第2页

关于记录的未来

Recorded Future提供安全情报以扩大
安全和IT团队在减少风险方面的效率
通过发现未知威胁并更快通知他人
决定。致力于提供单一的数字视图，
品牌和第三方风险，即“记录的未来”计划
提供事实和预测情报，分析数据
来自开放，专有和聚合的客户提供
资料来源。记录未来武器威胁分析师，脆弱性
管理团队，安全运营中心和事件
真正具有上下文丰富，可操作的情报的响应者
我已经准备好将其集成到整个安全生态系统中。
了解更多信息，请访问www.recordedfuture.com并关注我们
@RecordedFuture上的Twiter 。

第3页

威胁情报手册

第二版

迈向安全情报计划

Zane Pokorny编辑

˚F oreword由克里斯托弗·阿尔伯格博士

威胁情报手册第二版

由...出版：
CyberEdge Group，LLC
1997安纳波利斯交流公园大道
300套房
安那波利斯（马里兰州）21401
（800）327-8711
www.cyber-edge.com

有关CyberEdge Group研究和营销咨询的一般信息
服务，或为您的组织创建自定义的权威指南，请联系
我们的销售部门，电话：800-327-8711或info@cyber-edge.com。

ISBN：978-1-948939-06-5（平装）
ISBN：978-1-948939-07-2（电子书）

在美利坚合众国印刷。

10 9 8 7 6 5 4 3 2 1

发行人致谢

CyberEdge Group感谢以下个人的各自贡献：

复制编辑： Susan Shuttleworth
平面设计： Debbi Stocco
生产协调员：乔恩·弗里德曼

贡献者

Zane Pokorny（编辑兼撰稿人）是技术作家
代表Recorded Future的研究团队Insikt Group。他有一个
非政府组织的研究和报告撰写背景
tal组织。

Andrei Barysevich（撰稿人）专门从事分析
来自Recorded的网络犯罪社区的情报
未来。Andrei曾担任独立电子商务
欺诈研究人员，以及联邦调查局（FBI）网络的私人顾问，
犯罪单位。

Levi Gundert（贡献者）在过去的20年中一直在
在政府和私营部门中，捍卫
网络，逮捕国际罪犯，并发现
民族国家的对手。他拥有高级信息
技术和金融领域的安全领导职位
服务初创企业和企业。他是值得信赖的风险顾问
财富500强公司，多才多艺的演讲者，博客和
专栏作家。

Allan Liska（撰稿人）是
记录的未来。艾伦拥有超过15年的经验
信息安全领域，撰写了大量书籍和著作，
作为安全从业者和道德黑客。

Maggie McDaniel（撰稿人）是
记录了Future的Insikt Group研究团队。还有更多
在威胁情报行业拥有15年以上的经验，
分析和生产，Maggie以前的角色包括
Fidelity Investments的情报生产总监。

John Wetzel（撰稿人）在Recorded负责培训
未来。约翰曾担任反情报专家，
他曾在国防部工作的特工

与美国国防界一起防御外国
针对国家技术的威胁。

共同创始人**克里斯托弗·阿尔伯格（Christopher Ahlberg）博士的**前言
记录未来的首席执行官。

6页

目录

第7页

第8页

第9页

第10页

前言
第二版

当我打赌我打赌信息的未来
我大约十年前开始录制未来时，
安全性在于从被动式转变为主动式
安全专业人员将使用威胁的方法
情报从互联网的各个角落收集到
让我们深入了解我们的意图和技术
对手。

此后的十年中，
网络安全。似乎每天的新闻都充满故事
有关重大数据泄露的事件影响了数百万人，
整个城市的网络被人质绑架
勒索软件攻击，以及操纵国家行为者
选举，影响舆论并迫害选举
敌人。“网络战”正在成为一个熟悉的词-
今天我们无法想象没有网络因素的战争
在每个运营级别都扮演着至关重要的角色。

我们最宝贵的信息不再被锁定
文件柜或保险箱，但在我们的计算机和
云。仅仅锁定您的端点并
对您自己的网络内的可疑行为保持警惕。
目前，威胁的范围太大了。我们需要
以获得实时，自动化的威胁情报
可以迅速采取行动，帮助他们制止的人
快速威胁-有时甚至还没有发生。

该目标激发了我们在《唱片未来》中所做的所有工作。
我们的工作基于以下三个原则：

***1.*威胁情报必须提供背景信息**
做出明智的决定并采取行动。

威胁情报需要及时，清晰并采取行动-
能够。它必须在正确的时间以某种形式出现
可以理解的。它应该丰富您的知识，而不是
决策过程复杂化。应该有帮助

第11页

将您组织中的每个人都放在同一页面上。

*2.***人与机器更好地协作。**

机器可以处理和分类原始数据订单
比人类快得多。另一方面，
人类可以执行直观的大图分析
比任何人工智能都要好-只要它们是
不被庞大的数据集分类所淹没，
做乏味的研究。当人与机器
配对时，每个工具都会更智能地工作，从而节省时间和金钱，并减少-
改善人的职业倦怠，提高整体安全性。

*3.***威胁情报适合所有人。**

无论您扮演什么安全角色，威胁情报
有所作为。它不是secu-的单独领域
道德–无论您是靠什么背景，都可以帮助您更聪明地工作
您正在维护SOC，管理漏洞或制造
高级别的安全决策。但是为了使事情变得容易，
不难，威胁情报应与
您已经依赖并且应该是的解决方案和工作流程
易于实现。

在Recorded Future，我们全心全意地相信这些核心
原则，并且我们的方法已在当年得到验证
自该手册第一版问世以来。我们正在帮助-
在《财富》杂志的90个安全部门中制止威胁
美国排名前100位的公司
周围无数的组织和政府机构
世界。现在，我们已经从现在的400多名员工
40个国家。

我们继续创新并提高我们的智慧
解决方案。其中包括本手册，
第二版更新了三个新章节。我们已经
赋予此版本副标题为“迈向安全
情报计划”，而这些新章节将对此进行介绍
每个组织都必须采取的转变：向
安全情报，其中一种新的安全范式
威胁情报只是其中一部分。

威胁无处不在（开放网络，黑暗网络，
合作伙伴，内部，品牌攻击）以及对您的真实看法
需要整个威胁面，否则您将很脆弱。那
采用包含威胁情报的安全解决方案

第12章

您可以将其与内部网络数据，数字风险相关联
保护和第三方风险管理。

我们希望本手册能在帮助您实现
通过提供实用的信息和建议来实现这一转变
您今天就可以申请解决具有威胁的现实问题
情报。

我要感谢所有为内容做出贡献的人
本手册中的内容：我们的用户和客户，行业专家，
和“记录的未来” sta列在**贡献者上**
本卷开头的页面。

我们希望您能从这本更新的书中找到有用的信息，
在应用威胁情报以解决安全问题时恐慌
您面临的挑战。

Christopher Ahlberg博士
联合创始人兼首席执行官
记录的未来

第13页

介绍

迈向安全
情报计划

牛逼

并放网络和黑暗网络，还有合作伙伴和其他
第三方，品牌攻击和内部威胁以及数字化
商业风险空前高涨。这让每个人
没有真实，全面地了解其整个威胁
景观脆弱。

全面的网络安全策略要求
积极实施技术
降低风险并快速阻止威胁。这本书解释了如何
安全情报可帮助从事安全工作的团队
操作，事件响应，漏洞管理，
风险分析，威胁分析，欺诈预防和安全性
领导制定更好，更快的决策并扩大他们的决策
影响。

我们称这种方法为“安全情报”，因为
不仅仅是威胁情报（尽管威胁情报
仍然是中心支柱），并且还包含数字风险
保护和第三方风险管理。这是一个框架
通过以下方式增强了安全团队和工具的有效性：
揭露未知威胁，提供更好的决策，以及
达成共识以最终提高风险

减少整个组织。

在本手册的第二版中，您会发现
关于威胁情报的全新介绍性章节
可以分解什么是威胁情报，以及如何
安全功能从中受益，还有两个全新的功能
各章—一章涉及降低第三方风险，一章涉及
数字风险保护。在一起，这三个安全支柱
智能为您提供全面的了解
每个组织的内部和外部威胁情况

今天需要减少网络风险并领先于威胁
所有种类。

这仅仅是开始。录制的未来即将出版
新材料将在以下三个方面进行更深入的研究
安全情报，它们如何相互增强，以及如何
它们可以通过单个技术平台解决。对于
更多信息，请定期访问recordedfuture.com。

—记录下来的未来团队

章节一览

第1节：什么是威胁情报？

第1章“什么是威胁情报”概述了
威胁情报的价值以及操作和防御的作用
战略威胁情报。

第2章，“威胁情报生命周期”
描述威胁情报生命周期的各个阶段，并
查看威胁情报的来源。

第2节：威胁情报的应用

第3章，“威胁安全智能”
运营”一文，探讨了情报如何为
分流并帮助SOC团队做出更好的决策。

第4章，“事件的威胁情报”
回应”，讨论如何最大限度地降低智力
在事件响应中的反应性，并提出了三个用例。

第5章，“威胁的威胁情报”
管理”一文，探讨了智能如何帮助确定优先级
基于对企业的真实风险的漏洞。

第6章，“安全主管的威胁情报”
探索如何构建全面的威胁情报
能力可以帮助CISO管理风险并提高效率
投资决策。

第7章，“用于风险分析的威胁情报”
解释风险模型的价值以及情报如何
提供有关攻击概率和成本的硬数据。

第8章，“欺诈威胁情报”
预防”，列举了智力如何提供帮助
预测并击败欺诈行为。

第9章，“减少第三人称的威胁情报”
政党风险”，建议情报如何帮助评估
供应链合作伙伴，降低第三方风险。

第10章，“针对数字风险的威胁情报”
保护”，说明了智能如何帮助识别
并纠正品牌假冒和数据泄露行为。

第*3*节：您的威胁情报计划

第11章，“威胁分析框架”
情报”，解释了三个主要威胁框架的方式
提供用于思考攻击的有用结构。

第十二章“您的威胁情报之旅”
提供有关如何从简单开始并逐步扩大规模的建议
威胁情报程序。

第13章，“开发核心威胁情报”
团队”，描述了一支敬业的团队如何应对威胁
智力提升到新水平。

有用的图标

小费　提示提供实用建议，您可以自己应用
组织。

别忘了　当您看到此图标时，请注意，作为相关内容
包含您不会忘记的关键信息。

警告　谨慎行事，因为如果您不这样做，可能会付出高昂的代价
给您和您的组织。

技术交流　与该图标关联的内容本质上是技术性的
适用于IT从业人员。

在网上　想了解更多？按照相应的URL
发现网络上可用的其他内容。

第1节：什么是威胁情报？

第1章

什么是威胁情报?

在这一章当中

- 了解为什么威胁情报很重要
- 了解运营和战略威胁情报
- 探索威胁源的作用和监视的价值
- 私人频道

“每场战斗都将赢得胜利。”

—孙子

您听到了什么威胁情报?

会议贸易展览演讲或由威胁情报提供外部信息的顾问

安全决策的环境。也许您阅读了有关
国家发起的攻击，并且想知道如何保护您的
企业。您可能已经注意到，在组织中
从跨国企业到中型企业，
信息安全团队正竞相增加威胁情报，
对他们的安全计划有兴趣。

但是您可能也听到了一些误解：
威胁情报只是数据馈送和PDF报告，仅仅是
事故响应小组的研究服务，或需要
高价，精英分析师的专业团队。

第20话

这些都是谬论！在本书中，我们将展示这种威胁
情报：

- ☑包含来自丰富阵列的信息和分析
  的来源，以易于实现的方式呈现
  了解和使用
- ☑对
  网络安全组织
- ☑可以帮助每个安全功能节省时间
- ☑大部分可由现有安全人员处理
  （使用正确的工具和支持）

为什么是威胁情报重要？

如今，网络安全行业面临众多挑战
-越来越顽固和狡猾的威胁行动者；每天
充满大量无关信息和错误警报的数据
跨多个未连接的安全系统；和一个严重的
缺乏熟练的专业人员。

尽管在全球范围内将花费约1,240亿美元
2019年网络安全产品和服务投入巨资
这些问题还远远不够。马上：

- ☑四分之三的安全组织都有经验-
  缺乏技能
- ☑未调查44％的安全警报
- ☑66 ％的公司至少被违反一次

来源：*Gartner*预测分析：信息安全，
全球，*2018*年第二季度更新；*ESG*和*ISSA*研究报告：
网络安全专业人员的生活和时代*2018;* 思科公司
*2017*年年度网络安全报告；*Ponemon 2019*的成本
数据泄露研究

第21话

数字技术是几乎每个行业的核心
今天。他们的自动化和更大的联系
奥德正在改变世界，但他们也在带来
网络攻击的脆弱性增加。

威胁情报是使您能够预防的知识
并减轻对数字系统的攻击。根植于数据，威胁
情报提供背景信息，例如谁在攻击您，
他们的动机和能力是什么，以及
在系统中寻找危害（IOC）。它可以帮助你
对您的安全性做出明智的决定。

谁可以受益
威胁情报？

大家！威胁情报被广泛认为是
精英分析师领域。实际上，它可以在整个安全领域增加价值
适用于各种规模组织的功能。例如：

☑**安全运营团队**通常无法执行
处理大量的警报
接收。威胁情报可以与
他们已经使用的安全解决方案，可以帮助他们
自动确定优先级并过滤警报和其他
威胁。

☑**漏洞管理团队**需要
准确地确定最重要的脆弱性的优先级
联系。威胁情报可提供对外部威胁的访问
有助于他们与众不同的见解和背景
对其特定企业的直接威胁来自
仅仅是潜在的威胁。

☑**欺诈预防，风险分析**及其他
高级别安全人员面临的挑战是-
抵御当前的威胁形势。威胁情报
Ligence提供了有关威胁行为者，他们的关键见解
意图和目标及其战术，技巧，
和程序（TTP）。

第22话

图1-1列出了显示巨大改进的指标
在安全性和效率方面，威胁情报程序
可以提供。

图1-1：威胁情报程序可以产生戏剧性的效果
改善安全性和运营效率。来源
数据：IDC

本书的第2节专门探讨这些内容和其他内容
安全用例的详细信息。

资料与资讯
不是智力

在继续之前，我们先清除一下有关
数据，信息和情报。

这三个术语有时使用时并没有多大注意。
例如，某些威胁源被宣传为情报
当它们实际上只是数据包时。经常，
组织将威胁数据源整合到他们的网络中
只是发现他们无法处理所有多余的数据
只会增加试图对威胁进行分类的分析师的负担。在
相比之下，威胁情报通过帮助减轻了负担
分析人员决定要优先考虑的事项和要忽略的事项。的
图1-2中的表格突出了重要的区别。

第23话

数据由离散事实和统计**数据**组成
进一步分析的基础。

信息是多个数据点的组合
回答特定问题。

智能分析数据和信息以发现
有助于决策的模式和故事。

图1-2：数据，信息和数据之间的区别
情报

在网络安全方面：

- ☑数据通常只是IP地址，URL或哈希。数据不能告诉我们很多
  分析。
- ☑信息回答诸如“我的组织在社会上曾被提及过
  媒体这个月？”虽然这是更多用途-
  比原始数据更有效的输出，它仍然不会直接
  通知特定的动作。
- ☑情报是识别周期的产物，问题和目标，收集相关数据，
  处理和分析该数据，产生可操作的

情报，并分发该情报。好
深入了解威胁情报生命周期
第2章中的深度。

数据，信息和情报之间的关系
如图1-3所示。

第24话

图1-3：数据，信息和数据之间的关系
情报

两种威胁情报

威胁情报是一个广泛的概念，是一个真正的概念
两种情报-**运营**情报和**战略**情报。
这两类情报的来源各不相同，
它们提供的服务及其显示的格式。

做出这种区分的目的是要认识到
各种安全功能具有不同的目标和程度
技术知识。就像我们上面说的，智力
需要采取行动-但由于
漏洞管理团队与那些团队明显不同
对于CISO而言，“可操作性”对每个人都有不同的含义，
以及他们将从中受益的情报的形式和内容
大部分来自不同。

