数字政策办公室

信息安全

信息技术安全威胁管理
实务指南

第 1.1 版

2024 年 7 月

版权公告

修改记录				
修改次数	修改详情	经修改页数	版本编号	日期
1	将「政府资讯科技总监办公室」修改为「数字政策办公室」 在第 5.2 节更新威胁情报来源的例子。		1.1	2024 年 7 月

目录

1 简介

在现今互联互通的数字化环境中，决策局／部门的信息系统、网络和敏感数据皆面临日益增加的威胁。为协助决策局／部门应对复杂环境，本指南提供了全面的信息技术安全威胁管理框架，其中包含了所需的知识和策略，以建立完善的威胁监察能力、主动检测潜在安全漏洞，以及迅速有效地作出反应，以减少信息技术安全威胁的影响。管理层用户、信息技术经理、系统管理员及其他技术与操作人员可借助该框架更好地了解信息技术安全威胁管理流程，以在日益严峻的威胁环境中保护其数字资产。

1.1 目的

本文件展示了信息技术安全威胁管理的总体框架，且应与其他安全文件结合使用，例如《基准信息技术安全政策》[S17]、《信息技术安全指南》[G3]以及相关程序（如适用）。

本实务指南旨为政府所有需要处理安全风险评估或安全审计的人员，以及为政府进行安全风险评估或安全审计的安全顾问或供应商而设。

1.2 参考标准

以下参考文件对于本文件的应用必不可少。

- 《基准信息技术安全政策》[S17]，香港特别行政区政府
- 《信息技术安全指南》[G3]，香港特别行政区政府
- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022
- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022
- NIST SP 800-92 – Guide to Computer Security Log Management
- NIST SP 800-150 - Guide to Cyber Threat Information Sharing
- NIST SP 800-137 – Information Security Continuous Monitoring for Federal
- Information Systems and Organizations
- Guide to Cyber Threat Modelling, Cyber Security Agency of Singapore
- Cyber-threat intelligence information sharing guide, GOV.UK
- 安全风险评估及审计实务指南
- 信息安全事故处理实务指南
- Endpoint Detection & Response: A Malware Identification Solution, IEEE Xplore. 可供查阅：https://ieeexplore.ieee.org/document/9703010
- Best endpoint detection and response solutions reviews 2024: Gartner Peer insights, Gartner. 可供查阅：

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

1.3 定义及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用，以及以下的定义及惯用词。

缩写及术语	
ACL	访问控制列表
APT	进阶持续性威胁
CRM	客户关系管理
DDoS	分散式拒绝服务攻击
DLP	数据外泄防护
DNS	域名系统
EDR	端点检测和响应
EPP	端点保护平台
ERP	企业资源计划
ICS	工业控制系统
IDS	入侵检测系统
IOA	攻击指标
IoC	入侵指标
IP	互联网规约地址
IPS	入侵防御系统
ITSM	信息技术服务管理
KPI	关键绩效指标
MTTD	平均检测时间

MTTR	平均响应时间
NAC	网络访问控制
NDR	网络检测和响应
PAM	特权访问管理
PoC	概念验证
POS	销售点
ROI	投资回报
SEM	安全事件管理
SIEM	安全信息和事件管理
SIM	安全信息管理
SOAR	安全编排、自动化和响应
SOC	安全运营中心
TCO	整体拥有成本
TIP	威胁情报平台
TTP	策略、技术和程序
UEBA	用户和实体行为分析
URL	划一资源定位址
VM	虚拟机
VPN	虚拟私有网络
WAF	网络应用系统防火墙
XDR	扩展检测和响应

1.4 联络方法

本文件由数字政策办公室编制及备存。如有任何意见或建议，请寄往：

电邮：	it_security@digitalpolicy.gov.hk
Lotus Notes 电邮：	IT Security Team/DPO/HKSARG@DPO
CMMP 电邮：	IT Security Team/DPO

2 信息安全管理

信息安全是关于安全控制和措施的规划、实施和持续提升，以保护信息资产的机密性、完整性和可用性，适用于信息的存储、处理或传输过程及其相关信息系统中。信息安全管理是一套有关规划、组织、指导、控制的原则和以这些原则迅速有效地管理实体、财务、人力资源和信息资源的应用，以及确保信息资产和信息系统的安全。

信息安全管理涉及一系列需要持续监测和控制的活动。这些活动包括但不限于以下的范畴：

- 安全管理框架与组织；
- 管治、风险管理和遵行要求；
- 安全操作；
- 安全事件和事故管理；
- 安全意识培训和能力的建立；和
- 态势感知和信息共享。

安全管理框架与组织

决策局 / 部门须根据业务需要和政府安全要求，制定和实施部门信息安全政策、标准、指南和程序。

决策局 / 部门亦须制定信息安全的组织架构，并须向有关各方就安全的责任及问责提供清晰的定义和适当的分配

管治、风险管理和遵行要求

决策局 / 部门须采用风险为本的方法，以一致及有效的方式识别信息系统的安全风险、订定应对风险的缓急次序和应对有关风险。

决策局 / 部门须定期和在必要时对信息系统和生产应用系统进行安全风险评估，以识别与安全漏洞相关的风险和后果，并为建立具成本效益的安全计划和实施适当的安全保护和保障措施提供依据。

决策局 / 部门亦须定期对信息系统进行安全审计，以确保当前的安全措施符合部门信息安全政策、标准和其他合约或法律上的要求。

安全操作

为保护信息资产和信息系统，决策局 / 部门应根据业务需要实施全面的安全措施，涵盖业务上不同的技术领域，并在日常操作中采取「预防、侦测、应急和复原」原则。

- 预防措施避免或阻止不良事件的发生；
- 侦测措施识别不良事件的发生；
- 应急措施是指在发生不良事件或事故时，采取相应行动来遏制损害；和
- 复原措施是将信息系统的机密性、完整性和可用性恢复到预期状态。

安全事件和事故管理

在现实环境中，由于存在不可预见并致服务中断的事件，故此安全事故仍可能会发生。若安全事件危及业务的连续性或引起数据安全风险，决策局／部门须启动其常规安全事故管理计划，以实时识别、管理、记录和分析安全威胁、攻击或事故。决策局／部门亦应准备与有关各方适当地沟通，透过分享对有关安全风险的应急以消除不信任或不必要的猜测。当制定安全事故管理计划时，决策局／部门应规划和准备适当的资源，并制定相关程序，以配合必要的跟进调查。

安全意识培训和能力建立

因为信息安全是每个人的责任，所以决策局／部门应不断提升机构内的信息安全意识，透过培训及教育，确保有关各方了解安全风险，遵守安全规定和要求，并采取信息安全的良好作业模式。

态势感知和信息共享

因应网络威胁形势不断变化，决策局／部门亦应不断关注由安全行业和政府计算机安全事故协调中心发布的现时安全漏洞讯息、威胁警报和重要通知。应将即将或已经发生具威胁的安全警报传达及分享给决策局／部门内的负责同事，以便采取及时的应对措施来缓解风险。

决策局／部门可以利用威胁情报平台接收和分享安全事务、安全漏洞和网络威胁情报的讯息。

所有人员亦可以通过参与安全演习和参加研讨会、展示会或浏览载有安全情报信息和一般安全信息（例如网络安全资讯站、资讯安全网）的专页来提高安全意识。

3 信息技术安全威胁管理

3.1 信息技术安全威胁管理简介及其重要性

信息技术安全威胁是指通过未经授权的访问、破坏、披露、修改信息或拒绝服务，使该组织的运营、资产、声誉或人员有可能造成任何负面影响的情况或事件。该等威胁在数字化环境下日趋普遍，为世界各国政府和组织带来重大风险。

为有效应变此等威胁，决策局／部门需要了解与信息技术安全威胁管理相关的各种要素。威胁者，即构成威胁的个人或团体，在此情况下发挥着至关重要的角色。此外，决策局／部门需要获取威胁信息，包括指标、策略、技术和程序、安全警报、威胁情报报告和工具配置。这些信息有助决策局／部门保护自身并检测威胁者的活动。

在信息技术安全方面中，威胁与风险、漏洞和影响密切相关。

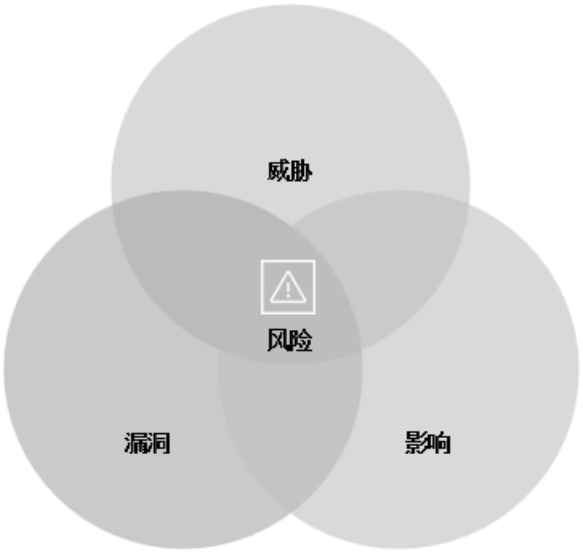

图 3.1 风险被定义为威胁、漏洞和影响的组合

威胁者利用决策局／部门系统或网络的漏洞，可造成各种负面后果。决策局／部门需要识别和评估威胁、漏洞和潜在影响，以有效管理和减低风险，保障其数字资产的机密性、完整性和可用性。请参阅《**信息技术安全风险管理实务指南**》和《**安全风险评估及审计实务指南**》以了解更多详情。

换言之，管理威胁可为管理风险奠定基础。信息技术安全威胁管理包括以一种全面的方式减低和应变数字化环境中的信息技术安全威胁。通过构建稳健的信息技术安全威胁管理能力，决策局／部门可持续监控威胁环境、迅速识别潜在

攻击、推行控制措施减少漏洞，并迅速遏制威胁。这增强了态势感知能力、降低风险，并能够敏捷应对潜在的信息技术安全事故。

有效的信息技术安全威胁管理对于建立抵御信息技术安全攻击的复原能力、保护敏感数据和维护公众信任至关重要。为了建立情报导向和风险为本的信息技术安全威胁管理方法，决策局／部门需充分了解其面临的威胁。基于此理解，决策局／部门能够评估其防御措施的成熟程度，并判断发生安全事故的可能性。同时使决策局／部门有效地评估风险并排列先后次序，从而分配其安全资源。

信息技术安全威胁分析可分为三个层面：部门层面、系统层面，及设备或应用层面。每个层面都提供了关于威胁分析不同方面的见解，有助决策局／部门确定整体威胁管理方向。

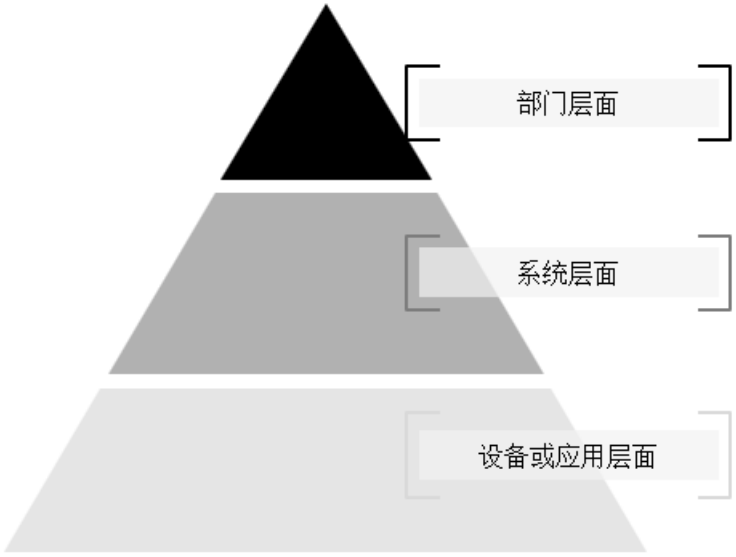

图 3.2 威胁分析的层级

部门层面

部门层面的威胁分析涉及分析部门层面的情报来源和趋势，重点关注于外部因素，例如地缘政治。决策局／部门会根据其入侵前后的动机和行动进行敌方剖析。这一层的分析通常从宏观角度进行，供管理层使用。

系统层面

系统层面的威胁分析考虑系统的架构、关系和行为。这涉及对环境中的资产、数据流通和界线建立模型，以判断与系统相关的威胁事件。有关此层面威胁分析的详情，请参阅《**安全风险评估及审计实务指南**》。

设备或应用层面

设备或应用层面是威胁分析中最精细的层面。这涉及威胁搜寻、日志关联、详细数据分类、进阶分析和试探技术等活动。此层面的分析旨在识别和解决对已公布漏洞详细的规避和利用。

通过推行信息技术安全威胁管理，决策局／部门能够通过有系统的框架更了解威胁，并主动采取措施有效地预防、检测和应变威胁。推行信息技术安全威胁管理有数项主要优点：

- ***保护政府敏感资料。***决策局／部门通常需要处理敏感资料，包括市民记录、财务信息和机密文件。保护这些信息对维持公众的信任和信心至关重要。通过有效的威胁管理实践，决策局／部门可建立完善的安全措施，例如访问控制、加密和保护数据存储，以防止未经授权的访问和数据外泄。

- ***确保必要服务的连续性。***任何关键系统的中断或入侵都可造成严重后果，阻碍其向公众提供重要服务。决策局／部门可以通过主动管理信息技术安全威胁，识别潜在漏洞，实施减低措施，并建立事故应变计划，使决策局／部门迅速检测和应对安全事故，降低对必要服务的影响并确保其服务提供不受干扰。

