下一代安全概念及特性分析

NSFOCUS

目录

一. 引言

近年来，网络攻防环境正在发生快速的变化。首先，攻击者的动机已不再是为了技术突破，而是更具功利性。受政治、经济、意识形态等多方面的影响，攻击者正在形成拥有强大技术、经济实力的有组织攻击团体。其次，攻击者的目标选择更明确、攻击更为专注。第三，针对 CII 及工业控制系统的攻击事件的日益频繁，也说明了网络攻防战场正在从通用网络向专用的网络逐步扩展。此外，云计算、虚拟化、大数据、移动互联网等新 IT 应用技术的快速发展，在为用户提供更为灵活、实用的 IT 应用及服务模式的同时，也不可避免的引入新的安全问题并对当前的信息安全防护能力提出新的挑战。

为了应对这些挑战，业内提出了下一代安全的概念。但对于什么是下一代安全？下一代安全具有什么特征？却没有一个明确的定义和论证。绿盟科技提出，下一代安全是指**为应对因新的安全威胁与 IT 技术发展，而造成的安全技术水平及安全服务能力严重不足的问题（挑战），所提出的新安全理念、技术、产品以及服务模式等对策的集合。**

绿盟科技还从下一代安全的重点发展趋势（安全运营、安全智能、云及虚拟化）及其相关特性的分析与讨论中，归纳总结出了下一代安全的 7 个主要特性。这些重要信息是依据绿盟科技的下一代安全研究模型（即下一代安全研究的关联角色模型与下一代安全研究的分析模型），通过对攻防环境的变化及新型威胁特征的综合分析和归纳推导而得到的，能够体现当前信息安全领域的主要发展趋势。这对于大家规划下一代安全产品架构，应对未来安全挑战，应具有较高的参考价值。

本文将绿盟科技关于下一代安全的研究内容分享给大家，欢迎大家与我们交流及探讨下一代安全！同时，绿盟科技下一代安全研究也在持续进行中，欢迎大家关注后续进展。

二. 下一代安全的研究模型

本章内容着重介绍绿盟科技下一代安全的研究模型，期望在尽可能全面地考虑各种影响因素和实际需求的基础上，通过严格的逻辑推导与归纳分析来保证我们关于下一代安全研究成果的合理性和可信性。

2.1 下一代安全研究的关键角色模型

下一代安全研究的关联角色模型（如图 2-1 所示）的引入是为了研究过程中能够尽可能全面地考虑影响下一代安全的各种变化因素。该模型定义了下一代安全研究所涉及到的五种相关角色：IT 用户、IT 系统提供商、监管机构、攻击者与信息安全厂商。

