安全团队年终绩效评估模板

[前言 2](#_Toc26517764)

[声明 2](#_Toc26517765)

[一级安全分析师 3](#_Toc26517766)

[岗位描述 3](#_Toc26517767)

[2019年评估模板 3](#_Toc26517768)

[2020年KPI模板 4](#_Toc26517769)

[二级安全分析师 5](#_Toc26517770)

[岗位描述 5](#_Toc26517771)

[2019年评估模板 5](#_Toc26517772)

[2020年KPI模板 7](#_Toc26517773)

[三级安全分析师 8](#_Toc26517774)

[岗位描述 8](#_Toc26517775)

[2019年评估模板 8](#_Toc26517776)

[2020年KPI模板 10](#_Toc26517777)

[安全运营经理 11](#_Toc26517778)

[岗位描述 11](#_Toc26517779)

[2019年评估模板 11](#_Toc26517780)

[2020年KPI模板 13](#_Toc26517781)

[安全架构师 15](#_Toc26517782)

[岗位描述 15](#_Toc26517783)

[2019 年评估模板 15](#_Toc26517784)

[2020年KPI模板 17](#_Toc26517785)

[安全总监 18](#_Toc26517786)

[岗位描述 18](#_Toc26517787)

[2019年评估模板 18](#_Toc26517788)

[2020年KPI模板 20](#_Toc26517789)

# 前言

评估安全团队的绩效是首席信息安全官（CISO）掌握团队在安全保障方面的表现的重要方法，对后续评估应采取哪些措施来改进安全产品、人员配置、培训、工作流程的安全态势是至关重要的。本文档是首次尝试总结主要利益相关者在设计、运行安全工作时的关键任务和关键绩效指标（KPI），为CISO提供一个全面、灵活的工具来评估绩效，制定未来目标。

本文档包含五个关键角色：负责设计和维护安全产品的安全架构师；分别负责识别、响应和主动检测威胁的一、二、三级安全分析师；以及监督安全工作的安全运营中心（SOC）经理。

不言而喻，在这些问题上并没有万能的标准，很可能我们分配给多个角色的任务在你的组织内部是由同一个岗位承担，并且岗位命名也不相同。但这无关紧要——重要的是，所有核心安全功能的KPI都有记录在案，你能够轻松地将它们映射到团队中的每个人。

每个角色包括两个模板：一个用于评估2019年，一个用于规划2020年。这些表格在很大程度上是相似的。在某些地方，我们提供了模拟数据，让你了解要填写哪些数据。在填写自己的数据之前，请记得删除模拟数据（表格中红字为模拟数据）。当然，你可以随意添加删减，根据你的具体情况加以修改。

# 声明

本文档是基于与CISO以及全球安全组织之间的大量交互而形成的。评估安全团队的绩效，虽然被广泛认为是获得良好安全态势的关键，但在不同的组织中实施方法各不相同。我们的目标是简化和优化这一过程，并为CISO提供一个简单易用的模板，该模板可以轻松地根据你的实际需求进行调整。

本文档来自[Cynet 360](https://www.cynet.com/)，由[安数网络](https://www.anshuw.com/)编译整理，不足之处，欢迎指正。如涉及侵权，请及时与我们联系，我们会在第一时间删除或处理侵权内容。

电话：400-869-9193 ，负责人：张明

# 一级安全分析师

## 岗位描述

一级安全分析师的职责是在前线对安全事件进行初步识别和分类，提供24x7x365全天候支持。该岗位遵循标准操作流程，在安全运营中心（SOC）经理的监督下，与二级安全分析师协作，检测、鉴别、报告安全事件。