行动威胁情报

运营威胁情报是关于
持续的网络攻击，事件和活动。它给事件
响应团队的专业见解可帮助他们-
承受特定攻击的性质，意图和时机
正在发生。它通常来自机器。

第25话

运营智能有时被称为**techni-**
校准威胁情报，因为它通常包括技术
有关攻击的信息，例如哪些攻击媒介
正在使用，正在利用哪些漏洞以及哪些漏洞
命令和控制域被攻击所利用-
ers。这种情报通常对人员最有用
直接参与组织的防御，例如
系统架构师，管理员和安全人员。

常见的技术信息来源是威胁数据
饲料。这些通常只关注一种威胁指标，
例如恶意软件散列或可疑域。当我们讨论
在下面，威胁数据提要为威胁情报提供输入，
但它们本身并不是威胁情报。

小费 操作威胁情报的一种用途是指导改进-
现有安全控制，流程和速度的评估
事件响应。因为运营情报可以
回答您组织特有的紧急问题，例如
如：“是这个严重漏洞，正在被利用吗？
我的行业，出现在我的系统中吗？”—整合了
从网络中获取数据非常重要。

战略威胁情报

战略威胁情报提供了对
组织的威胁格局。这对于提供信息最有帮助-
制定高管的高层决策，内容是
通常面向业务，并通过报告呈现
或简报-确实不能由以下人员生成的材料
机器，但只能由具有专业知识的人员操作。

这种智能需要人为因素，因为
评估和测试新对手需要时间和思想
现有安全性的战术，技术和程序
控件。这个过程的各个部分可以自动化，但是人类
完成这项运动在很大程度上需要大脑。

良好的战略情报应能洞悉
与某些行动相关的风险，威胁的广泛模式
演员的策略和目标，地缘政治事件和趋势，以及
类似的话题。

26页

战略威胁情报的通用信息来源
权限包括：

- ☑来自民族国家或非政府组织的政策文件-
  精神组织
- ☑来自当地和国家媒体的新闻，
  行业和特定主题的出版物，以及
  主题专家的意见

☑白皮书 网络安全组织制作 研究报告和其他内容

组织必须制定战略威胁情报要求，
通过提出针对性的，具体的问题进行思考。分析师
典型网络安全技能以外的专业知识-尤其是，
对社会政治和商业道德的深刻理解
cepts –收集和解释战略威胁是必需的
情报。

生产战略威胁情报的某些部分
应该是自动化的。尽管最终产品是非技术产品，
产生有效的战略威胁情报
深入研究和大量数据（通常跨多个
尖语。这些挑战可以使初始数据集
处理和处理非常困难，无法手动执行，即使对于
那些拥有正确语言技能，技术-
道德背景和技巧。威胁情报解决方案
自动化数据收集和处理的功能有助于
减轻这种负担，使专业知识较少的分析师可以
更有效地工作。

威胁数据馈送的作用

前面我们提到数据不是智能，
威胁数据源可能使已经负担沉重的分析师不堪重负
每天都有无数的警报和通知。但是当使用
正确地，威胁数据源可以提供有价值的原材料
用于威胁情报。

威胁数据馈送是提供以下内容的实时数据流
有关潜在网络威胁和风险的信息。他们是我们
集中于单个指标的简单指标或工件的盟友列表
感兴趣的区域，例如可疑域，哈希，不良IP或

第27话

恶意代码。他们可以提供一种快速获得收益的简便方法，
实时查看威胁情况。

但是许多供稿，尤其是免费供稿，充满了错误，
裁员和误报。这就是为什么重要
选择高质量的数据供稿。

评估威胁数据源

使用这些标准评估威胁
您的组织的数据提要：

数据来源：网络威胁情报
gence提要从所有提要中获取数据
各种来源，其中许多是
与您的组织无关。
例如，您将获得最大收益
从收集的数据中获取价值
您所在行业的组织。

来源的透明度：了解
数据来自哪里
帮助您评估其相关性，以及
用处。

唯一数据的百分比：一些
付费提要只是以下内容的集合
数据来自其他提要
他们列出了几个相同的项目
梅斯。

数据周期：多长时间
数据相关吗？与spe-有关吗？
重要的，即时的行为，并且确实
它提供有关以下方面的战略情报
长期趋势？

可衡量的结果：计算
一个可测量的结果
特定的饲料通常涉及
跟踪相关率
是警报的百分比
与您的内部相对应
在给定的一周，一个月内进行遥测
或四分之一。

小费 使用威胁，而不是分别查看几十个提要
情报平台，将它们全部合并为一个供稿，
删除重复项和误报，并将其与
内部遥测，并生成优先警报。最多
强大的威胁情报平台甚至可以组织
创建自定义威胁情报源或策展和
设置自动警报。

私人频道的作用和黑暗网

威胁数据源和公开信息不是
威胁情报的唯一外部数据源。重要
针对特定攻击的运营和战略情报，
攻击者TTP，黑客主义者和国家行为者的政治目标，

第28页

其他关键主题可以通过渗透或突破来收集-
进入威胁使用的私人通信渠道
组。其中包括加密的短信应用和专有
黑暗网络上的sive论坛。

但是，收集此类
情报：

- ☑**访问**：威胁组可以通过优先级进行通信
  vate和加密的频道，或需要一些证明
  识别。
- ☑**语言**：在许多论坛上进行的活动
  以俄语，中文，印尼语或
  阿拉伯语，使用当地语和专业术语。
- ☑**噪音**：可能很难或无法手动进行
  从大量资源中收集良好的情报
  例如聊天室和社交媒体。
- ☑**混淆**：为避免被发现，许多威胁
  小组采用混淆策略，例如使用
  代号。

克服这些障碍需要对工具进行大量投资
和专业知识来监控私人频道-或使用
已经做出的威胁情报服务提供商
这项投资。

小费 寻找采用的威胁情报解决方案和服务
机器学习过程，用于在机器上自动收集数据
规模大。使用自然语言处理的解决方案，
例如，可以从外语收集信息
无需人工就可以破译。

第29话

第2章

威胁情报生命周期

在这一章当中

检查威胁情报生命周期的各个阶段

审查威胁情报的来源

查看威胁情报工具和人员的作用分析师

“您必须相信自己的过程。”

—汤姆·布雷迪

威胁的六个阶段情报生命周期

牛逼

几十年来，由政府和军事机构threat情报是建立在磨练分析技术提示。传统情报关注六个不同的阶段组成所谓的“智能周期”：威胁情报为许多这些问题提供了解决方法。除其他用途外，它还可用于滤除虚假信息警报，加快分类并简化事件分析。

1个方向

2.收集

3.加工

4.分析

5.传播

6.反馈

第30话

图2-1显示了这六个阶段如何与威胁保持一致情报。

图2-1：威胁情报和英特尔-的六个阶段
潜伏周期。

方向

生命周期的方向阶段是您设定目标
威胁情报程序。这涉及理解
并阐明：

- ☑信息资产和业务流程
  需要保护
- ☑失去这些资产或相互之间的潜在影响
  破坏那些过程
- ☑表示安全性的威胁情报类型
  组织需要保护资产并做出回应
  面对威胁
- ☑有关保护内容的优先事项

确定高层次的情报需求后，
国家化可以提出满足需求的问题。
信息变成离散的需求。例如，如果一个目标
是为了了解可能的对手，一个合乎逻辑的问题是
是的，“地下论坛中的哪些参与者正在积极征集-
有关我们组织的数据？”

第31话

目标库

Recorded Future已创建一个列表
预先配置的情报目标
其中包括最常见的
全球情报需求
500个组织。此列表有帮助
公司面临威胁
智力思考他们的问题
和优先级，并决定如何
可以插入威胁情报
进入他们现有的流程。
从该库中选择的目标是
包含在本附录中
书。

对抗模型，例如
洛克希德·玛恩网络杀人链
和MITER对抗战术，
技术与常识
（ATT＆CK）矩阵（在
第11章），也可以帮助比较
nies专注于威胁的类型
他们需要收集的情报
防止违反。

采集

收集是收集信息以解决的过程
最重要的智力要求。信息
聚集可以通过多种方式进行，
包含：

和安全设备
☑从内部网络提取元数据和日志
☑订阅来自行业组织的威胁数据
民族和网络安全厂商
☑与
知识渊博的来源
☑扫描开源新闻和博客
☑抓取和收获网站和论坛
☑渗透到封闭的资源中，例如黑暗的网络论坛

通常收集的数据将是已完成的
信息，例如网络安全情报报告
专家和供应商，以及原始数据，例如恶意软件签名或
粘贴站点上的凭据泄漏。

第32话

16 | 威胁情报手册

威胁情报来源

技术来源（例如威胁
供稿）-数量庞大，
联系，通常是免费的。技术
来源易于整合
现有安全技术，但
通常含有很高的比例
误报和过时
结果。

媒体（例如安全网站，
供应商研究）-这些资源
经常提供有用的信息
关于新出现的威胁，但是
很难与技术联系
指标以衡量风险。

社交媒体-的社交渠道
提供大量有价值的数据，
但这是有代价的。错误的
ves和misinforma on都是
喘气，因此确定哪些见解
可用需要巨大
与的交叉引用量
其他来源。

威胁演员论坛—特别是
旨在举办相关讨论-
意见，论坛提供了一些
最有用的见解
任何地方。再说一次
分析和交叉引用是
essen al确定什么是真正的
有价值。

暗网（包括市场）
和论坛）-虽然通常
宝贵的发源地
情报，黑暗的网络资源
可能很难访问，
特别是那些主持
严重的刑事通讯。

您需要多种情报来获得完整的信息
潜在和实际威胁的图片。如图2-1所示，
它们包括**内部来源，**例如防火墙和路由器日志，
网络数据包捕获工具，以及漏洞扫描，**techni-**
校准源，例如漏洞数据库和威胁数据
饲料和**人类资源**，包括传统和社会
媒体，网络安全论坛和博客以及深色网络论坛。
错过其中任何一项都可能减慢调查速度，
造成补救方面的空白。

小费 自动化！分析师应该花费尽可能少的时间
选择数据，并尽可能多地评估和
传达威胁信息。

对威胁情报之间的差异感到困惑
来源，提要，平台和提供者？阅读记录
未来的博客文章“威胁情报：两者之间的区别
平台和提供商。”

第33章

处理中

处理是收集信息的转换
转换为组织可用的格式。几乎所有原始数据
收集到的需要以某种方式处理，无论是通过
人或机器。

不同的收集方法通常需要不同的手段
处理。人工报告可能需要关联，并且
排名，取消冲突和检查。一个例子可能是
从安全厂商的报告中提取IP地址，以及
将它们添加到CSV文件中，以导入到安全信息中-
动作和事件管理（SIEM）产品。在更多技术中
关键区域，处理过程可能涉及从中提取指标
一封电子邮件，用其他信息丰富他们，然后
与端点保护工具通信以实现自动化
封锁。

小费 自动化更多！使用正确的工具，大多数处理工作-
流程以及大多数收集过程可以自动化。
例如，安全自动化工具可能会识别出
恶意的国际奥委会，然后进行一系列检查，
发给国际奥委会的短信。这使分析师不必进行
那些手动检查。

分析

分析是将已处理的信息转化为人类的过程
可以指导决策的情报。取决于
在这种情况下，决策可能涉及是否要投资-
缓解潜在威胁，应立即采取哪些措施
阻止攻击，如何加强安全控制或如何
在额外的安全资源上进行大量投资是合理的。

分析师必须对谁去做有一个清晰的了解
运用他们的智慧以及那些人的决定
使。您希望将您提供的情报视为
可行，而不是学术性的。这本书的大部分致力于
让您清楚地了解威胁情报的确切方式
可以改善以下方面的决策和行动
网络安全。

信息的呈现形式尤其如此
重要。收集和处理无用且浪费

第34页

信息，然后以不容小\under的形式提供它-
由决策者站立和使用。

例如，如果您想与非技术人员进行交流
领导人，您的报告必须：

☑简明扼要（一页备忘录或几张幻灯片）

☑避免混淆和过分的技术术语和行话

☑用业务术语阐明问题（例如，直接和间接费用及其对声誉的影响）

☑包括推荐的行动方案

某些情报可能需要以多种方式传递
例如，通过实时视频供稿和
PowerPoint演示文稿。并非所有情报都需要
通过正式报告摘要。成功的威胁情报
团队向其他安全部门提供持续的技术报告
具有围绕IOC，恶意软件，威胁的外部环境的团队
行为者，漏洞和威胁趋势。

传播方式

传播涉及完成的情报输出
到需要去的地方。

如图2-1所示，大多数网络安全组织
至少有六支可以从威胁情报中受益的团队-
权限。对于这些受众中的每一个，您需要提出以下要求：

☑他们需要什么威胁情报，以及如何外部信息是否支持他们的活动？

☑应该如何展示智慧它对此很容易理解和可操作听众？

☑我们应该多久提供一次更新和其他信息？

☑情报应通过哪种媒体传播了吗？

☑如果他们有疑问，我们应该如何跟进？

第35页

反馈

毫无疑问，我们相信这是至关重要的
重要的是要了解您的整体智力优先事项
以及安全团队的要求
总结威胁情报。他们的需求指导着
情报生命周期并告诉您：

☑收集什么类型的数据

☑如何处理和丰富数据以将其转化为有用的信息

☑如何分析信息并将其呈现为可行情报

☑必须向每个人散布各种情报指定的传播时间，以及回答问题的速度

您需要定期反馈，以确保您了解
每个小组的要求，并根据自己的需要进行调整
需求和优先级改变。

小费 对于每个“客户”团队，都要建立一个快速渠道，非正式反馈（例如电子邮件地址，内部论坛或团队协作工具）和正式的，结构化的调查过程（例如在线调查或季度调查面对面的会议）。非正式渠道可帮助您做出反应并立即进行调整，同时结构化调查可确保您可以从所有人那里得到输入，并可以跟踪您的进度随着时间的推移。

工具和人员

工具对于自动化收集，处理，和生命周期中的传播步骤，以及支持和加速分析。没有合适的工具分析师将把所有的时间都花在这些任务，再也没有时间进行真正的分析。

第36话

大多数成熟的威胁情报组利用两种类型的工具：

- ☑旨在用于以下方面的威胁情报解决方案收集，处理和分析所有类型的威胁数据来自内部，技术和人力资源
- ☑现有的安全工具，例如SIEM和安全性分析工具，可收集和关联安全性事件和日志数据

人类分析人员同样重要，甚至更为重要。你不能依靠工具采访安全专家并调查关闭黑暗的网络论坛，您需要人们进行分析和综合，为安全组织中的人员提供规模情报，以及谁会消耗它的管理人员。

分析人员不需要属于主要的精英威胁情报部门。虽然有人需要组织范围内的威胁情报功能视图，做出有关资源和优先级的决策，并进行跟踪进步，我们已经看到许多成功的组织结构-tures。您可能会有一个中央小组，有专门的威胁情报分析师或事件内部的一小群人响应（IR）或安全运营中心（SOC）组织的位置。另外，不同网络安全的成员组可以负责分析威胁情报他们的同事。

在第12章中，我们将讨论组织结构通常随着威胁情报功能的成熟而发展。在第13章提供有关如何组织核心威胁的建议情报团队。

第37页

第2节：
威胁情报

第39部分

第3章

威胁情报
安全运营

在这一章当中

了解“警报疲劳”如何冒着破坏安全良好工作的风险运营中心（SOC）

了解情境对改善分类的价值

了解威胁情报如何减少浪费的时间，并SOC团队做出更好的决策

“最坏的情况会让您先行。”

—登录医院急诊室

中号

host持人质以产生大量警报。OST安全运营中心（SOC）团队发现他们-通过他们监控的网络。还要对这些警报进行分类时间长了，许多根本没有被调查过。“警惕疲劳”导致分析师对警报的重视程度不如应有。

威胁情报为其中许多提供了解决方法问题。除其他用途外，还可用于过滤错误警报，加快分类并简化事件分析。

SOC团队的职责

从表面上看，SOC团队的职责似乎很简单：

- ☑**监控**潜在威胁
- ☑**检测**可疑的网络活动
- ☑**包含**主动威胁
- ☑使用可用技术进行**补救**

第40话

当检测到可疑事件时，SOC团队会进行调查-减轻影响，然后与其他安全团队合作以减少攻击的影响和严重性。你可以想到的角色SOC内部的职责类似于紧急服务团队响应911呼叫，如图所示图3-1。