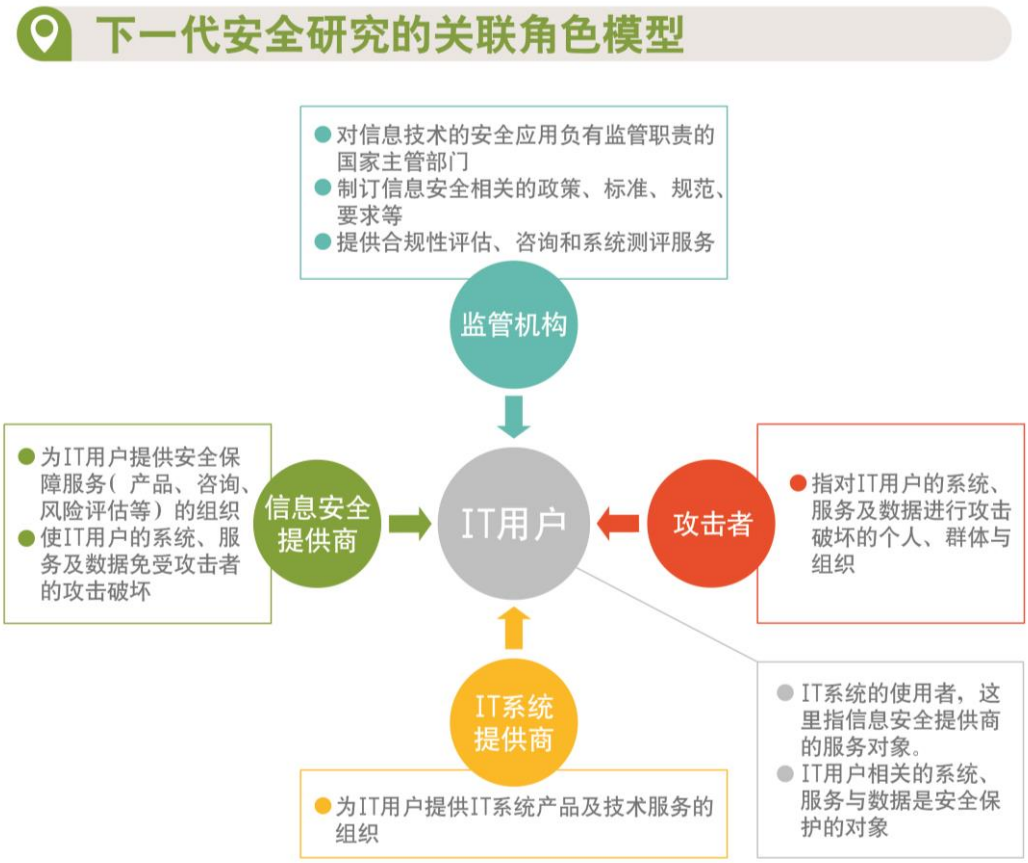

图 2-1　下一代安全研究的关联角色模型

其中，

IT 用户：这里指 IT 系统的拥有者和使用者。IT 用户相关的 IT 系统、业务服务与数据是安全攻击的对象，同时也是信息安全服务的防护对象。

IT 系统提供商：指为 IT 用户提供 IT 系统（软、硬件、网络及业务应用产品）及技术服务的组织。

监管机构：对信息技术的安全应用负有监管职责的国家/行业主管部门。制订信息安全相关的政策、标准、规范、要求等，并提供合规性评估、系统评测及咨询服务等。

攻击者：指对 IT 用户的系统、服务及数据进行攻击破坏的个人、群体与团体组织。

信息安全厂商：为 IT 用户提供安全保障服务（安全产品、安全服务、咨询等）的组织，帮助 IT 用户抵御攻击者的攻击。

由图 2-1 可知，这五种角色是以攻防研究的对象（IT 用户及其 IT 系统）为中心。图中各角色所涉及的技术与服务能力的变化都可能改变 IT 用户系统的安全攻防态势，甚至对被保护的 IT 系统带来新的安全威胁，并对信息安全提供商的技术与服务能力提出新的挑战。因此，为帮助 IT 客户能从容应对未来的安全威胁，我们将基于该模型尽可能全面地了解用户的安全新需求、攻击者的组织能力的变化、IT 最新技术的应用发展趋势以及监管部门的合规性要求，明确当前安全产品及安全服务能力的不足及可能面临的新型威胁。

2.2 下一代安全研究的分析模型

本节提出的下一代安全研究的分析模型，将在上文下一代安全研究的关联角色模型的基础上，明确定义下一代安全研究的逻辑分析流程（如图 2-2 所示）。

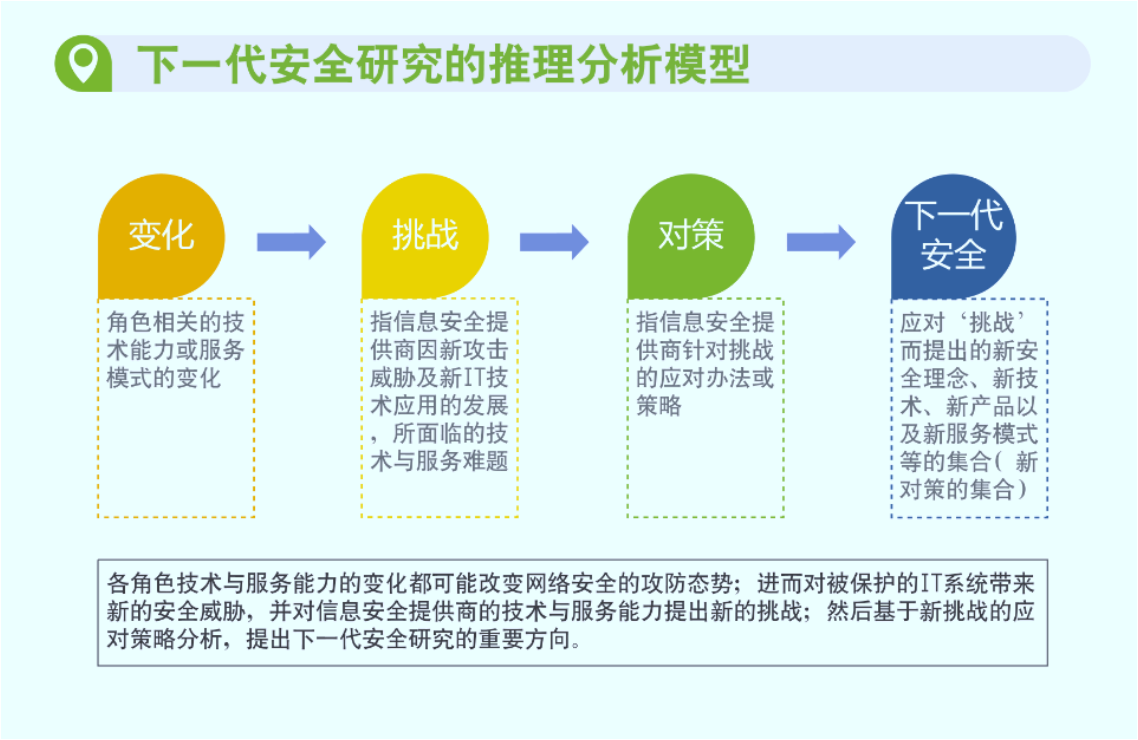

图 2-2　下一代安全的研究分析模型

基于该模型我们可通过分析各角色的技术能力和服务模式的变化，讨论当前 IT 系统所面临的新型安全威胁及对安全服务能力的挑战，提出适当的应对策略并归纳总结出下一代安全的发展趋势和主要特征。

