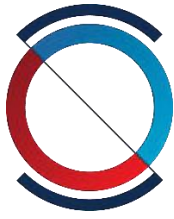


简译版

NCTOC：安全运营中心（SOC）五大原则

非官方中文译文·安天技术公益翻译组 译注

| 文档信息 | | | |
|--------|--|--------|------------|
| 原文名称 | NCTOC Top 5 Security Operations Center (SOC) Principles | | |
| 原文作者 | NCTOC | 原文发布日期 | 2018 年 3 月 |
| 作者简介 | NCTOC 负责执行美国国家安全局的全天候网络安全行动任务。 | | |
| 原文发布单位 | NCTOC | | |
| 原文出处 | https://www.nsa.gov/resources/cybersecurity-professionals/assets/files/top-5-soc-principles.pdf | | |
| 译者 | 安天技术公益翻译组 | 校对者 | 安天技术公益翻译组 |
| 分享地址 | 请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块 | | |
| 免责声明 | <ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 | | |



CYBERSECURITY OPERATIONS

NCTOC：安全运营中心（SOC）五大原则

美国国家安全局（NSA）的网络安全威胁行动中心（NCTOC）负责执行该局全天候的网络安全行动任务。基于对攻击者意图和谍报技术的独特见解，NCTOC 为美国最关键的网络安全开发和实施战略防御措施。NCTOC 拥有配备齐全的团队，这些团队与美国网络司令部合作，构成了防御非机密的国防部信息网络（DoDIN）的“前线”。DoDIN 是一个全球性的网络，其 300 万用户遍布世界各地——从华盛顿特区的办公楼到阿富汗的战场。这种巨大的覆盖范围导致该网络每天都会遭遇各种各样的网络威胁，根据多年的经验，NCTOC 为运营或监督安全运营中心（SOC）的人士提供了以下五项关键原则。

1) 建立一个防御边界

在过去的几年中，DoDIN 网络基础设施得到了整合——DoDIN 流量通过数量非常有限的、面向互联网的网关进行路由，不再是数百个区域（enclave）直接连接互联网。这可以集中覆盖超过 99% 的网络流量，能够提高检测威胁的能力，同时减少攻击者可能利用的潜在攻击面。防御边界也应该综合利用已知信标、启发式检测和行为分析，在一系列基于主机（计算机/端点）和基于网络的（边界防护）平台上部署，以便实时查看网络活动并采取相应的行动。

2) 确保整个网络的可视性

网络流量的可视性和持续监控必须涵盖所有的网络级别，包括网关、中间点和端点。如果一个规则集在网络级别发出告警，分析师必须能够查明并隔离产生该活动的实际终端主机。此过程的效能应以分钟而非小时来衡量。而且，随着大部分网络流量开始加密，SOC 必须构建解决方案以确保对高级威胁的可视性，防止混它们入合法活动中。

3) 强化最佳实践

发生安全事件最常见的原因是，存在漏洞的网络没有及时应用软件和硬件更新，以及安

全措施不合标准,例如使用不再受供应商支持的应用程序。此外,当漏洞被披露或补丁被发布后,威胁源将会在 24 小时内扫描 DoDIN,寻找未打补丁的服务器。因此,及时应用更新,以降低漏洞暴露风险并最大限度地提高软件可靠性和保护,仍然是 NCTOC 倡导的最佳防御措施之一。

4) 使用全面的威胁情报和机器学习

建议根据网络环境量身定制威胁情报源。例如,DoDIN 遭受的网络威胁活动可能与医院不同。SOC 应该理解已经存在的防御架构,确定哪些网络资产对攻击者有价值,并据此定制威胁情报源。此外,当面对海量的威胁情报或网络活动告警时,SOC 应该采用数据科学和机器学习概念,迅速将这些信息提炼为可支持行动的情报。安全团队应该有能力应对已经存在的告警,并在整个网络中积极寻找以前未检测到的威胁活动。

5) 创造好奇文化

基于事件告警关闭速度的网络安全指标可能会产生误导。响应者可能会专注于关闭告警,而不是全面了解威胁活动。持续性攻击者可能会继续探查网络的入口点,因此事件响应者应预测攻击者对新对策的反应。SOC 应先发制人地采取防御行动,并在其团队中注入创新思想,以了解攻击者的新型谍报技术。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队,为用户提供端点防护、流量监测、快速处置、深度分析等产品,以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门,提供高级威胁和新兴威胁解决方案和能力体系,产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点,全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴,安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可,安天已连续五届蝉联国家级安全应急支撑单位资质,亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点,在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面,提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动,进行了深度的解析,对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上,安天创始人、首席技术架构师作为网络安全领域的发言代表,向习总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了位于哈尔滨科技创新城的安天公司,对安天负责人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问: <http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问: <http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>