底是不是被受攻击了？大家很少愿意说这方面的话题。但是这个信息又确实是我们所需要的。因为现在其实监管机构随便遇到一个什么事情，比如说这次“永恒之蓝”，证监会直接很紧张，就发了相关的通知，虽然在国内没有什么应用，但我们实际上还是很希望得到一些基于现在的数据、基于现在的案例，一些客观的介绍这种类型的威胁情报。

**国家电投张萌**

我们电投行业是一个比较典型的层级化的企业，我们现在在安全这块是趋向于专业化的方式去运作。我们现在成立了一家信息公司，我们信息公司这块是网络安全部的部门。我们有200多家、300多家集团单位要通过信息公司的网络安全部的公共共享服务的输出，去保证集团的整体安全。我们有一个任务是要去补足二三级单位能力缺失，怎么去做？现在在考虑一个问题是通过“安全运营”来实现。那么“安全运营”里就涉及到很多问题，像各位专家提到的人、平台、体系问题。

目前我们面临最现实的问题就是“平台问题”，**我们去年跳个坑，没花多少钱，做了一点小事儿，就把集团几百家单位的终端安全，防病毒的数据收集到一起了，厂商定制化开发。**

我们运营中心是网络隔离的，在内网里有没有外联情况？内网里有没有病毒的肆意爆发？这块也没想太清楚。大家这一年就在坑里待着，挺难受，今年想把这个事情好好的去琢磨，因为我们现在的思想在转变、观点在转变，平时下面的运营、动态的观念一直在转变。

下一步要做的事儿就是，在现有的这个平台上看到它还能继续做哪些事情，因为我们意识到了，这个安全SOC一定是定制化的。如果要是定制，那前期肯定要把系统梳理清楚。就像刚才专家说的，**要把场景定出来。定场景的话，我们是围绕着集团的多级、多单位的架构下，如果用一个统一的SOC平台，或者用统一的这个运营监管中心来做，我怎么去梳理这个场景？因为几百家单位它可能有几百种需求，这个是比较头疼的事。**

**SOC需要有厂家不断的支持，不断的开发，根据需求不断的调整。但现在有没有能提供这种服务的，能跟得住用户需求的，因为SOC有些需求还是要到后台团队去开发的。**这个过程中实际上，他们不像互联网公司，互联网公司的迭代非常快，有了需求马上就会回应。可是对于我们来讲，有商户流程，有很多这些事情。这个问题怎么办？现在很困惑这两点。

一个是我们下一步SOC要建，前期需求怎么去梳理。

再一个是在后期运营过程中，如何去选择服务商来支撑这个事情，自己没能力怎么办？就是这两方面的困惑。

**农商银行的郭世荣**

我有两个问题，一个管理问题，一个技术问题。（郭是刚刚主管安全工作，想来公司参观）

大家今天都讲SOC，结合人工智能、大数据的新的技术特点，刚才江总也讲了这方面的成效。从更多的甲方来讲，目前这种技术采用的具体是什么样的效果？技术发展，目前乙方在研究技术上还有些什么新的方向？

**农业银行的李强**

刚才大家提到了很多安全部门是弱势的，安全部门人少，这种情况下怎么来推动这个大的工程？那我们就要解决一个问题，我们的SOC和态势感知到底是解**决什么问题，我们做这个事儿的目的是什么？**

你跟领导说我们要钱建这个，我要人建安全运营中心，那你到底是为了解决什么问题？你是为了合规吗？海外要求SIEM是必备的，解决合规问题。那国内你要建立这个中心到底是为了什么？你说有危险，是不是个假想敌，真有问题吗？这块面临着甲方的道路选择问题。我是一次性做个大的，还是我主动逐步的先解决一个问题，这里头有两个线的问题。第一个是这两条线路哪个更好的问题。

第一条线路是主动做，先发现问题，证明说这个确实有问题。在发现问题的过程中需要应急，需要处置，那就各条线去应急，去处置。各条线应急处置时需要收日志，流量，探针等等，我在推动后面的大规模的建设，再推动后面整个儿的在处置过程中平台的建设，这是一条路。