三. 下一代安全的技术发展趋势

依据上文提出的下一代安全研究模型，从攻击者、IT 系统提供商、IT 用户、监管机构以及信息安全提供商等不同的角度，对我们当前所面临的新型安全威胁、安全技术服务能力的变化与挑战进行了详细的分析讨论；提出了应对这些安全威胁及技术挑战的各种对策；进而通过对各种对策的统计、分类与归纳推导，得出了下一代安全的主要发展趋势及研究方向：安全运营、安全智能、云及虚拟化安全、数据安全以及 CII 安全等[1]。

3.1 安全运营

安全运营主要是指关于安全产品互联的体系化防护及新的安全运维服务模式方面的研究。在我们前期的研究工作中，对安全运营这个概念给出了如下定义：

安全运营：维持“闭环”系统正常运行和持续改进的周期性行为的总和，以“安全态势”信息为增速剂，按照“小时级”度量的标准确保交付质量，最终促进客户环境、生产环境和流转环境的持续改善。

通过开放的运营管理平台实现安全产品的互联、全局的安全情报采集与智能分析，能够洞察所管理网络范围内的安全态势，并提供可视化的直观展示；进而基于运营环境的安全态势、结合最佳实践与专家知识以及云安全服务模式，进行快速的智能决策、安全策略分发以及产品规则的智能配置；从而实现针对网络安全威胁的快速响应。

安全情报采集，智能分析、评估与决策，快速响应服务组成的安全闭环的持续、周期运行，将能够实现用户网络安全环境的持续改善。

云安全服务体系、安全产品互联、智能安全配置管理、大数据管理与智能分析等将是安全运营平台需要解决的关键问题或技术，也必将成为下一代安全研究的关注重点，并对当前安全产品提出相应的改进需求。

3.2 安全智能

安全智能主要关注智能信息处理及人工智能技术在信息安全领域的应用。

在现有的网络安全产品中，虽然已采用了一些智能信息处理技术，但多限于一些基本的基于规则或策略的相关处理，诸如安全信息管理系统（SIMS）的报警关联技术，安全检测类产品（入侵检测系统-IDS、入侵防御系统-IPS、防病毒软件-AV 等）与安全评估类产品（漏洞扫描）的基于模式匹配的检测评估技术等等。但安全产品的分散部署、独立管理的现状，使得各种安全信息难以得到共享和综合利用；缺少足够规模的高质量安全数据，是当前网络安全领域走向更进一“智能化”的一个关键瓶颈。

安全运营概念的提出，为安全智能技术的进一步发展提供了良好的空间。开放的安全运营平台可以汇集各种互联安全产品的安全数据（日志、报警等）、监测系统信息、利用蜜罐、蜜网或其他方式获得的安全威胁信息等，从而可以解决安全数据的规模问题。安全运营相关

的核心工作：大规模安全信息的管理、入侵行为的模式挖掘、全局网络安全态势的评估预测、威胁情报分析以及各种自动化配置管理等，都将归属于安全智能的研究范围。

同时，云及虚拟化应用越来越普及，在云中将更加强调各种网络资源的共享。显然，云中安全资源的分配、调度的管理，也离不开对云环境全局安全状态的综合分析与预测；自然安全智能技术的应用，也是必不可少。

综合上述，除 SIMS 的报警关联、IDS/IPS 的模式匹配检测、异常流量检测与清洗之外，安全信誉[2][8]、安全态势感知、威胁评估、安全度量[9]、行为异常检测、自动化配置管理等安全智能的相关概念、理论和技术的发展与应用都将成为下一代安全的重要关注内容。

3.3 云及虚拟化安全

云计算及虚拟化安全将关注重点云服务与虚拟化技术所带来的新安全问题、应对措施以及云与虚拟化技术在安全领域的应用。主要涉及云计算平台的安全性、安全产品的虚拟化、安全服务的云模式等几个方面。

其中，云计算平台的安全性重点关注虚拟机安全、云相关的软硬件系统、网络及应用协议的脆弱性。安全产品的虚拟化则关注使用虚拟机实现安全产品功能、利用 SDN 实现安全产品网络层面的虚拟部署与管理等。至于安全服务的云模式，依据[3]中的观点，当前主要有三种模式：

- 针对用户的安全云（Security Cloud For User）：将云服务和安全功能绑定，打包提供给用户。比如：FireHost 推出的安全虚拟主机。
- 针对用户的云安全（Security For Cloud User）：为使用各种云服务的用户，提供附加的安全解决方案。CipherCloud 的服务可以为用户使用的 Gmail、Amazon、Salesforce、Office365 等在线服务提供统一的内容加密功能。
- 针对云服务商的安全性（Security For Cloud Vendor）：安全厂商的虚拟设备，无缝的接入云服务商的环境中，并作为可选插件提供给最终用户。VMware 的 Rob Randell 曾详细阐述了这一思路的优势和实现步骤[4]。

随着云计算技术、虚拟化技术以及云服务模式在 IT 应用领域的日益成熟，安全产品的部署与服务模式也将发生较大的变化。同时，出于信息安全的体系化防护及安全运营服务的需

要，云及虚拟化技术也为安全运营平台的资源优化配置以及 SaaS 化安全服务奠定了基础。因此，安全云服务以及安全资源的虚拟化，也将是下一代安全的重要特性。

3.4 数据安全

数据安全主要研究以保护网络、系统中的重要数据为目的的各种安全机制。确保数据在其生成、存储、传输、使用以及销毁的整个生命周期中的机密性、完整性与可用性。

以前要保护的数据多限于政府、军队等国家重要部门的机密信息以及企业的商业敏感信息，这就需要重点考虑如何确保数据的机密性、完整性。基于密码技术的数据加密存储、加密传输、认证授权以及各种数据防泄露技术是其研究的重点。

