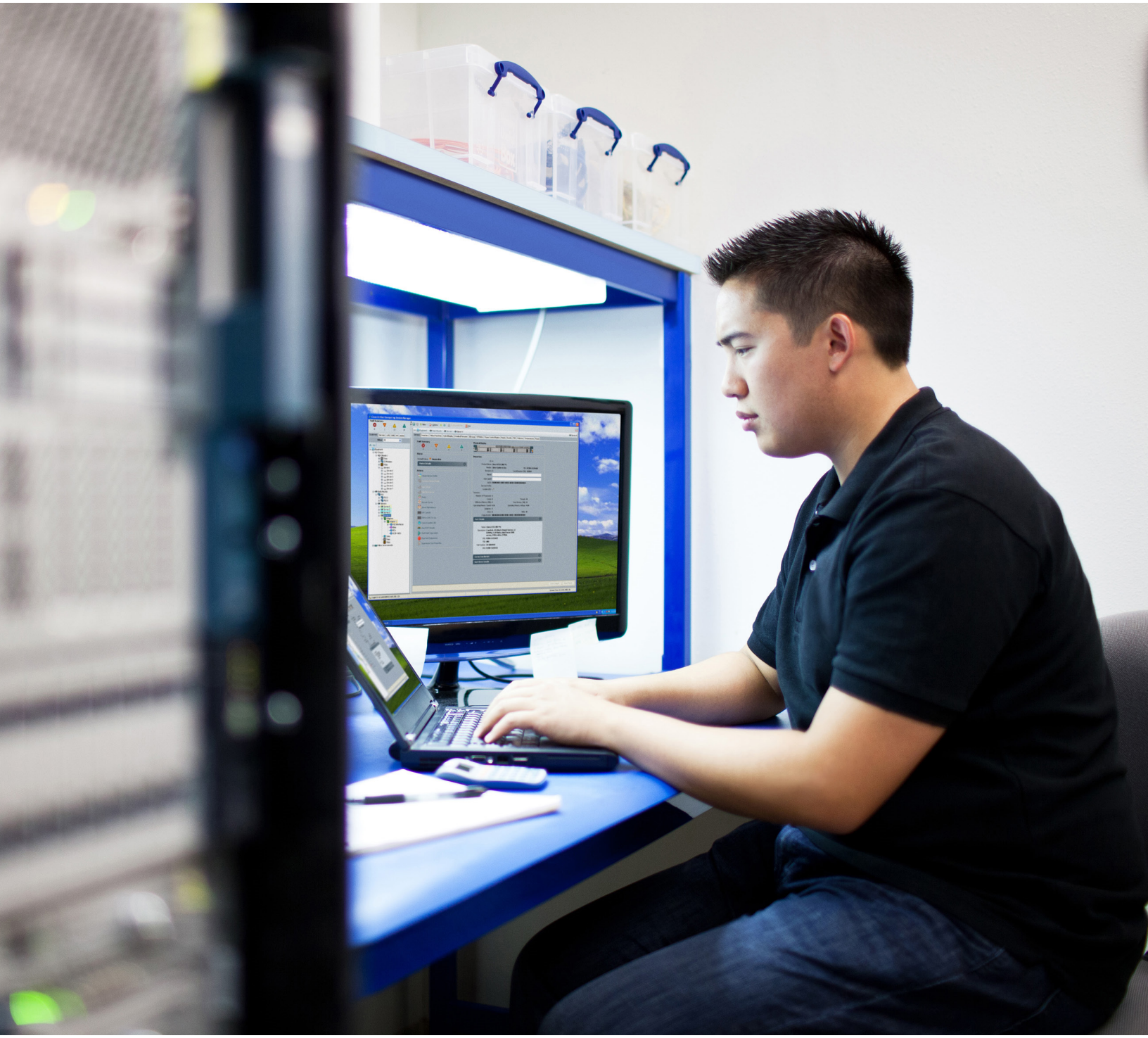
安全分析及其他信息

综合所有要素制定有效的事件响应计划



内容提要

本白皮书旨在帮助 IT 和安全团队成员了解制定有效的事件响应计划所必须具备的要素：

- 了解当前事件响应计划为何失败
- 正确组建事件响应团队
- 制定成功的响应程序
- 选择适当的安全技术
- 利用 NetFlow 和安全分析显著提高事件响应及调查分析能力

攻击持续增加

从大型零售商到医疗服务提供商和政府机构，没有人能够保证免于现今复杂的针对性网络攻击。无论攻击者的目标是财务数据、商业秘密还是机密信息，不断变化的威胁形势和快速增长的网络环境为他们提供了更多非法入侵网络的方式。