第二条路是做一个全面的咨询，启动大规模的统一化的建设。这两条路从咱们的实践上看，哪个会更适合一个规模比较大的企业？因为第二条路直接推，投入会非常大，我们系统的规模非常大。

第二个问题是我们讲安全隐忧是离不开态势感知，离不开运营。大家说了很多建设，我怎么建，建的过程中更重要的是运营。建设的事儿乙方都能帮你解决，但是运营的事儿他不一定能帮你解决，很多前边失败的都是在运营上，或者是职责、规则、流程方面的设计上出现了问题。

这就需要设立一个安全运营中心，它和系统管理部门、网络管理部门，终端的管理部门，应用的安全管理部门。因为我们的企业很大，它就分工比较细，我们跟它的职责边界到底怎么划？哪些该他管，哪些该我管，之间的流程、互动这个职责边界有哪些流程，这块是怎么解决的。

我们既然是安全运营中心，它就涉及到基础的运维，这个基础的运维和传统的运维关系是怎么样的？哪些是我要扔到他那儿去应急，因为生产运营有它应急的规则、流程，应急的组织方，各条线在组织方的协调下进行。那你这个安全运营中心和原有的生产运营的组织方到底是什么关系？你调整它还是它调整你，是他来指挥各条线还是你来指挥各条线？在运营上的边界怎么解决？

这个是我们行业今年在大量的态势感知和运营领域，明年打算推动建设，但建设的前提一定要想好。有这些疑问，希望能够得到解惑。

**人民银行吕毅**

态势感知这四个字其中某几个字做好，很不容易的事情，态势管理，至于感知是更虚的东西，我对它的概念理解。还有从单位，**我们人民银行，我是金融信息中心**，它是面向银行机构提供服务，我们系统比较多，在这么一个背景下，**我们整个信息安全发展，从过去的注重防御的模式逐步转移到需要加强检测监测的阶段，这是提升的过程，并不是说我学态势感知，要提高感知能力，加强检测监测能力，特别对外部威胁，央行这块作为监管机构，树大招风，老找我们，怎么办？**我们需要这样的机制去应对，需要对全局有一个掌控，从我们设计上有态势管理的需求，也许在市场上，厂商能够提供这样的产品，来提供这样的需求，从这个角度，不是因为态势感知而建态势感知的思路，**这里边态势感知更多觉得是一种方法，它核心还是对整个信息安全风险的展示，刚才有领导提到叫可视化，这个词从我来讲很关键，应该说我们安全做的工作更重要的手段是可视化，让别人看到，这里边应该以风险为载体，有一些材料说信息安全管理就是风险管理，这个还有它的道理，**整个风险从资产，到它的威胁，应该说在我这个范围内应该有一个全程的掌控，至少安全部门哪有问题，什么状态，这里还牵扯到后面风险带来的事件处置，事件的管理，事件处置的可视化和整个事态过程，我比较担心刚才领导提到的，要在项目中要注意这个问题。最后要实现一个目标，最开始安全工作的价值，这块我也是做安全很多年，**希望通过这样的态势感知平台，能把安全的工作做一个展现，能把安全工作的价值定位，让别人知道，这里包括工作的量化和考核指标的细化，通过这样的过程，让大家知道它的重要性，这是我对整个态势感知也好，**SOC平台建立的理解。

在大的框架下提几个问题，意识到有这方面的风险，做了一些尝试，在新的环境下有几个问题，**第一个态势感知后台技术平台技术路线的选择，**很多种术语，我也不太清楚，作为技术平台建设，对平台的定位需要什么样的技术合适，这个技术选择，我个人觉得是到位的，选了选，最后再调的可能性不大，如何选择的事情，根据公司的规模，但这个规模有哪些策略。

