思科网络技术学院教程

CCNA网络安全运营

CCNA Cybersecurity Operations

Companion Guide

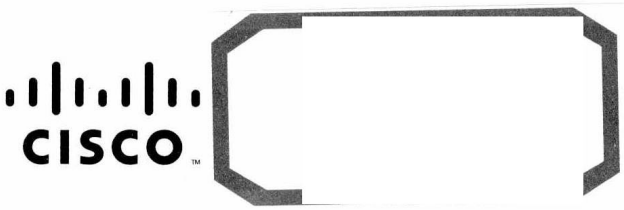
[美] 艾伦 · 约翰逊（Allan Johnson） 著

思科系统公司 译

中国工信出版集团

人民邮电出版社 POSTS & TELECOM PRESS

Cisco | Networking Academy® Mind Wide Open™



思科网络技术学院教程

CCNA网络安全运营

CCNA Cybersecurity Operations

Companion Guide

[美] 艾伦 · 约翰逊（Allan Johnson） 著

思科系统公司 译

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

思科网络技术学院教程. CCNA网络安全运营 / （美）艾伦·约翰逊（Allan Johnson）著 ；思科系统公司译. -- 北京 ：人民邮电出版社，2019.8
ISBN 978-7-115-51424-0

Ⅰ. ①思… Ⅱ. ①艾… ②思… Ⅲ. ①网络安全－计算机网络管理－高等学校－教材 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2019)第105578号

版权声明

◆ 著　[美] 艾伦·约翰逊（Allan Johnson）
译　思科系统公司
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
中国铁道出版社印刷厂印刷

◆ 开本：787×1092　1/16
印张：25.75
字数：760 千字　2019 年 8 月第 1 版
印数：1－3 000 册　2019 年 8 月北京第 1 次印刷

著作权合同登记号　图字：01-2018-7751 号

定价：80.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

思科网络技术学院项目是 Cisco 公司在全球范围内推出的一个主要面向初级网络工程技术人员的培训项目，旨在让更多的年轻人学习先进的网络技术知识，为互联网时代做好准备。

本书是思科网络技术学院 CCNA 网络安全运营（Cybersecurity Operations）课程的配套纸质教程，共分为 13 章，内容包括：网络和数据受到攻击的原因以及应对方法、Windows/Linux 操作系统的功能和特性、网络协议与服务、网络基础设施、网络安全原理、深入了解网络攻击、保护网络、加密和公钥基础设施、终端安全和分析、安全监控、入侵数据分析、事件响应和处理等。本书每章的最后提供了复习题，并在附录中给出了答案和解释，以检验读者每章知识的掌握情况。

本书适合开设了网络安全运营课程的学生阅读，还适合有志于进入网络安全行业的入门用户阅读。

关于特约作者

Allan Johnson 于 1999 年进入学术界，将所有的精力投入教学中。在此之前，他做了 10 年的企业主和运营人。他拥有 MBA 和职业培训与发展专业的教育硕士学位。他曾在高中教授过 7 年的 CCNA 课程，并且已经在得克萨斯州 Corpus Christi 的 Del Mar 学院教授 CCNA 和 CCNP 课程。2003 年，Allan 开始将大量的时间和精力投入 CCNA 教学支持小组，为全球各地的网络技术学院教师提供服务以及开发培训材料。当前，他在思科网络技术学院担任全职的课程负责人。

前言

本书是思科网络技术学院 CCNA Cybersecurity Operations v1.x（网络安全运营 v1.x）课程的官方补充教材。思科网络技术学院是在全球范围内面向学生传授信息技术技能的综合性项目。本课程强调现实世界的实践性应用，同时为您提供机会学习处理安全运营中心（SOC）助理级网络安全分析师的任务、职责和责任所需的技能。

作为教材，本书为解释与在线课程完全相同的概念、技术、协议以及工具提供了现成的参考资料。您可以在老师的指导下使用在线课程，然后使用本书帮助您巩固对于所有主题的理解。