## 2019年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 安全事件识别与鉴定  | 安全产品 – 安全监控系统 |
| 工具及技能 | 熟练程度 |
| SIEM | 中 |
| EDR | 高 |
| 网络流量分析 | 低 |
| 其他 |  |
| 安全产品 – 鉴别工具 |
| 工具及技能 | 熟练程度 |
| Sysinternals |  |
| Wireshark |  |
| 其他 |  |
| 文档与上报平台 |
| 工具及技能 | 熟练程度 |
| Ticketing System |  |
| 处理简单/低危的安全事件，并将复杂/高危的安全事件上报给二级安全分析师 | 能力 |
|  | 处理告警数量 | 占告警总数的比例 | 日均处理告警数  |
| 自行解决 |  |  |  |
| 上报 |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | KPI  |
| 安全事件识别与鉴定 | 安全产品 – 告警生成器 |
| 工具及技能 | 熟练程度 |
| SIEM | 指定等级（可提供详细信息） |
| EDR | 指定等级（可提供详细信息） |
| 网络流量分析 | 指定等级（可提供详细信息） |
| 其他 | 指定等级（可提供详细信息） |
| 安全产品 – 鉴别工具 |
| 工具及技能 | 熟练程度 |
| Sysinternals | 指定等级（可提供详细信息） |
| Wireshark | 指定等级（可提供详细信息） |
| 其他 | 指定等级（可提供详细信息） |
| 文档与上报平台 |
| 工具及技能 | 熟练程度 |
| Ticketing System | 指定等级 |
| 处理简单/低危的安全事件，并将复杂/高危的安全事件上报给二级安全分析师 | 能力 |
|  | 处理告警数量 | 占告警总数的比例 | 日均处理告警数  |
| 自行解决 | 定义目标 | 定义目标 | 定义目标 |
| 上报 | 定义目标 | 定义目标 | 定义目标 |

# 二级安全分析师

## 岗位描述

二级安全分析师的职责是对一级安全分析师上报的关键事件进行技术响应。这包括及时抑制、侦查、修复补救，以及运用在响应过程中获得的新技术加强防御。

## 2019年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 有关安全事件的源头、范围、影响的侦查 | 安全侦查工具 |
| 工具及技能 | 熟练程度 |
| SIEM |  |
| EDR |  |
| 威胁情报反馈（详述） |  |
| 其他 |  |
| 抑制 | 修复行为摘要 |
| 类型 | 起因 | 数量 | 日均值 |
| 隔离主机 | 连接到C2C服务器 | 23 |  |
| 禁用用户账户 | 凭证已确认被窃取 | 2 |  |
| 其他 |  |  |  |
| 加固 | 创建的工作流和自动化脚本 |
| 工作流 | 威胁 | 详情 | 涉及工具/团队成员 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 能力 | 按持续时长分类的安全事件数量 |
|  | >6小时 | 1天 | 1-3天 | >3天 |
| 安全事件数量 |  |  |  |  |
| 按规模分类的安全事件数量 |
|  | 自行解决 | 与其他安全分析师协作 | 非安全团队成员参与 | 第三方参与 |
| 安全事件数量  |  |  |  |  |
| 按响应过程的自动化级别分类的安全事件数量  |
|  | 全自动（现有脚本） | 部分自动 | 全手动 |
| 安全事件数量 |  |  |  |
| 按类型分类的安全事件数量 |
| 类型 | 数量 | 平均修复耗时 | 响应过程中使用的工具 |
| 勒索软件传播 |  |  |  |
| 恶意内部攻击 |  |  |  |
| SaaS帐户凭证被盗 |  |  |  |
| 其他 |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 有关安全事件的源头、范围、影响的侦查 | 安全侦查工具 |
| 工具及技能 | 熟练程度 |
| SIEM | 指定等级（可提供详细信息） |
| EDR | 指定等级（可提供详细信息） |
| 威胁情报反馈 （详述） | 指定等级（可提供详细信息） |
| 其他 | 指定等级（可提供详细信息） |
| 抑制 & 加固 | 创建的工作流和自动化脚本 |
| 工作流 | 威胁 | 详情 | 涉及工具/团队成员 |
| 指定 | 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 | 指定 |
| 能力 | 按持续时长分类的安全事件数量 |
|  | >6小时 | 1天 | 1-3天 | >3天 |
| 安全事件数量 | 指定额度 | 指定额度 | 指定额度 | 指定额度 |
| 按规模分类的安全事件数量 |
|  | 自行解决 | 与其他安全分析师协作 | 非安全团队成员参与 | 第三方参与 |
| 安全事件数量 | 指定额度 | 指定额度 | 指定额度 | 指定额度 |
| 按响应过程的自动化级别分类的安全事件数量  |
|  | 全自动（现有脚本） | 部分自动 | 全手动 |
| 安全事件数量 | 指定额度 | 指定额度 | 指定额度 |

# 三级安全分析师

## 岗位描述

三级安全分析师的职责是通过持续监测环境中的漏洞，搜寻可能利用漏洞的威胁来主动发现未知的威胁。此外，三级安全分析师还需要根据威胁情报反馈的IOC（入侵指标）进行威胁追踪，并通过主动渗透测试实时掌握环境的安全态势。