**第二个问题，整个安全事件生命周期管理，**大家都提到了，这个事情比什么都重要，通过管理流程的设计，包括场景，我们需要应对什么样的场景，我们需要产生那些数据，需要什么样的分析模型，最核心事件如何分级的，这里我们也面对同样的问题，对大量的问题，你说它是问题，出问题了吗？实际上没有出问题，但是都属于漏洞，高危漏洞，这个时候我们怎么去识别这个问题的严重程度，现在我们慢慢转变意识，出事了，这是最严重的事件，出事带来了内部的漏洞，这个漏洞本身它的级别一定要高于其他漏洞，核心问题就是如何把一个分级的方法客观的，可执行的找出来，这样在未来平台上有处置的过程，就是避免对事件淹没掉，这个确实多少都是无底洞，在这个时候我们需要定策略，来控制这个东西。

**第三个问题，刚才提到态势感知的全局，我们是希望通过这个平台，把所有防控手段展现，这全局和建平台本身不可能一步到位，局部的关系如何平衡，**我先做资产还是做漏洞，这里边有顺序选了，看厂商有没有最佳实践，我现在隐约感觉到有些还是做了，在我们行业有做，这块虽然有选择，基本上还是有最佳实践，至少是个建议，希望能给一些这方面的策略。

**第四个问题，这可能跟刚才那个问题相关，内控的事情，我们行网络有一部分属于内部封闭的网络，**内控的风险，我个人感觉未来可能是个点，是重点关注的，内控控制，态势感知能做什么，这个在策略上有关系的，希望大家给一些建议。

**最后，我从实践角度来看交付能力，**说太好了，说得越好，期望值越高，希望越多，交付能力在座各位都是公司级领导，都是业内专家，**但是到用户这端，具体交付什么东西，这些人水平和能力，**有的时候不敢恭维，这是通病。这个交付往往这个环节上真正给用户带来价值的过程，这个环节上我个人觉得公司策略上都有些需要完善的地方，用户的需求响应和他的处置流程的周期，对我来看，我是不能接受的，但是我没有办法。刚才电信的领导说得有点那意思，大佬是甲方，从定位上是不清的，但是没有办法，公司的资源变成大公司，周期很长的，多个部门需要协调资源，来应对你的需求，这个周期，我个人觉得是这类项目做不好的主要原因。用户也提了，用户的项目经理也好，公司领导，他也有考核的，这个事出东西，干脆别做了。这个问题解决不好的话，也是后面没法再推项目，定制开发不可避免，但是周期一定要可控，这是从我来讲，对厂商提的要求。

**国开行的林东升**

**（已经开始规划，还没有部署）**

我在这里结合实际工作，向大家报告一下我们行关于SOC的考虑。我们现在还没有部署SOC平台，我们也是规划做完了，准备上这个东西。我们现在初步想的把它分成规划和建设实施两个部分，前期我们是专门立了一个项目去做SOC平台建设规划，我们请了独立的第三方以咨询和服务的方式，形成参考方案，在参考方案基础之上，内部准备决策去推动这个东西的实施，我们也感觉到这个东西在实施过程中，还是具有相当的复杂度的。它涉及到整个信息科技部门的各个条线，为了更好的让它落地，我们初步考虑的是把它放到数据中心去做实施，主要考虑它是贴近一线，更有利与今后的运维，运行管理，在安全运行上，我们考虑的是现在把安全管理和建设运维有独立的团队来负责，有专门的团队负责运维和监控。

这个独立的团队，我们的人也是很少，大量也是采用专业的外包服务的方式来解决自身的人力和专业能力不足的问题。

将来SOC很可能是由安全运营团队去负责实施，这种考虑也是考虑和我们现有的安全工具发挥协同的作用，因为我们已经部署很多IPS、WAP等等一系列安全产品，这样做下去，我可以在现有的流程里解决一些问题。第二尽量实现资源的共享，比如说在规划的时候就提到SOC将来要上屏幕去做展示的，我们可以利用现有的资源，把SOC将来能出的成果进行显现化的展示，刚才几位领导提到的，我们安全效益溢出，不管从内容和形式上，尽可能形成显现化的尝试，我就说这些。