图3-1：应急服务的作用和职责
团队和SOC团队相似。

大量的警报

在过去的几年中，大多数企业都增加了新的
网络威胁检测技术的类型。每一个
看到异常或可疑时，工具会发出警报
行为。结合起来，这些工具会产生刺耳的声音
安全警报。安全分析师根本无法
自行检查，设置优先级并调查所有这些警报。
由于警报疲劳，他们常常忽视警报，追逐
误报，并犯错误。

研究证实了这些问题的严重性。行业
分析公司ESG向网络安全专业人员询问有关
他们最大的安全运营挑战，还有35％
表示“正在跟上安全警报的数量”。在
其SOC的2018国家报告，SIEM供应商Exabeam
揭示SOC的利用率不足45％
在其中工作的专业人员中，占63％

第41话

认为他们可以在另外两个到十个地方使用
雇员。思科2018年安全功能基准测试
研究发现组织只能调查56％
他们在某一天收到的安全警报，以及
经调查的警报中，只有34％被认为是合法的
（图3-2）。

图3-2：许多威胁警报未得到调查或补救。
（来源：思科）

情境为王

从根本上讲，SOC的威胁情报就是要丰富
内部警报以及外部信息和上下文
做出基于风险的决策所必需的。上下文对于
快速分类，这对于范围界定和遏制也很重要-
事件。

第42话

分流需要很多背景

在平均SOC分析师的日常工作中，很大一部分时间用于响应-
由内部安全系统生成的警报，例如
SIEM或EDR技术。内部数据的来源至关重要
识别潜在的恶意网络活动或数据
违反。

不幸的是，这些数据通常很难在isoola中解释-
tion。确定警报是否相关且紧急需要
收集各种各样的相关信息（上下文）
内部系统日志，网络设备和安全工具
（图3-3），以及来自外部威胁数据库。正在搜寻
每个警报周围的所有这些威胁数据源都是
非常耗时。

关键方面	安全监控要求
业务流量 穿越 边界	
活动在 边界	
内部 工作站， 服务器或设备	
内部网络 活动	
网络 连接数	
会议活动 通过用户和 工作站	
提醒 大事记	
准确的时间 在日志中	
数据备份 状态	

图3-3：安全监控和内部的关键方面
上下文的来源。（来源：英国NCSC）

第43话

用例：相关和丰富警报

分析师试图对没有访问权限的初始警报进行分类
足够的上下文就像一个试图理解新闻的人
阅读标题后的故事。即使当分析师
可以以威胁源的形式访问外部信息
（图3-4），该信息很难吸收和
与与警报有关的其他数据相关。

图3-4：在原始中查找相关信息非常困难
威胁提要，并将其与与警报相关的其他数据相关联。

威胁情报，或更准确地说，是传递的信息
通过威胁情报解决方案，可以完全
改变局势。这样的解决方案具有
自动将威胁数据充实为情报并进行关联
它带有警报，如图3-5所示。提供的上下文
可能包括对某件物品的首次引用和最新引用
恶意软件或可疑IP地址，发现次数，
与攻击类型和特定威胁参与者的关联，以及
恶意软件行为描述或使用
IP地址（例如，作为僵尸网络的一部分）。

第44页

图3-5：威胁情报解决方案可以自动丰富
具有上下文的警报，例如先前的目击事件，关联
攻击类型和威胁参与者以及风险评分。（资源：
记录的未来）

这种丰富的功能使SOC分析人员可以快速确定
最重大的威胁并立即采取明智的行动
解决它们。

充实可以让SOC中相对较低的分析师进行
通过建立与其他人的联系来“超重”
明智的做法将需要更多经验。它还提供了
通过提供深入的培训来加快在职培训的形式
有关最新威胁的信息。

举一个提升初级分析师的技能为例，
当未知的外部IP地址生成警报
尝试通过TCP端口445连接。经验丰富的分析师
可能知道，SMB最近使用了一个漏洞
勒索软件自行传播，并将IP标识为
可能因拥有者，位置和开放而受到损害
源数据。较新的分析师可能无法做到这些
独立的连接，但上下文化的威胁情报
可以向他们显示网络上的其他设备使用SMB
在端口445上以在服务器之间传输文件和数据。它可能

第45话

还告知他们新的漏洞利用和勒索软件具有
与该IP地址相关联。

改善“无为时”

对于SOC分析人员而言，收集信息同样重要
更快，更准确地了解实际威胁，
有理由提出迅速排除错误的能力
警报更为重要。

威胁情报可为SOC sta提供更多信息
即时分类警报所需的时间和上下文
少得多 它可以防止分析师浪费时间
根据以下条件寻求警报：

- ☑更无害的动作
  比恶意
- ☑与该企业无关的攻击
- ☑已有防御和控制的攻击
  到位

一些威胁情报解决方案会自动执行
通过自定义风险Feed忽略了大部分此类过滤
或降级与组织和
行业特定标准。

威胁情报使IT安全
团队效率提高32％

IDC的调查和分析发现
威胁情报解决方案

调查中的团队是
能够检测到**22％**以上

使IT安全团队能够
减少威胁所需要的我
调查，威胁解决方案，
和安全报告编制
通过**32%**，节省的平均
的**每年64万$**。另外，

威胁才影响到
组织并解决事件
快**63%**。阅读全文
IDC白皮书，请访问https：//
go.recordedfuture.com/idc 。

第46部分

超越分流

威胁情报不仅可以加速分类，还可以帮助SOC
团队简化了事件分析和控制。

例如，通过揭示某种恶意软件是
网络犯罪分子通常将其用作攻击的第一步
财务应用程序，SOC团队可以开始监控
这些应用程序会更紧密地结合在其他证据上
那种攻击类型。

第47页

第四章

威胁情报
事件响应

在这一章当中

了解威胁情报如何最大程度地减少反应性

查看威胁情报解决方案的特征
使它们有效应对事件响应挑战

探索将威胁情报用于事件的用例
响应

“护理不应在急诊室开始。”

—詹姆斯·道格拉斯

在所有安全小组中，事件响应团队都是也许是压力最大的。原因之一：

- ☑的网络事件数量稳步增长
  二十年。
- ☑威胁变得更加复杂和难以控制
  分析; 站在不断变化的威胁领域之上
  花scape本身已成为一项主要任务。
- ☑应对安全事件时，分析师
  被迫花费大量的时间手动检查和
  从不同来源传播数据。
- ☑遏制攻击并消除脆弱性
  能力不断变得越来越难。

结果，事件响应团队通常在
巨大的时间压力，往往无法控制
立即发生网络事件。

持续的挑战

虽然很难准确地确定事件的数量
典型组织的经验，毫无疑问
网络攻击量正在迅速增长。根据
SonicWall，全球恶意软件攻击量增加了
仅在2017年就超过18％。其他流行的攻击
诸如加密的tra c和网络钓鱼之类的向量也正在出现
数量每年都在大幅增加。虽然其中一些
预防性技术缓解了日益增长的压力，
尽管如此，巨大的额外压力仍然在事件上

响应团队的原因如下。

技能差距

事件响应不是入门级的安全功能。
它涵盖了广泛的技能，包括静态技能和
动态恶意软件分析，逆向工程，数字
法医等等。它需要有经验的分析师
在行业中，可以依靠它执行复杂的
在压力下运作。

广为宣传的网络安全技能差距日益扩大
在过去十年中持续扩大。根据2017
ISSA的研究报告，将近四分之三的安全性
专业人士声称他们的组织受全球影响
技能短缺。在他们最新的全球信息中
Frost＆Sullivan进行的安全劳动力研究预测了该技能
到2022年，这一差距将增长到180万。

警报太多，时间太少

在缺少人员的情况下，事件
响应小组遭到难以控制的人数轰炸
警报。根据Ponemon的“恶意软件成本
遏制”报告，安全团队可以期望几乎记录
典型的一周内有17,000个恶意软件警报。超过100
每小时以24/7运作的团队发出警报。这些是
仅来自恶意软件事件的警报。

第49部分

为了正确理解这些数字，所有这些警报都可能导致
安全团队每年花费超过21,000个工时
追逐误报。那是2,625个标准的八小时
仅需进行轮班以区分不良警报和良好警报。

反应时间在增加

当您的技术人员太少而警报太多时，
结果只有一个：解决真正安全问题的时间
事件会上升。根据分析源数据
最近的Verizon数据泄露调查报告，而
进行事件检测的中位时间是一个相当合理的四
小时，平均解决时间（MTTR）超过四
天。

当然，网络罪犯没有这种时间限制。
一旦他们在目标网络中立足，就可以
折衷通常以分钟为单位。我们会讨论
第6章中有更多介绍。

零星的方法

大多数组织的安全小组已经有机成长
同时增加网络风险。结果，他们有
零散添加了安全技术和流程，而无需
战略设计。

尽管此临时方法是完全正常的，但它强制
事件响应团队花费大量时间进行汇总
各种安全技术（例如，
SIEM，EDR和防火墙日志）和威胁源。此项
大大延长了响应时间并增加了可能性
罩将犯错误。

您可以找到原始的“恶意软件遏制成本”
在Ponemon网站上进行报告。

第50话

反应性问题

标记警报后，必须对其进行分类，补救和
尽快跟进以最小化网络风险。

考虑一个典型的事件响应过程：

1. **事件检测**-接收来自警报的警报
   SIEM，EDR或类似产品。
2. **发现**-确定发生了什么以及如何发生
   回复。
3. **分类和围堵**-立即采取
   减轻威胁并最大程度减少损害的措施。
4. **修复**-修复损坏并清除
   感染。
5. **推送到BAU**-将事件传递给“业务
   常规”小组采取最后行动。

注意此过程的反应性。对于大多数组织，
补救事件所需的几乎所有工作是
反向加载，这意味着只有在收到警报后才能完成
被标记。尽管这在某种程度上是不可避免的，但它仍然遥不可及
当事件响应团队已经努力奋斗时
希望足够快地解决事件。

最小化反应
事件响应

为了减少响应时间，事件响应团队必须
减少反应。两个方面需要提前准备
识别可能的威胁可能特别有用
和优先级。

如果事件响应小组可以确定最常见的情况
预先面对威胁，他们可以发展强大，持续的
处理它们的过程。这项准备大大
减少了团队控制个人事件的时间
凹痕，防止错误，并解放分析人员以应对
出现新的意外威胁。

第51章一更

优先次序

并非所有威胁都是平等的。如果事件响应小组可以
了解哪些威胁向量构成了最大程度的威胁
对组织的风险，他们可以分配时间，
资源相应。

了解安全专家如何使用威胁情报来
降低事件响应中的反应性，注意关节
记录的未来和LIFARS网络研讨会“燃料事故”
借助威胁情报来降低违规影响。”

加强事件响应
具有威胁情报

到目前为止，从我们的讨论中应该可以清楚地看出安全性
技术本身不足以降低压力-
可以肯定人类分析家。

威胁情报可以最大程度地降低事件压力
响应小组并解决我们遇到的许多问题
审核者：

- ☑自动识别和消除错误的位置
  主动警报
- ☑利用来自各地的实时上下文来丰富警报
  开放而黑暗的网络
- ☑汇总并比较来自
  最终和外部数据源，以识别真实
  威胁
- ☑根据组织的计分威胁
  具体需求和基础设施

换句话说，威胁情报可提供事件响应
团队，他们需要做出切实可行的见解
更快，更好的决策，同时遏制了irrel-
紧急和不可靠的警报通常会使他们如此工作
困难

第52话

行动中的威胁情报

让我们看一下三个用例和一个滥用案例，它们展示了
威胁情报真正影响事件响应团队
世界。

用例：准备
预先处理

如前所述，典型的事件响应过程是
高度反应性，大多数活动仅在
事件发生。这延长了确定范围和
补救事件。

威胁情报可以帮助事件响应团队做好准备
通过提供以下手段预先防范威胁：

- ☑全面，最新的威胁描述景观
- ☑有关流行的威胁演员策略的信息，技术和程序（TTP）
- ☑特定行业和特定地区的攻击重点趋势

利用这种情报，事件响应团队可以发展
并为最常见的事件保持强大的流程
和威胁。这些过程可用加快
事件发现，分类和围堵。也很大
提高整个行动的一致性和可靠性
事件响应功能。

用例：范围和包含事件

发生事件时，事件响应分析人员必须
确定：

1. 发生了什么
2. 事件可能对组织意味着什么
3. 采取哪些行动

必须尽快对所有这三个因素进行分析-
高度准确的sible。威胁情报可以
协助：

- ☑自动消除误报，启用团队专注于真正的安全事件
- ☑利用来自以下方面的相关信息丰富事件跨开放和黑暗的网络，使其更容易确定他们构成了多少威胁以及如何该组织可能会受到影响
- ☑提供有关威胁的详细信息以及有关攻击者的TTP，帮助团队快速做出有效的遏制和补救决策

时间是您的朋友还是敌人？

曾经想过如何平衡
功率在以下情况之间波动：
随行随从
通过？要找到答案，请阅读记录
未来的博客文章“中的第4
第五名：网络的时间方面
歌剧由grugq撰写。

用例：修复数据风险和资产被盗

组织通常需要很长时间才能实现
发生违反。根据《Ponemon 2018年的成本

数据违规研究：美国的组织
平均197天才能发现违规情况。

毫不奇怪，被盗的数据和专有资产通常会转向
在其合法所有者意识到之前在暗网上出售
发生了什么。

强大的威胁情报功能可能是巨大的
优点。它可以通过提早通知您违规
警告：

☑您的资产在线暴露

☑有人要出售您的资产

第54页

实时获取此情报至关重要，因为它将
使您能够尽快遏制事件，并且
帮助您确定何时以及如何破坏网络。

滥用案例：一半措施
比没有更糟

我们要警告您有关威胁的“滥用案例”
情报实际上会破坏事件响应。

在他们的威胁情报之旅开始之初，一些组织
位置选择了极简解决方案，例如威胁情报
解决方案与各种免费威胁源配对。他们可能
相信这种“将脚趾浸入水中”的方法将
最小化前期成本。

尽管此类实施可以对事件做出反应
具有一些可行情报的团队，通常可以
迫使分析人员精疲力尽，让情况变得更糟
误报与无关警报之间的联系。为了充分解决
主要事件响应痛点，威胁情报
能力必须是全面的，相关的，上下文相关的，
和整合。

威胁的基本特征
事件响应情报

现在是时候检查一下电源的特性了，
强大的威胁情报功能，以及它们如何解决
事件响应团队最大的痛点。

全面

对事件响应团队有价值，威胁情报
必须从最大范围自动捕获
开源，技术供稿和
黑暗的网络。否则，分析师将被迫进行
他们自己进行手工研究以确保没有重要的东西
被错过了。

假设分析师需要知道一个IP地址是否具有
与恶意活动有关。如果她有信心
她的威胁情报来自全面的
她可以立即查询数据，并且

第55章一更

确保结果准确无误。如果她不自信，她
将不得不花费时间手动检查IP地址
针对几个威胁数据源。图4-1显示了如何
威胁情报可能会将IP地址与
Trickbot恶意软件。这种智能可以关联
内部网络日志可以揭示危害指标。

图4-1：威胁情报将IP地址与
Trickbot恶意软件。（来源：记录的未来）

虽然它们经常互换使用，但威胁情报，
信息和数据不是同一回事。找出哪里
不同之处在于，请阅读Recorded Future博客文章“ Threat
情报，信息和数据：区别是什么？”

相关的

努力避免所有误报
识别并遏制事件。但是威胁情报应该
帮助事件响应团队快速发现并清除错误信息
安全技术（例如SIEM和
EDR产品。

第56章一更

有两类误报要考虑：

1.与组织相关但属于
不准确或无益

2.准确和/或有趣的警报，但
不相关的组织

两种类型都有可能浪费大量的
事件响应分析师的时间。

先进的威胁情报产品现已开始使用

机器学习技术识别并丢弃虚假信息
自动产生积极影响，并引起分析师对
最重要（即最相关）的情报。

如果您不选择威胁情报技术，
完全，您的团队可能会浪费大量时间在智力上
与您的组织不正确，过时或无关。

情境化

并非所有威胁都是一样的。即使在相关威胁中
警报，不可避免地会更加紧急和重要
比其余的 来自单一来源的警报可能同时是
率和相关性，但优先级仍然不是很高。
这就是为什么背景如此重要的原因：它提供了关键的线索
关于哪些警报最有可能对您重要
组织。

与警报相关的上下文信息可能包括：

- ☑来自多个相同来源的证实
  警报类型与最近的攻击有关
- ☑确认它与威胁有关
  活跃于您行业的演员
- ☑时间线显示警报略有发生
  与攻击有关的其他事件之前或之后