本书的读者

本书与在线课程一样，均是对网络安全运营的介绍，主要面向旨在成为网络安全分析师的人们。本书简明地呈现主题，从最基本的概念开始，逐步进入对安全监控、入侵分析、事件响应的全面理解。本书的内容可用于备考 CCNA 网络运营认证考试（SECFND 和 SECOPS）。

本书的特点

本书的教学特色是将重点放在支持主题范围、可读性和课程材料实践几个方面，以便于您充分理解课程材料。

主题范围

本书每章中的特色内容有助于读者全面了解本章所介绍的主题，从而科学分配学习时间。

- **目标**：在每章的开头列出，指明本章所包含的核心概念。该目标与在线课程中相应章节的目标相匹配；不过，本书中提问的形式是为了鼓励读者在阅读本章时勤于思考，发现答案。
- **注意**：这些简短的补充内容指出了有趣的事实、节约时间的方法以及重要的安全问题。
- **小结**：每章最后是对本章关键概念的总结，它提供了本章的摘要，以辅助学习。

实践

实践铸就完美。本书为您提供了充足的机会将所学知识应用于实践。您将发现下面这些有价值且有效的方法帮助您有效巩固所接受的指导。

- **复习题和答案**：每章末尾都有复习题，可作为自我评估的工具。这些问题的风格与在线课程中您所看到的问题相同。附录 A 提供了所有问题的答案及其解释。

本书的组织结构

本书与思科网络技术学院 CCNA 网络安全运营 v1 课程密切相关，分为 13 章和一个附录。

- **第 1 章，“网络安全和安全运营中心”**：本章探讨网络和数据受到攻击的原因以及如何为网络安全运营事业做好准备。
- **第 2 章，“Windows 操作系统”**：本章讨论 Windows 操作系统的功能和特性，包括其操作以及如何保护 Windows 终端。
- **第 3 章，“Linux 操作系统”**：本章讨论 Linux 操作系统的特点和特性，包括 Linux shell 中的基本操作、基本管理任务以及 Linux 主机上安全相关的基本任务。

- **第 4 章，“网络协议和服务”**：本章讨论网络协议和服务的操作，包括网络运营、以太网和 IP、通用测试实用程序、地址解析、传输功能以及提供网络服务的应用程序。
- **第 5 章，“网络基础设施”**：本章讨论网络基础设施，包括有线和无线网络、网络安全设备和网络拓扑。
- **第 6 章，“网络安全原理”**：本章讨论各种类型的网络攻击，包括网络受到攻击的方式以及各种类型的威胁和攻击。
- **第 7 章，“深入了解网络攻击”**：本章深入探讨网络攻击，包括如何使用网络监控工具识别攻击。此外，还讨论了 TCP / IP 和网络应用程序的漏洞。
- **第 8 章，“保护网络”**：本章讨论防止恶意访问网络、主机和数据的方法，包括网络安全防御方法、访问控制方法以及使用各种情报来源来查找当前安全威胁。
- **第 9 章，“加密和公钥基础设施”**：本章讨论加密对网络安全监控的影响，包括加密和解密数据的工具以及公钥基础设施（PKI）。
- **第 10 章，“终端安全和分析”**：本章讨论如何调查终端漏洞和攻击，包括恶意软件分析和终端漏洞评估。
- **第 11 章，“安全监控”**：本章讨论如何识别网络安全警报，包括网络安全技术如何影响安全监控以及安全监控中使用的日志文件类型。
- **第 12 章，“入侵数据分析”**：本章讨论如何分析网络入侵数据以验证潜在漏洞，包括评估警报、确定警报来源以及确保攻击正确归因的证据处理过程。
- **第 13 章，“事件响应和处理”**：本章讨论如何应用事件响应模型来管理安全事件。 响应模型包括 Cyber Kill Chain、Diamond 入侵模型、VERIS 架构和 NIST 800-61r2 标准。
- **附录 A，“复习题答案”**：本附录列出了每章末尾的复习题的答案。

