大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

平安金融安全研究院
PingAn Academy of Financial Security

CAICT 中国信通院

# 网络安全态势感知

## 技术及应用发展蓝皮书

2019

# 版权声明



# 编写说明

### 牵头单位：

大数据协同安全技术国家工程实验室 – 金融行业安全研究中心

### 参与单位：

大数据协同安全技术国家工程实验室 – 金融行业安全研究中心

平安金融安全研究院

中国信息通信研究院

### 编委会成员名单：

大数据协同安全技术国家工程实验室 – 金融行业安全研究中心、平安金融安全研究院：

李洋、谢晴、王小波、苏云凤

中国信息通信研究院：魏亮、卜哲、郑威

# 目 录

# 前 言

对于高度网络化的社会，网络空间安全已经成为当前面临的挑战之一。个人、企业和政府也越来越关心网络犯罪、网络间谍活动和网络空间战争对他们造成的威胁。在网络空间防御领域，态势感知尤为重要。随着全球范围内国家文件相继出台，态势感知在许多国家被提升到了战略高度，政府、企业、监管机构等相继开始建设和积极应用态势感知系统，美国在这方面无疑走在了世界前列，形成了其较为完善的网络空间（安全）态势感知体系。在中国，习近平主席在 4 · 19 讲话中也提出了“全天候全方位感知网络安全态势”的基本要求。

态势感知系统具备网络空间安全持续监控能力，能够及时发现各种攻击威胁与异常；具备威胁调查分析及可视化能力，可以对威胁相关的影响范围、攻击路径、目的、手段进行快速判别，从而支撑有效的安全决策和响应；能够建立安全预警机制，来完善风险控制、应急响应和整体安全防护的水平。在未来，态势感知技术将在各行各业中得到广泛应用，其应用前景非常光明。

本蓝皮书通过收集、整理全球范围内的网络空间态势感知发展情况，特别是中美发展对比，从态势感知的发展背景、网络空间态势感知的基本概念、国内外发展现状、态势感知 1.0 到态势感知 2.0、态势感知在金融行业的应用等维度进行详细分析，向读者展示态势感知技术及发展的全貌。

# 01 态势感知概述

## 1.1 态势感知发展背景

“态势感知”早在 20 世纪 80 年代由美国空军提出，其包含感知、理解和预测三个层次。到 90 年代，态势感知概念开始被广泛接受，并伴随着网络的兴起而升级为“网络态势感知（Cyberspace Situation Awareness，CSA）”，它是指在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解和显示，并对最近发展趋势的顺延性预测，其最终目的是要进行决策与行动。值得注意的是，态势强调环境、动态性以及实体间的关系，是一种状态和趋势，一个整体和宏观的概念，任何单一的情况或状态都不足以称之为态势。

### *1.1.1 态势感知的通用定义*

人们对于态势感知的定义和理解有着很大的不同，其中认同度较高的是 1995 年 Endsley[1] 博士所给出的动态环境中态势感知的通用定义，这也是最早的态势感知定义之一，该定义对态势感知的描述是：“在一定时间和空间内观察环境中的元素，理解这些元素的意义并预测这些元素在不久的将来的状态。”

通过该定义，可以提炼出态势感知的三个要素：感知、理解和预测，也就是说态势感知可以分成感知、理解和预测三个层次的信息处理，其输出将被直接馈送至决策和行动的周期中。

[1] 席荣荣，云晓春，金舒原，等 . 网络安全态势感知研究综述 [J]. 计算机应用 ,2012,32(1):1-4,59. DOI:10.3724/SP.J.1087.2012.00001.

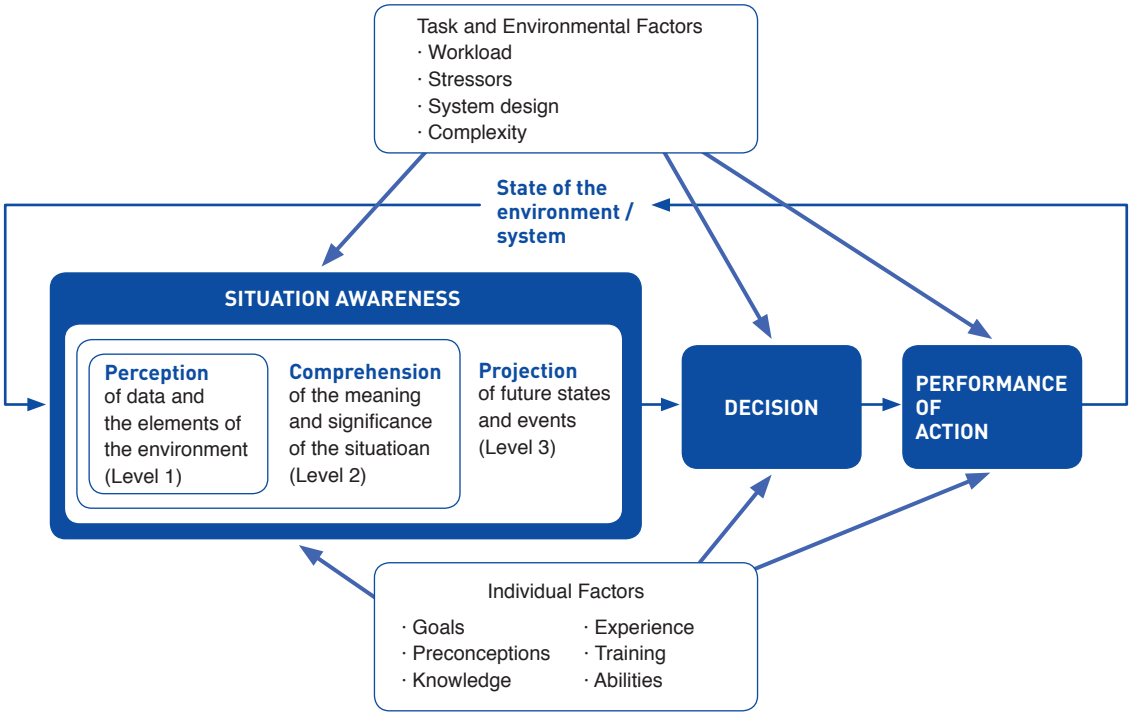


**图 1. 动态决策中的态势感知模型（Endsley，1995）**

1. 感知：感知和获取环境中的重要线索或元素。在网络安全中，可以指防御系统的告警，如防火墙、入侵检测系统（Intrusion Detection System，IDS）和入侵防御系统（Intrusion Prevention System，IPS）等，这些类型的数据必须是准确的以保证后面做的决策基于事实。

2. 理解：整合感知到的数据和信息，分析其相关性。这是一个重要的层级，因为态势感知远远不止步于感知屏幕上所显示的一堆数据。真正需要做到的是，结合操作人员的目标来理解这些信息的意义或显著性。

3. 预测：基于对环境信息的感知和理解，预测相关知识的未来的发展趋势。该层级包含对信息进行的前向时间判断，以确定其将如何对运行环境的未来状态产生影响。这结合了当前个体对态势的理解，以及对系统形成的心智模型，从而可以预测下一步可能发生的情况。

在上述定义基础之上，为了深入探讨如何在动态的系统环境中通过态势感知支持高效的决策制定和行动执行，Endsley 博士进一步明确了相关术语的定义，提出态势感知应当被作为一种“知识的状态”，而“实现、获取或维持态势感知状态的过程”则应该称为态势评估，并且强调应该对这两个概念加以区分。

### 1.1.2 态势感知分析模型

除了上述 Endsley 博士提出的态势感知模型，在态势感知的分析过程中，会应用到很多成熟的分析模型，这些模型的分析方法虽各不相同，但多数都包含了感知、理解和预测的三个要素。

| Abbrv. | Model | Focus | Reference |
|---|---|---|---|
| SAM | Situation Awareness Model | Cognitive decision making | (Endsley, 1995) |
| OODA | OODA Loop | Cognitive decision making | (Byod, 1996) |
| JDL DFM | JDL Data Fusion Model | Processing and fusion of data and SA | (Steinberg et al., 1998) |
| CSAM | Cyber Situational Awareness Model | Business continuity planning and CSA | (Okolica et al., 2009) |
| SARM | Situational Awareness Reference Model | Situational awareness | (Tadda and Salerno, 2010) |
| ECSA | Effective Cyber Situational Awareness | CSA in computer networks | (Evancich et al., 2014) |

**表 1. 态势感知分析模型**

其中，网络安全态势感知模型被普遍接受的是基于数据融合理念（Joint Directors of Laboratories，JDL）的模型，其主要包含的一些关键技术，例如海量多元异构数据的融聚融合技术、面向多类型的网络安全威胁评估技术、网络安全态势评估与决策支撑技术、网络安全态势可视化等。有关态势感知分析模型此处不作赘述，后续章节将主要针对网络安全态势感知展开讨论。

## 1.2 网络安全态势感知基本概念

本章节主要针对网络安全态势感知进行论述，因此，本章节所提“态势感知”皆指“网络安全态势感知”。

### 1.2.1 网络安全态势感知的定义

Tim Bass[2] 于 1999 年首次提出网络空间态势感知 CSA 的概念，指出“下一代网络入侵检测系统应该融合从大数据异构分布式网络传感器采集的数据，实现网络空间的态势感知”，并基于数据融合的 JDL 模型，提出了基于多传感器数据融合的网络态势感知功能模型，如图 2 所示：