随着互联网、移动通信、云计算及虚拟化技术的发展，在互联网及云环境中，如何确保用户的身份信息、个人隐私信息，甚至是重要的工作数据不被泄露？如何确保大规模用户数据的安全存储、灾备及授权使用？ 如何保证大规模数据的可用性？ 如何确保互联网上信息不被恶意篡改？ 以及互联网舆情与不良信息的管控等等都将成为当前重要的数据安全问题。而这是仅靠密码技术解决不了的。

我们将重点关注：安全运营服务体系中安全信息的安全存储、加密传输与授权使用，安全产品中配置信息的授权管理以及网站监护服务中的网页内容防篡改、挂马检测等。

3.5 CII 安全

CII 安全是指国家关键信息基础设施（CII）重要组成部分的电力、交通、石油化工等国家重要行业的信息系统的安全问题。

近年来，出于政治、军事、意识形态的目的，敌对方有组织攻击团队的“网络战”威胁越来越频繁，在这些攻击活动中，国家关键信息基础设施、重要行业的工业控制系统、重要的信息系统都将会成为主要的攻击目标，要么破坏其可用性、要么窃取敏感数据，甚至是掌控舆论影响社会稳定。因此，加强 CII 安全防护极其重要，已成为国家安全战略的重要内容；也必然成为未来信息安全领域的研究热点与重要的业务增长点[5]。

近几年针对 CII 的攻击事件表明，这些攻击多采用有组织的、目的性很强的新型攻击手段（例如，高级可持续威胁——Advanced Persistent Threat，简称 APT）。为达成 APT 攻击

目的，需要长时间地集中高端人才和技术，需要具备无孔不入的情报收集能力，往往需要掌握最新的 0-day 漏洞，拥有能够规避当时检测工具的传播和控制程序，以及利用所掌握资源快速展开连续行动的组织力和行动力。显然这样的攻击不是能够依靠单一技术实现防范和检测的，需要多层面安全措施的综合防御。这必然对安全厂商及相关研究机构的安全服务能力提出了更高的挑战。

而电力、交通、石油化工等国家重要行业的信息系统对安全要求最高的是其生产系统相关的工业控制系统，虽然这些工业控制系统相对独立、且多采用专有的通信协议；但这些因素也导致了系统在设计时对安全性考虑不足。随着工业控制系统的智能化发展（比如，智能电网）以及互联网技术的应用，工业控制网络的封闭性也逐渐被打破，再加上敌对方的有目的攻击。CII 系统中的工业控制系统安全也将是下一代安全的研究热点。在业内也必将出现针对工业控制系统安全的下一代安全产品。

目前我们在工业控制系统安全研究方面已有一定的研究成果（参考文献[5]），将持续对其保持密切关注。此外，智能终端和移动互联网的快速发展，也使其相关的安全问题成为当前安全研究的热点之一。

综上所述，安全运营、安全智能、云及虚拟化安全、数据安全、CII 安全以及移动互联网安全等领域的相关概念、技术与服务模式，都将是下一代安全研究的重点内容，并不可避免地影响下一代安全产品的功能和产品形态。

四. 下一代安全的特性分析

本章将在继承和发挥绿盟科技自有技术与产品优势的基础上，重点选择安全运营、安全智能、云及虚拟化安全这三个领域，来详细讨论下一代安全的主要特征。

4.1 安全运营的 NG 特性

依据§3.1 对安全运营概念的定义可知，安全运营过程将是一个集威胁感知、态势评估、快速响应及主动防御为一体的周期性地、能够实现用户网络安全状态持续改善的动态“闭环”控制过程。

安全运营作为下一代安全的重要发展方向，体现其核心思想的主要特性：基于产品协同与智能分析的威胁感知、面向安全态势及资源管理的可视化、基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善闭环，都将成为描述下一代安全概念的重要内容。

1. 基于产品协同与智能分析的威胁感知

1) 特性解析

该特性主要是指通过安全产品互联构成的威胁感知网络，实现网络安全威胁情报（如系统的漏洞及补丁配置信息、报警信息、审计日志等）及其他影响网络或系统安全状态变化的各种因素的信息的快速采集、管理与智能分析（统计、关联、融合、预测等），预测网络或系统安全状况的发展趋势，评估其所面临的安全风险。

2) 典型应用场景

- 安全威胁信息的采集
  - 安全产品（FW、IPS、UTM、WAF、抗拒绝服务攻击系统等）的审计日志/报警信息采集 ；
  - 漏洞扫描、配置核查类产品输出的漏洞、补丁及配置等系统脆弱性信息的采集；
  - 安全产品支持标准的数据接口，以支持安全威胁信息的采集 ；
- 安全威胁信息的智能分析
  - 网络中系统漏洞、补丁及系统配置脆弱性分析 ；
  - 网站挂马及恶意代码监测 ；
  - 网络流量监测；