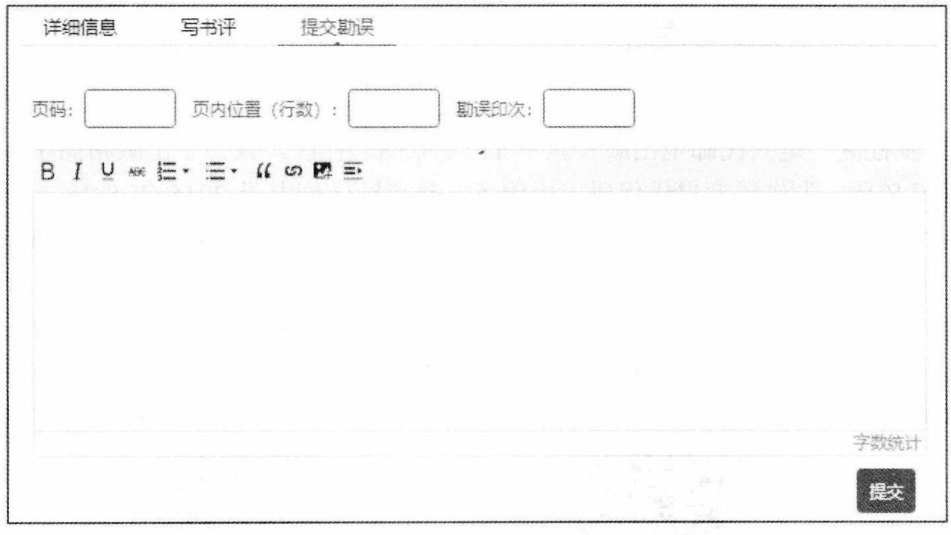
资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目　录

第 1 章　网络安全和安全运营中心 …… 1
学习目标 …… 1
1.1　危险 …… 1
1.1.1　战争故事 …… 1
1.1.2　威胁发起者 …… 2
1.1.3　威胁的影响 …… 3
1.2　打击网络犯罪的斗士 …… 4
1.2.1　现代安全运营中心 …… 4
1.2.2　成为守卫者 …… 7
1.3　小结 …… 9
复习题 …… 9
第 2 章　Windows 操作系统 …… 11
学习目标 …… 11
2.1　Windows 概述 …… 11
2.1.1　Windows 发展史 …… 11
2.1.2　Windows 架构和操作 …… 15
2.2　Windows 管理 …… 24
2.2.1　Windows 配置和监控 …… 24
2.2.2　Windows 安全 …… 35
2.3　小结 …… 41
复习题 …… 42
第 3 章　Linux 操作系统 …… 44
学习目标 …… 44
3.1　Linux 概述 …… 44
3.1.1　Linux 基础知识 …… 44
3.1.2　使用 Linux Shell …… 46
3.1.3　Linux 服务器和客户端 …… 50
3.2　Linux 管理 …… 51
3.2.1　基本服务器管理 …… 52
3.2.2　Linux 文件系统 …… 57
3.3　Linux 主机 …… 61
3.3.1　使用 Linux GUI …… 61
3.3.2　使用 Linux 主机 …… 63
3.4　小结 …… 71
复习题 …… 72
第 4 章　网络协议和服务 …… 74
学习目标 …… 74
4.1　网络协议 …… 74
4.1.1　网络设计流程 …… 75
4.1.2　通信协议 …… 77
4.2　以太网和互联网协议（IP） …… 89
4.2.1　以太网 …… 89
4.2.2　IPv4 …… 91
4.2.3　IPv4 编址基础知识 …… 95
4.2.4　IPv4 地址的分类 …… 100
4.2.5　默认网关 …… 102
4.2.6　IPv6 …… 104
4.3　验证连接 …… 106
4.3.1　ICMP …… 106
4.3.2　ping 和 tracerout 实用程序 …… 109
4.4　地址解析协议 …… 115
4.4.1　MAC 和 IP …… 115
4.4.2　ARP …… 117
4.4.3　ARP 问题 …… 119
4.5　传输层 …… 121
4.5.1　传输层的特征 …… 121
4.5.2　传输层操作 …… 129
4.6　网络服务 …… 136
4.6.1　DHCP …… 136
4.6.2　DNS …… 138
4.6.3　NAT …… 143
4.6.4　文件传输和共享服务 …… 145
4.6.5　邮件 …… 147