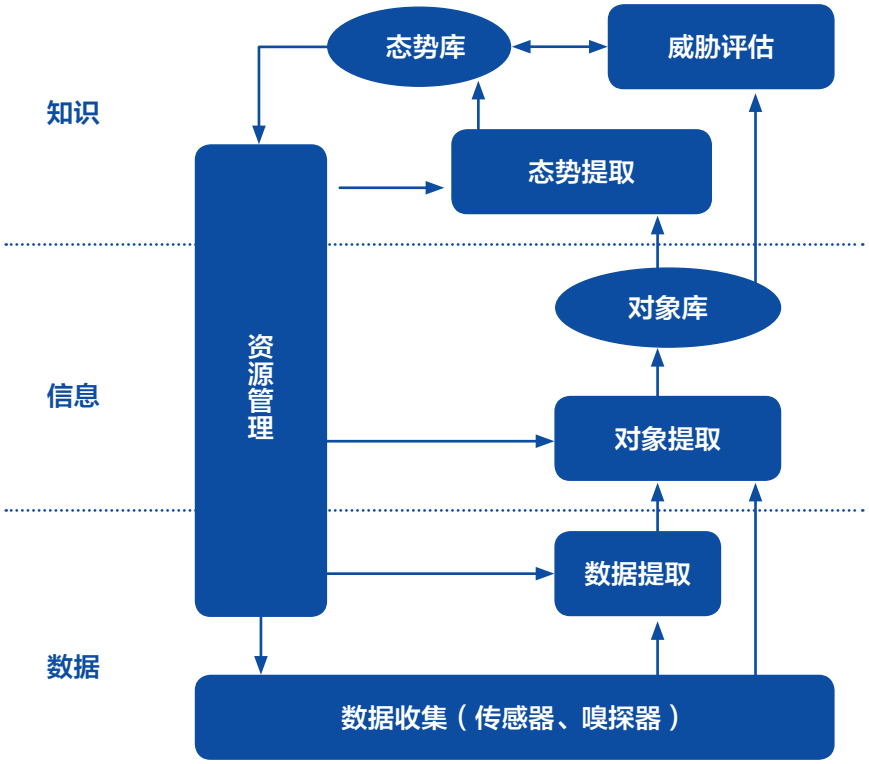


图 2. 网络态势感知的功能模型

Tim Bass 模型最早基于多传感器数据建立了网络态势感知框架，描述了多台安全传感器和入侵检测设备之间数据融合的原理及流程：

1. 底层为数据感知层，包括数据采集层和数据预处理层，主要完成数据清洗和校准、多元数据格式化、数据关联分析等工作

2. 中层是在底层数据分析的基础上对网络态势进行动态智能推理的评估

3. 上层进行知识转化，预测当前网络中可能发生的安全事件，并对网络威胁的程度进行评估

4. 有独立的“查询选择和反馈循环”单元，负责跟踪和评估整个系统的运行情况，协调各个层次之间的关系使其正常运行

[2] 席荣荣 , 云晓春 , 金舒原 , 等 . 网络安全态势感知研究综述 [J]. 计算机应用 ,2012,32(1):1-4,59. DOI:10.3724/SP.J.1087.2012.00001.

截止目前，业界对网络安全态势感知还没有一个统一全面的定义，例如基于 Endsley 博士的理论对网络安全态势感知做出的定义：“网络安全态势感知是综合分析网络安全要素，评估网络安全状况，预测其发展趋势，并以可视化的方式展现给用户，并给出相应的报表和应对措施。”

根据上述概念模型，网络安全态势感知过程可以分为以下四个过程：

1. 数据采集：通过各种检测工具，对各种影响系统安全性的要素进行检测采集获取，这一步是态势感知的前提。

2. 态势理解：对各种网络安全要素进行分类、归并、关联分析并进行处理融合，对融合的信息进行综合分析，得出影响网络的整体安全状况，这一步是态势感知基础。

3. 态势评估：定性、定量分析当前网络的安全状态和薄弱环节，并给出相应的应对措施，这一步是态势感知的核心。

4. 态势预测：通过态势评估输出的数据，预测网络安全状况的发展趋势，这一步是态势感知的目标。

网络安全态势感知要做到深度和广度兼备，从多层次、多角度、多粒度分析系统的安全性并提供应对措施，以图、表和安全报表的形式展现给用户。

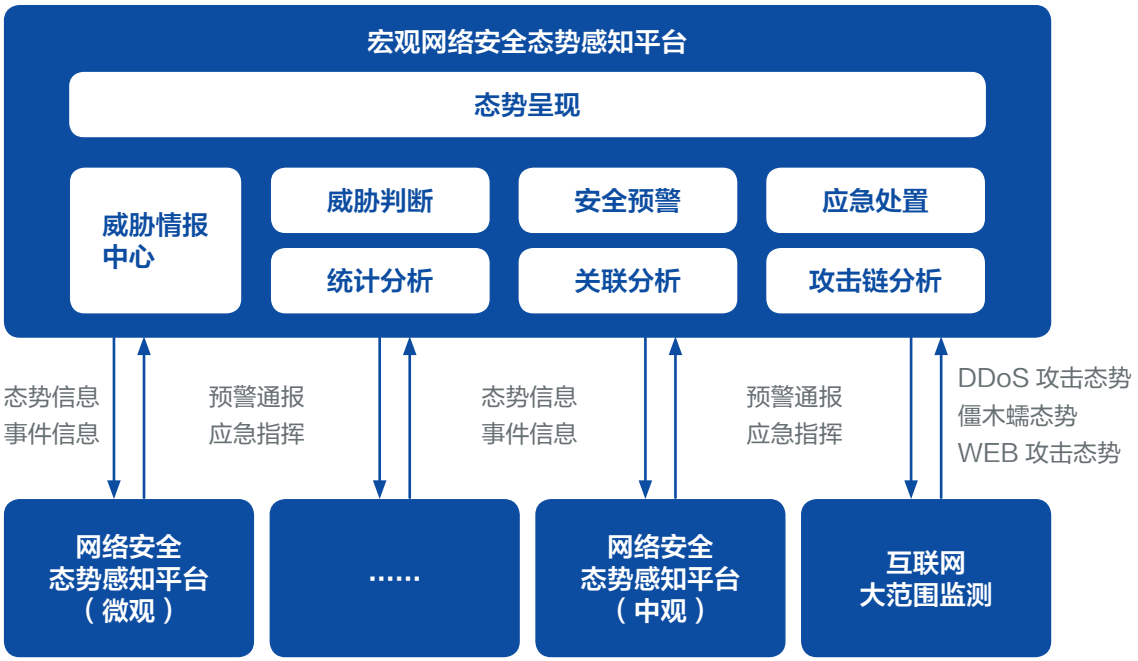


**图 3. 宏观层面网络安全态势感知平台功能架构** [3]

[3] 宋进，唐光亮 . 网络安全态势感知技术研究与应用 [J]. 通信技术 ,2018,51(6):1419-1424. DOI:10.3969/j.issn.1002-0802.2018.06.032.

### *1.2.2 态势感知建设目标及能力*

#### 1.2.2.1 态势感知建设目标

建设态势感知系统首先要明确建设的目标和范围，梳理清晰需要监测与防护的最关键的业务资产，然后应用合适的技术从微观层面获取完整的安全数据，再结合态势感知系统平台、来自商业或开源的大数据威胁情报能力，从中观层面来分析数据、发现威胁和异常，并合理运用安全服务来落地安全能力。因此，态势感知不仅仅是宏观层面的大屏展示，更是结合了微观、中观层面的安全数据、平台和安全能力。

安全运营是业务网安全保障体系的重要组成部分。安全运营体系以安全防御技术为核心，从安全威胁监测、响应、调查、处置全流程，安全漏洞发现、确认、修复、验证全生命周期，安全防御技术部署，威胁情报收集等多维度综合出发来应对网络攻击的安全保障能力。态势感知系统作为安全运营体系的技术平台，旨在实现“安全集成、智能分析、态势感知、协同处置、运营可视”五大目标。

#### 1.2.2.2 态势感知建设能力

通过态势感知与安全运营平台建设，构建安全防护的“大脑”，更好地加强纵深防御，建设主动防御、持续检测、应急响应、溯源取证、风险预警等安全能力，实现安全运营的闭环管理。

## 1.3 态势感知国内外发展现状

### *1.3.1 态势感知国家政策*

#### 1.3.1.1 态势感知美国政策

近年来，美国通过国家战略制定，新型网络力量筹建，大型国家性技术项目建设、关键技术突破，相关产品研发、网络安全产业化发展支持等多种措施，形成了“政府主导、军方协同、业界支撑”为特点的多层次网络空间安全态势感知能力体系。

2009 年，美国白宫在公布的网络空间安全战略文件中明确提出要构建态势感知能力，并梳理出具备态势感知能力和职责的国家级网络安全中心或机构，包含了国家网络安全中心 NCSC、情报部门、司法与反间谍部门、美国计算机应急响应小组 US-CERT、网络作战部门的网络安全中心等，覆盖了国家安全、情报、司法、公私合作等各个领域。

虽然世界其他国家也在日益重视网络安全态势感知技术研发和项目建设，但以美国为首的发达国家已经在该领域投入大量资源，并形成了整体战略布局和发展建设流程，正逐步掌握当前网络空间整体安全态势，取得了网络空间中的战略优势。

本蓝皮书通过对美国信息安全发展脉络进行梳理，收集整理了自 1998 年到 2018 年，美国与“安全感知”相关的 11 份重要文件。这 11 份文件构成了美国在网络空间安全感知领域比较完整的文字表述，下文会以这 11 份文件为基础，分析美国信息安全战略的发展演进，详情如表 2 所示：

| 时间 | 名称 | 主要目标 | 单位 |
|---|---|---|---|
| 1998 | 保护美国关键基础设施 PDD-63总统令 | 对关键基础设施建立基本保护能力(通过部署安全网关类、终端类产品) | 白宫 |
| 1998 | 信息保障技术框架IATF | 倡导：纵深防御；安全保障能力 | NSA |
| 2002 | 联邦信息安全管理法FISMA | 1.关注联邦政府网络安全 2.对网络进行分级，实行不同的安全策略 | 司法部 |
| 2007 | 国家网络安全综合计划CNCI | 1.联邦政府网络集中接入2.网内数据深度审计、分析 | 白宫 |
| 2011 | 网络空间行动战略 | 首次提出网络空间“积极防御”的概念 | 国防部 |
| 2012 | PLAN X | 快速绘制Cyber地图，提供高效网络作战能力 | DAPRA |
| 2012 | SHINE | 本土关键基础设施网络组件安全态势感知 | DHS |
| 2012 | 藏宝图计划 Treasure Map | 1.全网态势感知2.公共作战地图支撑3.全网侦察 4.攻击/刺探效果评估 | NSA |
| 2015 | 网络空间战略 | 要有能力破坏敌方网络系统、关键军事设施和武器装备 | 国防部 |
| 2017 | 2018财年国防授权法案 | 明确授权美国国防部“可在外国网络空间中采取适当规模的行动以实现扰乱、挫败及威慑等目的” | 国会 |
| 2018 | 网络空间战略 | 可以通过网络，对外国行动方通过网络手段对美国国防、关键基础设施等造成损害的行为进行反制 | 国防部 |

**表 2. 美国网络安全感知重要文件 [3]**

[3] 宋进 , 唐光亮 . 网络安全态势感知技术研究与应用 [J]. 通信技术 ,2018,51(6):1419-1424. DOI:10.3969/j.issn.1002-0802.2018.06.032.