现代机器学习和人工智能（AI）技术-
智能使威胁情报解决方案成为可能
同时考虑多个来源并确定
警报对于特定组织最重要。

第57页

集成

威胁情报的最关键功能之一
系统具有与广泛的安全性集成的能力
工具，包括SIEM和事件响应解决方案，
他们生成的警报，以及：

- ☑确定是否应取消每个警报
  作为误报
- ☑根据警报的重要性对警报评分
- ☑通过有价值的额外上下文丰富警报

这种集成消除了分析师手动进行分析的需要
将每个警报与具有不同安全性的信息进行比较，并
威胁情报工具。更重要的是，整合
自动化流程可以过滤掉大量的虚假信息
积极的，无需人工分析者的检查。的
此功能节省的时间和挫折感
也许威胁情报的最大好处是
事件响应团队。

第五章

威胁情报
漏洞管理

在这一章当中

检查当前解决漏洞的挑战
根据实际风险

了解漏洞情报如何提供洞察力
威胁者行为

了解基于风险的情报如何简化运营
漏洞管理的要素

“承认我们的弱点是迈出的第一步
弥补我们的损失。”

—托马斯·肯皮斯

Vulnerability management is not a new idea, yet it is one
您可以通过采取以下方法来确保安全
您的组织。它作为函数的重要性不能是
夸大其词。

漏洞管理成功的关键在于转移
从试图修补每一个补丁到安全团队的想法
做出基于风险的决策。这很关键，因为
每年披露的巨大漏洞之广
负责确定团队的临界点
易受攻击的资产和部署补丁。而麦芽的关键
基于风险的良好决策可以利用更多优势
威胁情报来源。

第60话

漏洞问题按数字

根据分析公司Gartner，Inc.的研究，过去每年披露约8,000个漏洞十年。该数字每年仅略有上升，并且实际上只有大约八分之一的人被利用。但是，dur-在同一时期，新软件的数量使用量大大增加，威胁数量增加了呈指数增长。

换句话说，尽管违规和威胁的数量在过去10年中增长了，只有很小的百分比基于新的漏洞。正如Gartner所说，“更多威胁正在利用同样的一小部分漏洞。”

零日不意味着最优先

零日威胁通常会吸引大量的注意力，tion。但是，绝大多数“新”威胁被标记为零日实际上是主题的变体，同样的旧漏洞，但方式略有不同。进一步，数据表明实际存在的漏洞数量零日被剥削仅占总数的0.4％过去十年中利用的漏洞。

这意味着最有效的方法是能力管理不是专注于零日威胁，而是而不是识别和修补特定于您的组织使用的软件。

时间就是生命

威胁参与者已越来越快地利用漏洞。根据Gartner的调查，识别漏洞和外观野外利用的时间从45天减少到15天最近十年。

这有两个含义：

1. 您大约有两个星期的时间来修补或补救您的系统免受新的攻击。
2. 如果您无法在该时间范围内打补丁，则应该减轻损害的计划。

第61章一更

IBM X-Force的研究表明，如果存在漏洞在两周到三个月内未被利用宣布后，从统计学上讲不可能如此。因此，“旧”漏洞通常不是优先考虑的事项修补。

漏洞通常针对使用最广泛的技术。一个Recorded Future播客的一集，标题为“ 7 of the Top针对Microsoft的10个漏洞”解释了原因。

所有这些统计数据都得出一个结论：您的目标应该
不是修补最多或什至最多的漏洞
零日威胁，而是识别并解决威胁
最有可能被您的组织利用。

基于可利用性评估风险

让我们用一个比喻：如果修补漏洞以保持您的
网络安全就像买疫苗来保护自己免受感染
疾病，那么您需要确定哪些疫苗是优先接种的
联系，这是不必要的。您可能需要每天注射一次流感疫苗
保持健康的季节，但无需保持疫苗接种
抗黄热病或疟疾，除非您会接触到
他们。

因此，您必须进行研究：最伟大的研究之一
威胁情报解决方案的价值在于它可以识别
对您的组织构成风险的特定漏洞
并让您了解他们被剥削的可能性。

图5-1说明了这一点。在成千上万的
目前公开的各种功能，数百种
被利用。确实，其中至少有一些漏洞
可能存在于您的环境中。但是你真正唯一的
需要担心的是那些位于
这两个类别。

第62章

图5-1：最大的风险是存在的漏洞
在您的组织中，目前正在被利用。（资源：
Gartner）

严重等级可能会误导

管理漏洞的一个常见错误是关注
按照严重性对威胁进行排名。排名与分类
常见漏洞和披露（CVE）等系统
命名和通用漏洞评分系统（CVSS）
不要考虑威胁行为者是否真的

立即利用您所在行业或本地的漏洞
位置。仅依靠漏洞的严重性就好比获得
在感冒发作前接种了鼠疫疫苗，因为
瘟疫在历史的某个时刻杀死了更多的人。

威胁情报的起源：漏洞数据库

漏洞数据库整合了有关已披露信息的信息
漏洞并对其可利用性进行评分。

实际上，威胁情报的最早形式之一就是
NIST的国家漏洞数据库（NVD）。它集中化
有关已披露漏洞的信息，以帮助您更轻松地进行
让组织查看他们是否有可能受到关注。对于
NVD已经收集了20多年的信息
超过100,000个漏洞，使其成为无价之宝

第63章

信息安全专业人员的来源。其他国家
包括中国和俄罗斯在内，都跟随NIST的领导，
整理漏洞数据库。

您可以在https://nvd.nist.gov/上找到NIST NVD 。目录
漏洞数据库由行业组织发布-
最初的zation：https : //www.first.org/global/sigs/vrdx/vdb-catalog 。

但是，对于大多数易受攻击的人来说，存在两个明显的限制-
能力数据库：

1. 他们专注于技术可利用性而不是
   积极利用。
2. 它们的更新速度不足以提供警告
   一些迅速蔓延的威胁。

可利用性与可利用性

漏洞数据库中的信息几乎全部
专注于技术可利用性，判断可能性
就是利用特定漏洞会导致
对系统和网络造成的损害或多或少。在里面
NVD，这是通过CVSS评分系统测量的。

但是技术可利用性和积极利用并不是
一样。CVSS基本分数提供的指标是-
准确且易于理解-只要您知道
分数传达的信息是什么。但是除非有基地
分数由时间分数或环境修改
分数，那真的只是告诉你该漏洞是多么糟糕低渗
从理论上讲，不是在野外实际使用它。

图5-2显示了可用的威胁情报
关于漏洞及其带来的风险。在这种情况下，您可以
还可以查看涉及CVE的报告的显示方式
NVD已给CVSS评分。

第64话

48 | 威胁情报手册

图5-2：与漏洞相关的威胁情报。（来源：记录未来）

NVD的“社交”与“社交”之间的区别
CVE-来自野外漏洞的风险”和“实际风险”
2017-0022。尽管其CVSS严重性得分仅为
4.3（中等范围），最近包含了Recorded Future
它是网络犯罪分子使用的十大漏洞的列表。
实际风险非常高，因为威胁参与者已添加了
易受普遍存在的Neutrino Exploit Kit的影响
扮演关键角色，检查安全软件是否
安装在目标系统上。

下周与现在

缺少许多漏洞数据库的另一个缺点
的及时性。例如，有75％的已披露漏洞-
能力出现在其他在线资源上之前
NVD，平均每个星期需要处理这些漏洞
出现在那里。这是一个非常严重的问题，因为它
妨碍安全团队在对抗之前进行修补-
可以利用，如图5-3所示。

漏洞披露的非正式方法，以及
宣布有助于延迟识别他们
漏洞数据库。通常，供应商或研究人员会发现

第65章

第5章：用于漏洞管理的威胁情报| 49

将漏洞关闭到NVD，NVD分配了CVE，
开始分析。同时，供应商或研究人员
在自己的博客或社交媒体上发布更多信息
帐户。祝您好运，整理这些不同且
在犯罪者发展证据之前难以找到来源
概念恶意软件，并将其添加到攻击工具包！

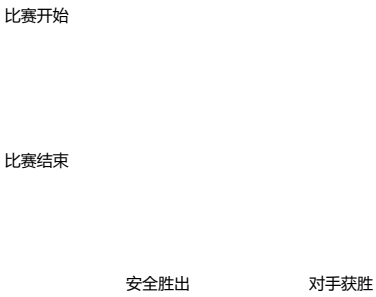

图5-3：安全专业人员与
对手。

用于研究报告漏洞的延迟及其
含义，请参见“录制的未来”博客文章“竞赛
在安全专家和对手之间。”

威胁情报和真实风险

评估漏洞真正风险的最有效方法
对您的组织来说是：

☑内部漏洞扫描数据

☑来自多种来源的外部情报

☑了解威胁因素为何成为攻击目标
某些漏洞而忽略其他漏洞

第66章一更

内部漏洞扫描

几乎每个漏洞管理团队都会扫描他们的
内部漏洞系统，将结果与
漏洞数据库中报告的信息，并使用
结果以确定应修补的内容。这是基本的
使用作战威胁情报，即使我们通常不
这样想。

常规扫描是取消优先级的绝佳方法
系统中未出现的漏洞。通过它自己，
但是，扫描并不是准确确定优先级的适当方法。
调整发现的漏洞。

漏洞的风险里程碑

评估漏洞风险的一种有效方法是查看
从最初的识别发展到可用的程度
功能，武器化和商品化工具包中的商品。

实际风险水平通过
里程碑如图5-4所示。基础广泛的威胁情报
gence可以揭示此漏洞的进展情况。

图5-4：当漏洞出现时，实际风险急剧上升
武器化和商品化的进展。

了解对手

如本书其他地方所述，良好的威胁情报
不应该简单地以分数的形式提供信息

第67页

和统计信息，还可以更深入地了解
为什么威胁参与者针对特定漏洞，以及
无视别人。下面我们讨论情报来源
可以促进这种理解。

如何创建有意义的风险评分

技术之外还有哪些因素
特性可以用来
计算易感性的风险评分
es？记录未来的幼稚风险
计分系统整合了数据
关于犯罪分子，模式
在漏洞利用共享中，数量
链接到恶意软件。此信息-
经常来自
难以访问，例如论坛
在黑暗的网络上。

情报来源

资产扫描和外部漏洞数据库中的数据
只是可以帮助您的信息的起点
评估漏洞的风险。威胁情报应
包括来自各种来源的数据，否则分析员将面临风险
错过新出现的漏洞，直到为时已晚。

宝贵的信息来源，可用来评估您的真实风险
业务包括：

- ☑**信息安全站点**，包括供应商
  博客，有关脆弱性的公开信息-
  关系和安全新闻站点
- ☑**社交媒体**，其中链接共享提供
  跳动点以发现有用的情报
- ☑产生GitHub等**代码存储库**
  深入了解概念验证的发展
  漏洞代码
- ☑**粘贴网站**，例如Pastebin和Ghostbin（某些
  时间错误地定义为黑暗的网站），
  通常包含可利用漏洞的列表
- ☑**暗网**，社区组成和

有漏洞披露和拍卖市场

第68章一更

☑没有进入或禁止进入的**论坛**
使用威胁威胁参与者的特定软件
交流有关漏洞和利用的信息

☑**技术提要**，提供以下方面的数据流：
潜在的恶意指标，增加了有用的
有关恶意软件和漏洞利用工具包活动的文字

黑暗网络上的漏洞Chat不休

窃听
威胁的渠道
演员进行沟通和操作：

- 地下论坛是不同的
  难以找到（毕竟，
  没有适用于深色网络的Google）。
- 威胁行为者改变地方
  每当他们感到自己的
  匿名存在风险。
- 寻找可能的碎屑
  与您的安全有关
  不小的努力。
- 可能有酒吧
  进入，无论是财务还是
  来自其余部分的荣誉
  社区。
- 这些论坛很多都在运作
  完全使用当地语言。

威胁情报供应商
进行收集和分析
黑暗的网络情报进入
在这里玩。他们可以为您提供
具有上下文信息
来自vulner-上的黑暗网络论坛
与您直接相关的能力
网络。

图5-5：一个暗网论坛中的帖子显示了威胁参与者
交流信息。（来源：记录的未来）

第69页

用例：交叉引用情报

为了准确评估实际风险，您必须能够关联

来自多个威胁情报来源的信息。一旦
您开始了解各个参考如何结合
讲述整个故事，您将能够绘制情报
您必须承担漏洞通常会带来的风险里程碑
通过。

例如，您可能会注意到一个新漏洞被披露
在供应商的网站上。然后，您会发现一条推文，其中包含指向
GitHub上的概念验证代码。稍后您发现漏洞利用代码
在暗网论坛上出售。最终您可能会看到
有关在野外被利用的漏洞的新闻报道。

小费 这种智能可以帮助您将注意力集中到
真正带来最大风险和最大风险的漏洞
摆脱“争夺一切”的运行模式。

弥合风险差距在安全性，运营，和业务领导

在大多数组织中，防范
漏洞分为两个团队：

1. 漏洞管理团队进行扫描和
   按潜在风险对漏洞进行优先级排序。
2. IT运营团队部署补丁程序并
   修复受影响的系统。

这种动态产生了趋向脆弱性的趋势
管理“按数字”。例如，漏洞
安全组织中的管理团队可能会阻止-
我发现Apache Web服务器中的几个漏洞构成了
对企业的风险非常高，应优先考虑。
但是，IT运营团队可能会提供很多支持
Windows系统比Apache服务器更多。如果团队成员-
严格按照修补的系统数量来衡量bers，
他们有动力继续专注于低优先级
Windows漏洞。

第70页

有关可利用性的情报还可以为您的组织做准备
在修补脆弱性之间取得正确的平衡
系统并中断业务运营。大多数组织
强烈反对干扰业务连续性。
但是，如果您知道补丁程序将保护组织
面对真正的迫在眉睫的风险，那么短暂的中断就是
完全有道理。

上面概述的风险里程碑框架使之成为可能
更容易传达漏洞的危险
在您的安全和运营团队中，直至高级
经理，甚至董事会。这种可见度
围绕漏洞制定决策的基本原理
将增强整个团队对安全团队的信心
组织。

小费 缩小漏洞管理与
IT运营团队会引入可利用性风险。武装
漏洞管理团队具有更多的上下文相关性
有关可利用风险的数据，以便他们可以查明
较少的高风险CVE和较少的需求
在运营团队中。然后，运营团队可以

少数关键补丁仍然是第一要务
有时间解决其他目标。

第六章

威胁情报
安全负责人

在这一章当中

了解威胁情报如何支持风险管理和
网络安全计划的目标投资

探索CISO认为最有价值的威胁情报类型

回顾威胁情报如何帮助减轻安全性
技能差距

“对知识的投资才是最大的利益。”

- 本杰明·富兰克林

牛逼年份。它曾经以制定有关购买的决策为中心
追逐和实施安全技术。现在的CISO
与首席执行官和董事会互动的可能性更大，并且
进行微妙的平衡行为，以防范风险，同时
确保业务连续性。

今天，安全领导者必须：

☑评估业务和技术风险，包括
新出现的威胁和“已知未知”可能
影响业务

☑确定正确的策略和技术以
减轻风险

☑与最高管理者沟通风险的本质
调整防御措施并证明其合理性

威胁情报可能是所有这些的重要资源
活动。

第72章

风险管理

现代CISO的最大责任也许就是风险
管理：利用可用的资源和预算
以最有效地减轻
网络事件和攻击的威胁。图6-1概述了
安全负责人在接近此阶段时所经历的阶段
挑战。

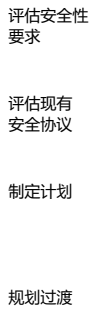

图6-1：评估风险和发展的标准方法-
制定安全策略。

内部数据不足

图6-1中概述的安全性方法取决于
获得有关相关风险因素的良好信息，以及
现有安全程序中的潜在弱点。问题
问题是，这种情报往往只收集
来自内部审核，已知问题和先前的安全性
事件。这产生了您已经知道的问题列表
关于，而不是您需要担心的问题列表
今天或将来。