4.6.6 HTTP ····· 149
4.7 小结 ····· 152
复习题 ····· 153
第 5 章 网络基础设施 ····· 155
学习目标 ····· 155
5.1 网络通信设备 ····· 155
5.1.1 网络设备 ····· 155
5.1.2 无线通信 ····· 167
5.2 网络安全基础设施 ····· 171
5.2.1 安全设备 ····· 171
5.2.2 安全服务 ····· 178
5.3 网络表示方式 ····· 184
5.4 小结 ····· 190
复习题 ····· 190
第 6 章 网络安全原理 ····· 192
学习目标 ····· 192
6.1 攻击者及其工具 ····· 192
6.1.1 谁在攻击我们的网络 ····· 192
6.1.2 威胁发起者工具 ····· 195
6.2 常见威胁和攻击 ····· 197
6.2.1 恶意软件 ····· 197
6.2.2 常见网络攻击 ····· 201
6.3 小结 ····· 209
复习题 ····· 211
第 7 章 深入了解网络攻击 ····· 213
学习目标 ····· 213
7.1 网络监控和工具 ····· 213
7.1.1 网络监控简介 ····· 213
7.1.2 网络监控工具简介 ····· 215
7.2 攻击基础 ····· 218
7.2.1 IP 漏洞和威胁 ····· 218
7.2.2 TCP 和 UDP 漏洞 ····· 224
7.3 攻击我们的操作 ····· 227
7.3.1 IP 服务 ····· 227
7.3.2 企业级服务 ····· 233
7.4 小结 ····· 237
复习题 ····· 237
第 8 章 保护网络 ····· 239
学习目标 ····· 239
8.1 了解防御 ····· 239
8.1.1 纵深防御 ····· 239
8.1.2 安全策略 ····· 242
8.2 访问控制 ····· 244
8.2.1 访问控制概念 ····· 244
8.2.2 AAA 使用与操作 ····· 245
8.3 威胁情报 ····· 248
8.3.1 信息来源 ····· 248
8.3.2 威胁情报服务 ····· 250
8.4 小结 ····· 251
复习题 ····· 251
第 9 章 加密和公钥基础设施 ····· 253
学习目标 ····· 253
9.1 加密 ····· 253
9.1.1 什么是加密 ····· 253
9.1.2 完整性和真实性 ····· 259
9.1.3 保密性 ····· 263
9.2 公钥基础架构 ····· 272
9.2.1 公钥密码学 ····· 272
9.2.2 机构和 PKI 信任系统 ····· 276
9.2.3 密码学的应用与影响 ····· 282
9.3 小结 ····· 284
复习题 ····· 286
第 10 章 终端安全和分析 ····· 288
学习目标 ····· 288
10.1 终端保护 ····· 288
10.1.1 反恶意软件保护 ····· 288
10.1.2 基于主机的入侵防御 ····· 293
10.1.3 应用安全 ····· 295
10.2 终端漏洞评估 ····· 297
10.2.1 网络和服务器配置文件 ····· 297
10.2.2 通用漏洞评分系统 ····· 300
10.2.3 合规性框架 ····· 304
10.2.4 安全设备管理 ····· 306
10.2.5 信息安全管理系统 ····· 311
10.3 小结 ····· 314
复习题 ····· 315
第 11 章 安全监控 ····· 317
学习目标 ····· 317
11.1 技术和协议 ····· 317
11.1.1 监控常用协议 ····· 317
11.1.2 安全技术 ····· 321
11.2 日志文件 ····· 325
11.2.1 安全数据的类型 ····· 325
11.2.2 终端设备日志 ····· 328
11.2.3 网络日志 ····· 334
11.3 小结 ····· 340