纵览美国在信息安全方面的国家战略，可以看到其战略从“基础建立”的网络空间安全态势感知基本组件构建阶段；到“监听感知”的网络空间安全态势感知基本能力构建阶段；再到“探测感知”的网络空间安全态势感知扩展能力构建阶段；最后到“溯源反制”的网络空间安全态势感知溯源反制能力构建阶段的演进历程。这也展示了美国国家信息安全战略从被动保障到主动威慑的变化过程，详情见表 3。

| 时间 | 构建阶段 | 总结 |
| --- | --- | --- |
| 1998-2002 | 态势感知基本组件构建 | 美国DOD开发了信息安全领域比较重要的 [彩虹系列文件]，其中的橘皮书就是现在被广泛应用的CC的前身（GB/T 18336）。美国的总体目标是建立应对传统信息安全威胁的技术和管理能力，这些基本能力为日后网络空间态势感知能力的构建打下了深刻基础 |
| 2005-2010 | 态势感知能力构建 | 美国已逐步构建成自己的态势感知体系。借助第一阶段输出的安全能力（安全设备）和商业领域刚发展起来的SIM&SEM技术，将大量日志和流量监控起来，在牺牲本土公民个人隐私权利的基础上，形成基本的态势感知体系 |
| 2010-2015 | 态势感知扩展能力构建 | 美国在已建立的态势感知体系基础上，通过集成主动探测、海外信息搜集等技术，在无视Internet全球用户隐私权利的做法基础上，进一步扩展态势感知能力 |
| 2011-至今 | 态势感知溯源反制能力构建 | 美国国家战略逐渐从“积极防御”转向“攻击威慑”。在网络进攻方面，Stuxnet工业病毒和WannaCry勒索病毒都对全球网络造成了严重危害；在溯源反制方面，推动Lockheed Martin和Mitre开发KillChain和Att&CK模型，促进威胁情报标准STIX/TAXII等的落地，强化APT发现能力 |

**表 3. 美国网络空间态势感知构建阶段**

#### 1.3.1.2 态势感知中国政策

近几年，我国非常重视网络安全的发展，国家从战略、立法、机构、网络人才培养等方面都加强了布局，努力把我国建设成为网络强国，特别是在立法方面，出台了《 中华人民共和国网络安全法 》，其包含了网络安全发展战略、网络安全监测预警与应急处置制度、关键信息基础设施保护措施等内容。但总体来说，我国网络安全起步较晚。本蓝皮书收集到的与中国网络安全态势感知相关的国家政策如表 4 所示：

| 时间 | 名称 | 内容 |
| --- | --- | --- |
| 2016 | 419网络安全和信息化工作座谈会 | “要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”态势感知首次被提升到了国家高度，并迅速成为网络安全领域的热点。 |
| 2016 | 国务院发布《“十三五”国家信息化规划》 | 要求“加强网络安全态势感知、监测预警和应急处置能力建设。建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。建立政府和企业网络安全信息共享机制，加强网络安全大数据挖掘分析，更好地感知网络安全态势，做好风险防范工作。” |
| 2017 | 《中华人民共和国网络安全法》 | 明确规定：“国家建立网络安全监测预警和信息通报制度。”“负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。”由此可见，我国的关键信息基础设施和重要信息系统保护工作对网络安全态势感知关键技术和系统建设有着非常明确和迫切的要求。 |

**表 4. 中国网络安全感知重要发言及文件**

如今，在政策、企业实际需求等多方面因素的驱动下，“ 态势感知 ”已经成为国内网络空间安全领域聚焦的热点，也成为网络安全技术、产品、方案不断创新、发展、演进的汇集体现。

### *1.3.2 态势感知产品和服务*

对中国、俄罗斯、英国、美国等国家开展调研与研究，可以了解到，中国和美国非常重视态势感知。其中，俄罗斯、英国、美国把态势感知当做一种手段去解决网络威胁问题。另外，国外一般不提态势感知系统，而国内，很多厂商都推出了态势感知系统。

在中国，态势感知平台分为政府部门使用的监管平台和企业使用的实施监测预警平台，目前态势感知平台在公安部、网信办、金融、电信、能源等行业增长迅猛。态势感知平台是目前大数据安全领域规模增长最迅速的产品，据统计，2017 年国内态势感知市场规模约计 20 亿人民币，占整个安全市场的 5% 左右，预计 2020 年态势感知整体市场规模将超过 50 亿。下面将主要针对中美两国网络安全态势感知作进一步挖掘。

### 1.3.2.1 国外态势感知

在国外公司资料中，暂时没有发现有公司研究和推出态势感知系统。国外公司普遍研究的是威胁管理、威胁发现等产品，而非研发宣传态势感知产品。国外更多地把网络安全态势感知作为一种由多个系统或工具整合实现的状态效果、一种综合利用已有技术和系统的产品设计模式和运行使用方式。

### 1.3.2.2 国内态势感知

在国内，态势感知被寄予了很高的期望，它被塑造成一个非常智能的“机器人”，能够知道过去，预测未来。但实际上，任何系统都缺少不了人员的参与。我国目前的态势感知相关情况如下：

1. 目前国内安全厂商提供的“态势感知产品”包含的功能模块有：资产管理、漏洞管理、大数据平台、日志分析平台、威胁情报、沙箱、用户行为分析、网络流量分析、取证溯源、威胁捕捉等能力。

2. 态势感知目前主要应用于监管、金融、运营商、政府、教育、能源等行业，依据行业特性，各行业客户对态势感知所提供的技术需求也存在差异，例如：

（1） 金融行业有着更多的业务场景，注重态势感知系统的关联分析能力、威胁告警精确度、用户行为分析能力，以达到更深入的安全运营能力。

（2） 运营商的安全运营中心（Security Operation Center，SOC）基础良好，除了自身的安全，也会注重利用本身的数据资源优势，拓宽其他行业市场。

（3） 能源行业由于 IT 设备的种类繁多，生产安全关系重大，因此更注重产品的兼容性、保障生产运营的可连续性等。

（4）政府机构的需求重点，在对外部攻击防范，高级威胁检测和自身的威胁感知。

3. 监管机构注重掌握全网或本行业安全状态及威胁告警、可监控攻击态势、定位安全事件，例如，公安系统关注管辖范围内的关键基础设施，企事业单位的安全态势感知，发现安全隐患，推动等级保护和整改。

下面列举了一个态势感知与安全运营平台作为参考，功能架构如图4所示，系统可实现日志检索、资产管理、关联分析、威胁情报利用、告警响应中心、报表中心、安全监控、安全仪表板、可视化的事件溯源分析态势感知大屏功能。其采用了大数据技术，可实现事件的分布式采集、分析、存储和检索，对海量的日志数据、流量数据、数据包等做到实时关联分析、快速检索、高效统计，并以高度可视化的方式进行展现；云端安全数据提供安全态势分析与展示的数据服务；利用高级威胁情报在本地数据中进行比对，发现本地高持续威胁（Advanced Persisting Threat，APT）和僵尸网络 Botnet 主机；提供与网关设备和终端控制系统的联动（如 NetFlow Traffic Analyzer，NTA 和 Endpoint Detection and Response，EDR）实时阻断攻击和违规访问，实现安全运营闭环操作。