您需要担心的问题已不再是攻击者是否会侵入您的网络，而是何时会侵入您的网络。他们会利用零日攻击、窃取的访问凭证、已感染的移动设备、易受攻击的业务合作伙伴等各种方法发动攻击。

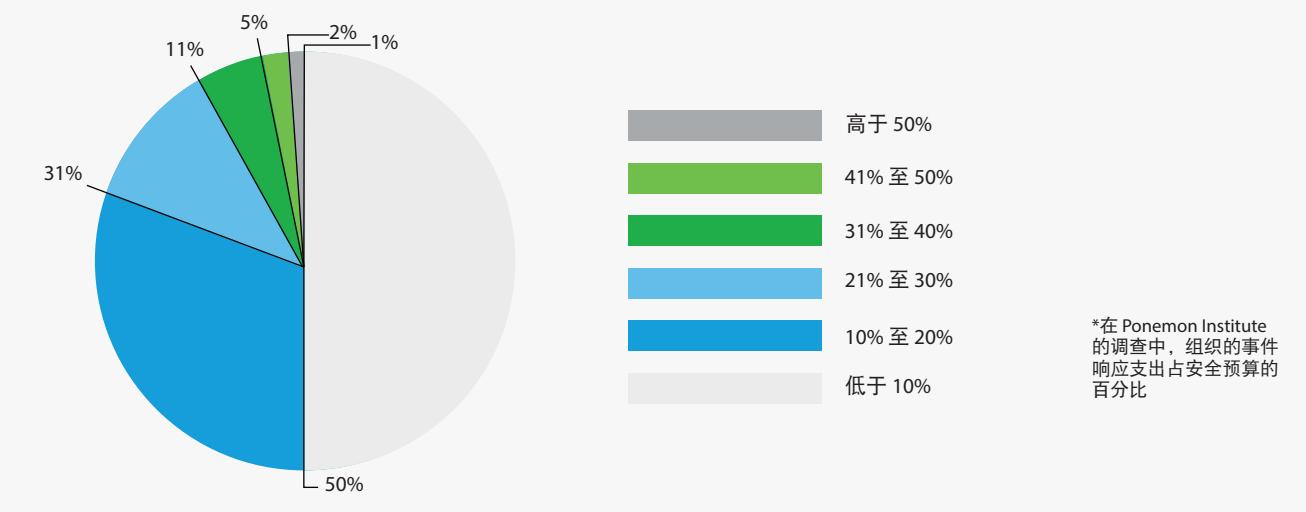
在安全方面取得成功不仅仅取决于使您的网络免遭威胁，而且取决于在受到攻击时能够快速做出响应并进行抵御。

据 Gartner 报告显示，“目前，组织在早期漏洞检测方面的表现不能令人满意：在存在漏洞的组织中，有 92% 以上的漏洞未被检测到。”[1]显然，我们需要更积极主动地保护我们的组织。我们需要持续监控基础设施内发生的情况，并制定一套完善、周期性的响应方案，防止攻击对我们的网络和声誉造成重大灾难。

事件响应能力成为短板

在 Ponemon Institute 进行的一项调查中，大多数受访者认为，其组织缓解未来攻击的最好办法是提高事件响应能力。但与此同时，一半的受访者表示，他们在事件响应方面的支出还不到整体信息安全预算的 10%（图 1）。[2] 根据另一项调查，90% 的大型企业表示他们一年到头都会经历重大的 IT 事件，但是仅约一半的企业配有事件响应团队专门处理此类事件。[3]

图 1. 事件响应花费



世界知名品牌和机构一直不断面临大量攻击，因此可以看出，事件响应重任在肩。现今的黑客可以在网络上潜伏很长时间不被检测出来：平均为 100 到 200 天。[4]

[1] Gartner，“Magic Quadrant for Security Information and Event Management”（安全信息和事件管理魔力象限），2013 年 5 月

[2] Ponemon Institute，“Cyber Security Incident Response - Are we as prepared as we think?”（网络安全事件响应 - 我们的准备是否像我们想象的那样充分？）2014 年 1 月

[3] Dimensional Research，“Major Incident Management Trends 2016”（重大事件管理趋势 2016），2015 年 12 月