  等。

2. 面向安全态势及资源管理的可视化

1) 特性解析

该特性主要是指把安全产品产生的各种安全信息（报警、日志、配置等信息）、分析过程、评估数据（安全态势、分析结果等）以及安全产品的系统配置管理、性能管理、策略管理等安全管理功能，通过直观的、便于理解的图表化方式，为用户提供更好的安全产品管理与使用界面，以提高安全产品的易用性。

2) 典型应用场景

- 安全态势的可视化展示 ；
- 安全日志、报警等安全信息的可视化分析与管理；
- 安全产品的配置管理的可视化 ；

等等。

3. 基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善闭环

1) 特性解析

闭环通常用于描述反馈控制系统，指将系统输出量的测量值与所期望的给定值相比较，利用测量值与期望值的偏差对系统进行调节控制，使输出值尽量接近于期望值。

这里主要指安全运营管理平台基于网络安全状态持续改善的闭环运营特性：

- 在安全威胁情报的采集、智能分析及态势评估的基础上，通过洞察网络全局安全态势，及时优化、调整安全防护策略，实现安全威胁的实时发现、快速响应及主动预防。
- 每经过一次完整的闭环周期（威胁感知、态势评估、快速响应、主动预防），都可能有效实现网络状态的改善。

2) 典型应用场景

- 安全运营管理平台的闭环运营
  - 基于威胁感知网络的安全威胁情报汇集 ；
  - 基于安全智能的威胁情报分析、安全态势（威胁、漏洞等）评估及可视化展示 ；
  - 优化安全防护能力。例如，安全规则的在线自动升级、安全策略的快速部署等 。
  - 构建安全服务云。例如，提供最佳安全实践建议与知识的快速分享或在线服务。

此外，在安全产品的功能协同或联动时也会涉及到闭环控制。

4.2 安全智能的 NG 特性

随着安全攻防技术的快速发展，安全产品的智能协同、自动配置；安全信息的融合分析、威胁评估以及入侵攻击的异常行为监测等等都将涉及到智能信息处理技术以及自动化控制技术在安全产品中的具体应用；这都将归属到本文所说的安全智能的范畴。

基于行为模型与安全信誉的异常监测以及面向攻防环境的协同能力，是发现入侵攻击并通过多产品系统实现体系化、综合防御的关键。在入侵攻击技术日益先进、复杂的现在，异常行为检侧与多产品协同能力必将是下一代安全的必备特性。

1. 基于行为模型与安全信誉的异常检测

1) 特性解析

该特性所说的**异常检测**主要是指基于行为及流量模型来发现系统的异常行为。具体过程是首先构建被保护系统中主体(用户、进程等）正常访问系统客体（数据、 系统等）的正常行为基线或网络流量特征模型；检测时通过判断是否违背正常行为基线（或网络流量特征模型）来识别异常行为（或异常网络流量）。

- 这种基于行为模型的异常检测方法可**提高**发现未知安全威胁、系统未声明功能及应对 0-day 攻击的能力。
- 利用安全信誉技术，可帮助提高产品的入侵检测及威胁评估的效率。

安全领域的信誉可指对网络中指定主体行为的长期表现及其被关注属性内容不具有危害性的可信性评估。 诸如：IP 信誉、WEB 信誉、 ID 信誉等。安全信誉是基于历史数据的动态评估值，可以由权威机构评测或依据多安全检测设备的评测结果的加权评估得到。必要时可通过对关注对象进行持续评估，构建安全信誉库 。

2) 典型应用场景

- 提升入侵检测系统(IDS)、入侵防御系统(IPS)、web 应用防火墙(WAF)等检测类产品的能力
  - 基于白环境（BWG 模型，参考附录 A.1）或行为基线的**异常行为检测** ；

- 网络层通过网络链接识别的异常检测机制；
- 应用层基于业务流程及用户授权操作规范的异常检测 。

- 提升抗拒绝服务类产品识别攻击流量的能力
  - 基于流量统计特征实现网络层**异常流量的识别与控制。**
- 利用安全信誉提高安全产品的威胁检测及风险评估效率。

2. 面向攻防生态环境的协同能力

1) 特性解析

该特性主要指攻防生态环境中，多个安全防护系统通过系统互联、信息共享、任务合作等方式，加强安全防护系统间的关联与协同能力，实现多安全防护系统的综合安全防护能力及安全效益的提升。

2) 典型应用场景

- 系统间协同
  - Web 应用防火墙与漏洞扫描产品的协同；
  - 安全运营管理平台与所管理安全产品间的协同；
  - 系统漏洞扫描及配置核查任务的自动化 。
- 用户间协作
  - 基于安全运营平台的知识分享与安全服务 ；
  - 最佳实践、解决方案。

4.3 云及虚拟化安全的 NG 特性

依据§3.3 对云及虚拟化安全研究内容的分析，面向云计算环境的安全产品虚拟化与基于云计算环境的安全云（MSS\SaaS）将成为近期相关安全厂商推出下一代安全产品或服务的重要切入点。

1. 面向云计算环境的安全产品虚拟化

1) 特性解析

面向云计算的安全产品虚拟化，这里有两层含义： 其一是利用虚拟化技术实现虚拟化安全产品；其二是安全产品在云环境中进行快速、灵活虚拟化部署。

- 利用虚拟化技术实现虚拟化安全产品
  - 产品硬、软件平台虚拟化，支持虚拟机资源的调度及迁移管理 ；
  - 支持虚拟安全镜像实现产品的安全功能；
- 安全产品在云环境中进行快速、灵活虚拟化部署
  - 主要考虑通过网络虚拟化技术实现安全产品在云环境中的虚拟化部署 ；比如，安全产品可基于 OpenvSwitch 支持 OF/SDN。