- ***致力于维护监管要求和国际标准。***规管框架到位以保护个人数据、确保私隐并维护信息技术安全。遵守这些法规和标准对决策局／部门履行法律义务和维持公众信任至关重要。通过实施信息技术安全威胁管理措施，决策局／部门可以展示其致力于保护敏感资料、遵守相关保护数据的法例，并维持高水准的信息技术安全。

3.2 信息技术安全威胁管理框架

为建立一致且有效的信息技术安全威胁管理方法，各决策局／部门应采用标准化的信息技术安全威胁管理框架。此框架与国际良好作业模式和行业标准保持一致，为管理信息技术安全威胁和确保全面的信息技术安全提供有系统的方法。

采用标准化框架可为决策局／部门提供共同基础，以就管理信息技术安全威胁开展交流和协作，并加强决策局／部门与数字政策办公室之间的协调和信息共享。

信息技术安全威胁管理分为六个主要阶段（如下文概述），且每个阶段的工作在相应的章节中有更详细的描述。

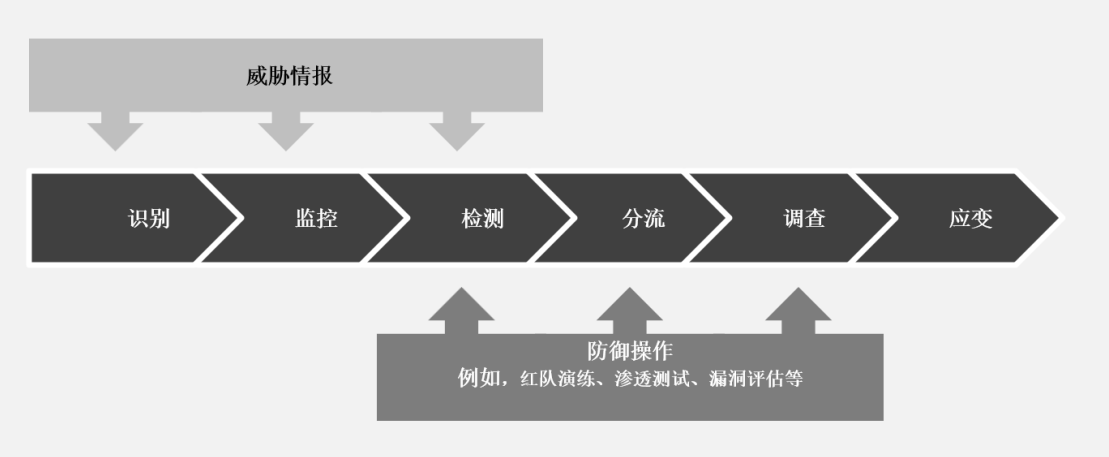

图 3.3 信息技术安全威胁管理框架中的主要阶段

A. 识别（部门与系统层面）（第 4 节）

此阶段中，决策局 / 部门应识别可能损害信息系统、数据、操作或声誉的潜在威胁。这阶段涉及的主要工作如下所示：

- 识别和分类相关信息技术安全威胁
- 使用威胁情报来源和共享平台

B. 监控（设备或应用层面）（第 5 节）

此阶段中，决策局 / 部门应持续监察网络流量、系统日志和安全事件。这阶段涉及的主要工作如下所示：

- 设计和实施全面监控策略

C. 检测（设备或应用层面）（第 5 节）

此阶段中，决策局 / 部门应分析已收集的数据，如日志文件和网络流量，以识别可能存在安全漏洞或恶意活动的模式或异常。这一阶段涉及的主要工作如下所示：

- 数据收集、日志分析和威胁情报集成
- 行为分析、异常检测和威胁情报应用

D. 分流（设备或应用层面）（第 6 节）

一旦检测阶段得出潜在威胁警报，决策局 / 部门需要根据警报的严重程度和潜在影响对其排序和分类。此分流流程有利于有效分配资源以迅速解决关键威胁。分流阶段的概述如下：

- 警报收集和分析
- 警报验证
- 严重程度分类
- 持续监察和重复分流

E. 调查（设备或应用层面）（第 6 节）

从分流队列中选择警报后，决策局 / 部门应进行彻底调查，以确定潜在威胁的真实性及其性质。调查阶段对在准确评估是否存在实际攻击方面有至关重要的作用。这阶段涉及的主要工作如下所示：

- 证据收集
- 威胁分析

F. 应变（设备或应用层面）（第 7 节）

在此阶段，决策局 / 部门应制定和执行行动和措施，以应变潜在的威胁或警报，以避免其演变成真实事故，或在调查阶段确认为真实事故后造成损害。主要工作可涉及：

- 遏制
- 拦截
- 修补
- 培训

下表列出针对不同信息系统保安等级的信息技术安全威胁管理机制的示例。安全要求是以**累计**横跨不同等级的信息系统（即所有第 1 级信息系统规定的安全要求须扩展到第 2 级和第 3 级信息系统）。

阶段	第 3 级信息系统	第 2 级信息系统	第 1 级信息系统
识别	建立机制排序和监察涵盖所有威胁组件的威胁情报来源。 分析威胁情报以生成全面的威胁摘要报告，其中包含网络风险详细信息和建议措施。	威胁情报和分析的流程分配给特定群组或个人。	制定流程用以监察威胁情报，以识别新兴的威胁。

	利用威胁情报为决策局 / 部门提供风险状况信息，确定缓解措施的优先次序，并更新信息技术安全架构和配置标准。 采用多种情报来源和分析技术以预测未来攻击及识别趋势。		
监控	建立中央保安监察流程，包括专责的 24 / 7 监察团队。 建立用于监察和分析用户行为（如互联网协定地址、网络使用模式、工作时间和已知设备），并提供异常活动警报的系统。	备份审计日志到中央日志服务器或媒体，以防止日志被未经授权的更改。 使用主动监察安全日志异常行为的工具，并提供在既定参数范围内的警报。	定期覆检系统日志中是否存在异常或可疑活动。 建立通过环境监察检测异常活动的流程。
检测	安装自动化工具以检测对关键系统文件、防火墙、入侵防御系统、入侵侦测系统或其他安全设备未经授权的更改。 使用实时网络监察和检测工具。 使用可主动关联多个来源的事件信息，并根据既定参数发送警报的工具。	建立流程以在攻击者遍历系统、建立立足点、窃取信息或对数据和系统造成损害之前发现渗透迹象。 端点行为检测能力（如端点检测与响应解决方案）应可用于各端点（即用户工作站、膝上电脑和服务器）。	建立机制（如防毒警报、日志事件警报等）以提醒安全监察功能和管理层注意潜在的攻击。
分流	基于严重程度和潜在影响对威胁进行排序。		
调查	调查威胁的特性、动机和潜在影响。		
应变	开发和执行措施应变威胁。		

表 3.1 针对不同系统关键程度信息技术安全威胁管理机制的示例

在信息技术安全威胁管理流程的不同阶段，可能存在不同的输出或交付成果，如下表 3.2 所示。

阶段	输出 / 交付成果示例
识别	• 提供有关新兴威胁、攻击趋势和相关安全新闻的最新信息的威胁情报报告。 • 威胁分类，已识别威胁的完整列表。
监控	• 威胁监察目标、工具和采用的技术。
检测	• 基于可疑活动、异常行为或已知威胁模式生成警报和事件的既定规则和阈值。
分流	• 既定机制、分类标准、程序和工作流程。
调查	• 潜在威胁调查过程的步骤、工具和技术的记录，包括数据收集、分析和证据保存。
应变	• 既定的行动和措施，以便在威胁演变成真实事故之前作出应变。

表 3.2 信息技术安全威胁管理框架的输出 / 交付成果示例

4 部门背景建立

4.1 了解威胁环境和新兴趋势

了解威胁环境和新兴趋势对决策局 / 部门有效管理和降低信息技术安全风险至关重要。以下是了解威胁环境和新兴趋势的一些工作：

- ***保持了解。***定期监察和收集来源可靠的信息，例如来自信息技术安全新闻网站、行业报告和政府公告。订阅相关邮件列表、关注安全博客，并加入专业网络以保持了解最新的威胁和趋势。

- ***参与威胁情报。***利用提供有关信息技术安全威胁、漏洞和新兴趋势实时信息的威胁情报服务或平台。此类服务集成了来自不同来源的数据，并提供可行的见解。

- ***定期进行风险评估。***通过定期建立威胁模型和风险评估以识别潜在威胁和漏洞，包括分析网络基础设施、系统、应用和数据资产。

- ***参与信息共享活动。***参与信息共享活动和政府资助的方案。这些平台有助于决策局 / 部门与数字政策办公室交换威胁情报，并使其了解其他决策局 / 部门所面临的威胁。

- ***分析事故数据。***定期覆检和分析安全事故数据。查找模式、趋势和常见攻击途径。此分析可帮助决策局 / 部门了解威胁者采用不断演变的策略、技术和程序。

- ***持续学习和培训。***决策局 / 部门应持续提升信息技术安全威胁管理意识，并安排培训和教育，以确保有关各方了解风险、遵守安全法规和要求，并符合安全良好作业模式。

鉴于信息技术安全威胁持续演变的性质，决策局 / 部门应积极参与上述活动以收集和交流见解、威胁指标和良好作业模式。这种协作方法加强了对攻击的整体防御能力，并能够及时识别和应变新兴威胁，包括以下优势：

- ***共享态势感知。***信息共享利用共享伙伴的集体知识和经验，增强了各决策局 / 部门的防御能力，从而提高了整个社区的安全。

- ***改善安全态势。***共享威胁信息使得决策局 / 部门能更了解威胁环境，促使知情的信息技术安全实务、识别受影响的系统、实施保护措施，以及更有效的事故应对和复原能力。

- ***增强认知成熟度。***共享和分析看似无关的观察结果可以丰富信息、增强指标和了解威胁者的策略、技术和程序，从而提高整体理解和应对能力。

- ***提升防御敏捷性。***共享信息可让决策局 / 部门了解不断演变的威胁者的策略、技术和程序，从而实现快速的检测和应变。这加快了操作节奏，降低了攻击成功的可能性，并且由于威胁者需要被迫建立新的策略、技术和程序，为其造成了成本劣势。

决策局 / 部门可能面对各种严重影响国家安全、公共安全及政府运作的信息技术安全威胁。以下列出多项主要类型的威胁者：

- ***网络罪犯。***这些个体或团体进行网络犯罪，主要为了获取经济利益。常见网络犯罪包括勒索软件攻击和网络钓鱼诈骗，诱骗人们进行汇款或泄露信用卡信息、登录凭证、知识产权或其他私人或敏感资料。

- ***国家级网路攻击者。***国家级和有关政府频密资助威胁者窃取敏感数据、收集机密信息或破坏另一政府的关键基础设施。这些恶意活动通常包括间谍活动或网络战争，并且资金充裕，使其威胁复杂且难以检测。

- ***黑客行动主义者。***黑客行动主义者使用黑客技术宣扬政治或社会议程，例如传播自由言论或揭露侵犯人权的行为。黑客行动主义者认为他们正在积极影响社会变革，并认为有理由针对个人、组织或决策局 / 部门揭发秘密或其他敏感资料。

- ***寻求刺激者。***寻求刺激者攻击计算机和信息系统主要为了娱乐。一些寻求刺激者想看到自己可以窃取多少敏感资料或数据；另一些则希望使用黑客技术更了解网络和计算机系统的运作原理。尽管他们并不总是试图造成伤害，但寻求刺激者仍然会通过干扰网络安全，并为未来攻击建立途径，而造成无意的损害。

- ***内部威胁者。***内部威胁者的意图并不总是恶意的。有些内部威胁者因人为错误而损害公司，如无意间安装恶意软件，或遗失公司发放的设备，这些设备被网络罪犯拾得并访问公司网络。除此之外，内部人员的恶意损害亦存在，例如心怀不满的员工滥用访问权限窃取数据以获取金钱利益，或损害数据或应用以报复其晋升失败或给予其不公平对待的上级。

- ***网络恐怖分子。***网络恐怖分子出于其政治或意识形态的动机，发起网络攻击，威胁或造成暴力行为。这些网络恐怖分子可能包括国家级网路攻击者，以及独立行动或代表非政府组织行事的个体。

威胁者在执行攻击时会部署多种策略，包括但不限于以下内容：

- ***进阶持续性威胁。***进阶持续性威胁为复杂且有针对性的安全攻击，通常由国家资助的威胁者，或技术高超的黑客组织执行。这些威胁涉及对政府网络的长期隐蔽渗透，以收集敏感资料、破坏运营或进行间谍活动。

- ***勒索软件攻击。***勒索软件攻击日趋普遍，对决策局／部门构成重大威胁。攻击者对关键数据进行加密，并要求公司支付赎金以换取恢复访问权限。此类攻击可能会造成政府系统瘫痪，扰乱公共服务，并泄露敏感资料。

- ***分散式拒绝服务攻击攻击。***分散式拒绝服务攻击使政府网站或网络不堪流量重负，导致用户无法访问。该等攻击可能会扰乱公共服务，损害市民信任，并分散对其他入侵的注意力。

- ***社交工程和网络钓鱼。***社交工程技术，例如网络钓鱼电子邮件和欺诈电话，通常用于欺骗政府雇员，以泄露敏感资料或提供未经授权的系统访问，可能导致数据外泄、未经授权的访问或安装恶意软件。

- ***供应链攻击。***决策局／部门依赖庞大的供应商和承包商网络使其容易受到供应链攻击。恶意威胁者可能会破解这些供应商提供的软件或硬件，从而利用恶意软件或后门感染政府系统。

- ***关键基础设施攻击。***决策局／部门通常负责营运和监督关键基础设施，例如电网、运输系统和滤水厂。针对这些系统的信息技术安全攻击可能会造成严重后果，包括关键服务中断、经济损失甚至生命损失。