## 2019年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 威胁追踪 | 威胁追踪工具 |
| 名称 | 类型 | 熟练程度 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 威胁追踪结果 |
| 威胁类型 | 数量 | 侦测方法 |
| 后门 | 113 | 从VT搜索SHA256 |
| 连接到钓鱼网站 | 16 | Wireshark流量分析 |
| 其他 |  |  |
| 提升安全态势 | 在安全产品注入已知威胁 |
| IOC类型 | 数量 | 注入产品 |
| SHA256 |  |  |
| IP |  | 防火墙 |
| Domain |  |  |
| 路径 |  |  |
| 漏洞签名 |  | IDS |
| 其他 |  |  |
| 渗透测试 | 测试细目 |
| 时间 | 焦点 | 动机 | 结果 | 建议 |
| 年/月/日 | 端点保护 | 在Word文档中利用恶意宏的几种成功攻击 | 78%的模拟恶意宏完全执行，避免了端点保护 | 通过电子邮件保护或高级端点保护产品弥补差距 |
| 年/月/日 | 网络设备（路由器和交换机）中的漏洞 | 季度测试 | 发现4个关键漏洞 | 申请供应商修补程序 |
| 其他 |  |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 威胁追踪 | 威胁追踪工具 |
| 名称 | 类型 | 熟练程度 |
|  |  | 指定等级（可提供详细信息） |
|  |  | 指定等级（可提供详细信息） |
|  |  | 指定等级（可提供详细信息） |
|  |  | 指定等级（可提供详细信息） |
| 威胁追踪结果 |
| 威胁类型 | 数量 | 侦测方法 |
| 指定 | 目标数量 | 指定 |
| 指定 | 目标数量 | 指定 |
| 指定 | 目标数量 | 指定 |
| 提升安全态势 | 在安全产品注入已知威胁 |
| IOC类型 | 数量 | 注入产品 |
| SHA256 | 目标数量 | 指定 |
| IP | 目标数量 | 指定 |
| Domain | 目标数量 | 指定 |
| 路径 | 目标数量 | 指定 |
| 漏洞签名 | 目标数量 | 指定 |
| 其他 | 目标数量 | 指定 |
| 渗透测试 | 2020年计划进行的测试 |
| 时间 | 焦点 | 动机 | 结果 | 建议 |
| 年/月/日 | 指定 |  |  |  |
| 年/月/日 | 指定 |  |  |  |
| 年/月/日 | 指定 |  |  |  |

# 安全运营经理

## 岗位描述

安全运营经理主要负责安全事件的监控、管理和响应。安全运营经理要确保安全事件识别、评估、量化、报告、沟通、缓解和监控等过程的顺利进行，还需确保工作遵循服务等级协议（SLA）、过程控制及过程灵活原则，以实现运营目标。