2) 典型应用场景

- 防火墙、入侵防御系统、流量清洗系统等安全产品的虚拟化；
- 安全产品虚拟组网为用户提供安全防护服务的“安全云”，例如，流量清洗服务云 ；
- 云中安全产品的虚拟配置和优化管理（管理更方便、灵活）等。

2. 基于云计算环境的安全云（MSS\SaaS）

1) 特性解析

这里是指利用云和虚拟化技术，基于虚拟化安全产品、SaaS 化安全服务以及安全运营平台，构建能够为用户提供安全监护服务的安全云 。

2) 典型应用场景

- 提供“云端检测+云中分析+云端预防”的专业安全监护服务，例如：
  - 绿盟科技网站安全监测服务(绿盟科技 PAWSS)；
  - 绿盟科技云监护抗拒绝服务系统（绿盟科技 PAMADS）；
  - 绿盟科技云监护 WEB 应用防护系统（绿盟科技 PAMWAF）等 。
- 安全运营管理平台支持的安全评估及共享服务
  - 全局安全态势评估、风险预测服务 ；

– 最佳安全实践建议与知识的快速分享或在线服务（SaaS 服务）等。

4.4 下一代安全的主要特性汇总

在上文对下一代安全的重点发展趋势（安全运营、安全智能、云及虚拟化）及其相关特性的分析与讨论的基础上，汇总整理出下一代安全的主要特性，如表 5-1 所示。

表 5-1 下一代安全的主要特性汇总表

技术趋势		相关 NG 特性
安全运营		基于产品协同及智能分析的威胁感知
		面向安全态势评估及资源管理的可视化
		基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善闭环
安全智能		基于行为模型与安全信誉的异常检测
		面向攻防生态环境的协同能力
云及虚拟化		面向云计算环境的安全产品虚拟化
		基于云计算环境的安全云（MSS\SaaS）

五. 下一代安全的概念定义

基于§2.2 的下一代安全研究分析模型以及对下一代安全发展趋势及主要特性分析的基础上，我们对下一代安全概念进行了描述性定义。

定义：下一代安全

下一代安全是指为应对因新的安全威胁与 IT 技术发展而造成的安全技术水平及安全服务能力严重不足的问题（挑战），所提出的新安全理念、技术、产品以及服务模式等对策的集合[1]。

从目前来看，下一代安全主要应具有如下特性：

- 面向攻防生态环境的协同能力；
- 基于产品协同与智能分析的威胁感知；
- 基于行为模型与安全信誉的异常检测；
- 面向安全态势评估与安全资源管理的可视化；
- 基于云计算环境的安全云（MSS\SaaS）；
- 面向云计算环境的安全产品虚拟化；
- 基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善“闭环”。

六. 结束语

本文首先提出了下一代安全的研究模型，即下一代安全研究的关联角色模型与下一代安全的研究分析模型；其次，依据提出的研究模型，分析及描述了下一代安全环境的变化与挑战；再次，对攻防环境内的各种变化及新型威胁进行综合分析和逻辑推导，确定了当前或未来一段时间内需要提升的安全能力和需要突破的重要技术方向，包括安全运营、安全智能、云及虚拟化安全、数据安全及 CII 安全等。最后，结合绿盟科技在网络攻防方面的传统技术与产品优势，重点讨论了安全运营、安全智能、云及虚拟化安全等领域的主要技术特性，并据此归纳总结出了用于描述下一代安全概念的七个主要特性。

相信读者通过本文所给出的下一代安全研究模型，能够进一步理解下一代安全的定义及其特性，了解未来网络攻防环境的变化及新型威胁特征，从而把握未来网络安全及信息安全领域发展趋势的脉搏，为规划下一代安全架构，奠定基础！

附录A 智能分析与异常检测技术

以“智能化分析”为核心，通过对异构的大量威胁数据信息的智能处理、基于系统的白环境建模机及安全信誉进行异常行为监测，并配合新一代的智能安全产品、专业化的安全服务及运营模式；提供面向安全威胁的快速响应能力。