- ***零日漏洞利用。***零日漏洞利用针对尚未修补的软件或系统中以往未知的漏洞。对于在黑市上发现或购买这些漏洞的黑客来说，决策局／部门是他们吸引的目标，因其可用于获得未经授权的访问或开展有针对性的攻击。

- ***信息战和虚假信息。***决策局／部门也容易受到信息战和虚假宣传活动的影响。这些行为包括传播虚假信息、操纵公众舆论或进行信息技术安全操作，以影响政治流程或破坏公众信任。

4.2 范围制定

制定范围对决策局／部门至关重要，可使其根据特定需要在信息技术安全威胁管理中有效分配资源、建立监察措施，以及建立安全措施的优先次序。

在部门层面明确制定范围，可使决策局／部门确定其需要保护的特定部门或分部（例如财务部、人力资源部或研发部）免受潜在威胁。通过制定该层面的范围，决策局／部门可以分配资源和实施安全措施，以解决与有关部门或分部的特定漏洞和风险。

至于系统层面，范围制定涉及识别决策局／部门需要保护的系统，例如企业资源计划系统（ERP）、客户关系管理系统（CRM）或内部通信系统。通过制定系统层面的范围，决策局／部门可以集中精力保护这些关键系统，并确保其能够抵御潜在威胁。

在设备或应用层面，范围制定涉及识别需要保护的特定设备或应用，例如服务器、路由器、防火墙或关键业务的应用。通过制定该层面的范围，决策局／部门可以实施有针对性的安全控制措施，以保护这些关键组件免受潜在威胁。

此外，在制定信息技术安全威胁管理的范围时，必须识别依赖关系。举例来说，决策局／部门应考虑对供应商或服务供应商等外部利益相关者（例如第三方软件供应商、云端服务供应商或关键组件供应商）的依赖关系。通过识别依赖关系，决策局／部门可以评估相关风险，并采取适当的安全措施，以确保系统和数据的安全。

5 威胁识别和情报收集

5.1 识别和分类信息技术安全相关威胁

威胁可分为三个主要类别：

- ***社会威胁。***直接与人为因素相关有意或无意的威胁，例如人为错误、遗漏或疏忽、盗窃、欺诈、误用、损害、破坏、披露和修改数据。
- ***技术威胁。***源自技术问题，例如错误流程、设计缺陷、布线等通信路径中断。
- ***环境威胁。***源自火灾、水灾、供电、地震等环境灾害。

识别和分类相关的信息技术安全威胁有助于有效降低风险。为此，开发全面准确的威胁分类至关重要。威胁分类组织并分类不同类别的信息技术安全威胁，以清楚了解威胁环境，使得决策局 / 部门能够相应地分配资源和工作。

为识别和分类信息技术安全威胁，决策局 / 部门应遵循以下建议步骤：

1. ***进行威胁评估：***全面评估决策局 / 部门信息技术安全的潜在威胁，这可能涉及分析历史数据、研究行业趋势、咨询安全专家，以及考虑决策局 / 部门信息技术基础设施的个别特征。
2. ***识别威胁类别：***根据评估将威胁划分为相关类别。可以上述三类威胁（社会威胁、技术威胁和环境威胁）为起点。确保该类别涵盖决策局 / 部门特有的威胁范围尤其重要。
3. ***制定威胁类别：***在每个类别中，制定与决策局 / 部门相关的特定威胁类别。例如，在社会威胁下，其可能包括恶意软件、网络钓鱼攻击、内部威胁、社交工程等。建议尽可能全面地撷取决策局 / 部门可能遇到的各种威胁。
4. ***定期更新和完善：***威胁环境为不断变化的动态，新威胁和现有威胁都在不断演变。定期覆检和更新威胁分类以保持最新状态至关重要。决策局 / 部门应保持了解新兴威胁、攻击技术、漏洞和行业良好作业模式，并将知识纳入威胁分类，以确保其相关性和成效。
5. ***记录和沟通：***决策局 / 部门应以清晰易读的格式记录威胁分类，建立资料库或知识库，以便相关持分者能访问和了解分类威胁，并向相关持分者传达威胁分类，以提高风险意识并确保共同了解相关风险。

威胁分类应适应决策局 / 部门的需要，并随着威胁环境的变化而发展。威胁分类属于动态文件，需要定期更新和完善，以有效指导决策局 / 部门的信息技术安全工作。另见**附件 A** 了解威胁分类的样本和具说明作用的示例，以协助决策局 / 部门使用威胁分类识别特定威胁并确定其优先排序的方式。

威胁分类和安全风险评估在信息技术安全中是相互关联且相辅相成。威胁分类提供结构化框架，用于组织和分类不同的信息技术安全威胁，使决策局 / 部门能够了解其所面临的威胁环境。该分类通过将威胁划分为特定类别，为进行全面的安全风险评估奠定了基础。

安全风险评估使用威胁分类，识别和评估每个威胁的漏洞和潜在后果。它考虑了决策局 / 部门的资产、价值、现有控制措施，以及漏洞利用的可能性，以确定每种威胁构成的风险水平。威胁分类为风险评估过程提供信息和指导，确保所有相关威胁已基于其潜在影响对其进行优先排序。

相反地，风险评估结果（例如已识别的风险及其相关的可能性和严重程度）为完善和更新威胁分类提供了有价值的见解。此迭代流程可确保威胁分类保持最新状态，并与不断演变的风险环境保持一致。

因此，应使用威胁分类和安全风险评估以有系统地识别信息技术安全风险、订定风险的缓急次序和缓解相关风险。有关更多详情，请参阅《**信息技术安全风险管理实务指南**》和《**安全风险评估及审计实务指南**》。

5.2 使用威胁情报来源和共享平台

威胁信息是指可帮助组织保护自身或检测威胁者活动的所有信息，例如：

- **入侵指标**（IoC）是技术上的产物或可观察物，表明攻击即将发生或正在发生，或可能已经发生。这些指标可作为线索，用于检测和防御潜在威胁。指标示例包括单一可疑命令和控制服务器的互联网协定（IP）地址、可疑的域名系统（DNS）域名、标记恶意内容的划一资源定位址（URL）、恶意可执行文件的文件哈希或恶意电子邮件主题文本。
- **策略、技术和程序（TTPs）**描述了行为者的表现。策略是对行为的高层次描述，技术是在策略条件下对行为的详细描述，而程序是对技术较低层次、高度详细的描述。策略、技术和程序可以描述行为者使用特定恶意软件变体、操作顺序、攻击工具、发送机制（例如网络钓鱼或水坑攻击）或漏洞利用的倾向。
- **安全警报**，也称为公告和漏洞说明，是关于当前漏洞、利用和其他安全问题，通常人类可读，简短的技术通知。
- **威胁情报报告**通常是散文般的文件，描述策略、技术和程序、行为者、系统类型和目标信息，以及其他为组织提供更强态势感知能力的威胁信息。威胁情报是经汇总、转换、分析、解释或扩充的威胁信息，为决策流程提供必要的背景信息。
- **工具配置**是设置和使用工具（机制）的建议，该工具（机制）支持自动收集、交换、处理、分析和使用威胁信息。例如，工具配置信息说明可能包含有关安装和使用隐匿软件检测程式和软体删除工具，或创建和自定义入

侵检测标识符、路由器访问控制列表（ACLs）、防火墙规则或网络过滤器配置文件。

威胁情报是指有关潜在信息技术安全威胁的信息和见解，包括新兴的攻击技术、漏洞和入侵指标。利用威胁情报，决策局 / 部门可以增强其信息技术安全能力，并主动防御不断演变的威胁。

威胁情报是了解和解决信息技术安全威胁的关键部分，涉及收集和分析有关潜在威胁的信息，包括其策略、技术和指标。不同类型的威胁情报为决策局 / 部门提供有价值的见解：

- ***战略性情报。***战略性情报侧重长期趋势、地缘政治因素以及威胁者的能力和动机，有助决策局 / 部门预测风险，并相应地调整安全策略。战略情报通过提供有关业务风险通俗易懂的报告，协助制定长期战略。

- ***技术性情报。***技术性情报提供有关直接威胁（例如新型恶意软件或漏洞）的具体和可执行信息，使决策局 / 部门能够迅速有效地应变该等威胁。技术性情报包括威胁者使用的策略、技术和程序，并提供可用于更新防御系统的入侵指标。

- ***操作性情报。***操作性情报侧重威胁者的策略、基础建设和活动，提供对威胁者所使用策略和方法的见解。操作性威胁情报通常涉及针对组织的潜在且即将开展的行动详情，可帮助决策局 / 部门预测和准备特定的威胁活动。

威胁情报应：

- 具有相关性（即与决策局 / 部门的保护相关）；
- 具有见解的（即为决策局 / 部门提供对威胁形势的准确而详细的理解）；
- 具有情境性，提供态势感知（即根据事件发生的时间、地点、以往经验和在类似组织盛行为信息提供更多前因后果）；
- 具有可行性（即决策局 / 部门可以快速有效地就信息采取行动）。

威胁情报供应商从各种来源搜集信息，例如入侵指标、客户端生成数据、深网、暗网、讯息平台、社交媒体、人力情报、恶意软件分析、地缘政治发展、代码仓库和内容公开张贴网站。多样化的来源信息能够提供全面的威胁洞察，包括威胁者使用的策略、技术和程序、需要修补的漏洞，以及可能的入侵或攻击指标。有效的威胁情报供应商会验证并汇总不同来源的信息，以提供对威胁的全面理解。理想的多源情报报告应结合至少两种来源的信息。请参阅**附件 B** 以了解评估信息技术安全威胁情报供应商的问题示例。

威胁情报透过各种方式传递，包括订阅、威胁情报平台（TIP）和数据源。订阅提供对当前和历史情报的访问、交互式调查功能，且能够与现有流程整合。威胁情报平台整合并关联不同的数据源，允许用户在各种威胁情报来源间切换并进行调查。数据源提供持续更新的威胁情报，可整合到安全系统和流程中，实现实时保护。

鼓励决策局／部门采用威胁情报平台，以主动有效地利用威胁情报。这些平台是集中式存储库，用于收集、分析和传播来自各种来源的威胁情报。决策局／部门可利用威胁情报平台简化威胁情报的收集和分析，从而能够识别相关威胁并及时主动采取措施来降低风险。威胁情报平台还能促进不同决策局／部门之间的合作和信息共享，促进集体和协作的信息技术安全方式 。

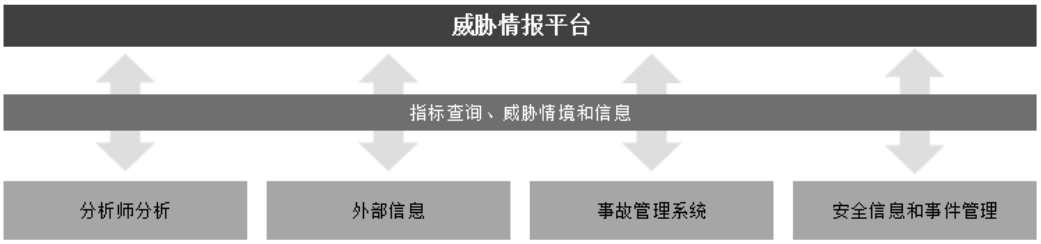

图 5.1 威胁情报平台的使用情况

此外，决策局／部门可与可信任的信息技术安全组织，例如行业协会、研究机构和私营资讯保安公司，建立战略合作伙伴关系。这些合作伙伴可以为决策局／部门提供专业知识、研究发现、额外的威胁情报来源，在决策局／部门现有能力基础上提供补助。

为有效利用威胁情报来源和共享平台，建议采取以下步骤：

1. ***确立目标：***明确决策局／部门内制造威胁情报的目的和目标，考虑到决策局／部门运营的具体需求和优先事项。

2. ***识别和选择信息来源：***识别和审视提供相关可靠威胁情报的内部和外部信息来源。这些信息来源可以是政府来源（例如政府电脑保安事故协调中心）、特定行业组织、信息技术安全供应商以及国际信息共享平台。这些来源提供了关于新兴威胁趋势、已知漏洞以及网络罪犯使用的策略的及时可靠信息。

3. ***收集信息：***从选定的内部和外部渠道收集信息，建立一个全面的数据集用于分析。收集的信息可能来自入侵指标、客户端生成数据、深网、暗网、讯息平台、社交媒体、人力情报、恶意软件分析、地缘政治发展、代码仓库和内容公开张贴网站。

4. ***处理和准备信息：***对收集到的信息进行处理，使其便于分析。此过程中可能需要翻译、格式化或核实数据，以确保其准确性和一致性。

5. ***分析信息：***对收集到的信息进行彻底分析，了解其与决策局 / 部门的相关性和重要性。识别与威胁者、策略、技术和程序（TTP）、漏洞以及入侵指标（IoC）相关的模式、趋势和潜在风险。

6. ***沟通和共享：***与决策局 / 部门内相关人士和分部有效沟通和共享已分析的威胁情报。以易于理解和可行动的格式呈现信息。

7. ***纳入信息技术安全流程：***将从各种渠道收集到的威胁情报整合到决策局 / 部门的信息技术安全威胁管理流程中。这可能涉及使用相关的入侵指标和策略、技术和程序来更新技术性的预防和检测控制，例如防火墙、入侵检测系统、反恶意软件解决方案等。

8. ***加强信息安全测试：***使用威胁情报作为信息安全测试过程和技术的输入。这有助于识别决策局 / 部门系统和基础设施中的漏洞和弱点。

下文以案例形式阐述决策局 / 部门如何有效处理威胁情报：

决策局 / 部门收到了一份威胁情报报告，报告显示行业内某类恶意软件的使用频率正在逐渐上升。该报告包括技术细节，例如恶意软件可执行文件的哈希值，而文件哈希值是关键的入侵指标。