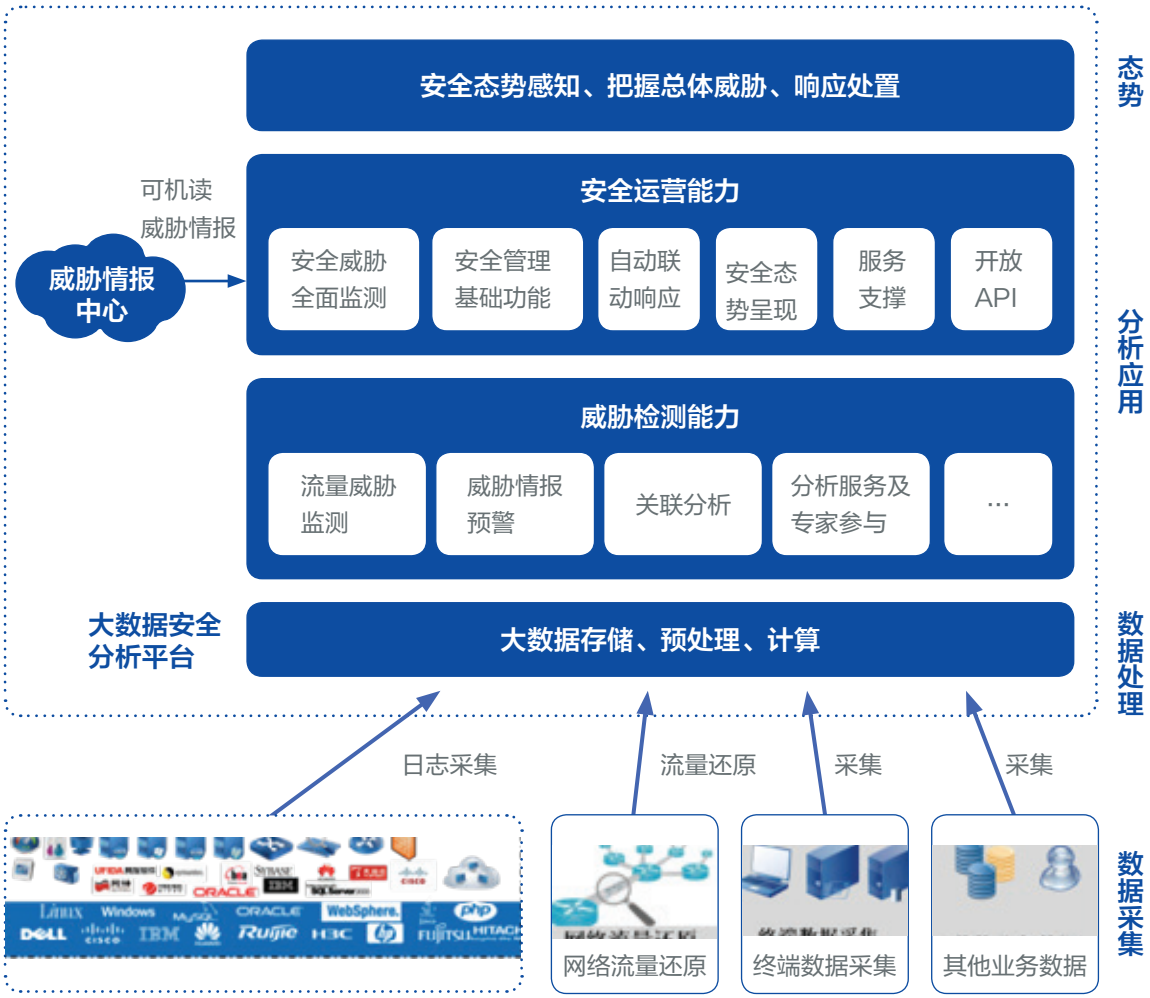


**图 4. 态势感知与安全运营平台功能架构**

### 1.3.3 态势感知应用现状

在国内过去十多年的各类安全规划中，由于态势感知概念具有比较宽泛的内涵，其几乎与网络安全检测、防护、分析、研判、决策、处置等各种能力和动作都产生关联，所以导致网络安全从业者很容易从自身岗位的视角去理解和实践态势感知。

但无论态势感知作为一种状态、过程、活动还是一个复杂的能力体系，都需要落实到具体的目标和场景，而非单纯宏观全局地整理展示威胁情况。从业界对网络安全的实践来看，以下三种场景[4]中的工作更多地涉及到态势感知能力建设，他们分别是：

1. 赋能企业或其他机构建立防御体系。

2. 赋能监管部门建设监测通报预警能力。

3. 安全厂商对威胁捕获、威胁分析、客户支撑等工作体系的自我建设完善。

目前，态势感知系统大多是提供数据分析结果和全网的安全风险情况，辅助管理者做安全战略决策，并根据最终结果对态势感知的模型进行调整。大数据分析技术与态势感知结合不是特别紧密，深度学习、知识图谱仍有广泛的应用空间。另外，许多已经建设网络安全态势感知系统的单位对网络空间安全态势的整体感知能力有限，无法及时探测深层次的安全威胁，快速发现攻击，更无法实现跨组织的信息共享、协同行动、实施应急响应和威胁反制措施。网络安全态势预测尚不成熟，仍需进一步加强。

[4] 亚历山大·科特（Alexander Kott）著，黄晟 安天研究院 译，《网络空间安全防御与态势感知》

# 02 态势感知发展阶段

## 2.1 态势感知的重要性

目前可以观察到，网络空间的攻击行为呈现“体系化”趋势，攻击阶段越来越多也越来越复杂，因此需要体系化的防御来对决体系化的攻击。

在应对单点威胁的过程中，一些单点防护技术逐渐成型，形成了基础的网络安全产品（例如耳熟能详的安全网关、端点防护、入侵检测、扫描器、虚拟专用网络 VPN 等），这些产品为了应对不同的威胁而产生，而传统的网络安全解决方案往往是从这些类别中抽取一些产品进行搭配组合，但这种堆砌产品的解决方案仅仅是部分解决了防御体系的“能力分工”问题，而无法做到“深度结合、全面覆盖、掌握敌情、协同响应”的工作要求。

Gartner 于 2014 年提出的面向下一代的安全体系，新体系以持续监控和分析为核心，覆盖防御、检测、响应、预测四个维度，可自适应于不同基础架构和业务变化，并能形成统一安全策略应对更加隐秘、专业的高级攻击。其强调防御、检测、响应、预测是一个持续性的过程，而不应当仅仅局限在防御阶段。

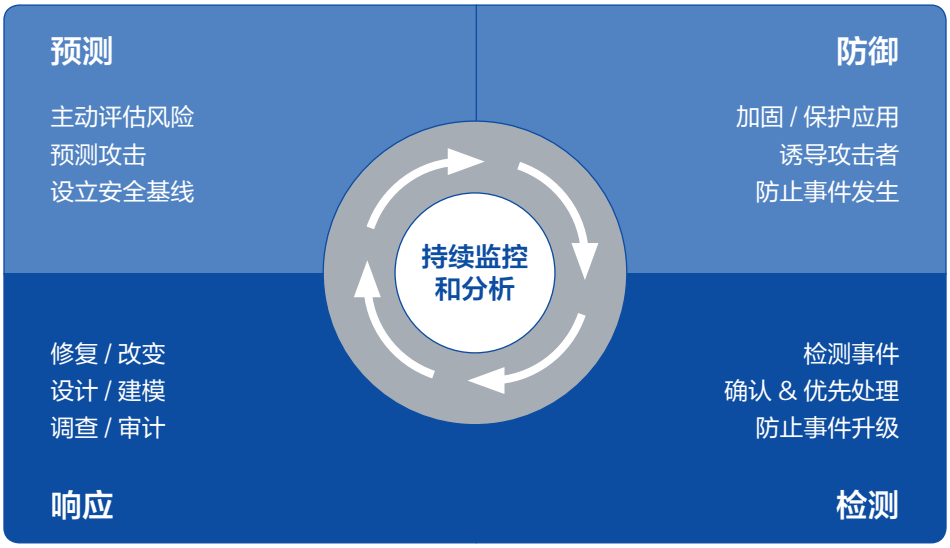


**图 5.Gartner 自适应安全架构**

当前的态势感知和 SOC、安全信息和事件管理（Security Information and Event Management，SIEM）平台等恰好可以满足上述要求，而态势感知已经成为目前大数据安全领域规模增长最迅速的产品。

# 2.2 态势感知 1.0

## *2.2.1 态势感知 1.0 概述*

### 2.2.1.1 态势感知 1.0 定义

态势感知 1.0 版本定义从其平台功能特性、技术特点和应用定位等方面来看主要有以下几个特点。

1. 传统安全防御架构中，各类安全产品采用各自的防御规则、告警策略、日志处理和存储在各自的安全产品内，不利于企业了解整体安全风险。因此态势感知平台应运而生，打破安全设备告警功能和日志孤岛，将各类安全设备日志、主机日志、网络日志、Web 日志等采集到统一的日志存储平台，实现了集中存储。

2. 态势感知 1.0 阶段主要以资产为核心，通过获取互联网已公开漏洞信息、恶意 IOC 信标、恶意域名、代理攻击 IP 地址、恶意 Hash 值等信息与资产进行匹配，来呈现组织的安全风险状况。

3. 态势感知1.0阶段视图呈现有限，多以汇总数据和静态呈现为主，采用定期刷新统计数据，主要以统计型、规则型和特征匹配型算法方式为主，分析维度有限，关联分析和智能分析技术较少应用。

4. 态势感知 1.0 阶段主要定位是辅助 IT 管理员或安全管理员进行事件分析、风险可视、告警管理和应急响应处理的集中式安全管理系统。

5. 企业合规性要求越来越严，多数企业对内控工作越来越重视，态势感知 1.0 阶段在系统上增加了产生合规性报告的功能，满足内控和审计方面的要求。

### 2.2.1.2 态势感知 1.0 系统框架

随着企业信息化进程加快，信息化系统和网络每天产生各种安全日志。面对互联网安全形势越来越严峻，需要应对复杂的攻击和威胁。如分布式拒绝攻击（Distributed Denial of Service，DDoS）、命令与控制 C&C 攻击、SQL 注入等安全威胁，这些威胁具有攻击性强、手段多样化的特点。面对这些新的挑战，传统纵深防御架构的安全运维方式已不再满足需要了。参照美军从军事角度提出的态势感知概念，以及 Gartner 于 2014 年提出面向下一代的安全体系概念，从而诞生了早期的 SIM、SIEM 系统雏型，代表性产品有商用的 Splunk、ArcSight 等，以及基于开源架构的 OSSIM（Open Source Security Information Management）态势感知系统，其通用的系统框架和功能如下。

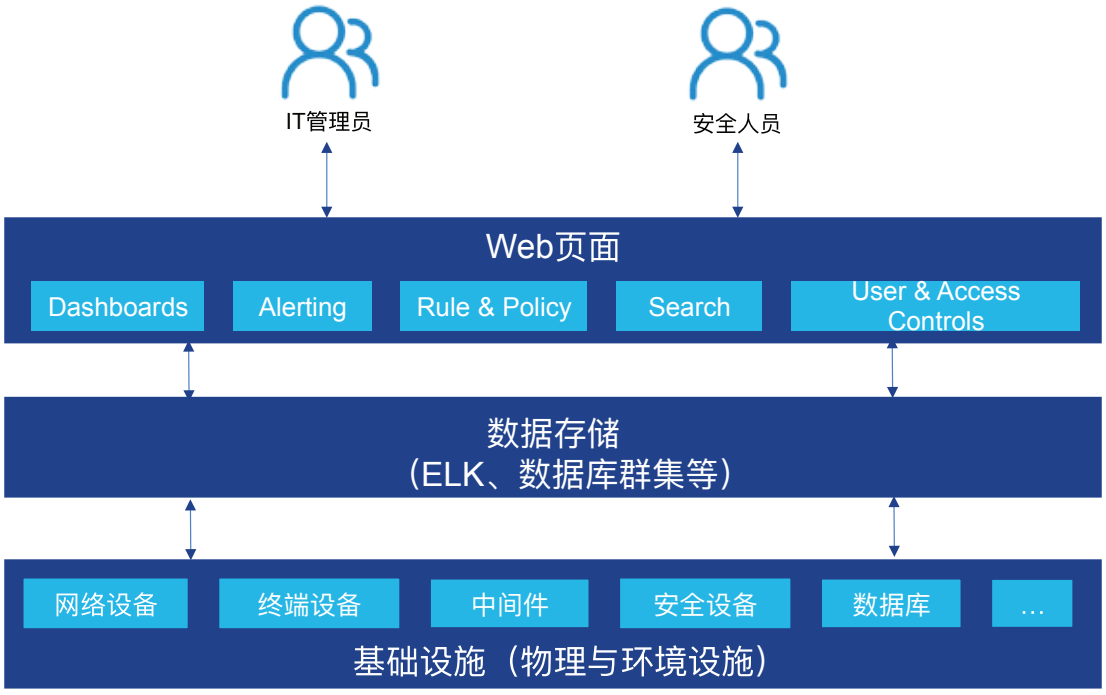


**图 6. 态势感知 1.0 系统框架图**

从系统架构和功能图上看，态势感知 1.0 主要功能集中在数据采集、公开漏洞获取、规则告警、合规报告、事件查询 / 检索、可视化视图、系统用户权限管理、事件告警等功能。