需要外部环境来验证与已知风险相关的风险
问题并提供有关新出现和不可预见的警告-
看到威胁。

内部网络流量数据，事件日志和警报排除
确实为风险管理带来了价值，但它们没有提供
有足够的背景来建立全面的风险状况，以及

第73页

当然不足以定义整个策略。安全
专业人士必须主动发现未知

风险，背景是帮助安全领导者确定哪些因素的原因
潜在威胁最有可能成为对
他们的企业。

重点突出

威胁情报包括有关总体趋势的信息
如：

- ☑哪些类型的攻击越来越多（或更少）
  经常
- ☑哪种攻击对受害者造成的损失最大
- ☑将会出现什么样的新型威胁参与者，
  以及他们针对哪些资产和企业
- ☑具有以下特征
  的安全实践和技术
  事实证明，最成功（或最不成功）的是停止或
  缓解这些攻击

这些趋势的数据可以帮助安全组织预测
担心哪些威胁将成为明天的热门新闻。

但是情境化的外部威胁情报可以发挥很多作用
进一步，使安全小组能够评估是否
威胁可能会基于
像这样的因素：

- ☑**行业**：威胁是否正在影响其他行业？
  我们的垂直行业？
- ☑**技术**：威胁是否涉及损害-
  使用的软件，硬件或其他技术
  在我们的企业？
- ☑**地理**：威胁是否以目标设施为目标？
  我们开展业务的地区？
- ☑**进攻方式**：在比赛中使用技巧
  攻击，包括社会工程和技术
  方法，已成功应用于我们的com-
  内裤还是类似的？

第74页

如果没有这些类型的情报，
极其广泛的外部数据源集，这是不可能的
让安全决策者全面了解
网络风险状况及其对企业的最大风险。

图6-2说明了如何自定义威胁情报
仪表板可以突出显示与
具体的企业。

图6-2：威胁情报仪表板可以查明威胁
与特定行业或技术最相关。（资源：
记录的未来）

缓解措施：人，流程和工具

漏洞扫描和渗透测试等技术
和红色团队可以帮助安全组织了解
他们的防守存在差距。

但是今天的企业存在更多的技术漏洞，
安全流程和策略中的更多弱点，以及更多
易受社会工程技术影响的员工
他们可能会立即修补，硬化和训练
未来。

第75页

威胁情报可帮助安全领导者确定漏洞-
首先需要解决的能力和弱点
指示：

- ☑哪些威胁参与者最有可能针对企业
- ☑威胁行为者使用的TTP，因此他们倾向于利用的弱点

预警

有时，威胁情报甚至可以更加具体。
例如，分析师在黑暗的网络上发现了黑客
宣布他们打算攻击特定行业，并且
即使是特定的公司（有时也会招募志趣相投的人
黑客协助他们）。

监控暗网市场的分析师还可以跟踪
开发和销售针对黑客工具和漏洞利用工具包
特定漏洞。正如本书前面所讨论的，
对修补漏洞和缓解漏洞很重要
在解决别人之前就被利用了
剥削是理论上的。

小费 您可以使用一些威胁情报解决方案来扫描
深色网络和其他参考资料，以引用您的公司，
您的行业，以及您所安装的特定技术
企业。

投资

决定如何投资网络安全已成为一项艰巨的任务-
最近面临挑战。金融投资顾问
Momentum Partners确定了1,700多家公司
2017年专门研究网络安全技术和服务。

有这么多选择，CISO如何识别最多
作为积极安全措施的一部分而实施的有效解决方案
战略？

唯一合乎逻辑的方法是根据
风险。每个组织都有自己独特的风险状况，
按其行业，地理位置和内部基础架构来划分。威胁
情报可帮助安全领导者了解其组织结构-

第76页

最紧迫的威胁，需要确定
（并证明）投资领域要简单得多。结束
目标是能够判断该风险并进行投资
基于对真实威胁状况的全面了解。

通讯

CISO通常面临描述威胁的挑战
并用能激发动机的术语来证明对策
非技术业务领导者，例如成本，投资回报率
客户，竞争优势。

用有关每个威胁的消息轰炸他们不是
不错的选择。

威胁情报可以为
这些讨论，例如：

- ☑类似攻击对公司的影响
  其他行业规模相同
- ☑黑暗网络中的趋势和情报表明-
  认为企业很可能成为目标

支持安全主管

我们已经多次提到威胁情报
需要全面，相关且因地制宜
对安全组织的成员有用。当谈到
对于CISO和其他安全领导者来说，也需要简明扼要
及时。

例如，威胁情报可以提供安全领导
实时了解最新威胁，趋势和
事件。威胁情报仪表板或其他类型的
“一目了然”的格式可以帮助安全领导者响应
威胁或传达新威胁的潜在影响
输入业务负责人和董事会成员。

威胁情报不仅适用于事件响应团队，而且
SOC。安全领导者还是威胁情报的主要消费者-
限制，如图2-1所示。想一想
情报安全领导者每天都需要（例如，
董事会和之前的主要新情报发现清单
前一天），定期（某天的摘要和趋势）

第77页

季度风险报告）和危机（有关
刚刚检测到的攻击），并确保流程
并提供了威胁情报工具来解决这些问题
需要。

安全技能差距

CISO的职责之一就是确保IT
组织有人力资源来执行其错误-
sion。然而，网络安全领域具有广泛宣传的技能
短缺，现有的安全人员经常发现自己
面临应付难以应付的工作量的压力。

威胁情报可以部分解决该危机
通过自动化一些最劳动密集型任务
网络安全，使人们有时间进行其他工作。对于
例如，它可以减少生成的大量警报
通过SIEM和其他安全工具迅速收集并纠正
关联来自多个情报来源的上下文，并提供
数据以优先考虑风险。

威胁情报解决方案可用于
安全功能可以节省大量时间，因为SOC和
事件响应分析师，漏洞管理专家-
专家和其他安全人员得到的信息
和背景，他们需要做出准确的决定。

强大的威胁情报还可以帮助初级人员
快速“提升技能”并在他们的经验水平以上发挥作用，因此
CISO不必招聘那么多高级职员。

更好地管理的智慧

显然，对于CISO和其他安全专家而言，最大的挑战是
领袖们是如何平衡有限资源与
需要保护其组织免受不断发展的网络攻击
威胁。威胁情报通过帮助解决这些问题
他们可以准确地描绘出威胁态势
计算网络风险，并与智能手机武装安全人员-
他们需要做出更好，更快的决策。

威胁情报使CISO和安全领导者能够留下来
与当前和新兴威胁并驾齐驱
通过人工研究是不可能的。但是为此

笔，威胁情报功能必须是全面的，
相关的，上下文的，简洁的和及时的。威胁情报
没有这些特征的gence功能很可能
作为部分或不正确的信息，阻碍多于帮助
容易导致糟糕的决策。

案例研究：威胁情报和全球零售商的自动化

拥有近3600家及以上的商店
全球135,000名员工
连锁店面临的安全挑战
预防损失，欺诈，
和公司安全来保护-
客户的个人身份信息。

两者之间的良好关系
网络安全团队以及其他
组织中的部门。

一位高级经理说
公司的网络防御中心：
“我们每个人都没有在孤岛上操作。

零售商将自动应用于
集中化和定制化
每个安全威胁情报
rity func on。自动确保
进入SIEM的数据是
准确且高度相关，
并且数据出来了
灵活，易于使用的格式。

最大的投资回报率
-以及最大的优势
管理其威胁情报
通过多合一的平台-是

如果我们可以使用威胁情报
确保我们的安全，也帮助我们
程序可见性，有助于
做更多的商业案例
能力。拥护冠军
其他团队支持的好处
威胁情报确实可以帮助我们
投资回报。”

阅读完整的案例研究或观看
在https：// www的网络研讨会。
recordfuture.com/gap-threat-
情报需求/。

第七章

威胁情报
用于风险分析

在这一章当中

探索FAIR框架等风险模型的价值

查看正确和错误的方法来收集有关风险的数据

了解威胁情报如何提供有关以下方面的硬数据
攻击概率和成本

“建立和促进信息风险管理
.../实现/之间的适当平衡的最佳实践
保护组织和经营业务。”

—公平研究所的使命声明

一个

超过1,700家网络安全供应商。他们大多数
将他们的任务定义为“使您的环境-
安全。”但是企业如何才能设定优先投资目标?
技术和服务以及人员?

我们才能在前面的章节中提到的，今天有

风险建模提供了一种客观评估当前风险的方法，
并估算投资的清晰可量化的结果，

网络安全，但是当今许多网络风险模型
来自以下任一方的用户：

☑模糊，未量化的输出，通常为
显示绿色，黄色和红色的“交通灯图表”
威胁等级

☑有关威胁概率和成本的估计
根据部分信息匆忙编译，
充斥着毫无根据的假设

第80页

非量化输出不是很可操作，而模型
根据错误的输入结果导致“垃圾进垃圾出”
场景，其输出看似精确，但实际上
误导。

为了避免这些问题，企业需要精心设计的
风险模型和大量有效的当前信息，包括
威胁情报。

小费 网络安全风险评估不应仅基于
定义为证明符合法规的标准。用
这些标准，评估风险通常成为
针对诸如防火墙之类的网络安全控制复选框
和加密。计算已检查的箱子数
您对实际风险的印象非常令人误解。

公平风险模型

任何风险模型的核心方程式是：

“发生的可能性x影响”

但是很明显，上帝（或魔鬼）在细节上。幸好，
一些聪明的人开发了一些非常好的风险模型，
您可以使用或适应自己的选择和方法
需要。我们喜欢的一个是信息因素分析
来自FAIR Institute的风险（FAIR）模型。图7-1显示
此模型的框架。

FAIR框架可帮助您创建定量风险
包含特定损失概率的评估模型
来自特定种类的威胁。

您可以在FAIR Institute网站上了解有关FAIR的更多信息。
这种用于信息安全和运营的定量模型-
国家风险集中于理解，分析和量化
以实际财务术语交易信息风险。

第81章一更

图7-1： FAIR框架，其元素由情报告知
突出显示。（来源：公平研究所）

测量和
透明度是关键

FAIR框架（和其他类似的框架）使您可以创建
风险模型：

☑进行明确的风险评估

☑对假设，变量和
结果

☑以财务术语显示特定的损失概率

当测量，公式，假设，变量，
结果变得透明，可以讨论，
捍卫和改变。因为很多FAIR模型是
用业务和财务术语定义，高管，
业务经理和其他利益相关者可以学习说话
使用相同的语言并对资产，威胁和漏洞进行分类-
同样的能力。

小费 尝试合并有关未来损失的特定概率
尽可能将其纳入风险模型。特定概率
使风险管理人员和高级管理人员可以讨论
模型，以及如何改进
对模型和建议的信心更大，
从中出来。

第82章

哪个陈述更有用?

“ DDoS攻击的威胁
我们的业务已从
高到中（红色到黄色）。”

要么

“有20％的可能性
我们的业务将蒙受损失
在接下来的12年中超过$ 300,000
几个月，因为分布式
拒绝服务（DDoS）攻击
会破坏我们的可用性
面向客户的网站。”

“勒索软件对我们的威胁
业务已从低变到
中（绿色到黄色）。”

要么

“有10％的概率
我们的业务将蒙受损失
未来12个月的$ 150,000
由于勒索软件。”

威胁情报和威胁概率

如图7-1的左侧所示，创建
威胁模型涉及估计成功的可能性
攻击（或公平事件的语言中的“丢失事件发生频率”
框架）。

第一步是创建一个列表，列出可能的威胁类别。
影响业务。此列表通常包括恶意软件，网络钓鱼-
攻击，攻击工具包，零时差攻击，Web应用程序
漏洞，DDoS攻击，勒索软件和许多其他威胁。

下一步要困难得多：估计概率
攻击将会发生，并且攻击将会成功（例如，
企业包含与以下方面相关的漏洞的几率
攻击和现有控制措施不足以阻止它们）。

小费 尝试避免出现以下情况：GRC（治理，风险，
和合规性）团队成员问安全分析师，“
我们面对这种特殊攻击的可能性有多大？”的
安全分析师（谁真的赢不了）思考30秒
关于过去的经验和当前的安全控制措施，以及
做出一个疯狂的猜测：“我不知道，也许有20％。”

第83页

为避免显得笨拙，您的安全团队需要答案
比那更好的消息。威胁情报可以
通过回答以下问题来提供帮助：

- ☑哪些威胁参与者正在使用此攻击并
  他们针对我们的行业？
- ☑观察到这种特定攻击的频率
  最近像我们这样的企业？
- ☑趋势是上升还是下降？
- ☑此攻击利用了哪些漏洞（和
  我们的企业中是否存在那些漏洞？
- ☑造成了什么样的技术和经济损失
  这种攻击是在像我们这样的企业中引起的？

分析师仍然需要对企业有很多了解
及其安全防御，但威胁情报丰富了
他们对攻击的了解，背后的行动者以及他们的
目标。它还提供了关于
攻击。

图7-2和7-3显示了一些智能形式。
可能需要。图7-2列出了有关
威胁情报解决方案可以回答的恶意软件样本
对于分析师。

图7-2：有关威胁的恶意软件样本的问题
智能解决方案可以回答。（来源：记录的未来）

第84章

68 | 威胁情报手册

图7-3显示了勒索软件扩散的趋势
家庭。每个勒索软件系列右侧的趋势线
表示在一个巨大的范围内增加或减少参考
一系列威胁数据源，例如代码存储库，粘贴
网站，安全研究博客，犯罪论坛和.onion（Tor
无障碍）论坛。其他信息可能可用
关于勒索软件系列如何与威胁行为者联系的信息，
目标和攻击工具包。

图7-3：描述新勒索软件系列扩散的时间表。
（来源：记录的未来）

威胁情报和攻击成本

模型中公式的另一个主要组成部分是
成功攻击的可能代价。的大部分数据
估计成本很可能来自企业内部。
但是，威胁情报可以提供有用的参考
关于以下主题的要点：

☑对企业的类似攻击的成本
在相同行业中规模相同

☑发生故障后需要修复的系统
攻击及其所需的补救类型

第85章一更

深入了解风险

您可以找到更多有关风险建模及其作用通过查看威胁情报记录未来白皮书“的损失概率：威胁如何情报局冒着风险业务。”

为了更深入，我们高度推荐“如何测量任何网络安全风险”道格拉斯·W·哈伯德和理查德森森

第87章

第八章

威胁情报预防诈骗

在这一章当中

了解网络犯罪分子如何组织自己以进行欺诈和勒索

了解犯罪社区中的对话如何呈现收集有价值的威胁情报的机会

了解您可以通过申请解决哪些类型的网络欺诈相关威胁情报

“资本主义面临的挑战是，东西会滋生信任也滋生了欺诈的环境。”

詹姆斯

站立并交付！

从拥有者中轻松获利的方法

因斯电子商务的诞生，犯罪分子寻找资产并充分利用时间。例如，在17世纪的英格兰，客商阶级之间的教练旅行，与便携式fl发枪手枪的发明，公路工人。

在我们的数字时代，在线交易业务的公司查找各种形式的网络欺诈所针对的数据。

了解犯罪分子如何从您的利益中牟利业务，您不能只专注于检测和响应应对已经在积极利用您的系统的威胁。你需要收集有关网络犯罪团伙的威胁情报针对您以及他们如何进行运营。

第88页

了解你的敌人

Verizon的《2018年数据泄露调查报告》归因于超过60％的已确认有组织违规犯罪（图8-1）。

此数据与Recorded收集的情报保持一致黑暗网络社区的未来表明组织有序犯罪集团（OCG）正在雇用自由黑客欺骗企业和个人。这些团体只是像合法企业一样，在许多方面团队合作创建，运营和维护的成员欺诈计划。

图8-1：数据泄露中的外部**参与者**最多。
（来源：Verizon数据泄露调查报告2018）

第89章一更

图8-2：网络犯罪集团的典型组织结构图
美食。（来源：记录的未来）

典型的OCG由单个策划者控制。的
该组可能包括在
金融业安排洗钱，伪造
负责伪造文件和辅助文书工作，
负责技术监督的专业项目经理
运营方面，编写代码的软件工程师，
和熟练的黑客。一些团体包括前执法
收集信息并进行反情报的特工
操作。

这些网络犯罪集团的成员倾向于
在现实生活中有着牢固的联系，并且经常受到尊重
他们的社会群体。他们当然不尊重自己
作为普通的街头罪犯。他们很少与
每天的徒，宁愿留在阴影中
并避免执法和当地黑手党的注意
分支机构。但是，需要大量
人员，例如涉及从多个机构中提取现金的人员
同时使用自动柜员机，可能涉及连锁
招募和管理“士兵”的中间人
做腿部工作。