收到该情报后，决策局 / 部门立即展开行动。由决策局 / 部门的信息技术安全管理组启动流程了解威胁情境，审查与报告的恶意软件相关的策略、技术和程序，包括感染方法（例如电子邮件附件、下载被篡改的软件）、恶意软件安装后的行为（例如数据外泄、系统损坏）以及任何已知的防御措施。

信息技术安全管理组将了解到的信息传达给关键持份者，包括高层管理人员、部门信息技术安全主任和相关信息技术团队。此确保每人都了解到威胁的性质以及减轻威胁需要采取的步骤。

然后，相关团队使用入侵指标（恶意软件可执行文件的哈希值）来更新防御措施，通过配置反恶意软件系统来识别并隔离任何具有报告哈希值的文件。同时，团队还应调整入侵检测系统，以寻找与恶意软件相关的网络流量模式。

最后，团队应检视威胁情报报告，寻找任何关于可能被恶意软件利用的软件漏洞的信息。如果决策局 / 部门的系统使用了任何易受攻击的软件或硬件，应尽快修补软件或硬件以进一步保护系统免受恶意软件侵害。

6 威胁监控和检测与威胁情报的整合与应用

6.1 明确监察目标、技术和工具

各决策局 / 部门应明确监察目标，包括识别需要保护的关键资产、系统和网络，并了解潜在的威胁和风险。通过全面了解这些要素，决策局 / 部门应继而使监察工作与总体信息技术安全目标一致。明确目标后，决策局 / 部门可选择适当的监察技术和工具。决策局 / 部门应评估并部署与监察目标一致的工具，确保工具的覆盖范围足够，且能够良好地与其他安全解决方案结合。

决策局 / 部门应根据其目标和具体要求选择适当的安全监察工具。以下工具仅供举例说明，在选择工具时应考虑特定部门要求、预算和现有基础设施：

- ***入侵防御系统（IPS）。***入侵防御系统理论上能够在入侵活动到达目标前，检测并尝试阻止其入侵活动。

- ***网络检测和响应（NDR）解决方案。***网络检测和回应解决方案集中对网络流量进行实时监察、分析行为，并检测潜在威胁。这方案提供了解网络可见性、识别异常，并有助发现隐藏威胁。

- ***端点检测和响应（EDR）解决方案。***端点检测和响应解决方案集中于监察和保护个别端点，并收集和分析端点数据以检测和应变高级威胁。有关 EDR 的更多详细信息，请参阅附件 D。

- ***端点保护平台（EPP）。***端点保护平台结合了防病毒、防恶意软件和主机为基础入侵防御功能，以保护端点免受各种威胁。

- ***威胁情报平台（TIPs）。***威胁情报平台汇总、分析并传达各种来源的威胁情报数据，有助于识别新兴威胁和入侵指标。

- ***用户和实体行为分析（UEBA）。***用户和实体行为分析是一种利用行为分析、机器学习算法和自动化来识别异常和潜在危险的用户和设备行为的保安软件。

- ***扩展检测和响应（XDR）解决方案。***扩展检测和回应解决方案从组织的技术堆栈中以往分离的安全工具收集威胁数据，以便更轻松、更快速地调查、搜索和应变威胁。扩展检测和响应平台可从端点、云端工作负载、网络电子邮件等方面收集安全遥测数据。

- ***安全信息和事件管理（SIEM）系统。***安全资讯和事件管理系统收集并分析不同来源的安全事件日志，将事件进行关联并根据预先定义的规则和模式生成警报。

- ***安全编排、自动化和响应（SOAR）解决方案。***安全编排、自动化和回应解决方案平台监察威胁情报源，并触发对安全问题的自动响应，这有助快速高效地减轻横跨多个复杂系统的威胁。

附件 E 中的图表说明了综合的威胁监控架构，展示了信息技术安全威胁监控中相互关联的监控工具，以供参考。

在选择适当的信息技术安全威胁监控解决方案时，各决策局 / 部门应考虑以下因素：

- ***可扩展性：***确保解决方案能处理随决策局 / 部门规模的扩大而不断增加的数据。
- ***兼容性：***确保解决方案应能与现有系统和技术兼容。
- ***实时监控能力：***解决方案应能实时监控和检测威胁。
- ***威胁情报汇总能力：***解决方案应能汇总各种来源的外部威胁情报。
- ***可调整性和灵活性：***解决方案应具备可调整性，以配合决策局 / 部门的特定需求。
- ***报告和分析能力：***具备全面报告和分析的能力。
- ***供应商声誉和支持：***考虑供应商的声誉和提供的支持。
- ***成本效益：***评估解决方案的成本，确保其物有所值。

此外，决策局 / 部门应战略性地在整个网络基础设施中部署传感器，以捕获相关数据并检测潜在威胁。部署决策应考虑以下要素：

- ***网络拓扑：***考虑网络的布局和结构。
- ***关键资产：***识别并优先保护重要资产。
- ***进出点：***关注网络流量进出区域。
- ***网络段：***查看网络中的不同部分或分区。
- ***网络交汇点：***注意不同网络段相交的点。
- ***已知攻击途径：***考虑攻击者使用的常见方法。
- ***易受攻击的服务和协议：***识别服务和协议中的弱点。
- ***历史攻击：***从过去的攻击和漏洞中积累经验。
- ***威胁情报：***了解当前和新兴威胁。

采用风险为本的方法来部署传感器至关重要，优先考虑关键资产、高风险区域以及曾经出现漏洞的区域。应定期覆检和评估网络拓扑、攻击途径和新兴威胁，以确保持续有效。

信息技术安全威胁监控目标、技术和工具可用于及时识别和应变信息技术安全威胁，相关示例如下。

目标	技术和工具
尽可能减少影响、检测和应对恶意软件感染。	实施实时扫描端点和网络流量恶意软件，识别并阻止恶意文件或活动。
识别并拦截未经授权的访问尝试，以保护敏感数据和系统。	实施用户活动监察和异常检测，以检测可疑登录尝试、权限升级或未经授权的用户权限变更。
监控数据泄露的尝试，防止敏感数据从决策局 / 部门泄露。	部署数据外泄防护（DLP）解决方案，监控并阻止通过电子邮件、网站上传或流动装置传输未经授权的敏感数据。
监控用户行为，并检测员工或外判人员潜在的内部威胁或恶意活动。	实施用户行为分析，监控异常的数据访问模式、过多文件下载或未经授权对机密信息的访问尝试。
检测并防止网络入侵或未经授权的访问尝试。	部署入侵检测系统（IDS）或入侵防御系统（IPS），以监控已知攻击标识符或可疑活动的网络流量。
监控网络应用程序的安全漏洞，并防范基于网络的攻击。	实施网络应用程序防火墙（WAF），监控和过滤传入的网络流量，拦截恶意请求或对应用程序漏洞利用的尝试。
监控云端基础架构和服务，以检测并应对安全事故或配置错误。	利用云端服务供应商提供的云端特定监控工具和服务，追踪和分析安全事件，例如未经授权的访问尝试或可疑的应用程式介面（API）调用。

表 6.1 信息技术安全威胁监控目标、技术和工具示例

各决策局 / 部门在实现有效的网络安全监察和检测方面可能面临重大挑战，这通常依赖于专业工具和技术，而这些工具和技术需要大量资金投入。然而，有限的预算可能会妨碍决策局 / 部门获取和应用这些工具，使其难以充分监控系统并及时检测潜在安全事故。

尽管如此，有限预算的决策局 / 部门仍然可以采取措施来增强其监控和检测能力。采用富有策略的方法以尽可能地利用资源和替代方法至关重要。建议如下：

- ***排序监控目标和区域：***确定需要保护的最关键资产、系统和网络。根据风险评估和安全事故潜在影响来分配资源。通过排序这些领域的监控工作，重点保护高价值目标和敏感资料。

- ***利用内置安全功能：***充分利用现有基础设施和可用的系统内置安全功能。现代操作系统、网络设备和云端平台通常具有原生的安全监测功能，如日志汇总、审计和基本威胁检测。确保这些功能已启用并适当地配置。

- ***集中端点保护：***通过在决策局 / 部门所有设备上实施完善的防病毒 / 反恶意软件解决方案优先进行端点保护。配置这些工具以实现实时监控、威胁检测和事故应变。定期更新防病毒或恶意软件标识符，以防范最新的威胁。

- ***注重用户意识培养和培训。***开展用户意识培养和培训计划，帮助员工了解常见的安全威胁、网络钓鱼攻击和安全计算的最佳实践。对于用户意识非常了解的用户可作为安全风险的第一道防线，减少对监控工具的依赖。

- ***进行网络分段：***利用网络分段将关键系统和敏感数据与网络的其他部分隔离。此可实现更加集中的监控工作，并减少攻击面。通过虚拟局域网（VLAN）或防火墙等方式进行网络分段无需大量的资金投入。

6.2 数据收集、日志分析和威胁情报汇总

为有效监控和检测信息技术安全威胁，启用日志记录和数据收集机制是必要的。安全日志可能有各种来源，例如硬件设备、软件系统和应用程序。有关安全日志管理和相关安全注意事项，请参考《信息安全记录管理实务指南》。

集中的日志汇总和分析解决方案（例如安全信息和事件管理（SIEM）系统）可让决策局 / 部门全面了解安全事件，并分析信息技术基础设施中各种来源日志间的相关性。安全信息和事件管理（SIEM）是一种结合了安全信息管理（SIM）和安全事件管理（SEM）功能的安全软件产品和服务。除了安全信息管理和安全事件管理功能外，一些安全信息和事件管理产品还具备实时安全警报分析、威胁验证和事故工作流程自动化等额外功能。

安全信息管理自动收集来自网络和安全设备 / 终端（例如防火墙、代理服务器、入侵检测系统和防病毒软件）的事件日志数据，并将收集的数据和威胁情报日志进行关联和简化，以便长期存储、分析和报告。

安全事件管理提供事件管理功能，可导入安全事件进行分析和可视化呈现（以图表和仪表板等形式）作事故应变和安全操作。安全事件管理主要进行实时监测、事件汇总、相关性分析和通报来自操作系统、防病毒软件、防火墙和入侵检测系统的事件，以及由认证系统、服务器和数据库直接通报的事件。

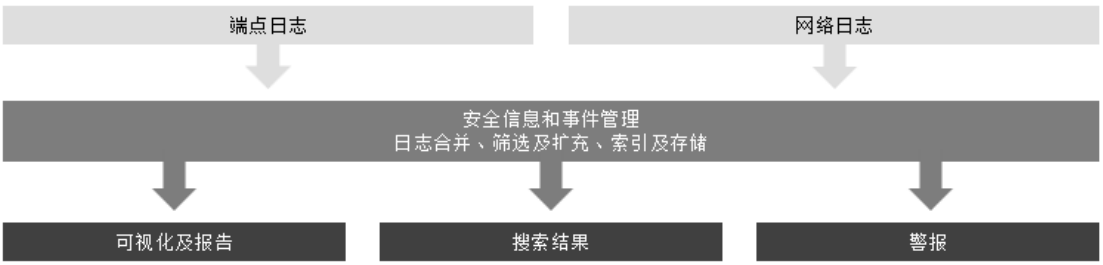

图 6.1 安全信息和事件管理功能

除安全信息和事件管理外，还有一些更具成本效益的替代方案可用于日志汇总和分析，例如主要用于从收集、存储和分析各种来源日志的日志管理工具。这些工具提供集中进行日志汇总和分析的功能，但不具备安全信息和事件管理的进阶安全功能。虽然这些替代方案可能更具成本效益，但可能不具备与完整的安全信息和事件管理解决方案相同级别的进阶安全功能和威胁检测能力。在选择替代方案之前，决策局／部门应仔细评估其需求和预算。

检测阶段的成功在很大程度上取决于前一阶段收集到的数据的可用性。收集功能运作越高效，检测功能效果越好。

工具的质量会影响检测阶段的成效，包括威胁狩猎能力、内外部威胁情报信息的可用性，以及检测工程功能的成效。

此外，为有效检测和分析威胁，决策局／部门应将威胁情报纳入监察和分析流程。威胁情报包括已知入侵指标、新兴威胁、攻击手法以及漏洞等相关信息。

- ***利用外部威胁情报。***将威胁情报源、数据库或平台整合至监察基础设施，以提高识别和应变特定威胁的能力。决策局／部门可以利用威胁情报主动防御已知威胁，应对不断变化的攻击技术。

- ***关联和警报生成。***利用威胁情报整合，将传入日志、网络流量和端点活动与已知威胁指标进行比较。这关联提高了威胁检测的准确性和成效，使系统能够在发现潜在威胁时发出警报或通知。

威胁情报源可提供有关最新攻击活动、恶意软件变体、漏洞和漏洞利用技术的数据。通过仔细分析这些信息，决策局／部门可以发现网络犯罪活动的模式和趋势，确定其动机，并了解所使用的工具和方法。

以下是对于数据收集、日志分析和威胁情报整合的一些建议执行步骤：

1. ***识别日志来源：***根据其对业务、监管和遵行要求的重要性，确定应监察的内容。这些可包括网络交换机、路由器、防火墙、主机操作系统、安全软件、网络应用系统、电子邮件应用系统等。

2. ***制定日志记录政策：***评估各组件对业务和运营的重要性，并确定应记录的信息。制定日志记录政策指明应记录的事件／活动。例如，决策局／部门宜记录所有登录尝试、访问控制变更和关键系统事件。