### 2.2.2 态势感知 1.0 技术要素

态势感知 1.0 系统从采集方式上来看，主要有主动式和被动式两种方式，主动式数据采集通过在 Web 应用程序中进行日志埋点和主动上报日志，被动式数据采集方式主要通过在网络关键位置部署数据采集探针和 Agent 代理程式采集。

日志采集的途径主要包含 Syslog、SNMP、ODBC、JDBC、API、FTP、SFTP 等，以及通过已知公开渠道获取的漏洞库信息。比如通过 CVE、国家信息安全漏洞库 CNNVD、漏洞盒子等漏洞平台，通过脚本或爬虫方式周期性地获取漏洞信息，将获取到的所有信息存储于态势感知的日志系统中，早期采用数据库集群技术来支撑日志存储，由于数据库技术的性能和存储容量限制，使得早期的态势感知未能大规模的应用和推广。后来随着大数据技术的发现和发展，Hadoop、HDFS 等技术越来越成熟，促进了态势感知的发展，广泛采用大数据技术平台来存储各种安全日志，大数据平台为其提供了更好的性能和容量。态势感知 1.0 阶段风险展现主要是在管理后台配置好视图更新的周期参数来刷新 Web 页面上的数据。采用周期性地执行指令、定时任务或脚本与已配置好的告警规则进行匹配，以资产为中心，统计事件发生的次数达到阈值而进行告警。其展示相对来说较为简单，通过定期提取汇总数据在 Web 页面上展现风险视图。由于态势感知早期是一个辅助的信息安全事件管理系统，用于事后事件调查，仅提供了用于事件查询和检索的入口，方便企业在发生信息安全事件时调查和查询安全日志。通过针对不同的安全日志表建立数据索引表，以加快安全日志查询和检索的速度。随着态势感知推广到企业部门进行实际应用，此时不同部门使用权限不同，权限管理由一个管理员发展成可配置的多种不同权限管理，多级分类授权，再到后来为简化管理任务，平衡安全与效率后多数态势感知产品加入了基于角色的权限访问控制（Role-Based Access Control，RBAC）管理功能。

### 2.2.3 态势感知 1.0 改进方向

随着互联网、通信和高科技技术的高速发展，大数据技术、4G/5G 技术、虚拟化 / 云计算技术和人工智能技术应用越来越广泛应用，给态势感知的发展带来了机会和挑战。使得态势感知可以用更好的技术进行支撑，例如采用大数据技术可以有效地支持海量的安全日志存储，可以更好的对安全日志进行使用、管理和挖掘。随着大带宽骨干网快速建设，可以提供更快的通路来远程存储安全日志，使分布式计算和存储成为可能。人工智能技术的发展可以为态势感知提供更丰富的分析方式和风险预测的模型。云计算技术的发展和成熟，可以为态势感知提供更具弹性和稳定的架构。给态势感知带来的挑战主要有（1）在 All in Cloud 云计算大环境中，虚拟主机之间或容器间访问的东西向流量获取将更加困难。（2）随着软件定义网络（Software Defined Network，SDN）技术在云环境下的应用，带有 VxLAN 标签的网络数据包给安全设备解析数据包带来了不少的挑战。（3）多租户环境下，区分租户的流量和安全日志给整个态势感知系统带来了技术上的新挑战。（4）在业务上云大趋势下，企业担心数据传输安全性，大多数采用加密传输协议，如使用 SSL 协议，这给态势感知获取加密流量带来了困难，为此催生了 EDR 和用户实体行为分析（User and Entity Behavior Analytics，UEBA）技术诞生，得以从终端采集安全日志和流量。

随着态势感知系统的广泛应用，使其从原来辅助进行安全管理的角色，转变成为以态势感知为中心的信息安全运营中心，转变为一个支撑信息安全领域里的安全运营的核心工具和平台。未来态势感知将朝以下几方面进行发展。

1. 融合威胁情报的态势感知平台。融合了内外部威胁情报信息，使态势感知更是如虎添翼，预测的结果更精准，同时分析的维度也得到了扩展和增强。

2. 横纵联合。态势感知与软件定义安全（Software Defined Security,SDSec）平台进行对接，可以实现自动化的策略下发和阻断，有效提升阻断恶意攻击的恶意行为效率。在云计算环境中，成千上万的物理机、虚拟机和容器应用，当发现攻击行为时，手工处理将是不可取的，是一个灾难性的事情，两者有效对接可实现自动化安全策略下发，快速响应信息安全事件，提升事件处置效率。

3. 态势感知可视化功能得到有效加强。随着 Web 技术的发展，采用 HTML5、WebGL、Canvas 组件和 GPU 加速功能相结合，可以实现复杂的图形以及动态图，以及从二维扩展到三维和四维空间，视图呈现力更丰富。新的可视化效率。丰富的视图插件不断集成，更能有效的展示态势感知的能量。

4. 集成运营流程的态势感知将是安全运营的基石。未来态势感知将与安全运营的流程无缝集成，使态势感知更为丰满，有效地支撑安全运营领域，使安全运营领域工作更轻松和有效。安全运营的工作更稳定和高效，同时也反映企业的安全工作执行的成功。

5. 新技术不断融入态势感知，丰富态势感知的应用领域和展现能力。大数据和人工智能技术的融入，使得态势感知在数据处理和应用方面场景更为丰富，而且智能分析和关联分析的维度得到扩展，大数据算法和人工智能模型有效弥补早期基于统计、规则、特征型态势感知系统的不足，降低了“误报率”和“漏报率”，使态势感知预测结果更具参考性和价值，从而提升态势感知在企业和安全行业的地位。

# 2.3 态势感知 2.0

## *2.3.1 态势感知 2.0 概述*

### 2.3.1.1 态势感知 2.0 定义

态势感知 2.0 将在 1.0 基础上，扩展大数据技术、人工智能技术和威胁情报，加入协作和联动的接口，集成安全运营流程功能。成为完整的安全运营核心支撑平台。其主要特征有：

1. 在数据采集阶段，态势感知 2.0 将要求安全厂商提供 API 接口与云计算环境和 SDN 网络进行对接，突破 VxLAN 技术限制，使得安全设备数据解析和安全日志理解更深入，同时通过在 Hypervisor 层安装 Agent 代理程序采集虚拟机和容器的东西向流量。与此同时还会广泛部署 NTA 网络流量分析设备对流量

进行深度分析和应用。会应用 EDR 和 UEBA 技术从终端收集行为日志，突破加密流量解析的难题。同时将提供更为丰富的接口和日志格式，广泛支持市面上的各种设备日志收集。

2. 态势感知与威胁情报深度集成，提升态势预测的精度，增加了暗网交易信息、安全通告、漏洞库、地理信息、信誉库等威胁情报信息，使安全阻断网络策略更准确。

3. 态势感知与大数据分析和人工智能技术的强强联合，丰富数据分析能力和维度，智能分析模型很好的解决了基于规则和特征型策略所产生的漏报和误报问题，将态势感知技术从辅助安全防御领域，扩展到业务风险控制领域。

4. 态势感知持续深耕安全领域，把技术 + 流程 + 人员有机地结合，成为支撑一个企业安全领域不可或缺的平台。构建和使用态势感知对提升企业信息安全水平有重要的意义，使企业的信息安全风险了然于胸，借助态势感知预测信息更好地实现风险预警、监控分析、响应处理、持续改进等全流程管理。

5. 态势感知将提供与内部管控平台、外部行业、协会、单位和组织进行对接，互惠互利、共享和获取风险态势信息。促进整个互联网大环境健康、有序和安全地发展。

### 2.3.1.2 态势感知 2.0 系统框架

态势感知 2.0 在 1.0 的基础上，从概念上更为清晰了，吸收 PPDR[5] 安全模型 ，同时也借鉴 Gartner 自适应安全防御理念，在获取、理解、评估和预测的基础上，增加了行动环节。使整个态势感知 2.0 更为完整，更好的支撑安全运营领域的应用。

通过在网络、中间件、主机等设备上部署探针和日志收集程序，获取基础设施、安全设施、网络和应用系统等相关的日志信息。将获取到的信息使用大数据技术存储到大数据日志平台，同时将资产信息、安全扫描结果、威胁情报等信息一并存储到大数据平台，利用规则引擎和智能分析模型对大数据仓库的数据进行统计、分析和挖掘，结合历史的基线数据与分析结果一起输出给到 Dashboards 视图和风险态势视图，运营人员通过监控告警或预测信息，即可全面了解安全风险，识别到安全风险即可生成工作流任务工单，按照企业事件管理流程，协调各责任方进行快速处置。在处置过程中，可通过软件定义安全（Software Defined Security，SDSec）平台与安全设备、系统或安全管理平台进行联动，自动下发拦截和阻断策略。态势感知平台上分析和预测的结果可以按要求生成合规报告，也可以通过第三方接口输出给行业共享与系统对接，让整个态势感知平台服务于更多的行业和应用场景。

[5] 在 Gartner 2017 年发布的《应用保护市场指南》报告中提出并获业界主流安全企业和研究机构认可的 PPDR 安全防护模型，是由 Predict（预测）、Prevent（防护）、Detect（检测）、Response（响应）四个阶段组成的新 PPDR 闭环安全防护模型。这种安全模型在不同阶段引入威胁情报、大数据分析等新技术和服务，旨在构建一个能进行持续性威胁响应、智能化、协同化的安全防护体系。