## 2019年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 通过招募、雇佣、培训和评估SOC人员，为SOC配备一支成熟的安全队伍。 | 新员工招聘 – 数量 & 岗位 |
| 姓名 | 入职日期 | 岗位 | 目的 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 2019年的培训安排（技能/产品/开源工具） |
| 听众 | 场所 (内部/外部) | 日期&时长 | 主题 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 为SOC建立各种安全事件的响应工作流程，包括为勒索软件攻击等常见场景准备行动手册，以及侦查高级威胁的流程。 | SOC主动事件响应工作流程：识别、评估、量化、报告、沟通、缓解 |
|  | 一级安全分析师 | 二级安全分析师 | 三级安全分析师 | SOC 经理 |
| 勒索软件传播 |  |  |  |  |
| 异常SaaS登录 |  |  |  |  |
| 可疑用户帐户行为 |  |  |  |  |
| 其他（根据需求添加） |  |  |  |  |
| SOC日常工作流程：持续监视并遵守内部和外部安全框架 |
|  | 一级安全分析师 | 二级安全分析师 | 三级安全分析师 | SOC 经理 |
| 持续监视 |  |  |  |  |
| 安全规则 A |  |  |  |  |
| 安全规则 B |  |  |  |  |
| 持续改善和优化现有工作流程 | 2019年期间实施的工作流程变更和更新 |
|  | 一级安全分析师 | 二级安全分析师 | 三级安全分析师 | SOC 经理 |
| 工作流程1 |  |  |  |  |
| 工作流程2 |  |  |  |  |
| 工作流程3 |  |  |  |  |
| 建立整个SOC的绩效考核机制 | 一级安全分析师的KPI |
| 二级安全分析师的KPI |
| 三级安全分析师的KPI |
| 与管理层沟通安全事件的处理 | SOC的事件报告 |
| 对象 | 类型 | 频率 | 内容 |
| 董事会 | SOC高层汇报 | 每年度\每季度 | 组织机构安全威胁态势的高层综述 |
| 高级管理层 | 攻击总结 | 严重安全事故的总结节点 | 攻击的根本原因、范围和影响摘要 |
| 其他 |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 通过招募、雇佣、培训和评估SOC人员，为SOC配备一支成熟的安全队伍。 | 2020 年招聘目标 |
| 岗位 | 数量 | 目的 |
|  |  |  |
|  |  |  |
|  |  |  |
| 2020年的培训计划（技能/产品/开源工具） |
| 听众 | 场所 (内部\外部) | 日期&时长 | 主题 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 为SOC建立各种安全事件的响应工作流程，包括为勒索软件攻击等常见场景准备行动手册，以及侦查高级威胁的流程。 | SOC主动事件响应工作流程：识别、评估、量化、报告、沟通、缓解 |
|  | 一级安全分析师 | 二级安全分析师 | 三级安全分析师 | SOC 经理 |
| 指定 |  |  |  |  |
| 指定 |  |  |  |  |
| 指定 |  |  |  |  |
| 指定 |  |  |  |  |
| 持续改善和优化现有工作流程 | 2020年计划实施的工作流程变更和更新 |
|  | 一级安全分析师 | 二级安全分析师 | 三级安全分析师 | SOC 经理 |
| 工作流程1  |  |  |  |  |
| 工作流程2  |  |  |  |  |
| 工作流程3 |  |  |  |  |
| 建立整个SOC的绩效考核机制 | 一级安全分析师的KPI |
| 二级安全分析师的KPI |
| 三级安全分析师的KPI |
| 与管理层沟通安全事件的处理 | 2020年SOC的报告计划 |
| 对象 | 类型 | 频率 | 内容 |
| 指定 | 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 | 指定 |

# 安全架构师

## 岗位描述

安全架构师负责在组织的IT网络中设计、构建、测试和实现安全系统，以保护业务和信息数据的安全。安全架构师必须对复杂的IT系统有深入透彻的了解，并掌握最新的安全标准、系统和身份验证协议以及最佳实践安全产品。

## 2019 年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 确保已实施的安全产品稳定运行 | 已实施的安全产品 |
| 类别 | 解决的威胁 |
| 端点 |  |
| 边界 |  |
| 身份 |  |
| 其他 |  |
| 建立良好清晰的工作流程以定期更新签名、规则和策略，同时负责临时更新（安全事件、紧急补丁等）。 | 工作流程描述 |
| 更新 | 负责人 | 频率 |
| IOC注入 |  |  |
| 防火墙规则 |  |  |
| 访问策略 |  |  |
| 其他 |  |  |
| 定义IT和安全团队在安全产品运维方面的职责 | 安全产品（防病毒、防火墙、身份和访问管理等） |
| 产品类别 | 职责 |
| IT团队 | 安全团队 |
| 防病毒 |  |  |
| 防火墙 |  |  |
| 其他 |  |  |
| 建立并执行安全产品对常见和高级的网络威胁的弹性测试。 | 2019年执行的渗透测试 |
| 日期 | 结果 | 推荐步骤 |
|  |  |  |
|  |  |  |
|  |  |  |
| 评估并购买新的安全产品，以满足安全和合规要求。 | 2019年的安全产品采购 |
| 产品类别 | 目的 | 补充\替换 | 部署状态 | 许可期限 | 价值测试方法 |
| 产品A |  |  |  |  |  |
| 产品B |  |  |  |  |  |
| 产品C |  |  |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 确保已实施的安全产品稳定运行 | 2020年计划实施的安全项目 |
| 类别 | 解决的威胁 |
| 指定 |  |
| 指定 |  |
| 指定 |  |
| 指定 |  |
| 建立良好清晰的工作流程以定期更新签名、规则和策略，同时负责临时更新（安全事件、紧急补丁等）。 | 2020年计划建立的工作流程 |
| 更新 | 负责人 | 频率 |
| 指定 |  |  |
| 指定 |  |  |
| 指定 |  |  |
| 定义IT和安全团队在安全产品运维方面的职责 | 安全产品（AV、防火墙、身份和访问管理等） |
| 产品类别 | 职责 |
| IT团队 | 安全团队 |
| 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 |
| 建立并执行安全产品对常见和高级的网络威胁的弹性测试。 | 2020年计划执行的渗透测试 |
| 日期 | 焦点 | 测试产品 |
| 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 |
| 指定 | 指定 | 指定 |
| 评估并购买新的安全产品，以满足安全和合规要求。 | 2020年安全产品详细购买计划 |
| 产品类别 | 目的 | 补充\替换 | 部署状态 | 许可期限 | 价值测试方法 |
| 指定 |  |  |  |  |  |
| 指定 |  |  |  |  |  |
| 指定 |  |  |  |  |  |

# 安全总监

## 岗位描述

监督组织内所有与安全相关的功能，包括遵守相关框架、购买、部署和维护安全产品以及入侵保护工作流程。安全总监向首席信息官（CIO）汇报，作为本组织内所有网络安全相关信息的窗口。

## 2019年评估模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 遵守法规和最佳实践框架 | 确定相关合规框架和法规，并确定其优先级 |
| 法规/框架 | 目的 | 合规状态 |
| PCI-DSS |  | 外聘审计员认证 |
| NIST CSF |  | 差距：ABC |
| GDPR |  |  |
| 其他 |  |  |
| 为符合框架/法规要求而采取的行动 |
| 法规/框架 | 行动 | 状态 |
|  |  |  |
|  |  |  |
|  |  |  |
| 安全堆栈的持续优化 | 评估已安装产品的投资回报率 |
| 产品 | 保留/替换 | 理由 |
| Firewall vendor X | 保留 | 交付预期保护 |
| EDR vendor Y | 替换 | 运营经费 |
| IDS vendor X | 重新评估 |  |
| 评估新安全产品 |
| 产品 | 状态 | 理由 |
| CASB | 已部署 | 监测SaaS日志 |
| UEBA | 正在评估3种产品 |  |
| SaaS based SIEM | 计划中 |  |
| 入侵保护 | 确保以下条目存在清晰良好的工作流程 |
| 条目 | 详细工作流程 |
| IT健康（漏洞、密码更改、管理员账户使用等） |  |
| 检测到的攻击鉴别 |  |
| 积极应对安全事件 |  |
| 主动搜寻威胁 |  |
| 安全团队 | 安全团队的招聘/离职 |
| 工作组 | 岗位 | 人员异动 | 编制情况 |
| SOC  | 二级安全分析师 | 入职1人，离职3人 | 在编5人，满员 |
| SOC | 一级安全分析师 | 无 | 在编3人，空缺2人 |
| 安全架构 | 端点专家 | 入职2人，离职1人 | 在编2人，满员 |
| 其他 |  |  |  |

## 2020年KPI模板

|  |  |
| --- | --- |
| 任务 | 绩效评估 |
| 遵守法规和最佳实践框架 | 2020年计划实施的法规/框架 |
| 法规/框架 | 目的 |
|  |  |
|  |  |
|  |  |
| 所需资源 |
| 法规/框架 | 时间表 | 第三方审计师 | 安全产品 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 安全堆栈的持续优化 | 2020年计划实施的安全项目 |
| 产品 | 理由 | 预算 |
| Firewall vendor X |  |  |
| EDR vendor Y |  |   |
| IDS vendor X |  |  |
| 2020年第三方参与的项目 |
| 服务 | 理由 | 预算 |
| Managed firewall  |  |  |
| MDR |  |  |
| Tier 1 IR |  |  |
| 入侵保护 | 更改并优化以下工作流程 |
| 条目 | 详细工作流程 |
| IT健康（漏洞、密码更改、管理员账户使用等） |  |
| 检测到的攻击鉴别 |  |
| 积极应对安全事件 |  |
| 主动搜寻威胁 |  |
| 安全团队 | 安全团队的招聘/离职 |
| 工作组 | 岗位 | 编制计划 |
| SOC  | 二级安全分析师 | 目标X人 |
| SOC | 一级安全分析师 | 目标X人 |
| 安全架构 | 端点专家 | 目标X人 |
| 其他 |  |  |

——（完）——