3. ***进行负载测试：***在生产环境中实施日志记录政策之前，在测试环境中对日志记录进行负载测试。这将有助于确保计划的日志配置能够处理预期负载，并且不会对系统性能产生不利影响。例如，决策局／部门可以模拟大量日志事件，以确保配置能够在不影响系统性能的情况下处理预期负载。

4. ***实施集中日志汇总与分析：***考虑实施集中日志汇总与分析解决方案，例如安全信息和事件管理系统。安全信息和事件管系统可就安全事故提供全面的可见性，并对信息技术基础设施内各种来源的日志进行有效分析。

5. ***评估安全信息和事件管理功能：***根据安全信息和事件管理产品的功能（例如安全信息管理、安全事件管理、实时安全警报分析、威胁验证和事故工作流程自动化）对其进行评估。选择最符合决策局／部门需求的安全信息和事件管理解决方案。

6. ***整合威胁情报：***将威胁情报纳入监察和分析流程，例如利用外部威胁情报源、数据库或平台来提高识别和应变特定威胁的能力。

7. ***关联和警报生成：***利用威胁情报整合，将传入的日志、网络流量和端点活动与已知威胁指标进行比较。这一关联提高了威胁检测的准确性和成效，使系统能够在发现潜在威胁时发出警报或通知。

8. ***分析威胁情报：***仔细分析威胁情报信息，以揭发网络犯罪活动的模式和趋势、识别动机，并了解攻击者使用的工具和方法。这种分析有助于加强决策局／部门的防御，并应对不断变化的攻击技术。

9. ***评估检测工具：***评估可用检测工具的质量，包括威胁狩猎能力的强度和内部及外部威胁情报信息的可用性。确保检测工程功能的成效。

10. ***确保数据收集的效率：***检测功能的成效取决于数据收集阶段获得的数据的可用性。确保收集功能有效运行，收集必要数据以有效检测威胁。

11. ***保持更新：***根据不断变化的安全威胁和新兴技术，持续监察和更新日志记录和威胁情报整合流程。

6.3 行为分析、异常检测和威胁情报应用

为有效监控和检测信息技术安全威胁，各决策局／部门应为其网络、系统和用户建立基准行为模式。通过了解什么构成环境中的正常行为，决策局／部门可识别出具潜在威胁或恶意活动的偏差或异常。在确定基准行为模式后，决策局／部门应利用行为分析技术识别异常或偏差。行为分析涉及通过监察和分析持续活动检测出偏离既定规范的行为。此可通过利用进阶的分析工具和技术，将当前行为与既定基准进行比较。

以下是一些建议执行步骤：

1. ***部署数据分析工具：***部署适当的数据分析工具或平台，例如安全信息和事件管理系统、日志管理解决方案或其他数据分析工具，以处理和分析历史数据。

2. ***数据准备和分析：***分析网络流量、系统活动和用户行为的历史数据，以深入了解决策局 / 部门基础设施内的典型模式和活动。通过标准化格式、将时间戳转换为通用时区以及解决数据源中的差异或不一致问题，使收集到的数据规范化。

3. ***识别相关数据参数：***识别与建立基准行为模式数据相关的关键参数或属性，例如网络流量、系统资源利用率、用户登录活动和应用系统使用情况。

4. ***统计分析和用户 / 系统剖析：***应用平均值、中位数、标准偏差或聚类算法等统计分析技术分析历史数据，以确定趋势、模式和分布。根据历史数据分析用户和系统剖析，针对典型用户行为、系统活动和网络流量模式创建个人档案或角色。

5. ***覆检、更新和存档：***建立流程持续监察运行数据，以持续更新基准行为模式，因决策局 / 部门基础设施和用户行为演化。记录基准行为模式建立的流程，例如数据收集计划、分析技术和识别的正常行为参数。建立文档总结基准行为模式，并指导持续的监察和检测工作。

在行为分析中应用威胁情报有助于决策局 / 部门将观察到的异常与已知攻击技术或指标关联。这一关联有助于确定和验证潜在威胁的缓急次序，减少误报，并将资源集中用于最重大风险。决策局 / 部门可通过分析威胁情报识别常见攻击途径，例如网络钓鱼电子邮件、社交工程技巧术或恶意软件传播方式。这有助决策局 / 部门主动实施防御措施，并教育员工有关潜在风险，从而降低被成功攻击的可能性。

决策局 / 部门可参考以下步骤在监控和检测过程中应用威胁情报源和数据：

1. ***选择相关威胁情报来源：***决策局 / 部门可以从多个威胁情报来源中选择，例如商业型供应商、开源信息源和行业特定的信息共享平台。这些来源提供相关新兴威胁和已知攻击技术的信息。

2. ***制定入侵指标（IoCs）：***决策局 / 部门可根据已识别的威胁和攻击途径制定入侵指标。这些入侵指标为是显示潜在安全事故的特定信息，例如互联网规约地址、域名、文件哈希值或与已知威胁相关的行为模式。

3. ***收集和汇总威胁情报数据：***决策局 / 部门通过各来源收集威胁情报数据，并将其集中存储。全面收集数据有助于更广泛地了解威胁环境。

4. ***标准化和丰富威胁情报数据：***决策局 / 部门对收集的威胁情报数据进行规范和丰富，以确保一致性并提高分析效用。这过程包括标准化格式、添加背景信息和关联不同来源的数据。

5. ***将威胁情报源纳入监控和检测流程：***将威胁情报源整合至决策局 / 部门的监控和检测系统。这可将观察到的异常与已知攻击技术或指标关联，从而实现更快和更准确的威胁检测。

6. ***将入侵指标与收集到的数据进行匹配和关联：***将已制定的入侵指标与收集到的数据进行匹配和关联，以确定并验证潜在威胁的缓急次序。这流程有助识别和集中于最相关和最高风险的安全事故。

7. ***持续更新和刷新威胁情报数据：***威胁情报数据并非一成不变，新的威胁和漏洞会定期出现。决策局／部门需持续更新和刷新威胁情报数据，以便及时了解新兴威胁，并相应调整其安全措施。

8. ***监察和评估成效：***决策局／部门对整合威胁情报源和数据于其监控和检测过程的成效展开监察和评估。这评估有助于识别需要改进的方面，并确保威胁情报程序在加强网络安全方面发挥作用。

7 威胁分流和调查

7.1 通过分流程序订定威胁的缓急次序

分流指对安全警报进行初步评估和分级，以订定其缓急次序和相应的应变。分流的目的是进行快速的修复或升级，以应对大量的安全警报。与医院急症分流程序类似，决策局 / 部门的目标是根据现有数据，合理地订定调查队列的缓急次序。利用以往的防御经验，决策局 / 部门作出明智的决策以确保有效的资源分配。

为便于分流，以下前提条件应予满足：

1. ***建立预先定义准则：***决策局 / 部门应建立明确的准则，以指导分流期间的决策程序。图 7.1 展示更多分流程序概览的示例。这些准则应定期覆检和更新，以适应威胁环境和新兴技术的变化。

2. ***利用威胁框架：***决策局 / 部门应利用各框架（例如 Lockheed Martin Cyber Kill Chain 以及 MITRE ATT&CK）以深入了解攻击的周期及其不同阶段，以及攻击者使用的常见技术。这些框架有助于理解和分类安全警报。

以下是分流程序的概览：

1. ***警报收集和分析：***警报由安全分析员和自动化工具收集和分析。分析员覆检各警报提供的详细信息，包括相关日志、网络流量数据和相关入侵指标。

2. ***警报验证：***下一步是验证警报以确认其准确性和相关性。这包括检查支持证据（例如网络日志、系统日志或入侵检测系统数据），以判断警报的安全事故是否属实或误报。配置错误、软件故障或良性的用户行为都可导致误报。识别误报后，应向检测工程团队反馈以完善准则。

3. ***严重性确认：***根据预先定义的准则，按照警报的潜在影响和迫切性对其分类，并指派其严重性等级。这使安全团队可集中优先处理最严重的威胁。常见类别宜包括攻击步骤 / 阶段或技术。常见的严重性等级可包括高、中、低，或根据决策局 / 部门的需求制定类似的等级判定方案。这步骤有助于为警报订定缓急次序作进一步调查。

4. ***持续监察和迭代分流：***在整个应变过程中进行持续的监察和进一步分流，以识别威胁环境中任何新的警报或变化，这确保及时发现和处理新出现的威胁或不断变化的事故。

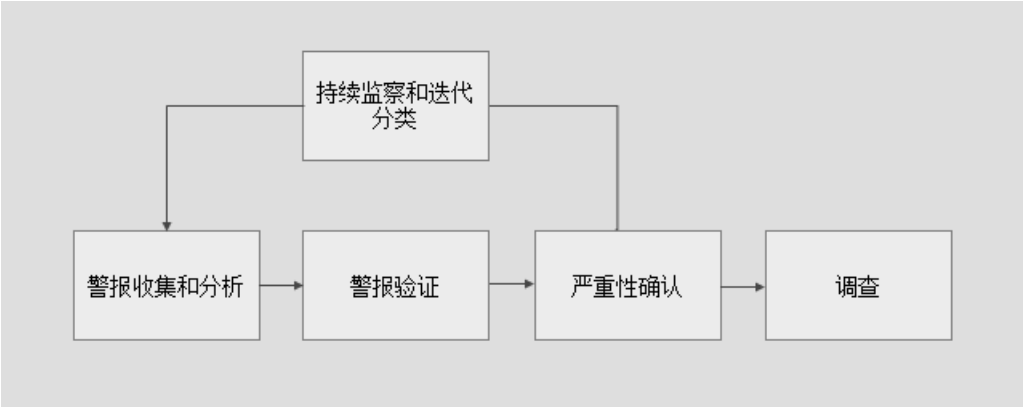

图 7.1 分流程序概览

分流程序的成效主要取决于决策局／部门在对警报进行分流时，安全工具和技术所提供的信息详细程度和额外背景。安全工具（例如事务跟踪管理系统和安全信息和事件管理系统）可提供功能促进决策、自动化工作流程，并提升分流程序的效率和成效。分流工具为安全团队提供了专用平台，以快速和一致地接收、评估和管理安全事故。

值得注意的是，分流过程是动态的，并可能需要根据从威胁情报中收集的背景情况持续地重新评估。威胁情报提供有价值的背景资料，有关威胁者的性质、能力、动机和目标。这些背景信息有助决策局／部门评估威胁对其系统、数据和业务运营的潜在影响。随着新信息的出现或威胁环境的变化，分流程序可能需要调整以反映不断变化的威胁环境。

以下示例阐述了使用 MITRE ATT&CK 框架预先定义的准则进行分流。假设决策局／部门收到警报，称内部系统与已知恶意的互联网规约地址存在可疑的向外连接，则需根据以下准则订定应变的缓急次序：

准则标准	描述	示例说明
警报的严重性	评估警报指派的严重性等级，表示着明确安全警报的潜在影响和迫切性。严重性较高的警报可能需要即时的关注和优先的缓急次序	团队评估警报的严重性程度。如果连接指出高风险事故，或与已知威胁者有关，其缓急次序应优先于严重性程度较低的警报。
对关键系统或功能的潜在影响	考虑警报对决策局／部门运行所需关键系统或功能的潜在影响。对于可能破坏或危及关键系统的警报，应给予更优先的缓急次序。	团队考虑恶意互联网规约地址连接对决策局／部门关键系统或基本功能的潜在影响。如果该连接存在未获授权访问、数据外泄或干扰关键业务的风险，则予其更优先的缓急次序。

监管与遵行要求	考虑检测到的技术可能对任何影响的监管或遵行要求的影响。对可能违反监管或遵行要求的技术，应给予较优先的缓急次序。	团队考虑恶意互联网规约地址连接可能牵连的任何监管或遵行要求。如因未获授权通讯与恶意单位连接而可引致违反监管或遵行要求，团队应给予更优先的缓急次序以确保遵行法律和行业标准。
运行中断的可能性	评估警报对造成重大运行中断或停机的可能性。就风险较高可中断业务运营或服务的警报，应给予较优先的缓急次序。	团队评估恶意互联网规约地址连接造成运行中断的可能性。如存在系统入侵、全网感染或服务中断的风险，则给予更优先的缓急次序，以尽量减少对业务运营的影响。
受影响系统的数量	考虑受警报影响的系统或资产数量。由于潜在的广泛影响，对于影响大量系统的警报，可能需要即时的关注和优先的缓急次序。	团队根据受恶意互联网规约地址连接影响的系统数量来考虑范围和规模。如多个系统与同一恶意互联网规约地址通信或涉及关键系统，考虑到潜在的广泛影响和增加的风险，团队给予较优先的缓急次序
情况的迫切性	评估警报的迫切性和立即采取行动的必要性。如警报表明当前或正在发生的安全事故需要立即控制或补救，应给予该警报更优先缓急次序，以尽量减少进一步的损害或入侵。	团队根据连接的性质、与恶意互联网规约地址相关的威胁程度或即时数据即时外泄的可能性等因素评估其迫切性。如需迅速采取行动阻断连接或控制威胁，团队则相应给予其更优先的缓急次序。
技术相关性	评估检测到的技术与决策局／部门基础设施和系统的相关性。对于已知能有效攻击决策局／部门环境的技术，给予更优先缓急次序。	团队评估恶意互联网规约地址连接的技术与决策局／部门基础设施的相关性。团队考虑是否曾发生类似事故或是否有类似攻击历史。如果威胁者经常使用该技术或对决策局／部门的系统构成重大风险，则相应给予其更优先缓急次序。