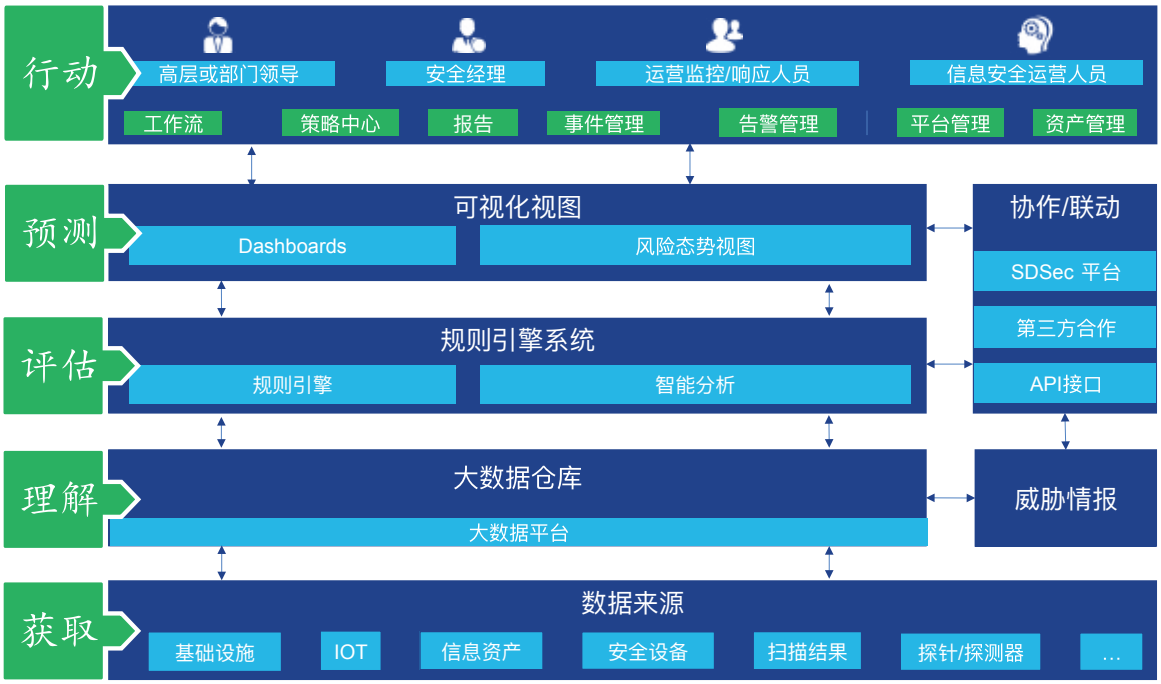


**图 7. 态势感知 2.0 系统框架图**

## *2.3.2 态势感知 2.0 技术要素*

态势感知 2.0 平台在技术要素层，相较 1.0 更为丰富和更具先进性，融入了大数据技术、人工智能技术、云安全技术、自动化防御技术、威胁情报等等。使整个态势感知 2.0 平台适用性更为广泛，服务领域也逐渐增多，同时也促进了安全行业的发展和进步。融入的技术有：

1. 在获取层融入的新技术有 VxLAN 和东西向流量获取技术，在 All in Cloud 的大环境下，云计算平台使用的网络相较传统 IDC 网络结构已发生了根本性的变化。广泛采用了先进的 SDN 技术，传统 IDC 环境下南北向访问流量占 80%，而东西向访问流量占 20%，因此在核心交换机上采集即可满足数据分析的需求。而在 All in Cloud 的环境下，访问流量走向则是东西向流量偏多，南北向流量相对偏少。只在核心交换机采集流量数据就无法满足态势感知的需要。因此在充分分析南北向流量和路径后，有针对性地选择在关键位置部署流量采集探针，同时采集虚拟主机层东西向流量来满足态势感知要求。另外针对物联网（Internet of Things，IoT）技术的发展，支持多协议和兼容将是一大趋势，且大多数 IoT 设备采用无线通信技术，在这一环境下采集数据将是一个挑战。

2. 在理解层融入 Hadoop、Storm、Spark、Flume、Kafka、Hive、Hbase 等新兴大数据技术，用来对日志进行处理、分析、存储和挖掘等，例如采用 Storm 对数据流进行实时处理，可以满足近乎实时的风险发现，相较以前离线数据分析技术，可有效缩短安全预警时效。采用了大数据平台后，有效地提升了数据分析效率，可以在短时间内对大批量数据进行分析和比对，有效发现潜在安全风险和实现提前预测风险。

3. 评估层在统计、规则和特征型的规则上融入数据挖掘、关联分析、智能分析模型，从数据仓库中收集的安全设备日志、埋点日志、网络日志、应用日志、终端日志以及第三方的威胁情报数据等。收集到的信息和安全事件通过检测分析引擎统计分析、关联分析、模式分析、机器学习发现高优先级安全事件，将发现的高优先级事件反馈到运营系统中，同时发现的高优先级安全事件将存储到数据样本库、知识库（案例库）中，便于后期的溯源和分析。


**图 8. 风险发现架构图**

（1）关联分析模型

关联模型通过实时关联技术过滤事件，在大量安全事件（甚至是误报事件）中提取有用的信息。例如登录异常，漏洞利用、蠕虫活动、网络入侵、主机失陷等，关联分析模型主要包括以下类型：

- 基于威胁情报的关联：关联主要集中在 IP、域名、URL、文件 MD5 等相关字段。判断用户、设备是否有异常外联以及主机失陷。
- 基于用户的关联：用户身份与访问记录、登录时间、相关资产进行关联分析，判断用户是否存在访问、登陆、下载等异常行为。
- 基于漏洞的关联：漏洞扫描数据与实时安全事件数据进行关联分析，减少假阳性，判断问题主机是否真的打开了一个端口、是否容易遭到攻击或感染病毒等。

- 基于端口的关联：开放端口的数据与防火墙数据进行关联分析，帮助检测攻击者何时尝试访问系统端口或不存在的服务，从而发现“慢速”或“低”类别的攻击。
- 基于安全事件的关联：安全设备告警事件之间进行实时关联分析，减少事件误报，提高告警准确率。
- 基于统计的关联：对每个类别的事件设定合理的阈值，当超过阈值可以产生一个更高级别的安全事件，同时与资产或其他安全事件进行关联，判断某个安全事件造成的影响和后果。

（2）机器学习模型

机器学习主要是使用算法和统计方法创建能够学习的系统。系统可以从采集的数据中学习，形成一个具有相关特征的分析模型。通过模型训练，完成 IP 非正常访问、账户安全、XSS 攻击（跨站脚本攻击），SQL 注入攻击、JavaScript 脚本注入等威胁的检测任务。

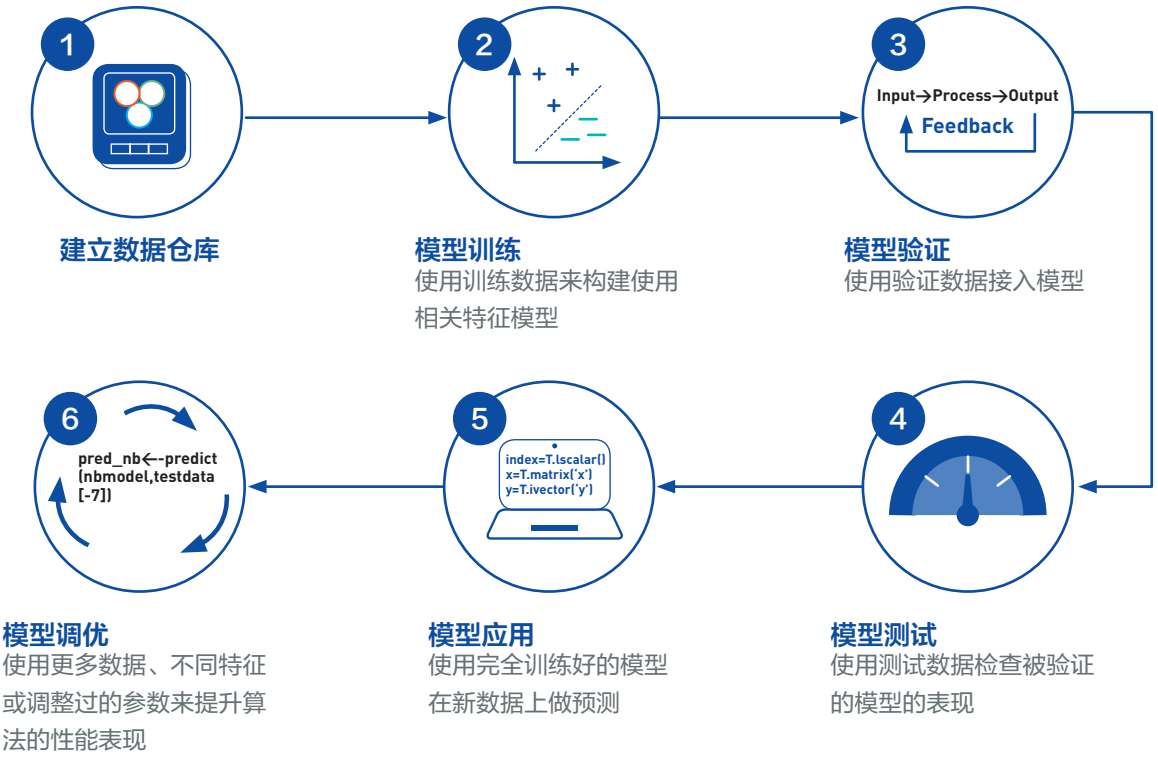


**图 9. 机器学习模型流程图**

（3）攻击回溯分析模型

通过对收集的数据和安全事件分析，从恶意程序感染、异常连接、C&C、传播、数据泄露等维度检测未知威胁。当攻击和规则模型关联后，自动从知识库调用相关知识信息，包括影响主机、影响用户、root 事件、连接和所有行为的时间轴轨迹，作为辅助参考。同时取证结果收入数据样本库、知识库（案例库）。