复习题 ····· 341
第 12 章 入侵数据分析 ····· 343
学习目标 ····· 343
12.1 评估警报 ····· 343
12.1.1 警报来源 ····· 343
12.1.2 警报评估概述 ····· 349
12.2 使用网络安全数据 ····· 351
12.2.1 通用数据平台 ····· 351
12.2.2 调查网络数据 ····· 354
12.2.3 提升网络安全分析师的工作能力 ····· 361
12.3 数字取证 ····· 362
12.4 小结 ····· 365
复习题 ····· 365
第 13 章 事件响应和处理 ····· 367
学习目标 ····· 367
13.1 事件响应模型 ····· 367
13.1.1 网络杀伤链 ····· 367
13.1.2 入侵的钻石模型 ····· 371
13.1.3 VERIS 方案 ····· 374
13.2 事件处理 ····· 378
13.2.1 CSIRT ····· 378
13.2.2 NIST 800-61r2 ····· 380
13.3 小结 ····· 386
复习题 ····· 387
附录 A 复习题答案 ····· 389

第 1 章

网络安全和安全运营中心

学习目标

在学完本章后，您将能够回答下列问题：

- 网络安全事件示例的主要特征是什么？
- 在特定的网络安全事件背后，威胁发起者的动机是什么？
- 网络安全攻击的潜在影响是什么？
- 安全运营中心（SOC）是什么？
- 为了从事网络安全运营职业，有哪些可用的资源？

在本章中，您将学习网络攻击的目标、经过和原因。不同的人实施网络犯罪的原因不同。安全运营中心致力于打击网络犯罪。人们通过获得认证、接受正规教育以及利用就业服务获取实习经验和工作等方式，为安全运营中心（SOC）的工作做好准备。

1.1 危险

在本节中，您将会了解一些在网络安全舞台上常见的攻击事件，以及一些主要的威胁发起者和威胁的影响。

1.1.1 战争故事

在本小节中，您将会了解网络犯罪的三类受害者：个人、组织和国家/地区。

1. 被挟持的个人

Sarah 来到她最喜欢的咖啡店喝下午茶。她下了订单，向店员付了款，然后等待，与此同时，咖啡师争分夺秒地工作，处理积压的订单。Sarah 掏出手机，打开无线客户端，连接到她认为的咖啡店免费无线网络。

然而，坐在咖啡店角落里的黑客刚刚设置了一个开放的“欺诈”无线热点，假装是咖啡店的无线网络。当 Sarah 登录到她的银行网站时，黑客劫持了她的会话，并且获得了对她银行账户的访问权限。

在本课程中，您将了解一些安全技术，轻松预防这类攻击。

2. 被勒索的公司

Rashid 在一家大型上市公司的财务部门上班，他收到了 CEO 发来的一封包含 PDF 附件的邮件。该 PDF 与公司的第三季度收益情况有关。Rashid 不记得他的部门创建过这份 PDF。他好奇心高涨，便

打开了附件。

相同的情景在整个公司上演，其他几十名员工也被成功引诱，点击了附件。在员工打开 PDF 时，勒索软件被安装到员工的计算机上，开始收集和加密公司数据。可以推测攻击者的目标是获得经济利益，因为他们拿着公司的数据进行勒索，直到公司向他们支付酬金为止。

3. 国家/地区

最近出现的某些恶意软件创建起来非常复杂，而且成本高昂，以致于安全专家认为，只有国家（地区）层面才可能有创建这种恶意软件的影响力和资金实力。此类恶意软件可以定向攻击他国的脆弱基础设施，例如供水系统或电网。