策略重要性	考虑与检测到的技术相关策略的的重要性。重点关注与高优先顺序策略一致的技术，例如初始接达、执行或渗透。	团队评估与恶意互联网规约地址连接相关策略的重要性。如果该连接是初始访问策略的一部分，或显示曾有试图在未获授权的情况下访问决策局 / 部门的系统，团队考虑到防止此类未获授权访问的重要性，给予其更优先缓急次序。
持续的可能性	评估检测到的技术在决策局 / 部门系统内持续存在的可能性。对于较可能允许长期访问的技术，给予其更优先缓急次序。	团队考虑恶意互联网规约地址连接在其系统内持续存在的可能性。如成功，是否可以让攻击者保持长期访问或为未来攻击建立立足点？如该技术持续存在的可能性很高，应给予其更优先缓急次序。
利用的成熟程度	考虑与检测到的技术相关漏洞利用的成熟程度。对已知的有效利用给予其更优先缓急次序。	团队评估与恶意互联网规约地址连接相关漏洞利用的成熟程度。如存在与互联网规约地址相关的已知有效的漏洞利用，或与复杂的攻击技术有关联，团队给予其更优先缓急次序以及时解决该技术。
已知攻击者的使用情况	判断检测到的技术是否被已知的威胁者使用，或是否与其典型策略、技术和程序一致。对于复杂或有针对性的攻击者使用的技术，可给予其更优先缓急次序。	团队判断确认已知的威胁者是否使用过恶意互联网规约地址。如互联网规约地址与进阶的持续威胁或已知恶意活动有关，团队考虑到被这些攻击者作为目标的潜在影响，给予其更优先缓急次序以解决该技术。
横向移动的可能性	评估检测到的技术促使于决策局 / 部门网络内横向移动的可能性。对于使横向移动容易的技术，应给予其更优先缓急次序。	团队评估恶意互联网规约地址连接在促使于其网络内横向移动的可能性。如成功，是否可以让攻击者横向移动并访问其他系统？由于横向移动的技术可能导致进一步的入侵和数据外泄，给予其更优先缓急次序。

可见性	考虑检测到的技术于决策局 / 部门安全控制的可见性和检测能力。对于可绕过或规避现有安全措施的技术，给予更优先缓急次序。	团队考虑其识别和监察向外连接的可见性和检测能力程度。如现有的安全措施能够有效检测恶意互联网规约地址访问和发出警报，与其他较难检测到的技术相比，团队可给予其较低缓急次序。

表 7.1 使用 MITRE ATT&CK 框架进行分流的预先定义准则示例

7.2 调查可疑活动和指标

对警报进行分流后，决策局 / 部门应采用有系统的方法，包括进行进阶分析，以调查已验证的警报是否构成威胁或实际攻击，例如，警报表示有更复杂的的攻击者触发行为警报和潜在持续攻击活动。

以下是调查过程中的关键步骤：

1. ***证据收集：***警报一经验证并分流为合法的安全警报，分析员便会收集更多证据以更了解潜在威胁。这步骤包括获取和保存相关日志、网络流量数据、系统快照或其他能够反映事故性质和影响的信息。

2. ***威胁分析：***调查分析员全面地分析威胁以确定其特征、动机和潜在影响。这步骤可包括利用威胁情报源、分析恶意软件样本，或研究与事故相关的已知攻击技术。威胁分析有助于识别攻击者的意图、潜在风险以及任何有助于检测和预防的入侵指标。

以下两个示例有助决策局 / 部门了解调查阶段的主要工作和流程。

- 决策局 / 部门收到恶意互联网规约地址连接尝试的已分流警报。团队收集网络日志、防火墙日志或其他任何能捕获连接尝试的网络数据。团队查阅威胁情报源和数据库以识别已知恶意互联网规约地址、其相关活动和潜在威胁者。然后，团队分析尝试连接的特征，例如来源地址、目标互联网规约地址和端口，以识别已知恶意活动的模式或相似性。

- 决策局 / 部门收到关于在客户端系统上检测到新管理员凭证的已分流警报。团队收集系统事件日志或身份验证日志等相关日志，以收集有关创建新管理员账户的信息。团队查阅威胁情报源和数据库，以识别与未获授权的账户创建或权限升级相关的已知技术或入侵指标。团队分析日志记录事件，包括时间戳、账户名称和系统活动，以识别新管理员凭证创建过程中存在的可疑模式或异常。

为确保调查有效，决策局 / 部门应接受严格培训进行有系统的分析，以避免认知偏差和常见错误。这使决策局 / 部门具备必要技能以进行彻底和公正的调查。

调查阶段的成效取决于数几项因素。有关人员的经验和分析技术、相关数据的可用性，以及有助生成证据和展示予决策局／部门的科技和自动化工具的使用，所有这些有助提高调查的效率。

通过进行彻底的调查并利用人员技术、知识和可用资源，决策局／部门可准确地确定威胁的性质、范围和根本原因源。这允许实施适当的应变措施。

8 威胁应变

威胁应变是一种在网络威胁升级为事故之前，减轻和预防网络威胁的主动方法。这方法包括及时采取行动抵消威胁，并将其影响降至最低。有效的威胁应变有赖于准确的威胁情报和预先定义的措施，以确保采取迅速而适当的行动。准确的威胁情报可以提供有关新兴威胁和漏洞的实时信息，使决策局 / 部门能够及时采取措施预防攻击。

当安全警报被确认为威胁时，应做出适当的应变。为了将威胁的影响减至最低和保护资产、系统和数据，决策局 / 部门应建立可执行已经预先定义的行动及措施，以应变潜在威胁或警报。严重性分类为选择适当的应变行动提供指导。对于严重性较高的威胁，需要采取立即和集中的控制、调查和根除等应变措施。相比之下，严重性较低的威胁可根据资源可用性和缓急次序采取相应进一步的控制。

以下是有效威胁应变中常见采取的关键行动和措施：

1.***遏制：***这包括从用户邮箱中撤回已发送的电子邮件、将用户添加到低权限组别、更新防火墙和网络过滤器的拦截列表，以及实施在邮件网关、防火墙、端点检测和响应（EDR）、网络网关、活动目录、网络访问控制（NAC）等各种解决方案中拦截机制的措施。

2.***拦截：***采取措施拦截恶意活动或未获授权的系统和网络访问。

3.***修补：***应安装必要的软件修补程序和更新解决漏洞，并增强安全态势。

4.***培训：***执行培训计划以教育用户和人员有关潜在威胁、良好作业模式和安全意识。

在应变威胁后，决策局 / 部门应从各来源收集到的威胁进行归纳和分组，并确定是否将其升级为事故。分析员应根据鉴证分析提供情境丰富的威胁视图。这允许决策局 / 部门确定需要进一步调查的范围，或触发所需的事故应变。详情请参阅**《信息安全事故处理实务指南》**。

以下是威胁应变示例：

当监察工具检测到可疑活动时，即时立即启动威胁应变行动便会启动。分析员对警报进行分析，确定其是否会对决策局 / 部门的安全构成潜在威胁。根据严重性分类，确定可以通过预先定义的行动来缓解威胁。

受影响的系统会立即与网络隔离，作为遏制措施防止潜在的威胁扩散。同时，分析员在不同解决方案中采用拦截机制，例如防火墙、网络过滤器和网络访问控制，以拦截恶意活动和未获授权的访问。

为解决可能已被利用的漏洞，分析员确保已即时安装必要的软件修补程式和更新，以增强整体安全态势。

在应变威胁后，分析员对收集的数据进行分组和分析，从而覆检和归纳威胁情报。这分析提供情境丰富的威胁视图。如有需要，这分析有助识别需要进一步调查的范围或上报到事故应变小组。

为提高人员的安全意识，决策局 / 部门定期进行培训计划，以教育用户和人员有关潜在威胁、良好作业模式和保安意识。这些培训课程有助建立具警觉性和主动通报威胁的文化。

在这情况下，威胁应变成功缓解了潜在事故。

决策局 / 部门可考虑制定操作手册，记录已定义的行动和措施，以便在威胁演变成真实事故前作出应变。有关操作手册示例，请参阅**附件 C** 。

9 持续改进和调整

9.1 定期监控、评估和安全态势评估

应进行定期监控、评估和安全态势评估，以衡量威胁监控的成效，并做出充分了解的明智决策，以增强整体安全态势。

决策局／部门应设置衡量威胁监控成效的关键绩效指标（KPI）。这些可衡量的指标提供决策局／部门在信息技术安全工作的表现和进展的见解。在确定关键绩效指标时，决策局／部门应考虑遇到的威胁数量和类型、事故应变时间、检测准确度以及已实施安全控制的成效等因素。这些关键绩效指标应与决策局／部门的目标一致，并反映其独特的风险环境。

持续监控威胁环境对于防范新兴风险和漏洞至关重要。这包括监控外部威胁情报源、安全警报和决策局／部门内部事故等。应定期评估威胁监控程序和技术的成效，以确保它们保持更新和高效。评估可包括威胁检测系统的准确性和及时性、安全控制的成效，以及事故应变程序的回应能力。信息技术安全威胁管理的特定关键绩效指标示例包括：

- ***平均检测时间（MTTD）。***这关键绩效指标衡量发现信息技术安全威胁或安全事故的平均时间。该指标提供决策局／部门监控效率和成效的见解。平均检测时间越低，决策局／部门越快做出可应变威胁，进而将潜在的损失减到最低。

- ***平均回应时间（MTTR）。***这关键绩效指标衡量应变并解决已发现信息技术安全威胁或安全事故所需的平均时间。该指标反映决策局／部门的事故应变效率以及控制和减轻威胁影响的能力。平均回应时间越低，应变越快越有效。

- ***误报率。***这关键绩效指标衡量监控系统生成的警报中被确定为误报（即并非实际安全威胁）的百分比。误报率越高，说明投入非威胁事件的不必要调查或资源越多。降低误报率有助提高威胁监控的效率，及减轻事故应变小组的负担。

- ***检测准确性。***这关键绩效指标衡量监控系统成功检测到的真实安全威胁的百分比。该指标能够反映系统准确识别和标记真正威胁的能力。检测准确性越高，说明监控能力越完善、越可靠。

- ***事故应变时间。***这关键绩效指标衡量检测到安全事故后，启动适当应变所需的时间。这包括事故分流、评估和启动事故应变程序所需的时间。缩短事故应变时间可更迅速地控制和缓解威胁。

- ***威胁情报使用。***这关键绩效指标衡量决策局 / 部门将威胁情报有效纳入其监控和应变程序的程度。该指标评估决策局 / 部门主动利用外部威胁情报来源识别和解决新兴威胁的能力。

- ***受监控资产范围。***这关键绩效指标评估主动监控潜在威胁的关键资产或系统的百分比。这确保全面覆盖并识别监控方面存在的缺口，使决策局 / 部门能够确定资源分配的缓急次序，并提高其整体监控能力。

- ***遵行监控政策和程序。***这关键绩效指标评估决策局 / 部门对既定监控政策和程序的遵行情况。该指标衡量对法规要求、内部政策和业界良好作业模式的遵行情况，确保监控活动符合既定标准。

安全态势评估提供全面反映决策局 / 部门整体安全准备的情况，这包括评估安全控制的成效、识别漏洞以及评估决策局 / 部门检测和应变威胁的能力。安全态势评估的示例包括：

- ***渗透测试。***渗透测试涉及模拟真实世界的攻击，以识别系统、网络或应用的安全漏洞。通过进行受控和授权测试，决策局 / 部门可以有效评估其检测和应变各种攻击场景的能力。渗透测试的结果有助于确定需要立即关注的具体领域，并根据其关键性确定补救行动的缓急次序。

- ***漏洞评估。***漏洞评估包括扫描系统和网络中的已知安全漏洞和不当配置。通过识别这些弱点，决策局 / 部门可以立即修补或缓解这些漏洞，从而降低被威胁者利用漏洞的风险。

- ***红队演练。***红队演练指通过设立专门小组模仿真实攻击者的策略和技术测试防御的能力。该模拟可对威胁监控控制和作业的成效进行真实评估。通过挑战现有的安全措施，红队演练有助于发现潜在的漏洞，并识别需要改进的领域。

- ***紫队演练。***紫队演练指，专家小组同时扮演红队和蓝队的角色，旨在通过更实质、更深入的保证活动提供更有针对性和更现实的保证。通过演练，团队相互学习改进进攻和防御策略，从而增强决策局 / 部门的整体信息技术安全态势。

决策局 / 部门应聘用资格和信誉良好的信息技术安全专业人员或外部服务供应商，具备必要的专业知识、工具和方法，以进行安全态势评估。

9.2 评估和更新威胁情报

应定期覆检和验证威胁情报来源的相关性和准确性。决策局 / 部门应建立程序作持续评估，其中可包括以下因素：

- 来源相关性；
- 来源准确性；
- 及时性；
- 质量和可信度。

根据评估结果，决策局 / 部门应视需要更新其威胁情报来源。这过程可包括新增的威胁来源、删除不相关或不可信的威胁来源，或根据不同威胁来源的表现和相关性调整其重要性和缓急次序。

9.3 评估和更新控制与技术

应定期评估和更新信息技术安全控制和技术，以跟上信息技术安全威胁迅速变化的步伐。决策局 / 部门在评估和更新控制和技术时应考虑以下因素：

- ***关注行业趋势。***主动关注威胁监控和检测方面的行业趋势和发展。随时了解信息技术安全领域的最新技术、工具和方法。通过业界刊物、相关会议和研讨会、参加业界论坛和工作小组，以了解最新情况。

- ***威胁监控和检测技术。***定期评估决策局 / 部门内部署的威胁监控和检测技术的成效。评估其对不断变化的威胁（包括进阶持续性威胁、零日漏洞和内部威胁）的识别和应变能力。考虑可增强威胁检测能力的新技术可用性，例如机器学习、人工智能和行为分析。