第90页

犯罪社区和黑暗网

您很少能将网络攻击归因于单个个人，隔离运行。高级攻击通常需要广泛的技能和工具，以及能够发起并支持利用勒索软件的活动，网络钓鱼以及其他技术设备和社会工程学技术。

今天，所有这些产品和服务都可以购买或在复杂的地下经济中以一定价格租来的。网络犯罪分子，黑客及其同伙之间的往来信息并进行与非法活动有关的交易在深层网络上的联系（网络上无法到达的区域通过搜索引擎）和暗网（只能是可使用特殊软件和工具（可隐藏身份）进行访问的访客）。

门控社区

并非所有网络犯罪分子都专门从事从技术上讲被称为“暗网”。有些人建立通讯基于相当标准的讨论区进行加密的实体进行登录，并使用Jabber和Telegram等技术开展业务。

该地下网络的准成员经过了审查由活跃的参与者在聊天室和论坛之前他们被接受了。他们可能需要支付入场费，价格从50美元到2,000美元不等。需要一个论坛准会员存款超过100,000美元。

优点和缺点

黑暗的网络和犯罪社区加强了网络-犯罪分子和OCG通过允许他们访问信息，工具，基础架构和合同服务力量和力量。但是，这些社区也是弱点，因为可以对其进行监视以提供威胁可用于预测和击败欺诈的情报计划。

第91章一更

了解您的黑暗网络

您可以获得更深入的了解-犯罪分子的地位地下维护等级制度来自Recorded的研究中的用户未来：“黑暗网络：社交暗网的网络分析社区。”我们发现黑暗的网络分为三部分不同的社区：低层黑暗网络论坛和黑暗网络市场。分析表明一大批演员较低和较高的位置er论坛上这两个通讯之间。但是，黑暗的网络市场很大程度上与这些脱节论坛。

地下论坛，高层

连接点
预防诈骗

来自地下犯罪分子的威胁情报
社区是了解动机，方法和
威胁行为者的策略，特别是当这种情报是
与来自表面网的信息相关，包括
技术提要和指标。

显示了真正的情境化威胁情报的力量
如何将各种各样的数据汇总到一起
来源并在不同的部分之间建立联系
信息。

例如，以下上下文信息可能
用于将有关新的恶意软件变体的新闻转化为
情报：

- ☑犯罪集团正在使用此恶意软件的证据-野外活具
- ☑报告称使用该恶意软件的攻击套件为可在黑暗的网络上出售
- ☑确认漏洞是漏洞利用工具包存在于您的企业中

第92页

小费 监视暗网和犯罪社区的直接
提及您的组织和资产。这些提及
通常表示定位或潜在的违规行为。还有moni-
提到您的行业和其他不太具体的术语
这可能指向您的操作。使用威胁情报
以这种方式评估风险将使您对
您的防御并帮助您做出更好的决定。

用例：付款欺诈

付款欺诈一词涵盖各种
网络犯罪分子从受害中获利的技术
付款数据。他们可以使用网络钓鱼来收集卡的详细信息。
更复杂的攻击可能会损害电子商务网站或
销售点系统实现相同的目标。一旦有
获取卡数据后，犯罪分子就可以转售（通常是打包出售）
的数字），并随着他们的削减而走开。

威胁情报可以提供即将到来的预警
与付款欺诈相关的攻击。监视像
犯罪社区，粘贴站点和其他论坛
相关的支付卡号，银行识别号或
对金融机构的特定引用可以提高知名度
进入可能影响您组织的犯罪活动。

用例：受损的数据

其他类型的个人信息泄露和

企业知识产权也可以拥有巨大的
内在价值。最近的例子包括受感染的
记录，克隆和受损的礼品卡以及被盗
用于“支付” Netflix，Uber和物品等服务的凭证
通过PayPal收费，如图8-3所示。

图8-3：受损数据– Spotify凭据在黑暗中泄露
网络。（来源：记录的未来）

第93章一更

大量与黑客相关的违规行为被盗
或弱密码。网络犯罪分子定期上传大量
用户名和密码的缓存，以粘贴网站和
暗网，或使其在地下出售
市场。这些数据转储可以包括公司电子邮件
地址和密码，以及其他登录信息
网站。

监视此类情报的外部来源将
大大提高您的可见度，而不仅仅是泄漏
凭据，但也可能破坏公司数据
和专有代码。

用例：打字抢注和欺诈性域名

敲击涉及操纵字符中的字符
公司的域名分为几乎相同的域；对于
例如，example.com可能会变成exanple.com。攻击者
可以注册与目标不同的数千个域
单个字符的组织网址，原因如下
从可疑到完全恶意。流氓网站使用
这些修改后的域名看起来像合法的
网站。流氓域名和网站可用于
针对公司员工或客户的鱼叉式运动
蜂鸣器，水坑攻击和偷渡式下载攻击。

收到有关新注册的网络钓鱼和域名抢注的警报
实时域缩小了可用于
犯罪分子冒充您的品牌，以欺骗自己
用户。一旦识别出该恶意基础架构，您就可以
运用移除服务来消除威胁。

我们已经看到犯罪论坛和市场是
以促进所有类型的秘密交易而闻名
位置。但是这些渠道不是
犯罪局外人。记录未来的报告描述
公司内部人员如何宣传他们接触犯罪分子的途径
演员，以及如何招募员工和承包商
进入犯罪地下。内幕人士是
欺诈手段，从零售兑现服务到刷卡
操作，以防止银行员工盗窃。阅读
报告“金融服务的内部威胁：发现
外部情报的证据。”

第95页

第九章

威胁情报
降低第三方风险

在这一章当中

探索增加第三方风险的影响

了解为何对第三方风险进行静态评估短

了解为什么使用实时，自动威胁情报是减轻第三方风险的最佳方法

“一条链并不比其最薄弱的环节更强大。”

—谚语

第三方风险隐约可见

Because今天的供应链是如此紧密集成，我们必须考虑我们的合作伙伴，供应商的安全性和其他第三方在评估我们的风险状况时自己的组织。

据研究公司ESG称，大多数IT专业人员认为网络风险管理变得越来越困难最近两年。许多人直接将此挑战归因于管理第三方风险所需的其他费用。最近Ponemon研究所的研究表明，组织的违规行为源于三分之一派对，只有29%的人相信他们的伴侣会通知他们的妥协。这些和相关的统计数据显示在图9-1中。

第96章一更

图9-1：大多数组织面临重大风险
通过他们与第三方的关系。资料来源：Ponemon
研究所和记录的未来

文字写在墙上：第三方攻击将变得更糟，
他们将使网络风险管理进一步复杂化，而您的
合作伙伴可能不会帮助您解决最关键的问题
问题。

许多传统的第三方风险评估都依赖静态
输出，例如财务审计，有关新产品的每月报告
组织使用的系统中发现的漏洞，
偶尔报告安全控制委员会的状态
顺从。这些很快就过时了，无法提供所有
您需要做出有关如何做出明智决定的信息
管理风险。

相比之下，实时威胁情报使您能够
评估第三方带来的风险并保持评估
当前随着条件的变化和新的威胁而出现。

传统风险评估不足

许多最常见的第三方风险管理
今天采用的做法落后于安全要求。
静态风险评估，例如财务审计和安全性
证书验证仍然很重要，但是通常缺少
上下文和及时性。

第97页

遵循传统方法进行管理的组织
第三方风险通常使用以下三个步骤：

1. 他们试图了解组织的业务-
   与第三方的关系以及如何暴露
   组织受到威胁。
2. 基于这种理解，他们确定了框架-
   致力于评估第三方的财务状况，
   公司控制以及IT安全和卫生
   以及它们与组织本身的关系
   安全方法。
3. 组织使用这些框架评估
   第三方，确定其是否符合
   安全标准，例如SOC 2或FISMA。有时
   公司对供应商进行财务审计
   或伴侣。

这些步骤对于评估第三方风险至关重要，
他们没有讲完整的故事。输出是静态的，不能
反映迅速变化的条件和新出现的威胁。
通常，分析过于简单以至于无法产生可操作的记录。
赞美。有时最终报告是不透明的，
无法深入研究背后的方法论
分析。这使决策者不确定是否

关键信息可能已被忽略。

小费 评估第三方风险时，请勿完全依靠自我
报告调查表或供应商的内向型观点
他们的安全防御措施。用外部的方法将其完善
对供应商威胁前景的公正看法。

思想实验

想象你经历了
风险的传统步骤
评估，如上所述。您
得出结论，您的一家供应商
供应链是安全的。

现在，该供应商经历了
可能（也可能不会）的数据泄露
公开了您的内部数据。
你能准确确定
什么是主动安全
您需要采取的措施以及
您应该多快采取行动？

第98页

寻找三件事
在威胁情报中

要实时准确评估第三方风险，您可以
需要一个解决方案，以提供当前的即时上下文
威胁态势。威胁情报是获得威胁情报的一种方法
并确定在防御方面有哪些缺点
您的供应链合作伙伴给您带来重大风险
组织。所添加的上下文不仅包括当前
风险，但可以提供更多背景的历史观点
帮助发现，预防和解决风险。

为了帮助您评估第三方风险，威胁情报
解决方案应：

1. 自动化和机器学习来快速和
   全面整理海量数据
2. 关于威胁和风险变化的实时警报
3. 透明化您的威胁环境
   第三方合作伙伴

自动化与机器学习

为了管理组织的风险，您需要访问大量-
来自开放网络，黑暗网络的大量威胁数据，
技术和新闻来源以及讨论论坛。相同
适用于评估第三方风险。

但是鉴于这些内容中与网络安全相关的内容的规模
来源，总计数十亿个事实，您需要一个威胁情报，
使用自动化和人工智能的gence解决方案
收集并分析这些细节。您的威胁情报
解决方案应该能够：

- ☑使用natu-分析，分类和索引数据点
  ral语言处理能力和多种
  机器学习模型。
- ☑使用以下方法生成客观的，数据驱动的风险评分
  简单的数学公式

第99章

实时更新风险评分

静态评估很快就过时了。每周或
人类分析家每月制作的情报报告
提供基本概述，但往往来不及启用
有效的行动。

实时更新风险评分更为有效
时间并利用大量数据。这些能力
使风险评分更可靠，可立即做出
评估和达成安全决策。

例如，通常可以将贸易伙伴视为
根据标准情报报告的风险低。
但是，假设合作伙伴发生数据泄露事件，
（或可能不会）影响您的组织。如果您完全依靠
静态风险评估，您可能不知道违规
首先发生，或者直到太晚才发生。或者您
可能要等到为时已晚才能获得情报
需要准确评估风险。是什么原因造成的
违反？它是系统中的一个被利用的漏洞吗？
被伙伴使用了吗？社会工程攻击？静态的
评估将不会提供证明正当性所需的证据
要求第三方将其他安全控制措施放入
地点。

托马斯·达文波特（Thomas H. Davenport）是总统杰出人士
信息技术与管理学教授
巴布森学院，麻省理工学院数字中心研究员
商业，德勤分析的独立高级顾问，
和15本书的作者。他写了一份使用报告
威胁情报以生成风险分数，以：（a）帮助
高管和董事会了解高风险环境
合作公司的职责；（b）为网络提供指导
情报小组优先考虑对第三杆的调查
关系及其风险。该报告“将第三方评为
缔约方网络风险”，请访问：https：//go.recordedfuture。
com / cyber-risk-scores 。

透明的风险评估

如果您找不到任何人，那么进行风险评估有什么意义？
行动？

第100页

没有上下文的信息问题使我们喜欢
卡桑德拉（Cassandra）在希腊神话中。为了表达对她的爱，上帝
阿波罗给了她预言的礼物，但她仍然蔑视他的
浪漫的进步。在他的愤怒中，他让她保持了远见。
但诅咒她，使没人相信她的警告
关于未来。

如今，许多风险评估的命运与
卡桑德拉的预言。当他们依靠模糊得分时
方法或不透明的来源，它们甚至难以接受
如果它们是正确的。很多时候，组织无法采取行动，
领导力，因为领导者不了解或不了解
资源。

为了帮助安全专业人员亲自了解为什么-
特定IP地址上的警报之类的东西可能代表
真正的风险，威胁情报解决方案应显示该风险
由警报触发且透明的规则
其来源。额外的细节也可以消除怀疑
该信息可能被忽略了。这种情况
允许更快的尽职调查和参考检查，包括
在评估静态评估时。

图9-2：威胁情报可提供上下文并帮助识别-
弥补供应链合作伙伴防御中的缺陷

第101页

回应高第三
团体风险评分

当您面对三分之一的高风险分数时，您会怎么做
派对？并非每个数据泄露都证明终止业务是合理的
和那个伙伴。几乎每个组织都与之抗衡
网络攻击和意外停机，而合作伙伴则没有
例外。更重要的问题是他们（和您）如何
处理事件并采取措施降低未来风险。

风险评分的变化可以提供与他人交谈的机会
您的业务合作伙伴有关他们如何处理安全问题的信息
ity。最终，您可以更仔细地查看
触发的风险规则将影响您组织的
网络。例如，公共合作伙伴的风险评分可能
增加，因为域名抢注网站非常相似
发现合作伙伴运营的合法网站。
您可以将自己网络中的那些网站列入黑名单以阻止
网络钓鱼活动，并调查采取了哪些步骤
合作伙伴计划采取措施保护其品牌形象。

对于明智的安全决策，而不是下意识的反应，您可以
需要最新的背景信息和提供的证据

威胁情报。

第102章一更

案例研究：保险公司获利实时查看第三方风险

多年来，财富100强保险公司努力维持当前清晰的视图合作伙伴的风险状况。的依靠这个组织来解决使用了经常过时的数据而且很少刷新。公司看不到伴侣的风险分数超过了我，缺乏对特定事件的了解表示得分的因素。

该组织采用了来自的威胁情报解决方案记录未来，有助于安全团队更好地了解，分析并迅速解决团体风险，包括：

- •公司电子邮件，信用凭证，和公司人员发现在黑暗的网络上
- •社交媒体聊天
- •域名滥用（通常是印度网络钓鱼攻击
- •使用易受攻击的技术
- •IT基础架构滥用或滥用

“ [Recorded Future提供]价值-对风险状况的洞察力我们所做的重要供应商与我打交道—来自我的风险评分和提醒自定义规则我们已经设定-并允许我们进行钻探在需要的时候更深，”公司第三方负责人的领导者-风险管理团队的形式。通过优先考虑威胁情报，Recorded Future解决方案有帮助团队迅速：

- •排除低风险警报和错误的态度
- •专注于最重要的威胁
- •立即采取行动解决他们

该解决方案有助于公司减少花在尽职调查和参考检查-减少50％，然后替换sta c，指向我的方法连续监控。

您可以找到完整的案例研究此处：https：//go.recordedfuture。com / hubfs / insurance-case-study。pdf格式

第103页

第10章

威胁情报
数字风险
保护

在这一章当中

审查多种形式的数字风险

了解威胁情报如何识别多种类型的数字冒险，以便可以补救

“每次接触都会留下痕迹。”

— Locard的法医学交流原则

中号情报可以加强特定团队的工作。在这本书的章节OST描述如何威胁网络安全组织。本章探讨威胁如何智能可以帮助检测和补救数字风险。这个场景跨越组织结构图，但仍需要解决以系统，有条理的方式。

正如我们下面讨论的那样，数字风险有多种形式。但是共同点是大多数网络攻击都会消失的事实在网络上的痕迹。通过发现这些痕迹，威胁情报收集过程可以查明和补救最严重的问题数字风险。

上网面临风险

如今，任何希望通过影响力必须具有强大的在线形象。有抱负的艺术家，精明的政客，大型公司和新兴企业

第104页

努力增加收入，简化业务流程，以及通过面向外部的网站，参与度提高知名度社交媒体以及许多其他在线活动。

有意义的在线业务需要您深入思考

关于如何保护自己免受数字风险的影响。在线参与
与听众的互动会引起来自
各种各样的威胁参与者：出于经济动机的网络犯罪分子，
试图获取您的秘密的竞争对手以及那些
想破坏你的努力。其中一些会成功
捕获专有信息。