这曾经是 Stuxnet 蠕虫的目标，它感染了一些 USB 驱动器，这些驱动器由 5 家某国组件供应商持有，目的是渗入这些供应商支持的核设施。Stuxnet 旨在渗入 Windows 操作系统，然后攻击 Step 7 软件。Step 7 是西门子公司为其可编程逻辑控制器（PLC）开发的软件。Stuxnet 寻找特定型号的西门子 PLC，它们控制核设施中的离心机。蠕虫从受感染的 USB 驱动器传送至 PLC 并最终损坏许多离心机。

Zero Days 是 2016 年发行的一部影片，记录了 Stuxnet 定向恶意软件攻击的开发和部署。您可以在互联网上搜索并观看这部影片。

1.1.2 威胁发起者

在本小节中，您将会了解到一些安全事件背后的威胁发起者的动机。

1. 业余爱好者

威胁发起者包括但不限于业余爱好者、黑客主义者、有组织的犯罪团伙、国家资助的黑客和恐怖组织。威胁发起者指的是对其他个人或组织执行网络攻击的个人或群体。网络攻击是蓄意的恶意行为，企图对其他个人或组织造成负面影响。

业余爱好者也称为脚本小子，他们几乎没有什么技能，而是经常使用从互联网找到的现有工具或教程发动攻击。其中有些只是出于好奇，而其他的则是想要造成危害以证明自己的技能。尽管他们使用的工具很基础，但结果依然具有破坏性。

2. 激进黑客

激进黑客指的是对抗各种政治和社会理念的黑客。激进黑客通过发布文章和视频、泄漏敏感信息以及在分布式拒绝服务（DDoS）攻击中利用非法流量中断 Web 服务，公开抗议组织或政府。

3. 经济利益

许多持续威胁我们安全的黑客活动以获取经济利益为动机。这些网络犯罪分子希望能够访问我们的银行账户、个人数据以及他们可以用来获得现金流动的任何其他信息。

4. 商业秘密和全球政治

过去几年，有许多关于黑客攻击其他国家/地区或干扰其内政的报道。有些国家/地区还对使用网络空间进行工业间谍活动感兴趣。抵御国家/地区赞助的网络间谍活动和网络战依然是网络安全专业人员的重要任务。

5. 物联网的安全程度如何?

物联网（IoT）无处不在，而且在迅速扩展。我们才刚开始从物联网中获益，而且还在不断开发万

物互联的新方法。物联网有助于人们连接万物从而改善生活质量。例如，现在有许多人正在使用可穿戴设备跟踪其健身活动。您目前有多少设备连接到您的家庭网络或互联网？

这些设备的安全程度如何？例如，谁编写的固件？程序员是否注意到安全缺陷？您的互联之家温控器是否易受攻击？您的数字视频录像机（DVR）是否易受攻击？如果发现了安全漏洞，能不能为设备中的固件安装补丁程序以消除漏洞？互联网上的许多设备没有更新到最新固件。有些旧设备甚至无法使用补丁程序更新。这两种情况给威胁发起者创造了机会，给设备所有者造成了安全风险。

2016 年 10 月，以域名提供商 Dyn 为目标的 DDoS 攻击摧毁了许多常用网站。这次攻击来自许多被恶意软件入侵的网络摄像头、DVR、路由器和其他物联网设备。这些设备形成了一个受黑客控制的“僵尸网络”。此僵尸网络被用来创建大规模的 DDoS 攻击，由此导致基础的互联网服务瘫痪。Dyn 发布了一篇博文，解释了这次攻击以及他们采取的响应措施。