- ***评估事故应变计划。***评估现有事故应变计划和程序的成效。覆检有效处理事故的措施，包括应变时间、控制措施和恢复程序。随时了解最新的事故应变框架和方法，确保与业界良好作业模式和不断变化的威胁场景保持一致。

- ***合作与共享信息。***加强与其他决策局 / 部门和行业合作伙伴的合作和共享信息。参与知识交流活动，了解其他成功实施的战略和技术。参与威胁情报共享社区等信息共享平台，以了解新威胁和有效的缓解战略。

决策局 / 部门应根据评估结果更新控制和技术，与不断变化的威胁环境和行业发展看齐。这过程可包括实施新技术、采用更新的框架和方法，或根据经验和新兴的良好作业模式修订事故应变计划。

完

附件 A：威胁分类示例

编号	威胁类型	威胁	威胁详情
1	社会威胁	欺诈行为	人为欺诈行为
2	社会威胁	盗窃（设备、储存媒体和文件）	窃取信息或信息技术资产。抢劫。
3	社会威胁	信息泄漏／共享	有意或无意的人为行为或错误造成的信息泄漏／共享。
4	社会威胁	未获授权的物理访问／未获授权进入场地	未经批准进入场所。
5	社会威胁	恐怖袭击	恐怖分子的威胁。
6	技术威胁	使用来源不可靠的信息	根据不可靠的信息来源或未获核实的信息做出错误决定。
7	技术威胁	设计和计划不足或调整不当	不当的信息技术资产或业务流程设计导致的威胁（信息技术产品规格不足、可用性不足、界面不安全、政策／程序流程、设计错误）。
8	技术威胁	通信链路（通信网络）故障或中断	通信链路故障或中断的威胁。
9	技术威胁	拒绝服务	大量服务请求导致服务不可用的威胁。
10	技术威胁	恶意代码／软件／活动	执行恶意代码或软件的威胁。
11	技术威胁	未获授权安装软件	未获授权安装软件的威胁。
12	环境威胁	火灾	火灾威胁。
13	环境威胁	雷击	雷击（过量电压）对信息技术硬件造成损坏的威胁。
14	环境威胁	水患	水患对信息技术硬件造成损坏的威胁。
15	环境威胁	爆炸	爆炸对信息技术硬件造成损坏的威胁。
16	环境威胁	不利的气候条件	由于气候条件对硬件产生不利影响而中断信息技术系统的工作。
17	环境威胁	野生动物	动物（小鼠、大鼠、鸟类）对信息技术资产造成破坏的威胁。

以上示例说明了威胁分类法如何协助该决策局／部门识别具体威胁，并确定其缓急次序，使其能够实施有针对性的安全措施，以保护纳税人信息并维护其业务的完整性：

该决策局／部门负责执行香港的税法，并确保税款征收，以支持政府运作和公共服务。作为保护纳税人信息和维护系统完整性工作的一部分，该决策局／部门开展威胁评估，以确定针对其业务的潜在信息技术安全威胁。

在威胁评估过程中，该决策局／部门识别可能会危及纳税人数据并破坏其业务的各种威胁。

在社会威胁类别，该决策局／部门识别到针对纳税人或决策局／部门员工的网络钓鱼攻击风险。该等攻击旨在诱骗人员泄露可用于欺诈的敏感资料，例如税务编号或登录凭证。

在技术威胁类别中，该决策局／部门确认勒索软件攻击加密其系统的可能性，使其在支付赎金前无法访问。该决策局／部门同时考虑未获授权访问纳税人数据库的风险，例如外部黑客攻击和员工滥用访问权限的内部威胁。

在环境威胁类别中，该决策局／部门辨认到停电或其他基础设施故障可能会破坏其信息技术系统，并危及数据可用性。该决策局／部门还考虑到物理漏洞的风险，如未获授权进入其数据中心或办公室，可能导致盗窃或篡改敏感纳税人信息。

根据这些已识别威胁，该决策局／部门建立适合其特定需求的分类。该决策局／部门在每个类别中定义特定的威胁类型，例如将有针对性的税务网络钓鱼电子邮件定义为社会威胁，将勒索软件攻击定义为技术威胁，将物理破坏定义为环境威胁。

通过明确定义的威胁分类，该决策局／部门就可以实施有针对性的安全措施，保护纳税人数据并保持业务的连续性。该决策局／部门投入完善的电子邮件过滤和安全意识计划，以教育纳税人和员工有关网络钓鱼攻击的风险。该决策局／部门还实施进阶端点保护、定期系统备份和事故应变协定，以减轻勒索软件和未获授权访问尝试的影响。

此外，该决策局／部门制定严格的物理安全措施，包括访问控制、监视系统和人员审查，以保护其场所和防止未获授权的访问。

定期的安全审计和渗透测试有助于识别漏洞，并确保实施安全控制的成效。该决策局／部门还与执法机构、行业协会和其他政府部门保持密切合作，共享威胁情报，协同促进网络安全活动。

附件 B：针对信息技术安全威胁情报供应商的问题示例清单

1. 使用的信息来源范围有多广？
   按照情报周期，供应商应从广泛的原始来源收集情报并加以融合。

2. 如何从原始来源收集情报？
   供应商应能提供足够的详细信息，以确保其收集能力，且理想情况下能够独立收集信息，而不必依赖第三方。

3. 情报涵盖什么类型的威胁者？
   供应商应涵盖决策局 / 部门所面临的所有类型的威胁者，这通常代表需要从不同来源来收集信息。

4. 所提供的情报是否及时？
   这应取决于所提供情报的级别，即战略性、策略性或操作性。

5. 情报以何种格式提供？
   这将根据资料的性质和级别而有所不同。然而，分析员访问、现场简报、定制的报告和情报报告与决策局 / 部门相关的可能比一般通用的威胁数据更有帮助。

6. 产品如何与现有的功能整合？
   如果决策局 / 部门拥有现行的供应商和基础设施，整合能力则非常重要。

7. 产品如何为决策局 / 部门定制？
   量身定制的产品通常比一般通用产品更有帮助，由技术性的分析员评估的情报相比于数据对决策局 / 部门而言更有帮助。

8. 对产生的情报采用什么评估流程？
   优质供应商将采用既定的方法评估情报，并确保其适用于决策局 / 部门。

9. 如何排除误报？
   人工审核资料可减少误报。

10. 团队的背景和语言能力如何？
    多元化且经验丰富的分析团队往往有能力提供最优质成果，团队成员的个人认证亦很可能是有用的指南。

11. 分析是否具有预测性和反应性？
    优质供应商应为决策局 / 部门提供前瞻性评估。

12. 团队成员是否获得了威胁情报专业人员认证？
    威胁情报实践有专业的资格认证，例如 CREST 认证和 SANS 等其他组织的资格认证。

13. 贵公司是否被公认的权威机构认证为威胁情报供应商？
    经例如 CREST 的认证除了证明供应商能力，更显示其具有高度的法律和道德标准。

14. 是否定期提供服务予该等受监管的框架？
    优质供应商将定期为该等框架提供支持服务。

15. 如何展示对我们（买方）行业的了解？
    供应商可能具有定制研究的经验，并在团队中拥有专门的主题专家。

16. 贵公司采取了什么安全措施确保我们威胁情报的安全？
    鉴于所提供情报的潜在敏感性，供应商应能向客户确保其安全，例如共同使用客户信息安全政策。

17. 如何证明产品和服务的质量？
    供应商应能提供合作成功的参考。

附件 C：威胁应变行动手册示例

请注意，以下行动手册是威胁应变的示例，决策局 / 部门应根据其具体需求进行调整，而非仅遵循以下步骤。

1. 威胁情报中的新漏洞

阶段	简介
识别	• 识别相关的信息技术安全威胁并进行分类，包括威胁情报中新发现的漏洞。
监控	• 持续监控网络流量、系统日志和安全事故，以查找与已识别漏洞相关的任何指标。
检测	• 分析收集的数据，例如日志文件和网络流量，以检测可能显示已识别漏洞被利用的模式或异常。
分流	• 根据可用的漏洞和资产关键性的信息启动分流。 • 通过分析入侵指标以及策略、技术和程序，检查是否有任何迹象表明攻击已经发生。 • 通过将资产与易受攻击的版本 / 配置信息进行匹配，验证资产是否存在漏洞。 • 根据分流结果升级处理情况。
调查	• 进行彻底的调查，以评估漏洞的影响、识别潜在的攻击途径，并为未来的预防收集额外的情报。 • 覆检防火墙规则和其他安全配置，以识别潜在的攻击途径。可利用自动化工具来进行此项工作。
应变	• 与安全运营中心、信息技术安全管理组和信息技术支援团队讨论缓解措施。 • 制定并执行行动和措施，以应对已识别的漏洞，这可能包括立即关机、应用修补程序、实施替代方案或考虑未来资产构建的预防措施。 • 重新扫描漏洞以确认完结。

2. 特权帐户强制身份验证

阶段	简介
识别	不适用。
监控	• 利用特权访问管理系统监控特权访问的使用情况。 • 监控并记录来自相关端点的身份验证活动。
检测	• 将特权访问管理日志与相关端点的认证日志相关联，以检测未经授权的使用并识别潜在被窃取的凭证。 • 对未经相应特权访问管理批准的特权帐户的任何登录活动触发警报。
分流	• 根据可用的漏洞和资产关键性信息启动分流。 • 通过分析入侵指标以及策略、技术和程序，检查是否有任何迹象表明攻击已经发生。 • 通过将资产与易受攻击的版本 / 配置信息进行匹配，验证资产是否存在漏洞。 • 根据分流结果升级处理情况。
调查	• 进一步调查以确定未经授权的访问的范围，评估潜在的安全漏洞，并为未来的预防收集额外的信息。 • 联系相关系统管理员，询问他们是否在指定的时间段内使用过该帐户。 • 如果没有管理员声称对该使用情况负责，则应将合作范围扩展到包括相关的应用程序支援团队。 • 如果没有得出结论，则将其视为事故并执行事故应变。
应变	• 开展事故应变程序，以缓解成功攻击的影响。 • 更新例外接受风险的关联规则，以完善检测流程和准确识别未经授权的特权访问事故。

3. 虚拟私有网络异常

阶段	简介
识别	不适用。
监控	• 鉴于攻击者经常利用虚拟私有网络来保持对组织环境的持续访问，应持续监控虚拟私有网络的异常。
检测	• 从身份管理系统接收警报，显示存在没有相应帐户创建批准记录的虚拟私有网络帐户。 • 如果身份管理系统不可用，可手动或通过编译，将导出的虚拟私有网络帐户列表与用户请求事务跟踪系统进行对照。 • 用户报告在未经其同意和非预期的情况下，虚拟私有网络密码被更改或注册的流动装置被重置。
分流	• 验证所涉虚拟私有网络帐户及其活动的合理性。 • 咨询虚拟私有网络管理员以确认帐户的合理性和活动。 • 收集已识别虚拟私有网络帐户的访问日志，并检查连接的来源地址。确认他们是否与合法的虚拟私有网络用户一致。 • 攻击者可能会租用决策局 / 部门用户群附近的机架空间（例如，同一城市的数据中心）来绕过基于位置的过滤器，因此，在仅依赖地理互联网规约地址信息时需谨慎。 • 鉴于虚拟私有网络系统可能并非攻击者的初始入口，需根据分流结果将情况上报给相关信息技术团队以确定根本原因。
调查	• 进行深入的鉴证分析，以了解虚拟私有网络异常的根本原因，并识别任何其他受损系统。
应变	• 将发现的异常情况通知虚拟私有网络帐户持有者，并建议更改其他系统（包括个人设备）的密码。 • 如果检测到未经授权的帐户或活动，则考虑相关帐户（甚至虚拟私有网络系统）为已遭破坏，触发事故应变。

4. 域名系统回调

阶段	简介
识别	不适用。
监控	• 持续监控与域名系统相关的恶意活动指标。 • 设置域名系统监控发出针对长域名查询、已知恶意查询（入侵指标 / 策略、技术和程序）以及异常域名系统流量和频率的警报。
检测	• 识别使用域名系统作为恶意软件的回调机制，该机制已经发生了演变。 • 入侵防御系统 / 入侵检测系统等网络安全设备可能会对异常的域名系统查询发出警报。
分流	• 确认是否存在恶意域名系统活动及其范围。 • 覆检域名系统日志，以确定类似域名系统查询的开始日期，并识别其他端点的类似行为。根据域名系统服务器配置将被拒绝的查询纳入日志覆检。 • 检查端点安全事故日志（例如扩展检测和响应），查找相关端点上恶意软件的迹象。 • 如有必要，对受影响的端点进行鉴取分析，以识别负责发送可疑域名系统查询的过程。
调查	• 进行详细的鉴取分析，以揭示域名系统回调的根本原因，并识别任何可能受损的系统。 • 分析收集的数据和证据，了解恶意软件的入侵点。
应变	• 如果确认存在漏洞，则触发事故应变以调查恶意软件如何获得访问权限。 • 在受损主机上实施适当的应变措施，这可能涉及隔离、检疫隔离或移除恶意软件。

附件 D：端点检测和响应采用及架构指南

在不断变化的网络安全威胁环境中，端点检测和响应解决方案已成为决策局 / 部门保护其数字资产的一道关键防线。这些指南旨在提供综合的端点检测和响应采用和架构指引，以协助决策局 / 部门有效实施这些解决方案。

D.1. 端点检测和响应简介

端点检测和响应解决方案扮演了警惕的前哨，强化了决策局 / 部门对潜伏在数字领域各种威胁的防御。通过采用端点检测和响应，决策局 / 部门可以提高其威胁检测能力、增强事故应变程序，并加强其安全态势。通过实时监控、行为分析和威胁情报集成，端点检测和响应赋予决策局 / 部门主动识别和消除恶意软件、勒索软件和内部攻击等进阶威胁的能力。