您还必须担心威胁行为者如何劫持
您的品牌并假冒您的网站来为其服务
自己的目的-例如，通过创建欺诈性域名来
用于网络钓鱼攻击或散布虚假信息
以你的名字

在我们探索威胁情报如何帮助阻止之前
这些威胁行为者，让我们回顾一些数字风险和
他们在网上留下的痕迹。

数字风险的类型

数字风险分为几类。最重要的
是导致网络失窃和数据泄露的网络攻击，
供应链中的问题造成的风险
员工的举动和品牌模仿。

这些风险汇总在图10-1中。

第105章一更

图10-1：数字风险的主要类别

揭露的证据
违反网络

威胁情报解决方案可以通过以下方式查明数字风险
监控网络，包括黑暗中的私人论坛
网络，以发现组织内数据泄露的证据，
化和合作伙伴生态系统。证据可以包括：

- ☑客户的姓名和数据
- ☑财务帐户数据和社会安全号码
- ☑员工的凭证泄漏或被盗
- ☑粘贴和合并包含您专有的站点
  软件代码
- ☑论坛提及您的公司并宣布
  意图攻击它
- ☑论坛销售工具和讨论技术，
  攻击像您这样的企业

第106页

及时发现这些指标可以帮助您：

- ☑保护数据源
- ☑查找并修复以下漏洞和错误配置
  您的基础架构
- ☑通过改进安全控制措施减轻未来风险
- ☑确定改善员工培训和
  编码惯例
- ☑使您的SOC和事件响应团队能够
  更快地识别攻击

小费 通常，您可以通过查看来缩小泄漏源
确切地说，可以在网上找到什么信息和工件，
找到它们的地方，以及在同一地方发现的其他东西
地点。例如，如果您找到产品设计或软件
暗网站上的代码，并意识到它们是共享的
只有几个供应商，您将知道要调查
这些供应商的安全控制，作为您的第三方的一部分
风险管理程序。如果您公司的名字是男的-
在黑客论坛上发现
攻击某些应用程序，则可以增强对
通过修补运行它们的系统来定位目标应用程序，
对其进行更密切的监视，并添加安全控制措施。

发现品牌证据
冒充与滥用

与数据保护相比，品牌保护是一个与众不同的游戏
tion。主要目标不是加强基础架构
和安全控制，而是“删除”（从
网络上的假冒行为）。

从网络收集的威胁数据可以揭示：

☑域名抢注域名
☑包括您公司或
产品名称或变体

☑包含您公司或产品的标签
它们的名称或变体

第107节

☑声称属于您的社交媒体帐户
或您的一名员工

☑使用您的商标未经授权的移动应用

☑提及拟假冒您的计划的论坛
牌

案例研究：打败打Ty
大型人力资源解决方案提供商

人力资源大，卫生好，
和财富利益解决方案
提供者帮助其他组织
管理他们的人力资源。
这家公司处理很多
个人认为可行的信息
（PII），包括健康和
财务数据。为了保护这些数据，
他们有广泛的安全操作-
时代中心，特色24/7/365
监控，事件响应，
调查和取证，以及
更多。

他们的安全副总裁
歌剧对我说
带领一支大约100人的团队
管理这些功能。用
记录未来，需要10。
“获得所有男人的名单-
我们公司在整个
到今天结束时，互联网是
完全不可行，即使我有10个人
或有20个人在工作，”
副总裁说。“当然，我们可以花一个
很多钱让人们燃烧
帐户和访问这些
私人空间，但真是浪费！
两人以外的任何事物
与只是比较没有任何意义
使用录制的未来。费用是
少于两个员工，而
我需要尝试的10或20
做类似的事情。”

例如，一个早晨
警惕了潜在的危险
域名抢注域名。此警报
是由监控规则触发的
团队已在Recorded中成立
将来检查欺诈行为-
类似于所拥有的电源
由组织。注册
这些域通常是第一个
进入网络钓鱼攻击。

团队收到警报后，
他们投资门控，发现网络钓鱼-
针对他们两个的尝试
组织及其一些
客户。他们立即发送
整个报告
组织及其所有客户
和合作伙伴。该报告提供了
关于可行的建议
如何应对攻击：封锁
您代理的域并使用
这些事件日志以扫描
威胁您的SIEM。许多
他们的合作伙伴报告了来自
该网站，但他们能够
在任何损坏之前阻止进入
已经完成。

借助实时威胁情报-
公司有能力
我可以在数小时内控制威胁，而不是
而不是几周内（或从未）。

第108页

威胁的关键素质

智能解决方案

当然，减轻数字风险不只是一个问题找到一些孤立的失窃数据或一次抢注域。某人或某事必须做更广泛的工作收集大量数据，筛选成千上万的数据点，分析数据点之间的关系，决定-确定优先事项并最终采取行动。

最好的方法是使用威胁情报解决方案能够：

☑**收集和扫描范围最广的数据来源：**数据收集阶段的自动化为分析师节省了宝贵的时间。最好的解决方案不仅从开放的Web来源收集数据，而且还收集来自黑暗的网络和技术来源。

☑**绘制，监控和评估数字风险：**通过自动化，高级数据科学和分析技术-机器学习和自然语言之类的话题处理，威胁情报解决方案应有所帮助分析师将业务属性与相关数字联系起来资产; 检测，评分和确定数字风险事件的优先级；并协调风险补救活动。

☑**协调补救：**强大的威胁情报-权限解决方案生成警报并报告提供有关如何解决问题的信息。它们还与可以执行补救措施的工具集成在一起立即签约，并提供服务取消域名抢注网站，误导性社交媒体帐户，和其他形式的品牌模仿。

109章

第三节：您的威胁情报计划

第十一章

分析框架威胁情报

在这一章当中

- 了解使用威胁情报的优势构架
- 了解三种最佳方法的优缺点-已知框架
- 了解三个框架如何相互补充

“结构是创造力所必需的。”

— Twyla Tharp

牛逼

考虑攻击和对手。他们提倡
广泛了解攻击者的想法，方法
使用以及在攻击生命周期中的特定位置发生特定事件。这个
知识可以使防御者更快地采取果断行动，
尽快阻止攻击者。

框架还有助于将注意力集中在需要的细节上
进一步调查以确保威胁已完全消除
移除，并采取措施防止将来
相同类型的入侵。

最后，框架对于在内部共享信息很有用
以及各个组织。它们提供了通用的语法
以及解释攻击细节的语法以及
细节彼此相关。共享框架使之成为可能
更容易从威胁等来源获取威胁情报
情报供应商，开源论坛和信息
共享和分析中心（ISAC）。

第112章

小费 以下概述的框架没有竞争力，但是
相当互补。您可以使用其中的一个，两个或全部三个
他们。

洛克希德·马丁
网络杀戮链®

该网络杀伤链®，首先由洛克希德·马丁公司研制中
2011年是网络威胁情报框架中最著名的-
作品。网络杀戮链基于军事概念
杀死链的方式，将攻击的结构分解为
阶段。通过以这种方式破坏攻击，防御者
可以查明它处于哪个阶段并进行适当部署
对策。

网络杀死链描述了攻击的七个阶段：

1. 侦察
2. 武器化
3. 交货
4. 开发
5. 安装
6. 指挥与控制
7. 行动和目标（有时称为
   渗透）

这些阶段通常以类似于图1的图的形式布置。
11-1。

图11-1： 洛克希德·马丁网络杀人链的示意图。

安全团队可以为每个阶段制定标准响应。

第113页

例如，如果您设法阻止攻击者攻击，
阶段，您可以高枕无忧
安装在目标系统上并获得完整的事件响应
可能不需要活动。

网络杀伤链还允许组织建立一个
针对击杀特定部分的纵深防御模型
链。例如，您可能会获得第三方威胁
专门监视的情报：

- ☑ 在网络上对您的企业的引用将指示侦察活动
- ☑ 有关针对新武器的武器化的信息报告您的应用程序中的漏洞网络

网络杀戮链的局限性

网络杀戮链是开始思考如何
防御攻击，但有一些限制。一
这种模式的主要批评是它没有考虑到
解释了许多现代攻击的工作方式。例如，
许多网络钓鱼攻击完全跳过了开发阶段，
而是依靠受害者打开Microsoft Oce
带有嵌入式宏的文档，或者双击
附加脚本。

但是即使有这些限制，网络杀手链仍然可以
讨论攻击及其可能的好基准
停了 这也使共享有关
使用标准进行组织内部和外部的攻击，
明确的攻击点。

您可以阅读以下内容，了解有关网络杀手链的更多信息
该开创性的白皮书并访问网络杀伤链
网站。

钻石模型

钻石模型由研究人员于2013年创建
现已解散的网络情报分析中心和
威胁研究（CCIATR）。用于跟踪攻击组
随着时间的流逝而不是个人攻击的进展。

第114章一更

钻石模型最简单的形式类似于
图11-2。它用于分类一个对象的不同元素。
攻击。攻击者或攻击组的钻石不是
静态的，而是随着攻击者改变基础架构而发展的
确定并确定目标并修改TTP。

对手

基础设施 能力

受害者

图11-2：一个简单的Diamond模型设计。

钻石模型可帮助防御者跟踪攻击者，
受害者，攻击者的能力和基础设施
攻击者使用。钻石上的每个点都是枢轴
捍卫者可以在调查期间使用的观点
与其他方面联系在一起。

旋转

假设您发现命令
并控制可疑流量
IP地址。钻石模型
会帮助您从中“透视”
初始指标以查找信息
关于与
该IP地址，然后进行研究
该功能的已知功能-
大头钉。了解这些功能
让您做出更多回应
快速有效地
事件。或者想象你的
威胁情报解决方案的使用
钻石模型。如果董事会
董事问谁在发射
针对其他组织的类似攻击
行业中的niza ons（属性-
tion），您也许可以快速
找到vic ms的列表，可能
atacker，以及对此的描述
atacker的TTP。这些会帮助你
决定需要什么防御
放置到位。

第115章一更

灵活性

Diamond Model的一大优势在于其灵活性-
强度和可扩展性。您可以添加攻击的不同方面
根据钻石上的适当点制造复杂
不同攻击组的概况。攻击的其他特征
可以跟踪的包括：

1.阶段
2.结果
3.方向
4.方法论
5.资源

钻石模型的挑战

缺点是钻石模型需要多加注意
和喂养。模型的某些方面，尤其是基础设施
现实，迅速变化。如果您不更新
攻击者不断，您冒着过时的风险
信息。

小费 为钻石的每次更新打上时间戳，以便每个人都可以看到-
信息时代的能力。

小费 如果您没有时间和资源来管理此类型
自己建模，您也许可以获取更新的信息
来自第三方威胁情报提供商。

即使面临这些挑战，钻石模型仍然可以
通过帮助使许多安全人员的工作更轻松
每个人都可以快速获得有关威胁的答案。

要了解有关钻石模型的更多信息，请阅读记录
来来的博客文章“将威胁情报应用于
Diamond Model of Intrusion Analysis ”，或下载origi-
最终白皮书“入侵分析的钻石模型”。

第116页

MITER ATT＆CK™框架

MITER是美国唯一的组织：
负责管理联邦资金的公司
多个联邦机构的研究项目。它有
对安全行业的巨大影响，包括
常见漏洞的管理和维护
暴露（CVE）和常见弱点枚举
（CWE）数据库。

MITER还开发了许多其他框架，
对于威胁情报非常重要，包括：

- ☑可靠的自动化情报交换
  信息（TAXII™），一种传输协议，
  使组织能够共享威胁情报
  通过HTTPS并使用通用应用程序-
  ming interface（API）命令来提取
  威胁情报
- ☑结构化威胁信息表达（STIX™）
  用于呈现威胁情报的标准格式
  权限信息
- ☑网络可观察的表达（CybOX™）
  框架，一种从
  网络安全事件

攻击者行为类别

MITRE对抗策略，技巧和共同点
创建知识（ATT＆CK™）框架是一种手段
随着时间的推移跟踪对抗行为的方式。ATT＆CK建立在
网络杀伤链，而不是描述一次攻击，
它着重于与特定目标相关的指标和策略
对手。

ATT＆CK使用11种不同的战术类别来描述adver-
严重的行为：

1. 初始访问
2. 执行
3. 持久性
4. 特权提升

117章

5.防御逃避

6.凭证访问

7.发现

8.横向运动

9.收集

10.渗透

11.指挥与控制

这些战术类别中的每一个都包括单独的技术-
可以用来描述对手行为的技巧。
例如，在“初始访问”类别下，行为
包括鱼叉附件，鱼叉链接，
信任关系和有效帐户。

您可以在以下位置查看MITER Enterprise ATT＆CK框架
https://attack.mitre.org/wiki/Main_Page 。

这种行为分类使安全团队可以
非常详细地描述和跟踪对抗行为
并易于在团队之间共享信息。

ATT＆CK™可用于多种安全功能，
从威胁情报分析师到SOC运营商以及
事件响应团队。追踪对手的行为
结构化和可重复的方式使团队能够：

☑优先处理事件响应

☑与攻击者联系

☑找出组织安全状况的漏洞

小费 威胁情报框架有助于整理您的安全防护方式
团队调查威胁，指标，漏洞和
演员。如果您不准备建立自己的框架，
进行分析，考虑与安全公司合作-
拥有围绕这些框架构建解决方案的企业。那
方法使您可以享受框架的好处
快速地进行安全活动
有效。

119章页

第十二章

您的威胁智力之旅

在这一章当中

审查明确威胁情报需求和目标的方法

检查有助于成功的关键成功因素

程式
了解如何从简单开始并逐步扩大规模

“无论您做什么，或者做梦都可以开始。大胆
拥有天才，力量和魔力。”

—约翰·沃尔夫冈·冯·歌德

我们开始您的威胁情报之旅和指导
走向全面计划。

在本书的这一章中，我们提出了一些该做什么和不该做什么

不要从威胁源开始

在第一章中，我们讨论了几种常见的误解-
有关威胁情报的说明，包括主要是
关于威胁数据源。实际上，许多组织开始
通过注册威胁来进行威胁情报计划
数据提要并将它们与SIEM解决方案连接。

这似乎是开始的好方法，因为许多威胁
数据Feed是开源的（即免费的），技术指标是
他们提供的行为似乎有用且易于解释。由于所有
恶意软件很糟糕，每个可疑的URL都可以被
攻击者，您掌握的线索越多越好，
对？

好吧，实际上，绝大多数恶意软件样本和
可疑网址与当前对您的威胁无关
企业。这就是为什么要喂入大量未经过滤的东西
几乎可以肯定，对您的SIEM的威胁数据将创建那种
我们在第4章中讨论了警报疲劳的问题。

要了解有关威胁情报来源的更多信息，
看看Recorded Future博客文章“超越Feed：A
深入研究威胁情报来源。”

阐明威胁情报需求和目标

因为威胁情报为许多团队提供了价值
网络安全，重要的是制定反映
企业的总体需求和目标。

回答这些问题

而不是假设任何一个团队，数据源或
威胁情报技术应该优先考虑
通过确定每个项目的需求来制定一套清晰的目标
您组织中的安全组及其优势
威胁情报可以带给他们。

首先考虑以下问题：

☑您最大的风险是什么？

☑威胁情报可以提供哪些帮助
解决这些风险中的每一个？

☑解决每个问题有何潜在影响风险？

☑资讯，技术ogy或人力资源来制作威胁情报在那些地区有效？

回答这些问题将帮助您弄清威胁所在
情报可以在最短的时间内带来最大的收益。
它还将指导您调查哪种威胁情报-
潜在来源，工具和供应商可以为您提供最佳支持，并且
您需要什么来加强您的程序。

第121页

记录的未来白皮书“最佳应用实践
威胁情报”阐述了为什么开始更好
不是通过研究技术或供应商，而是通过寻找
首先介绍可用的威胁情报类型，
他们如何使更多的网络安全领域
有效。

大部分来自威胁情报

您的安全组织中的团队可以从中受益
推动明智的决策和决策的智能
独特的观点。全面的情报
高效且易于食用，具有革命性的潜力
您组织中的不同角色每天如何运作。
图12-1显示了组织内部团队的示例
可以使用威胁情报。

图12-1：安全团队如何使用威胁情报。

在确定如何移动威胁情报策略时，
向前迈进，确定所有潜在用户很重要
在您的组织中，使智能与他们的独特性保持一致
用例。

第122页

深入研究每个组可以提供的威胁情报类型
使用以及它们在更快方面将如何受益
响应，更低的成本，更好地利用sta，更好的投资
决策等。通常，需求和收益并不明显。
记录这些详细信息将帮助您设置优先级，证明
投资，并发现令人惊讶的威胁新用途
情报。