美国约翰·霍普金斯大学计算机科学教授、信息安全学院技术主任 Avi Rubin 强调了不保护我们的互联设备的种种危害。您可以在互联网上找到他的 TED 演讲。

1.1.3 威胁的影响

在本小节中，您将会了解到网络安全攻击的潜在影响。

1. PII 和 PHI

网络攻击的经济影响很难精确地确定；然而，《福布斯》上的一篇文章表示，企业每年因网络攻击蒙受的经济损失估计达 4000 亿美元。

个人身份信息（PII）是指任何可用于确定个体身份的信息，例如：

- 名称；
- 社会保险号；
- 出生日期；
- 信用卡号；
- 银行账号；
- 政府签发的 ID；
- 地址信息（街道、电子邮件、电话号码）。

对于网络犯罪分子来说，更加有利可图的目标之一是获取 PII 列表，然后在暗网上销售。暗网只能使用特殊软件访问，被网络犯罪分子用来掩盖其活动。失窃的 PII 可以用来创建假账户，例如信用卡和短期贷款。

PII 的一个子集是受保护的健康信息（PHI）。医疗社区创建和维护包含 PHI 的电子病历（EMR）。在美国，PHI 的处理受健康保险转移与责任法案（HIPAA）管辖。欧盟也有同类法规，叫作“数据保护”。

大多数被新闻报道出来的针对公司和组织的黑客攻击都涉及失窃的 PII 或 PHI。仅在 2016 年的 3 个月里，就发生了以下攻击。

- 2016 年 3 月，一家医疗服务提供商的数据泄漏暴露了 220 万病人的个人信息。
- 2016 年 4 月，一家政府机构丢失了一台笔记本电脑和几块便携式驱动器，其中包含 500 万人的个人信息。
- 2016 年 5 月，一家就业服务公司的数据泄漏暴露了超过 60 万家公司的薪资、税费和福利信息。

2. 失去竞争优势

多家公司越来越担心网络空间里的商业间谍。另一个令人担忧的重要问题是，当公司无法保护客户的个人数据时，公司会失去信誉。有时，失去信誉（而不是商业秘密被另一家公司窃取）是导致公司失去竞争优势的更主要的原因。

3. 政治与国家安全

遭受黑客攻击的不仅仅是企业。2016 年 2 月，一名黑客公布了 20000 名美国联邦调查局（FBI）员工和 9000 名美国国土安全局（DHS）员工的个人信息。显然，这名黑客的动机是政治。

Stuxnet 蠕虫是为阻碍某国的铀浓缩进度而专门设计的。铀可以用在核武器中。Stuxnet 是以国家安全问题为动机的网络攻击的典型例子。网络战是非常有可能发生的。国家支持的黑客士兵会中断和破坏敌对国的重要服务和资源。互联网已成为商业和金融活动的重要媒介。这些破坏活动足以摧毁一个国家的经济。控制器（类似于 Stuxnet 攻击的那些设备）也可以用来控制水坝的水流和电网上的配电。针对此类控制器的攻击会产生可怕的后果。

1.2 打击网络犯罪的斗士

在本节中，您将会了解安全运营中心（SOC），以及如何成为网络安全舞台上的一名防卫者。

1.2.1 现代安全运营中心

在本小节中，您将会了解到 SOC 中的人员、流程和技术。

1. SOC 元素

抵御今天的威胁，需要格式化、结构化和纪律化的方法，而这正是安全运营中心的专业人员正在执行的方法。SOC 广泛提供各种服务，从监控、管理，到可以根据客户需求定制的全方位威胁解决方案和托管安全服务。SOC 可以完全在内部部署，归企业所有，由企业运营。也可以将 SOC 元素外包给安全服务提供商，例如思科的托管安全服务部。