D.1.1. 端点检测和响应的核心功能

端点检测和响应解决方案的核心功能独具特征，决策局 / 部门能因此应变复杂威胁。实时监控、行为分析、威胁情报集成、事故应变自动化和鉴证能力是制定端点检测和响应解决方案的核心功能。下文将深入探讨每个功能的重要性，重点介绍其如何有助于在决策局 / 部门环境中进行有效的威胁管理和事故应变。部分核心功能如下：

- ***端点可见性：***端点检测和响应解决方案可实时查看所有端点，包括膝上电脑、台式机、流动装置、服务器和物联网设备。此可见性使安全团队可监察和分析端点活动以识别可疑行为。

- ***威胁检测：***端点检测和响应解决方案使用进阶威胁检测技术，例如行为分析和机器学习，来识别入侵指标和攻击指标，亦可通过分析端点事故和遥测数据来检测潜在威胁并发出警报。

- ***事故调查：***端点检测和响应解决方案提供调查功能，以分析和了解安全事故。方案提供工具搜索和查询端点数据，使安全团队能调查事故的根本原因并收集证据进行进一步分析。

- ***威胁狩猎：***端点检测和响应解决方案使安全团队可在端点上搜索潜在威胁和入侵指标，从而实现主动的威胁狩猎。这功能有助于识别可能躲过传统安全措施的隐藏或进阶威胁。

- ***威胁情报集成：***端点检测和响应解决方案整合威胁情报源，以增强威胁检测和应变能力。通过利用最新的威胁情报，端点检测和响应解决方案能够识别已知的恶意活动，并提供有关攻击的背景信息。

- ***实时和历史信息可见性：***端点检测和响应解决方案扮演端点上的数字硬盘录像机，实时记录和提供安全相关活动的全面可见性，包括监察网络连接、用户登录、进程执行和文件创建。历史信息可见性使安全团队可分析过去的事故，并识别模式或趋势。

- ***事故应变和修复：***端点检测和响应解决方案通过提供实时应变功能，实现快速果断的事故应变。这包括在不影响性能的情况下，将受破坏的端点从网络中隔离、遏制威胁，并修复事故。

D.1.2. 端点检测和响应与其他产品的区别

在数项关键方面，端点检测和响应解决方案与传统的端点安全产品（例如防毒软件或入侵检测系统）有所不同，以下是主要区别：

1. 检测方法：

- 传统的防毒软件主要依赖基于标识符的检测，即把文件与已知恶意软件标识符的数据库进行比较。这种方法对已知威胁有效，但可能难以应对新的或未知的恶意软件。
- 端点检测和响应方案则侧重于基于行为的检测。通过实时监控和分析端点活动，查找可能预示潜在威胁的可疑或异常行为。这种方法使端点检测和响应能够检测已知和未知威胁，包括零日攻击。

2. 可见性和应对能力：

- 防毒软件通常提供有限的端点活动可见性，通常仅在检测到已知威胁时发出警报，缺乏详细了解攻击链的能力，以及有效的应对能力。
- 端点检测和响应解决方案增强了对端点的可见性和控制能力，收集并分析广泛的端点数据，包括文件修改、程序创建、网络连接等。这种全面的可见性使安全团队快速识别并应对安全事故，将攻击的影响降至最低。

3. 事故应变和威胁狩猎：

- 传统防毒软件主要侧重于检测和阻止恶意软件，可能无法提供完善的事故应变能力或支援主动的威胁狩猎活动。
- 端点检测和响应解决方案旨在支持事故应变和威胁狩猎，在同一控制台内提供集成的事故应变能力，安全分析员从而可以快速调查和应变安全事故。端点检测和响应还提供威胁狩猎支持，使决策局 / 部门能够主动搜索入侵指标，并识别可能已躲过其他安全措施的潜在威胁。

4. 自动化和补救：

- 防毒软件通常依赖于手动干预来进行事故应变和修复。安全分析员需要手动分析和处理检测到的威胁。
- 端点检测和响应解决方案可自动执行某些事故应变活动，并提供多种应对选项，如隔离或清除，以解决安全事故。这种自动化简化了事故应变流程，并降低了安全事故的影响和成本。

端点检测和响应解决方案超越了传统的防毒软件，提供了基于行为的检测、更强的可见性、事故应变能力以及主动威胁狩猎的支援。它们提供了一种更全面和主动的端点安全方法，决策局 / 部门从而能够检测、应变和缓解各种的威胁。了解这些区别，决

策局 / 部门可以避免混淆，并选择提供必要的深度和广度保护的端点检测和响应解决方案。

D.2. 端点检测和响应的部署和实施

部署和实施端点检测和响应解决方案是一个多步骤的过程，涉及在决策局 / 部门进行谨慎的规划、技术配置和安全基础架构中集成。部署和实施端点检测和响应的主要注意事项如下：

1. ***制定目标和要求：***首先制定部署端点检测和响应解决方案的目标和要求。识别决策局 / 部门利用端点检测和响应应对的安全挑战和风险。考虑因素例如需要保护的端点数量和类型、监管合规要求，以及所需水准的可见性和威胁检测能力。这些信息将指导选择适合的端点检测和响应解决方案。

2. ***评估和选择解决方案：***对可用的端点检测和响应解决方案进行全面评估。考虑因素例如解决方案的功能、可扩展性、整合能力、对端点的性能影响，以及供应商的声誉。利用行为分析、机器学习和威胁情报整合，评估解决方案检测和应变进阶威胁的能力。选择符合决策局 / 部门目标、要求和预算的端点检测和响应解决方案。

3. ***计划部署：***制定详细的部署计划，概述必要的步骤、资源和时间表。考虑因素例如端点覆盖范围、代理部署、网络考虑、与现有安全工具的整合以及用户和相关持份者的沟通等。

4. ***基础设施的准备情况：***确保决策局 / 部门的基础设施满足端点检测和响应解决方案的要求。验证必要的硬件、网络资源和存储容量是否可用。识别现有系统或软件的任何潜在兼容性问题。

5. ***安装和配置：***根据供应商的指引，在指定的服务器或设备上安装端点检测和响应解决方案。根据决策局 / 部门的安全目标和操作要求配置解决方案的设置、政策和规则。这包括定义应从端点收集的事件和数据，设置检测规则，以及配置应变操作。

6. ***部署端点代理：***在需保护的端点上部署端点检测和响应代理，可能涉及自动部署方法，例如软件分发工具或群组政策，以确保在所有端点进行一致和高效的安装。验证代理是否已在每个端点成功安装并运行。

7. ***与安全基础架构整合：***将端点检测和响应解决方案与决策局 / 部门环境中的其他安全工具和系统整合，可能涉及数据源配置、与安全资讯和事件管理系统的整合，或与威胁情报平台的连接。确保正确整合以及数据在端点检测和响应解决方案和其他安全组件之间的无缝流动。

8. ***调整和定制：***调整端点检测和响应解决方案，使其符合决策局 / 部门的特定需求和环境。根据决策局 / 部门的风险承受能力、合规要求和操作注意事项，调整检测规则、政策和应变措施。自定义警报和通知，以确保相关安全事件得到适当的优先处理并传达予安全分析员。

9. ***测试和验证：***对端点检测和响应解决方案进行全面测试和验证，确保其有效性和准确性。模拟各种攻击场景，评估解决方案检测和应变这些威胁的能力。验证解决方案是否生成准确的警报，捕获所需的端点遥测，并按预期执行。

10. ***监察和维护：***建立持续的监察和维护流程，确保端点检测和响应解决方案持续有效。定期覆检和分析端点检测和响应警报和事件，以识别安全事故和潜在威胁。通过产品供应商提供的更新、修补程序和威胁情报源，保持解决方案的最新状态。执行常规的维护任务，例如数据库优化、日志轮换和系统健康检查。

11. ***员工培训和意识：***提供端点检测和响应解决方案的特点、功能和最佳实践的培训予安全运营团队，确保团队能有效地使用解决方案进行威胁检测、调查和应变。此外，提高终端用户对端点检测和响应解决方案、其目的以及任何安全程序或政策变更的意识。

D.2.1. 端点检测和响应的覆盖范围

为确保全面覆盖和有效的威胁管理， 端点检测和响应解决方案必须将其保护范围扩展到传统端点之外。覆盖范围通常包括决策局 / 部门网络中的各种端点设备，包括：

- ***台式机和膝上电脑：*** 端点检测和响应解决方案通常涵盖运行各种操作系统（例如 Windows、macOS 和 Linux）的台式机和膝上电脑。这些端点通常由决策局 / 部门的员工使用。

- ***服务器：*** 端点检测和响应解决方案通常将其覆盖范围扩展到对决策局 / 部门基础设施至关重要的物理和虚拟服务器，包括文件服务器、应用服务器、数据库服务器和云端服务器。

- ***流动装置：***随着流动装置在工作场所的使用日益增多， 端点检测和响应解决方案也宜为智能手机和平板电脑提供保护，包括运行安卓或 iOS 操作系统的设备，确保流动装置端点免受安全威胁。

- ***虚拟机器:***大量使用虚拟化技术的决策局 / 部门可能需要能够监察和保护虚拟机（VMs）的端点检测和响应解决方案。这些虚拟机器可以存放在例如 VMware、Hyper-V 或 KVM 等管理程序上。

- ***物联网设备：***随着物联网在决策局 / 部门中日益普及， 端点检测和响应解决方案可能需覆盖连接到网络的物联网设备，包括的设备例如互联网规约地址摄像头、智能恒温器、工业传感器和其他物联网端点等。

- ***嵌入式系统：***部分决策局 / 部门可能需要对专用嵌入式系统或设备提供端点检测和响应覆盖，例如销售点系统、自动柜员机、工业控制系统或医疗设备。这些设备可能具有独特要求和限制需要加以解决。

- ***自助服务亭：***部分决策局 / 部门可能需要端点检测和响应覆盖专用的自助服务亭。这些自助服务亭可在公共场所、零售环境或其他允许自助互动的地点中找到。端点检测和响应解决方案可为其提供保护，确保端点免受安全威胁和漏洞。

建立强大的安全态势需要对所有端点类型进行一致的覆盖。决策局 / 部门应注意采用统一方式的端点检测和响应方法的重要性。通过将台式机、工作站、服务器、流动装置等集成到一个集中的监察和应变系统中，决策局 / 部门可以有效地检测、调查和应变威胁。应详细说明管理各种各样的端点环境的策略，包括策略执行和代理管理，以确保采取协调一致的防御策略。

附件 E：威胁监控架构示意图

下图为全面的威胁监控架构的例子，展示了相互连接的监控工具共同监控信息技术安全威胁。

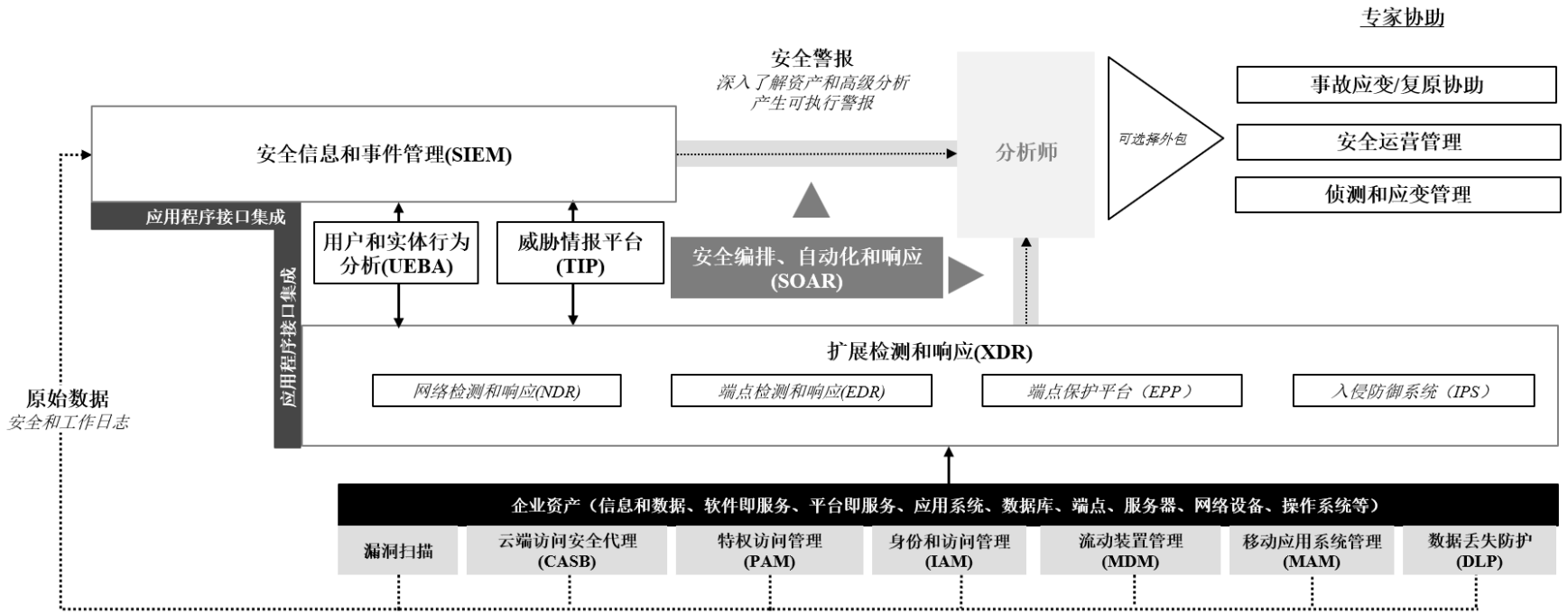

图 E.1 威胁监控架构示意图