（4）用户行为分析模型

以部门、个人、资产、资产群等为单位建立多维度行为基线，利用统计、特征、机器学习算法和预定义规则学习每个用户和设备的正常行为基线，通过关联分析和概率计算，计算用户异常分值以便及时发现异常的用户、恶意的内部用户和攻击者。

（5）场景分析模型

场景分析主要依据攻防、渗透经验和大数据分析技术检测网络中的威胁。解决了规则判定时，无法确定具体阈值的问题，根据企业组织中的网络特点和经验判断异常行为。常用场景如下（常用场景分析方法）：

- 创建非管理员用户后的权限升级，非管理员用户一般不会将其权限提升到管理员级别，或其他高级用户级别。
- 文件非授权访问，在很接近的时间内多次尝试访问用户没有权限的共享文件 / 目录。
- DNS 隐蔽隧道，通过数据包关键字段异常的编码监测，支持如下的 DNS 隐秘隧道发现：通过超长域名信息传递数据、通过 txt 请求传递数据、通过 AAAA 记录传递数据等。
- 数据泄漏，VPN 用户在工作时间外登录并向外网传输数兆字节或更多（VPN 连接期间）数据。
- 蠕虫 / 木马 / 恶意软件攻击，网络上一台主机开始攻击或探查网络上其他主机。
- 高风险主机检测分析，通过 DNS 解析行为分析服务器或终端的异常行为。可以确认已知、未知的恶意软件、APT 攻击以及实时监测内部的威胁。
- DNS 服务器发现，采集 DNS 解析过程的 server 信息，对不是白名单范围内的 server 解析行为进行监测预警

4. 在预测层会融入热力图、地理信息、威胁指数等元素，通过与资产、事件、弱点、威胁、风险及告警相关联分析，产生可视化的预测视图。使用可视化技术，将原本碎片化、零散化的行为告警、安全态势、资产管理等智能综合分析展现，形成多维度的安全态势感知展示，帮助安全运营人员及时理解及定位问题。

（1）整体威胁态势

通过风险计算模型，综合考虑资产的价值、脆弱性和威胁，按高危、中危、低危安全级别分类统计。同时通过中国地图以热力图形式展现资产的地理位置、个数和威胁指数；通过世界地图热力图查看攻击源，计算整体业务安全风险值，计算发起最多攻击次数的源 IP 列表，以雷达图显示最近的攻击类型，最近的攻击源分析。

（2）业务资产风险态势

对管理对象划分安全域，并进行资产化管理，可以自定义监控区域。提供基于拓扑的监控视力，可以按图形化拓扑模式显示资产，通过视图可直接查看该资产的状态、事件、弱点、威胁、风险及告警信息。

（3）外部攻击态势

利用时序图实时展示安全攻击事件数量，并按照攻击类型、受影响的 IP，受攻击的专业公司展示安全攻击事件，同时实时滚动显示最近攻击事件。

（4）内部攻击态势

内部安全态势展示已发现的安全事件，能够按照时间段以木马蠕虫、漏洞、流量、恶意软件为视角，进行安全事件的展示。从告警、处置、资产、日志、系统维护、类型、分布多个维度实时进行安全事件统计分析，并以 2D/3D、柱图、饼图、堆积图等形式进行可视化的展示。

（5）数据安全态势

数据安全态势 , 对企业组织的数据进行全面监测，与用户行为模型结合，依据相应业务场景，发现数据的不正当访问与调用、数据的异常流动等行为，从类型、用户、资产等维度在统一视图中展示。

（6）审计视图

运营人员可以根据内置或者自定义的审计策略，从事件的任意维度实时观测安全事件的走向，并可以进行事件调查、取证，并进行事件行为分析和来源定位。

5. 在行动层融入流行的工作流引擎，如 JBPM、Activiti、OSWorkflow 工作流引擎使已知风险处理更高效和可追溯。同时融入告警和事件管理使整个安全风险处置形成一个闭环。配合在行动层与 SDSec 平台进行对接功能，可以提高在风险处置环节的效率。

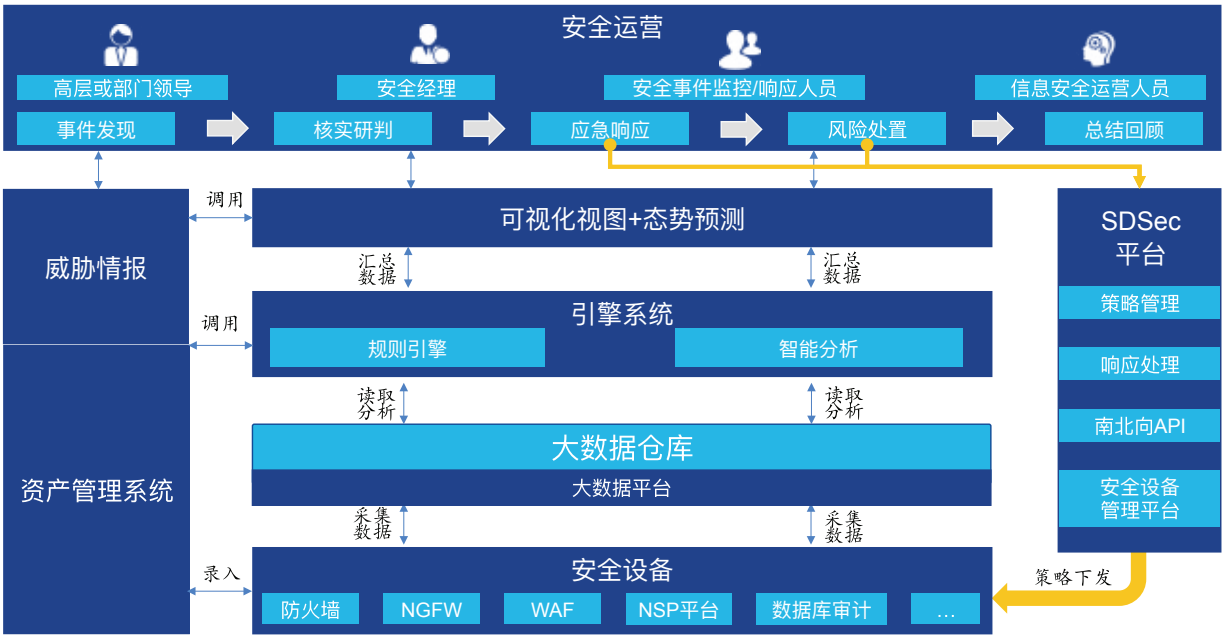


**图 10. 态势感知 2.0 平台与 SDSec 平台对接实现自动化策略下发逻辑图**

## *2.3.3 态势感知 2.0 与智能安全运营*

安全运营涉及面广，对技术和人员的依赖更强。而技术和人员又需要相应的平台支撑。只有将三者有机结合，协调发展才能使企业安全运营更加智能。

态势感知 1.0 之前往往都注重安全设施的建设，态势感知系统功能性的建设，而疏于安全运营体系的建设，导致虽然部署了大量的安全设施，但是对安全事件感知能力差，使用功能有限，通常用来作日志查询和事件调查使用，因此安全事件仍然会频发。发展到态势感知 2.0 阶段，在态势感知 1.0 版本的基础上，融合技术和人员，加入更多自动化和智能技术，将其作为智能安全运营很重要的部分进行体系化建设和运作。先进的态势感知 2.0 平台作为安全运营体系的核心工具，在风险预警、威胁分析、感知呈现、响应处置、策略管理、取证溯源方面发挥更大的效用。同时态势感知还需要具备相关能力的安全运营人员。如运维人员、安全分析人员、安全专家、安全策略管理和安全研究人员以及智能化、自动化、可重用的处置流程。三者合一则建成有效的安全运营体系。如下图所示意：

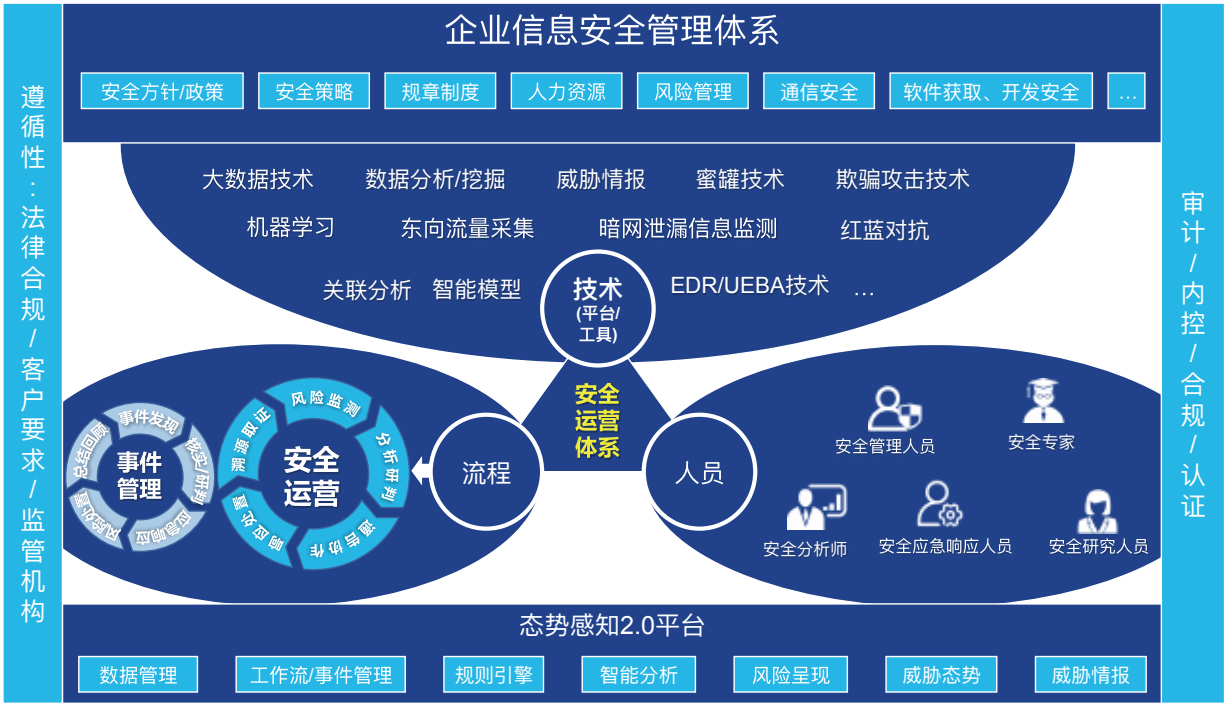


**图 11. 态势感知 2.0 平台支撑智能安全运营框架图**

态势感知 2.0 平台作为智能安全运营的载体，在风险监测、分析研判、通知协作、响应处置、溯源取证等各方面进行了增强，同时融入了当前流行的技术和平台作为支撑，如大数据技术、东西向流量采集技术，EDR 终端检测响应技术、机器学习、欺骗攻击技术等。同时态势感知 2.0 平台与 ITIL（Information Technology Infrastructure Library，ITIL）理念与信息安全管理标准相融合，将安全运营划分为不同角色，如安全管理人员、安全专家、安全运维、安全分析师、安全应急响应人员、安全研究人员等，在集成了安全事件管理全生命周期的流程中，通过工作流程将其串联起来，使安全运营流程更加规范和有序。