了解威胁情报如何补偿人才
通过阅读《已记录的未来》，许多公司面临的差距
博客文章“ Threat Analyst Insights：威胁情报
矫平机。”

关键成功因素

我们已经观察到一些经常导致
有效的威胁情报程序。

产生快速胜利
带监控

监视威胁信息可以带来快速收益
投资相对较少。关键是要寻找一个
几种对您特别有意义的数据
业务和信息安全策略，将为您提供帮助
预测新出现的威胁或提供实际威胁的预警
攻击。您的活动可能包括：

☑检查影响您的新漏洞
最重要的软件包，服务器和
终点

☑追踪可能造成潜在风险的威胁趋势
您的业务运作

☑注意是否有泄漏的公司凭证，数据
或出现在公共或黑暗网站上的代码

可能有一些至关重要的数据类型
到您的企业，您无需投资即可进行监控
在新的基础设施或sta中。监视它们可以生成
快速获胜，展示威胁情报的优势，
并培养对该计划的热情。

第123页

尽可能自动化

有效的威胁情报计划通常着重于
从一开始就实现自动化。他们从自动化开始
基本任务，例如数据汇总，比较，标签-
和情境化。当这些任务被执行时
机器，人类可以腾出精力去做有效的工作，
明智的决定。

随着威胁情报程序变得越来越复杂，
满足您的需求，您可能会发现更多的自动化机会。
您将能够自动在各个站点之间共享信息
更大范围的安全解决方案并实现更多自动化

为事件分析提供情报的工作流程
应对和欺诈预防团队。你将能够
对您的威胁情报有更多“思考”
解决方案，例如通过自动安装软件
关联威胁数据并产生风险评分。

在评估威胁情报解决方案时，请检查
他们采用自动化的水平。自动化是
被罚款以汇总和交叉引用数据，或者
解决方案增加了使您的团队承担风险的环境-
有信心地做出基于决策的决定？请记住，在威胁中
情报，更多的原始数据只有在适当的情况下才能增加价值
经过分析，整理并以易于理解的方式提供给您
sume格式。

将威胁情报与流程和基础架构

将威胁情报工具与现有系统集成是
一种使智能变得可访问和可用的有效方法
不用压倒性的团队掌握新技术。

集成的一部分使威胁情报工具具有可见性
进入另一方捕获的安全事件和活动
安全和网络工具。相互关联和关联
最终的和外部的数据点可以产生真正的情报
与您的业务相关并放在上下文中
范围更广的威胁。

集成的另一个关键方面是提供最大的
重要，特定，相关和情境化的情报
在正确的时间到达正确的组。

第124页

威胁情报解决方案可以与SIEM集成
和其他安全工具（通过API或接口）
与安全工具供应商合作开发。

小费 当您评估威胁情报解决方案时，这一点很重要
了解哪些可以与您现有的系统集成
软件并支持您的安全团队的用例。

获得专家帮助培养内部专家

您从威胁情报中获得的价值直接与
使它与您的组织相关并应用的能力
它适用于现有和新的安全流程。

如果您与供应商或供应商合作，则可以更快地实现这些目标。
提供技术能力和经验的顾问
使您的组织能够充分利用威胁的能力
情报。随着时间的流逝，与这样的合作伙伴一起工作将
使您的团队成员成为威胁情报
本身就是专家，这样您在实地的能力
可以有机生长。

寻找拥有广泛而深入的威胁情报的合作伙伴-
权限专家。这些专家应具备以下条件：
了解您的需求并准备帮助您获得最大收益
从您的投资。您应该可以致电他们
所需的专业知识，并与他们一起确定新的
在组织中利用威胁情报的优势
阳离子化。您选择的合作伙伴不仅应该帮助您成功

俞霖。还可以为您的安全团队提供支持

您可以获取有关选择正确威胁的更多信息
通过下载“智能解决方案的采购指南，以
“网络威胁情报”，来自Recorded Future。这包括
方便的RFP模板，用于评估以下功能
不同的供应商。

第125页

从简单开始并向上扩展

我们希望这本书向您展示了威胁情报
不是某种需要放到上面的整体
安全组织一次。相反，你有
选择利用各种数据源，然后
处理，分析和向每个人传播威胁情报
网络安全主要团体。

这意味着您可以从当前状态开始
（而不是专门的威胁情报小组），一些数据
来源，并与现有安全工具（如SIEM）集成
和漏洞管理系统。然后可以缩放
直至专用站，更多数据源，更多工具，更多
集成和更自动化的工作流程，如
图12-2。

图12-2：威胁情报程序的四个成熟阶段，从
没有内部资源，只有有限的资源和工具，才有完整的，高度
自动化威胁情报程序。

通过研究各个小组的需求来开始旅程
您的网络安全组织，并了解威胁如何
有能力可以帮助他们实现目标。

第126页

然后，随着时间的流逝，您可以应对全面的威胁情报计划：

- ☑搜寻尽可能广泛的技术，开放，和黑暗的网络资源
- ☑使用自动化交付易耗品情报
- ☑通过以下方式实时提供完全上下文相关的警报有限的误报
- ☑整合并增强了现有的安全技术，逻辑与过程
- ☑始终如一地提高效率和效率您的整个安全组织

第127页

第十三章

开发核心威胁情报小组

在这一章当中

了解产生的过程，人员和技术
建立专用的威胁情报功能

了解这些团队如何利用威胁情报而不仅仅是判断
风险，也可以推动业务连续性

审查与威胁情报社区互动的方法

“人才赢得比赛，但团队合作和智慧赢得胜利
冠军。”

- 迈克尔·乔丹

我们

信息安全组织中的团队
它会看到威胁情报如何使大多数人受益
现在，我们提出一些有关如何组织您的建议
核心威胁情报团队本身。

专用，但不专用必要分开

正如我们在上一章中讨论的那样，您可以开始
与继续玩游戏的人进行威胁情报之旅
组织中不同团队的其他角色。

将出现两个问题：

1.是否应该有专门的威胁情报小组？

2.它应该是独立的，还是可以存在于另一个内部
网络安全小组？

答案是：是的，这取决于。

第128节

一支敬业的团队是最好的

在制定全面的威胁情报程序时，
您应该组建一个致力于收集和分析的团队
威胁数据并将其转化为情报。的唯一重点
该小组应提供相关且可行的情报，
对主要利益相关者（包括高级管理人员和
董事会成员。

需要奉献和广阔的视野来确保
团队成员将足够的时间用于收集，处理，
分析和传播提供以下方面的情报：
对整个企业最大的价值，而不是收益-
倾向于把注意力集中在一个人的智力需求上
组或另一个。

它的位置取决于您的组织

组织独立性，如图13-1所示，
优势，例如更大的自主权和声望。

图13-1：威胁情报作为独立的组
网络安全组织结构。

第129章一更

但是，这些优势可以完全由
建立一支具有团队精神的团队而引起的嫉妒和政治问题
新的高级经理人和自己的预算使人萌芽
威胁情报分析师脱离了他们现有的团队。

专门的威胁情报团队不一定需要
成为直接向VP或
CISO。它可以属于已经受到威胁的小组
情报。在许多情况下，这将是事件响应
组。这种精明的方法可以避免与根深蒂固的冲突
安全团队。

接人

如果您采取循序渐进的方法
建立您的核心威胁
情报团队，从
已经在
网络安全组织
将威胁情报应用到他们的
特定的安全领域。他们
可能没有“威胁情报”
权限分析师”或自己查看
最初是这样，但它们可以形成
您新兴的中坚力量
威胁情报能力。

核心竞争力

我们强调了威胁情报功能
存在以加强网络安全组织中的其他团队-
以便他们可以更好地保护特定企业。在那儿
至关重要的是，威胁情报团队必须包括人员
了解核心业务，运营流程，
网络基础架构，风险概况以及供应链
作为技术基础设施和软件应用
整个企业。

随着威胁情报团队的成熟，您需要添加
具有以下技能的成员：

☑将外部数据与内部遥测相关

☑提供威胁态势感知并提出建议
安全控制的建议

第130章

- ☑主动寻找内部威胁，包括内部威胁
- ☑对员工和客户进行网络教育威胁
- ☑参与更广泛的威胁情报社区
- ☑识别和管理信息源

收集与充实威胁数据

我们在第2章中略谈了威胁数据的来源。在这里，我们探索威胁情报团队如何与之合作各种来源，以确保准确性和相关性。

人类的优势

威胁情报供应商可以提供某些类型的策略，智力，但您也可以开发内部功能收集有关主题和活动的信息最多与您的企业有关。

例如，您可以开发一个内部网络搜寻器，分析前5,000个网站的网页代码-您的员工拜访的职位。该分析可能提供洞悉潜在的偷渡式下载攻击。您可以与安全架构团队分享见解，以帮助他们提出防范这些攻击的控制措施。这种威胁情报会生成具体数据，比轶事，猜想和泛型有用得多有关攻击的统计信息。

聪明的一休第131集

其他来源

可以加强威胁情报的专有来源-权限资源包括：

- ☑供应商或ISAC供稿
- ☑白名单

☑黑名单

☑威胁情报团队研究

合并来源

自动化威胁情报解决方案可实现威胁
情报团队集中，合并和丰富来自
在其他安全性提取数据之前有多个来源
系统或由人工分析员查看的安全操作
团队。

图13-2显示了这种自动威胁的要素
解。在此过程中，来自威胁情报的信息-
筛选Ligence供应商以查找对
企业和特定的网络安全团队。那是
来自内部威胁情报来源的数据丰富了
以适合诸如SIEM和
事件响应系统。这种自动转换数据
进入相关洞察力是威胁情报的本质。

图13-2：威胁情报平台可以集中，组合和丰富
数据，然后将其格式化为多个目标系统。（来源：记录的未来）

第132页

智能机器的作用

机器学习和自然语言处理的进步-
入侵（NLP）可以为威胁情报带来更多优势-
权限团队。有了正确的技术，就可以提及威胁
可以使所有来源的语言均不受影响，因此可以
由人和机器分析，无论原始
使用的语言。我们已经到了AI组件的地步
成功地学习了威胁的语言，并且可以
准确识别“恶意”用语。

机器学习，NLP和人工智能的结合
组织利用威胁情报的巨大机会
权限。这些技术不仅可以消除语言
障碍，但它们也可以减少分析员的工作量
处理与数据收集和关联相关的许多任务。
当结合考虑多个数据和
信息源同时产生真正的威胁
智能，这些功能使构建
威胁态势的可理解图。

了解Recorded Future如何在白色中应用高级AI
论文“机器学习助力智能威胁的4种方式
情报。”

您可以了解金融服务巨头房利美（Fannie Mae）的情况

通过以下方式简化了最终情报的沟通
阅读“如何建立网络威胁情报团队（和
为什么没有足够的技术”，请参见“已录制的未来”博客。

参与威胁情报社区

威胁情报无法在真空中繁荣发展。外部关系是成功的威胁情报的命脉团队。无论您的团队有多先进，都没有一个小组可以像威胁情报一样聪明整个世界。

许多威胁情报社区允许个人企业共享及时的相关攻击数据，以便他们可以在受害之前保护自己。参与与ISAC等受信任的社区合作对于降低风险，不仅对您的单个企业，而且

也适用于整个行业和网络安全领域大。参与需要时间和资源，例如通过电子邮件与同行交流并参加安全性会议，但建立关系必须是优先事项威胁情报获得成功。

135章页

结论：移动迈向安全情报计划

“认识你的敌人，了解自己，你就可以战斗百战无灾。”

—孙子

书中的重点

W 情报可帮助网络安全中的每个人开始采用南团队预测威胁，更快地应对攻击，以及在降低风险方面做出更好的决策。在13章中在本书中，我们研究了智力如何适用于组织安全的多个方面策略，使之朝着更积极，更全面的方向发展全面的安全方法。

这就是安全情报-一种扩大安全性的方法通过揭露未知因素来确保安全团队和工具的有效性威胁，做出更好的决策并推动共同最终加速跨部门风险降低的理解组织。有了威胁情报的三大支柱，数字风险保护和第三方风险降低组织可以真正了解他们面临的风险，并且简化团队工作方式，以更好地利用价值强大的人力资源。

如本书前言所述，安全情报-留置权的方法植根于三个原则：

***1.*威胁情报必须提供以下内容：做出明智的决定并采取行动。**

威胁情报需要及时，清晰并采取行动-

136章

能够。它必须在正确的时间以某种形式出现可以理解的。它应该丰富您的知识，而不是决策过程复杂化。它应该帮助把您单位中的每个人都在同一页面上。

***2.*人与机器更好地协作。**

机器可以处理和分类原始数据订单
比人类快得多。另一方面，
人类可以执行直观的大图分析
比任何人工智能都要好-只要它们是
不被庞大的数据集分类所淹没，
做乏味的研究。当人与机器
配对时，每个工具都会更智能地工作，从而节省时间和金钱，并减少-
改善人的职业倦怠，提高整体安全性。

*3.***威胁情报适合所有人。**

无论您担任什么安全角色，威胁情报
有所作为。这不是一个单独的安全领域
-无论您身在何处，它都可以帮助您更聪明地工作
维护SOC，管理漏洞或使高
级别的安全决策。但是为了使事情变得容易，不是
更难的是，威胁情报应与解决方案集成
您已经并且应该依靠的位置和工作流程
易于实现。

无论您是在踢安全情报
主动，或者您的策略多年，
降低风险是最终目标。

137章

附录

威胁情报目标：快速参考指南

威胁情报并非“一刀切”。安全
威胁情报在企业中的应用取决于
您组织的性质和现有信息
安全策略和功能。

该威胁情报目标库与安全性保持一致
我们在本书中重点介绍的团队。您可以使用这些目标
帮助识别威胁情报活动并确定其优先级。

	安全运营
数据泄露事件	向受影响的人报告数据泄露事件 利益相关者进行补救
高风险恶意软件家族	研究恶意软件家族的演变和趋势 对我的组织有高风险
名誉风险	识别对我组织声誉的风险
	事件响应
数据泄露事件	向受影响方报告数据暴露事件 和利益相关者进行补救

漏洞管理

漏洞利用套件	识别有关漏洞利用工具包的信息
高危易腐生物	识别技术中的关键和高风险漏洞叠
未公开的漏洞	识别未公开的零日禁运漏洞

风险分析

第三方安全权限	评估第三方的信息安全能力
高架第三方风险	确定对我的风险较高的第三方组织
竞争研究	研究竞争市场

安全领导

高架第三方风险	确定对我的风险较高的第三方组织
攻击计划	确定可以针对我的攻击计划组织

第138页

行业攻击趋势	确定针对相关行业的广告系列
基础设施风险	我的基础架构的风险评分增加
网络钓鱼和垃圾邮件广告活动趋势	确定使用鱼叉式广告的趋势广告系列或带有恶意电子邮件附件的网络钓鱼或链接
名誉风险	识别对我组织声誉的风险
定向运动研究	识别与特定操作相关的IOC或运动以帮助跟踪和缓解网络攻击
目标威胁演员研究	确定与威胁行为者相关的IOC，以提供帮助跟踪并缓解网络攻击

预防诈骗

被盗资产发现	发现被盗资产（例如礼品卡，信用卡）在线发布

威胁情报分析

高架第三方风险	确定对我的风险较高的第三方组织
数据泄露事件	向受影响方报告数据暴露事件和利益相关者进行补救
漏洞利用套件	识别有关漏洞利用工具包的信息
高风险恶意软件家族	恶意软件家族的研究演变和趋势对我来说风险很高
高风险漏洞	识别技术中的关键和高风险漏洞叠
确定攻击计划	确定可以针对我的攻击计划组织
行业攻击趋势	确定针对相关行业的广告系列
基础设施风险	我的基础架构的风险评分增加
网络钓鱼和垃圾邮件广告活动趋势	确定使用鱼叉式广告的趋势广告系列或带有恶意电子邮件附件的网络钓鱼或链接
名誉风险	识别对我组织声誉的风险
定向运动研究	识别与特定操作相关的IOC或运动以帮助跟踪和缓解网络攻击
目标威胁演员	

研究	确定与威胁行为者相关的IOC，以提供帮助跟踪并缓解网络攻击
未公开的漏洞	识别未公开的零日禁运漏洞

139章

https://www.linkedin.com/company/threathunting

https://www.twitter.com/threathunting_

第141页一更