A.1 白环境建模及异常行为检侧

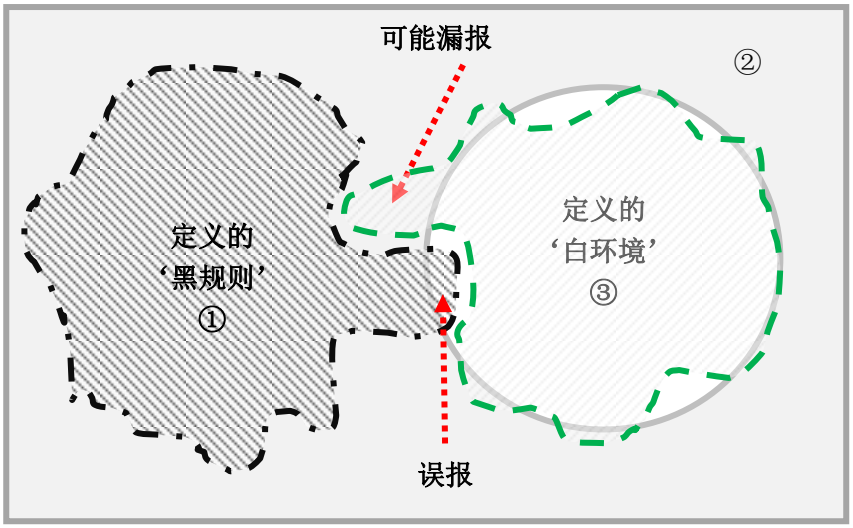

图 A-1 基于白环境的黑、白、灰检测分类概念图

入侵检测的工作原理在理论上的基本模型主要有两种：

其一是基于“入侵攻击特征”(黑规则)的模式匹配检测方法(Misuse Detection Model)，这类方法主要是针对入侵攻击样本进行分析，提取特征；在检测时如果发现了入侵特征（黑规则)则可以认定遭受到了攻击。这种方法的检测速度快，但缺点是只能检测出已知的攻击，对于特征未知的新型攻击检测不出来，只能漏报。而且如果黑规则的描述不精确，还有可能对正常的行为进行误报(这种模型下，误报的概率较小)。这个模型在 IDS、防病毒软件以及其他防止恶意代码的安全产品中得到广泛的应用。

其二就是针对被保护系统的正常行为特征进行建模，构建系统的正常行为特征（Profile），然后不合该 profile 的行为就被认为是违规行为加以禁止。这种模型被称为异常行为检测模型（Anormal Detection Model）。因为对系统正常行为特征建模的不易，该模型因误报、漏报较多，多作为辅助的入侵检测功能使用。

绿盟科技提出的白环境概念其本质也是要构建系统的正常行为模型（profile）的基础上实行异常行为检测，并融合基于黑规则的 Misuse Detection Model 的混合检测方法，提出了如图 A-1 描述的基于白环境的黑、白、灰检测分类概念图（BGW 检测模型）。在检测时，将遵循下面的规则：

- 符合白环境：按照白环境定义符合安全策略的流量、访问等
- 黑规则命中：IPS/IDS 设备中的攻防规则发现的攻击者入侵相关的流量、访问等
- ①②③表示不同的安全优先级或可信度。
- ①只要黑规则命中，则立刻识别为攻击入侵，需要深入调查或关注
- ②黑规则没有发现异常，但是不符合白环境定义的安全策略，属于“灰色”流量、访问，需要深入调查或关注
- ③黑规则没有发现异常，也符合白环境定义的安全策略，不需要特别的深入调查或关注。在特别的高安全场合，需要记录已备日后 Forensics 使用。

A.2 安全信誉

信誉(Reputation) 通俗的讲是口碑或声誉，这是来源于经济学的一个概念，其定义信誉是以信用为基础的抽象价值和社会声誉 。评估的是社会上人的信用，考虑的是其信用承诺的可信性及承诺不兑现的风险

而安全信誉，则主要是面对网络虚拟世界中的主、客体，判定的则是主体（服务）行为的安全可信性及相关客体（信息资源）内容的真实性问题，考虑的是保障用户在访问网络资源和享受服务时，如何降低受到危害的风险。

在网络安全领域，安全信誉是对网络中指定主体行为及内容不具有危害性的可信程度的综合评估，这是建立在历史数据上的动态评估概念。而且这种安全信誉的评估不是非此即彼的二选一硬判决，而是依据对实体状况的综合评估，赋予该实体一个信誉评估值，这个信誉评估值能够反映实体某一方面信誉好坏的程度。

我们在研究安全信誉时，引入了一个“信誉度”的概念，并注意考虑信誉库的区域有效性和时效性以及信誉库的及时更新。利用信誉过滤器、安全信誉评估策略服务等机制，实现基于信誉评估的阻断规则，可以有效的改善现有安全产品对网络中的不良资源，或服务攻击的检测和防护能力，并可以通过基于信誉库的安全评估及改善服务，提升用户信息系统的整

体安全状态，保护自己资源和信息的安全（如图 A-2 所示）。为生成安全信誉库，需要展开智能信息分析与评估决策方面的研究，以及研究网络主体行为监管技术、内容真实性判断技术、恶意代码检测技术、各种异常检测技术、系统完整性技术等多种网络实体可信性评估技术。