# 03

# 态势感知在金融行业的应用

在全球金融信息化快速发展的同时，金融风险也在不断产生和恶化，互联网每天新增的恶意代码和恶意网页都在数十万量级，还出现了 WannaCry[6]、Petya[7] 等威胁巨大的新型勒索病毒，这些安全威胁和传统病毒相比，变种更多，更新更快，严重威胁着金融用户的安全，给金融行业带来了很大的冲击。其攻击成本低、攻击收益大，导致广大金融机构容易成为不法分子眼中的“肥羊”，传统 SIEM 和 SOC 缺少具有高价值的元数据和具有金融行业特性的威胁情报支持，加之安全攻防信息的不对等，因此决策者很难根据当前网络安全环境的变化，做出恰当的决策。

2017 年 6 月 1 日国家正式颁布《网络安全法》，标志着中国在网络安全治理领域有了第一部有法可依的法律。习主席在 4.19 的讲话中提到要 “加快构建关键信息基础设施安全保障体系，全天候全方位感知网

[6]WannaCry（又叫 Wanna Decryptor），一种“蠕虫式”的勒索病毒软件，大小 3.3MB，由不法分子利用 NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播。WannaCry 勒索病毒全球大爆发，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分 Windows 操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

[7]Petya 是 2017 年 3 月出现的一种变体勒索软件，是一种类似于“WannaCry”的新勒索病毒，它的破坏性比传统的勒索软件更大，现已导致俄罗斯石油公司（RosneftPJSC）和丹麦 A.P. 穆勒 - 马士基有限公司等在内的多家大型企业被攻击，而且乌克兰的政府系统也遭到了该病毒的袭击。并已确认有国内企业中招。

络安全态势，增强网络安全防御能力和威慑能力”。为此，各级政府机关和行业采取了一系列增强信息安全的政策和措施，给态势感知技术的发展和应用创造了良好的外部环境。为促进金融领域信息安全发展和交流，就态势感知平台的应用列举以下三方面进行简述，抛砖引玉。

## 3.1 态势感知增强安全防御体系

在信息安全领域，综观整个发展过程，起初是从防病毒和恶意脚本开始，再到划边界垒城堡，再发展到边界消失。在全世界网络大互联的环境中，“云”“管”“端”的安全防御方案成为当前主流的防御思想。面对着复杂多变的网络互联环境，更加需要能洞悉战场瞬息万变的风险态势，从而实现高效地决策与响应行动。因此态势感知从配角的地位迅速转换为不可获缺的主导地位，其地位的提升主要有三个方面。其一，外部大环境不断恶化，威胁层出不穷，2018 年 11-12 月，20 家境内云遭受 DDoS 攻击次数占境内目标被攻击次数的 27702 次；其二，云计算技术不断成熟、大数据技术和机器学习技术的快速发展，以及威胁情报领域的兴起，给态势感知发展提供更好的动力和能量；其三，面对风险威胁要求安全从业者有更快速的响应，而传统 SIEM 和 SOC 侧重于以资产为核心的风险发现和系统功能性建设，仅覆盖事后安全事件调查。态势感知 2.0 平台一方面强化了 SIEM 的日志整合、分析、检索能力，同时与 SOC 整合，将流程、人员和技术（平台 + 工具）有机的融合，实现事前风险预警、事中风险处理和事后追溯取证。

1. 态势感知全面呈现组织的安全风险态势。整合了网络、各类日志和威胁情报的态势感知平台，通过自动化关联分析，更高效发现本地威胁和异常。采用大数据和智能分析技术将安全日志数据与情报进行关联，准确的发现失陷的信息资产。利用网络绘测技术可对全网信息资产进行全路径绘制，清晰的展示与某个资产相关联的风险及流量信息，标识通信的健康性。同时对收集的攻击数据与外部数据进行综合分析，可以刻画出攻击者的画像。通过对终端行为的全链路数据进行建模分析，可以预测员工的行为。例如发现员工近期有大量文件或机密信息访问行为时，可以预测员工即将为离职而准备。同时根据定义的规则集、智能分析模型可以生成不同的风险态势视图。如综合风险态势、网络入侵态势、漏洞态势、流量态势、木马蠕虫态势、攻击地图等等。通过自定义的视图满足各种不同人员的需求，方便各使用方快速做出决策和响应。

2. 态势感知增强安全防御体系。态势感知 2.0 平台的建设，将增强金融安全防御体系，具体表现形式有：

（1）态势感知对风险预测的结果可以为传统安全设备提供防御指导，为其提供风险预警，提前规划和制订安全措施应对即将到来的攻击威胁。

（2）态势感知平台与威胁情报平台进行融合，提升了风险研判的准确性，相比以往在安全设备部署策略后会存在“误杀”和“漏报”现象有了很大的改观。

（3）态势感知打造了一个统一支撑安全运营的平台，改变以往多套平台、多套系统林立的局面，提升了运营的效率。

3. 态势感知平台提高应急响应效率。态势感知 2.0 平台集成了 workflow 功能，构建了事件管理的全生命周期流程，在平台上呈现出来的风险，经安全分析师深入分析和专家判断后可直接按事件流程启动应急响应程序进行快速处置，提高了应急响应的效率，同时所有状态和事件处置记录可在平台存档和展现，更好的满足合规要求。

## 3.2 态势感知保障业务安全

随着互联网技术的发展和业务上云的大趋势，安全防御的边界已消失。业务所面临的风险将更多，每逢重大促销、发布会、抽奖、充值优惠、优惠券发放等活动，将是黑客攻击的最频繁的时期。2019 年 1 月某电商平台推出优惠券活动，因平台出现一个重大 bug，该漏洞被羊毛党发现并迅速在网上进行传播，导致该平台损失巨大。而态势感知 2.0 平台可通过与应用系统日志埋点，针对用户操作行为进行的监控分析，发现薅羊毛用户，创建风险分析模型，可以有效预防类似事件发生。同时可利用态势感知平台对运维人员操作行为进行分析，通过与历史基线对比和重点行为的定义进行分析，可发现违规行为和数据泄密事件。通过对访问敏感信息的监测与分析，可发现窃取用户隐私的行为，保障用户数据安全。态势感知平台在业务领域的应用场景很多，收集到充足的数据，有具体的业务应用场景，均可以利用态势感知平台的能力来进行风险方面的分析与预测。

## 3.3 态势感知促进安全运营智能化

态势感知平台已成为安全运营领域最主要、最主流的建设方式，除了态势感知集成安全运营流程、威胁情报等重要要素之外，同时还会集成 SDSec 平台，该平台可以承载对安全设备的统一策略管理、策略全自动下发等工作。各种安全产品的安全规则集不同，当组织有成千上万个安全设备时，手工配置阻断策略，这一工作将变得更恐怖。另外随着云计算的发展，采用 SDN 技术的云网络，设置安全策略将更加困难。通过与 SDSec 平台对接这一工作变得更为简单，只需要将阻断策略的要素推送给 SDSec 平台，即可实现在多种安全设备上自动下发配置策略，配置完成后将结果反馈到态势视图中，使得这一切变得更简单、更自动化和更智能。

# 04 总结

本蓝皮书通过详细阐述态势感知概念、国内外现状、态势感知 1.0 到态势感知 2.0 和其在金融行业的应用等内容，向读者展示了目前态势感知发展的全貌。面对传统安全防御体系失效的风险，态势感知能够做到全方位感知网络安全威胁态势、洞悉网络及应用运行健康状态、通过全流量分析技术实现完整的网络攻击溯源取证，帮助安全人员采取针对性响应处置措施。相信在未来，态势感知将得到更加广泛的应用，为保障网络信息安全发挥出更大效能。

## 大数据协同安全技术国家工程实验室 – 金融行业安全研究中心

大数据协同安全技术国家工程实验室是国家发改委批复成立的我国大数据安全领域的第一个国家级科研机构。金融行业安全研究中心在此基础上成立，由平安金融安全研究院作为实际承担单位，着重关注新金融环境下的信息安全建设和国家金融大数据安全。通过战略研究、人才培养、技术开发、成果转化、产学研结合等方式，整合国家、行业、高校、研究院等优秀资源，推动金融科技网络安全技术发展，助力增强国家金融科技及网络安全掌控能力。

## 平安金融安全研究院

由平安科技成立的业界首家综合性的金融安全研究及创新机构，以倡导和共建“科技 + 安全 + 生态”的科技创新及应用体系为核心，结合“政、产、学、研、金、介、用”生态体系，致力于构建“金融安全 3.0”时代的安全生态圈，在金融关键信息基础设施安全、金融科技安全、金融业务安全风控三方持续创新实践，打造金融安全领先品牌，并努力推动和引领国家网信事业发展。

## 中国信息通信研究院

始建于1957年，是工业和信息化部直属科研事业单位，多年来秉持“国家高端专业智库 产业创新发展平台”的发展定位和“厚德实学 兴业致远”的核心文化价值理念，在行业发展的重大战略、规划、政策、标准和测试认证等方面发挥了有力支撑作用，为我国通信业跨越式发展和信息技术产业创新壮大起到了重要推动作用。