图 1-1 所示为 SOC 的主要元素：人员、流程和技术。

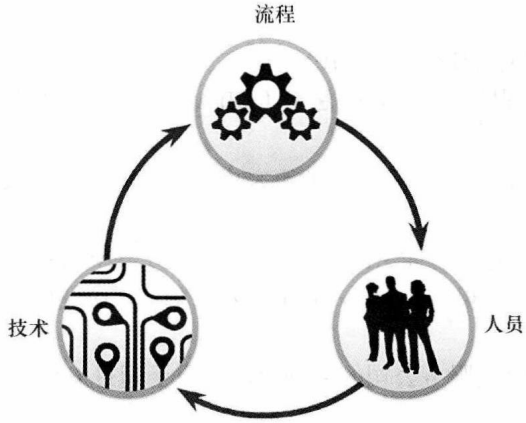


图 1-1 安全运营中心的元素

2. SOC 的人员

美国系统网络安全协会将人们在 SOC 中担任的角色分为 4 种职务。

- **一级警报分析师**：这些专业人员监控传入警报，确认发生了真正的事件，并在必要时将故障单转发给二级事件响应人员。
- **二级事件响应人员**：这些专业人员负责深入调查事件，并推荐应该要采取的补救措施或行动。
- **三级主题专家（SME）/搜索人员**：这些专业人员在网络、终端、威胁情报和恶意软件逆向工程等领域具备专家级技能。他们擅长跟踪恶意软件的进程，确定其影响，以及删除恶意软件。他们也深入地参与搜索潜在威胁并构建威胁检测工具。
- **SOC 经理**：该专业人员管理 SOC 的所有资源，并充当大型组织或客户的联系人。

本课程可以让您为获得适合一级警报分析师（也称为“网络安全分析师”）职位的认证做好准备。图 1-2 所示为这些角色相互作用的方式。

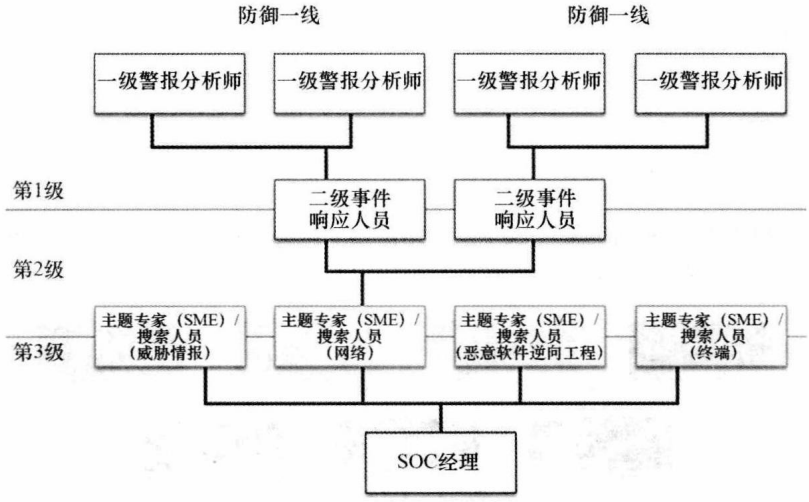


图 1-2 安全运营中心的人员角色

3. SOC 的流程

一级分析师的一天从监控安全警报队列开始。分析师通常会用故障单系统从队列中选择要调查的警报。因为生成警报的软件可能触发假警报，所以一级分析师的工作之一是确认安全警报代表真正的安全事件。确认成立的安全事件会被转发给调查者或者其他安全人员处理，其他的则被视为假警报。

如果故障无法解决，一级分析师会将故障单转发给二级分析师，进行更深入的调查和补救。如果二级分析师无法解决故障，则会将故障单转发给具有深厚知识积累和高超威胁搜索技能的三级分析师。

图 1-3 总结了一级、二级和三级分析师的角色。

4. SOC 中的技术

如图 1-4 所示，SOC 需要用到安全信息和事件管理系统（SIEM）或同等系统。此系统将来自多种技术的数据组合在一起。SIEM 系统用于收集和过滤数据、检测并分类威胁、分析和调查威胁，以及管理资源，以实施预防措施和抵御未来威胁。SOC 技术包括下列一项或多项：