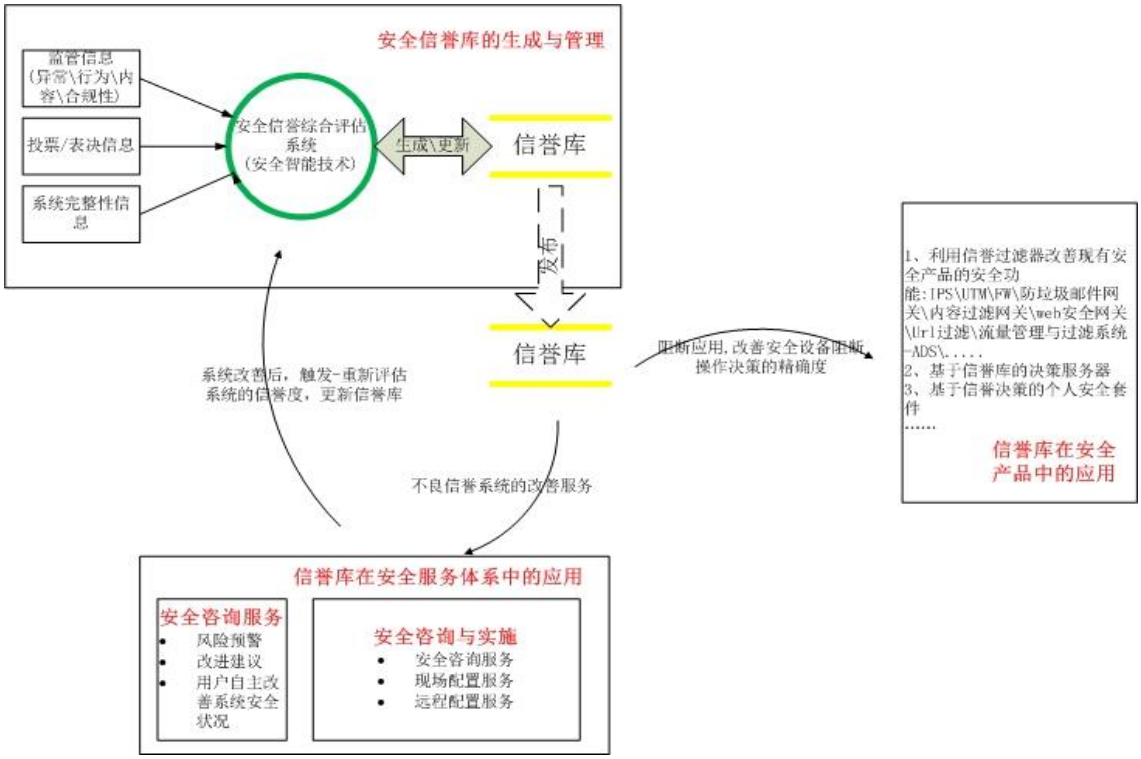

图 A-2　安全信誉库的管理及应用

A.3 大数据分析

目前，大量的各种各样的安全设备每天都产生海量的各种数据（例如日志和告警），但是，业界缺少安全数据相关的标准，并且对安全“元数据”的重视也远远不够，这些原因都间接地弱化了安全“智能化”的基石，同时也大大限制了 SIMS 这类安全事件管理类产品的实际功能效果，只能徘徊于在较为狭窄的“事件管理”领域，无法提供更高价值的策略优化和决策支持等功能。

《大数据时代》的作者维克托•舍恩伯格认为，大数据的核心在于预测。在安全行业，这无疑预示了一个美好的前景，但尚无坦途通向这一目标。最接近的可能是 Splunk 公司，他们认为，传统 SIEM（Security Information and Event Management）使用的是“数据缩减模型”，

大数据的解决方案使用的是“数据包含模型”。这种模型无需归一化，可以实时检索，易于统计、关联和分析[3]。

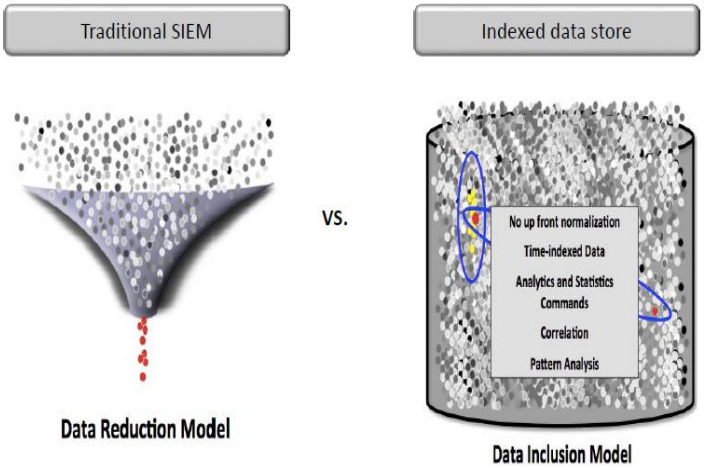

图 A-3 传统 SIEM 和大数据方案的区别

绿盟科技鲍旭华在其报告[3]中认为，“大数据”备受关注代表了业界对知识提炼的渴望和期盼；但其是否是取得知识的最好途径，依然有待证实。

参考文献

1. 李鸿培，下一代安全的分析研究模型，2012.4
2. 李鸿培，信誉技术在安全领域中的应用，2011.5
3. 鲍旭华，多样性引发的安全知识变革 - 浅谈 RSA 2013
4. https://ae.rsaconference.com/US13/connect/sessionDetail.ww?SESSION_ID=1693
5. 李鸿培、于旸、忽朝俭、曹嘉，工业控制系统及其安全性研究报告，2012.12
6. 赵粮，SDN/OF 下的安全构想，2012
7. 赵粮，下一代安全的思考-应对下一大威胁，2012.11
8. 卢小海，一种基于信誉的威胁分析方法，2010
9. 王卫东，安全度量综述，2010

作者信息

李鸿培

Email：lihongpei@nsfocus.com

Blog: http://www.i170.com/user/falcon

博士、高级工程师，绿盟科技研究院战略师。研究方向主要涉及网络安全、可信网络体系架构、安全信息智能处理技术及工业控制系统安全研究等。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS