协同安全运营综述

陈晔

国富人寿保险股份有限公司，广西 南宁 537000

摘　　要： 本文综述了协同安全运营的重要性及其在企业网络安全中的应用。面对网络攻防极不对等的挑战，企业面临技术能力、装备、组织、限制及价值等多方面的劣势。协同安全运营通过跨组织合作，共享安全信息和资源，提高响应时效性，降低经济和社会风险，增强整体安全防护能力。其核心在于协同机制与安全文化的构建，涉及人员组织、制度流程和技术工具的整合。协同安全运营相比传统模式更灵活高效，但也面临沟通协调、技术与标准不统一等挑战。在未来，协同安全运营将向自动化智能化、数据驱动、云原生安全和供应链安全等方向发展，为企业网络安全提供更强有力的保障。

关 键 词： 网络安全；协同安全运营

Overview of Collaborative Security Operations

Chen Ye

Guofu Life Insurance Co., Ltd. Nanning, Guangxi 537000

Abstract: This article summarizes the importance of collaborative secure operation and its application in enterprise network security. Faced with the challenge of extremely unequal network attack and defense, enterprises face disadvantages in various aspects such as technological capabilities, equipment, organization, limitations, and value. Collaborative security operation improves response timeliness, reduces economic and social risks, and enhances overall security protection capabilities through cross organizational cooperation, sharing security information and resources. Its core lies in the construction of collaborative mechanisms and safety culture, involving the integration of personnel organization, institutional processes, and technical tools. Collaborative secure operation is more flexible and efficient compared to traditional models, but it also faces challenges such as communication and coordination, as well as inconsistent technology and standards. In the future, collaborative security operations will develop towards automation and intelligence, data-driven, cloud native security, and supply chain security, providing stronger guarantees for enterprise network security.

Keywords: network security; collaborative security operation

一、引言 – 网络安全攻防不对等的局面

如果只能用一个词说明企业当前面临的网络安全挑战，那应该是“极不对等”。这种极不对等主要体现在技术能力、组织、装备、限制、价值。

（一）价值

能够认识到并且获益于网络信息安全能力带来价值的企业占比极少。即使是全球500强企业，也难免经常把安全看作负担与成本。反观攻击方，安全能力带来的价值包括且不限于经济价值和个人成就感。

（二）装备

企业级的安全防御和检测装备和攻击方的武器库相比差不止一个数量级。

（三）限制

企业的安全研究人员能够有条件完成的研究成果不仅受限于技术，更受限于每个国家和地区的法律 / 法规。再看黑产，本身就不是合法的营生，做事只受限于物理定律。这里就说还存在举国之力打造的网军。

（四）组织

企业的组织，特别是大企业，注重内控、合规，厌恶风险。黑产的组织，一切以攫取最大经济利益为目的，注重效率、效果，天然不在乎风险。

（五）技术能力

能够给高水平的安全人员开出足够好的待遇的企业占比极低。黑产则在发展过程中自然地形成了严密的分工和待遇与贡献匹配的机制。高水平的安全人员都是攻守兼备型的人才。只有内心足够强大，能够抵御黑化的诱惑才能安于相对低得多的待遇。

二、破局 – 跨组织协同缓解不对等

（一）经济效益

通过协同安全运营，企业可以共享安全信息和资源，及时发现并应对安全威胁，从而降低数据泄露、系统瘫痪等安全风险。这些风险的减少直接避免了潜在的经济损失，这种合作模式提高

作者简介：陈晔（1973.10.30），男，汉族，籍贯：湖北省枣强县，学历：硕士研究生，专业：电子与通信工程。

了安全管理的效率，降低了单个企业的运营成本。

（二）社会效益

在数字化转型的背景下，企业的网络安全水平已成为衡量其综合实力的重要指标之一。通过协同安全运营，企业可以提升自身的安全防护能力，进而增强市场竞争力。这种竞争力的提升不仅有助于企业在激烈的市场竞争中脱颖而出，还能为整个行业的健康发展贡献力量。

（三）响应时效性

协同安全运营通过建立一个集中的安全监控和响应机制，可以显著提升对安全事件的响应时效性。当一家企业检测到安全威胁时，可以迅速将这一信息分享给协同网络中的其他成员，从而实现快速响应和共同防御。这种及时的信息共享和协同作战能力，对于有效应对不断变化的网络威胁至关重要。

（四）能力可行性

在网络安全领域，一家单位仅靠自身能力往往难以应对所有挑战。通过融入协作网络，企业可以充分利用其他成员的专业知识和资源，共同应对复杂多变的安全威胁。这种协同作战的方式不仅提高了整个网络的安全防护能力，也使得每家企业都能在自身能力范围内有效地参与到网络安全保障工作中来。

三、协同安全运营：定义、起源、框架、核心

（一）定义

协同安全运营，顾名思义，强调的是在网络安全运营过程中的“协同”作用。从狭义层面来看，是以 IT 资产为核心，通过威胁事件管理的关键流程，利用安全运营平台来支撑事件发现、风险分析、预警管理和应急响应处置的集中安全管理体系。从广义层面，协同安全运营是一个融合了技术、流程和人员组织的复杂系统工程，其目标是通过聚合和挖掘多个组织的安全产品、工具和服务产出的数据，持续输出价值，更好地消减网络信息安全风险，确保网络安全。[1]

（二）起源与发展历程

协同安全运营的概念源于网络安全领域对更高效、更协同的安全管理模式的需求。随着网络技术的飞速发展和网络威胁的不断增多，传统的孤立、分散的安全管理方式已经难以应对。因此，业界开始探索如何通过协同合作来提升安全管理的效率和效果。协同安全运营应运而生，它强调多方协作、信息共享和资源整合，以共同应对网络安全挑战。协同安全运营在安全行业最常见的形式之一是 MSS（Managed Security Service）。[2]

（三）框架结构

1. 安全能力：企业自身的安全能力是协同安全运营的基础，包括各种安全技术、工具和专业知识。通过协同工作，互相借力，更有效地利用和发挥各参与方的安全能力。

2. 安全数据：在协同安全运营中，数据的共享和分析至关重要。各方需要共享安全数据，才能做到更深入的风险分析和更及时的威胁预警。

3. 运营能力：包括安全运营管理流程、应急响应机制等。通过协同合作，可以聚合各参与方的安全运营能力，提高安全事件的处置效率。

这三个要素之间相互作用、相互影响，共同构成了一个高效的协同安全运营体系。在这个体系中，各方通过共享资源、信息和经验，共同应对网络安全威胁，实现网络安全的整体提升。[3-4]

（四）核心：机制与文化

1. 协同机制

协同机制是指不同组织、团队或个人之间在安全运营过程中的协作方式和规则。协同机制促进信息共享、资源整合和共同决策，以实现更高效的网络安全管理。良好的协同机制能够打破信息孤岛，提升整体的安全防护效果，是协同安全运营不可或缺的一环。

2. 安全文化

安全文化是指组织内部对网络安全的重视程度、安全意识和行为习惯等。安全文化影响着员工的安全行为和组织的安全氛围，是协同安全运营的重要支撑。积极的安全文化能够增强员工的安全责任感，提高整个组织对安全风险的敏感性和应对能力。

机制与文化，一实一虚，相互影响，共同构成了协同安全运营的核心。前述的安全能力、安全数据、运营能力就是围绕这个核心构建的框架。[5-6]

四、协同安全运营与传统安全运营的对比

用 PPT 模型（People – 人员与组织、Process – 制度与流程、Technology – 技术与工具）分析协同安全运营与传统安全运营的差异如下表所示。

	协同安全运营	传统安全运营
人员与组织	•强调团队合作，多个人协同完成共同的任务。各成员之间需要频繁沟通、协调，以便实现良好的协同效果。 •注重跨部门、跨团队的协作，甚至可能涉及外部合作伙伴的联合。 •组织结构更加扁平化，鼓励信息共享和快速决策。	•由单个或少数人负责安全工作，沟通方式相对简单。 •组织结构可能较为层级化，决策和信息流动可能较慢。 •安全团队可能相对孤立，与其他部门或团队的协作有限
制度与流程	•有完善的协同工作制度和流程，明确各成员的角色和责任。 •强调流程的灵活性和快速响应，以适应不断变化的安全威胁。 •可能有专门的协同平台或工具来支持流程的执行和监控。	•制度和流程可能较为固定和繁琐，难以适应快速变化的安全环境。 •可能缺乏明确的协同机制和流程，导致响应速度较慢。 •流程的执行可能更依赖于人工操作和监控。
技术与工具	•充分利用现代科技手段，如大数据分析、人工智能等，来提升安全防护能力。 •使用在线工具来协调任务分工、进度跟踪、文件共享等，提高工作效率。 •可能采用专门的协同安全运营平台或系统来整合各种安全工具和数据源。	•可能更依赖传统的安全技术和工具，如防火墙、入侵检测系统（IDS）等。 •工具和技术的更新可能较慢，难以应对新型安全威胁。 •缺乏统一的安全管理平台来整合各种安全信息和资源。

从上图可以看出，协同安全运营在人员与组织、制度与流程、技术与工具这三个方面都表现出更强的灵活性、协同性和整合性，从而更好地应对网络安全挑战。

五、协同安全运营：资源共享、优势互补

下面分3种情况阐述两家（含）以上单位采取协同安全运营工作时所需的资源共享以及预期实现的优势互补效果：

	资源共享	优势互补
两家有业务往来的企业	1.安全信息和数据：双方可以共享各自的安全日志、威胁情报等，更全面地了解当前的安全态势。 2.安全工具和平台：通过共享安全工具和平台，如SIEM、威胁情报等，提高双方的安全监测和响应能力。 3.安全专家和资源：双方可以共享安全专家资源，共同应对复杂的安全威胁和挑战。	1.提升安全可见性：通过共享安全信息和数据，双方可以获得更全面的安全视角，减少安全盲区。 2.增强安全响应能力：共享安全工具和平台使得双方能够更快地检测和响应安全事件，降低损失。 3.专业知识共享：安全专家资源的共享可以帮助双方提升安全团队的专业水平，更好地应对不断变化的安全威胁。
企业和上级集团公司（或企业与主管单位）	1.安全政策和标准：集团公司可以提供统一的安全政策和标准，确保企业符合相关的安全要求。 2.安全基础设施：集团公司拥有更强大的安全基础设施，如安全运营中心（SOC）等，这些资源可以共享。 3.安全培训和教育资源：集团公司可以提供全面的安全培训和教育资源，帮助企业提升员工的安全意识和技能。	1.统一的安全管理：通过共享安全政策和标准，确保企业在安全运营上的一致性和合规性。 2.强大的安全后盾：借助集团公司的安全基础设施和资源，企业可以获得更强大的安全支持和保障。 3.提升员工安全素养：通过集团公司的安全培训和教育资源，企业员工的安全意识和防范能力将得到提升。
企业与安全运营服务商	1.专业的安全服务：安全运营服务商提供专业的安全服务，包括安全监测、事件响应、威胁情报等。 2.先进的安全技术：安全运营服务商通常掌握最新的安全技术和解决方案，这些技术可以与企业共享。 3.安全咨询和规划：安全运营服务商可以提供全面的安全咨询和规划，帮助企业构建更完善的安全体系。	1.专业的安全保障：借助安全运营服务商的专业服务和技术支持，企业可以获得更全面、更专业的安全保障。 2.及时的安全响应：与安全运营服务商合作可以确保企业在面临安全事件时能够得到及时、有效的响应和支持。 3.完善的安全规划：通过安全运营服务商的咨询和规划服务，企业可以构建更加完善、高效的安全体系，提升整体的安全防护能力。

六、协同安全运营：责任划分与协作机制

两家（含）以上单位开展协同安全运营是一个复杂而细致的过程，涉及多方面的责任划分与紧密的协作机制。以下是对这一过程的详细阐述，以及协同运营相比单独开展安全运营的优势和所需额外成本的探讨。

（一）责任划分与协作机制

1. 责任分配

主导单位：通常负责整体安全策略的制定，监督安全运营的执行情况，并确保各单位之间的有效协作。参与单位：根据自身的专业能力和资源，承担特定的安全运营任务，如威胁监测、事件响应、系统维护等。[7]

2. 协作方式

信息共享：各单位之间建立安全信息共享机制，实时交换威胁情报、安全事件数据等，以提高整体的防御能力。任务协调：根据安全事件的性质和影响范围，协同分配任务和资源，确保高效应对。

3. 沟通机制

定期会议：通过定期的安全会议，讨论当前的安全形势、存在的问题和改进措施。紧急联络渠道：建立24/7的紧急联络机制，以便在发生重大安全事件时能够迅速响应和协调。

（二）协同运营的优势

1. 提高运营效率

通过信息共享和任务协调，各单位能够更快地识别和响应安全威胁，减少重复工作和资源浪费。协同运营可以集中优势资源，共同应对复杂的安全挑战，提高整体运营效率。

2. 降低成本

共享安全设备和人力资源，避免不必要的重复投资，降低运营成本。通过集体采购安全服务和产品，可能获得更优惠的价格和更全面的技术支持。

3. 增强市场竞争力

协同运营有助于提升整个供应链或合作体系的安全性，从而增强市场竞争力。共同应对安全威胁能够提升客户信心，维护品牌形象。

（三）需要额外付出的成本

1. 资源投入

初期可能需要投入资金来建立信息共享平台、购置必要的安全设备和工具。为了确保协作的顺畅进行，可能需要增加网络带宽、数据存储等基础设施的投入。

2. 时间成本

在协同运营的初期阶段，各单位需要花费时间进行磨合和协调，以确保协作机制的有效运转。定期的安全会议和紧急联络可能需要占用一定的工作时间。

3. 人力成本

可能需要设立专门的安全协作团队或指派专人负责协同运营工作。为了提升团队的安全素养和协作能力，可能需要进行定期的培训和教育。

七、协同安全运营：挑战

多家单位开展协同安全运营过程中可能遇到包括“难以沟通与协调”“技术与标准不统一”和其他不能忽视的挑战。

（一）挑战一：难以沟通与协调

1. 产生原因

语言和文化差异：如果两家单位来自不同的国家或地区，可能会存在语言和文化上的差异，导致沟通障碍。组织架构不匹配：两家单位的组织架构和管理模式可能不同，使得在协同工作过程中难以找到对应的接口人和部门。信息不透明：各单位可能出于保护自身利益的考虑，不愿意完全共享信息，导致沟通不畅。[8]

2. 解决方案

建立共同沟通语言：确定一种双方都能接受的工作语言，并为需要的人员提供语言培训。文化建设与培训：为团队成员提供跨文化沟通的培训，以增加对不同文化背景的理解。明确沟通渠道和流程：建立清晰的沟通渠道和定期的会议机制，确保信息能够及时、准确地传递。

促进信息共享：通过签订保密协议等方式，建立信任，促进双方之间的信息共享。

（二）挑战二：技术与标准不统一

1. 产生原因

技术发展差异：两家单位可能使用不同的技术栈和安全解决方案，导致在协同工作时存在技术障碍。标准不统一：由于缺乏统一的安全标准和规范，两家单位在协同工作时可能难以达成一致。

2. 解决方案

技术对接与整合：明确双方的技术需求和标准，寻找或开发能够实现技术对接的解决方案。制定统一的安全标准：双方协商并制定统一的安全标准和操作规范，以确保协同工作的顺利进行。技术培训和交流：定期组织技术交流和培训活动，提高双方团队的技术水平和协作能力。[9]

八、协同安全运营：总结与展望

（一）协同安全运营的实践意义与价值

协同安全运营通过整合多方资源和技术，能够更高效地应对网络安全威胁。通过共享安全数据、工具和服务，各方能够更快地识别风险、验证问题并共同响应，从而提升整体安全防护的效果。协同安全运营促进了不同组织之间的紧密合作。这种合作模式不仅有助于提升单个组织的安全能力，还能加强整个行业的安全防线，共同抵御网络攻击。通过协同工作，组织可以共享安全投入，避免重复建设和资源浪费。这种成本效益的考虑对于资源有限的组织来说尤为重要。协同安全运营有助于组织更好地满足法规要求，保护关键业务数据和客户信息，从而确保业务的连续性和企业的声誉。[10]

（二）未来协同安全运营的发展趋势与预测

随着技术的发展，协同安全运营将更加依赖自动化和智能化

工具。这些工具能够实时监控网络状态，自动响应安全事件，从而减轻人工负担并提高响应速度。未来，协同安全运营将更加依赖数据驱动的决策。通过收集和分析大量安全数据，组织能够更准确地识别风险并制定相应的防护措施。随着云计算的普及，云原生安全将成为协同安全运营的重要组成部分。组织将需要更加关注云环境中的安全风险，并制定相应的防护策略。近年来，供应链攻击事件频发，未来协同安全运营将更加重视供应链安全。组织将加强与供应商的合作与沟通，共同确保整个供应链的安全性。

综上所述，协同安全运营在提升网络安全防护能力、降低安全成本、增强组织间协作等方面具有重要意义。未来，协同安全运营将朝着自动化与智能化、数据驱动、云原生安全和供应链安全等方向发展。

参考文献：

[1] 江旺，范海亮，周正虎等. 协同作战平台在网络空间安全运营中的研究与应用［J］. 网络安全技术与应用，2023,(10):23-26.

[2] 张慧. 网络安全的国家治理逻辑：内涵、标准与路径［J］. 天水行政学院学报，2021,22(03):20-25.

[3] 江旺，范海亮等. 协同作战平台在网络空间安全运营中的研究与应用［J］. 网络安全技术与应用，2021,23(10):23-26.

[4] 江黄翔，刘晓静等. 基于云边协同的数字电网通信信息网络安全策略研究［J］. 电力大数据，2023,26(10):42-49.

[5] 何春中. 筑牢网络安全防线 共享清朗网络空间［J］. 中国青年报，2023:3.

[6] 李阳，毕钰. 加强关键信息基础设施网络安全协同防护，健全网络安全保障体系［J］. 中国信息化，2023(08):29-32.

[7] 詹海宝，孙江，郭梦圆等. 基于人机协同的网络文化安全治理新模式［J］. 传媒，2023(15):75-77.

[8] 顾林晗，业界大咖共话数据安全［J］. 传媒，2023(05):2.

[9] 王皓，智慧城轨云平台和数据平台及网络安全融合协同技术研究［J］. 都市快轨交通，2022,35(06):64-68.

[10] 邱勤，徐天妮等，算力网络安全应用需求与关键技术研究［J］. 信息技术与标准化，2022,(11):19-24.