[4] 思科 2015 年年中安全报告

> “目前，组织在早期漏洞检测方面的表现不能令人满意：在存在漏洞的组织中，有 92% 以上的漏洞未被检测到。”
>
> – Gartner

加强事件响应计划

在考虑事件响应时，应包括用于检测和应对安全事件的人员、流程和技术。人员、流程和技术，其中每一项要素对制定和执行高效响应计划都同样重要。

人员

哪些人员应参与到组织的事件响应计划中？答案是每一个人。

CSIRT

首先，企业组织需要组建一个由训练有素的专业安全专家组成的职能完备的计算机安全事件响应团队 (CSIRT)。每个组织，无论大小，都应该指派至少一名专员负责计算机安全事件响应。遗憾的是，安全专家不一定就是事件响应的专家。事件响应人员必须拥有特定的背景或经过培训，能够顶住极大的压力做出响应。同时，组织还必须指定专门的事件响应人员，这些人员不能身兼其他多种 IT 和安全职能。

事件响应团队应该非常了解网络及网络资产。在如今的许多情况下，攻击者会执行全面的侦测，他们比受害者自己的 IT 或安全团队更了解其目标网络。适当的技术可以帮助事件响应人员发现其网络中的资产，确定哪些资产需要重点保护，并制定正常行为基准来快速识别可能喻示着受到攻击的异常情况。

非 IT 人员

但是，对于事件响应来说，组建精干的技术团队还远远不够。在 IT 团队之外，法律、行政管理、人力资源、公共关系和其他部门的关键利益相关者在组织的事件响应计划中应扮演不可或缺的角色。组织需要确定这些团队在发生事件时所应采取的行动，也需要在事件发生前确定相应的角色和职能，并尽早将这些人员纳入流程。同时，组织还应保证高级管理层了解事件响应程序、成就和挑战，以确保这些工作获得合理的关注和必要的资金支持，能够真正发挥效果。

最后，理想情况下，每一位员工，甚至与组织合作的第三方都应为事件响应团队提供支持。对员工进行培训，以便他们了解在遇到社会工程攻击尝试时应如何寻求帮助。仔细筛选，开展背景调查，并了解有权访问您的网络甚或公司机密信息的任何第三方的安全性。切勿忽视内部威胁。对管理人员和人力资源部进行相应培训，使管理人员注意可疑员工的行为，并将此信息汇报给人力资源部，由人力资源部将这些问题传达给 IT 部。

> “StealthWatch 可以帮助安全和事件响应团队更快地对事件做出补救，这有助于减少停机时间以及网络和网络服务的整体管理成本。”
>
> – Telenor Norway

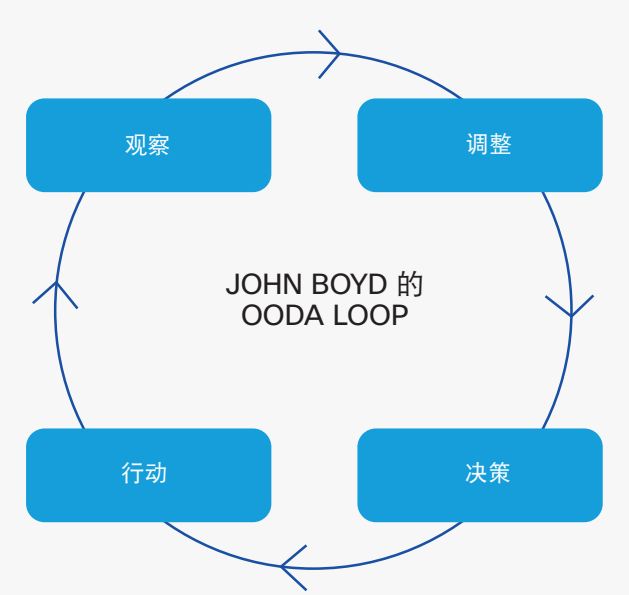
流程

事件响应不能“事后诸葛亮”。企业组织需要审慎地制定一个考虑周详的响应计划，并且让整个公司的关键人员和团队均参与其中。

为了确保真正有效，事件响应计划应考虑以下几点：

1. **针对所有参与人员制定明确的角色、职责和批准流程**，确定可以采取和不能采取特定行动时应遵循的规则。例如，是否允许事件响应团队在未获其他批准的情况下使设备脱机，以遏制攻击？能否清除计算机或阻止对特定服务的访问？是否可以在必要时允许这些操作？此外，发生攻击时，公司应履行哪些法律、监管和合同义务？在事件发生前以书面形式解答类似于这样的问题至关重要。理想情况下，您的事件响应计划应在策略之间取得适当的平衡，确保在出现危机时做出合理的决策，而不需要经过多个层级的审批，以免影响专业响应人员的办事效率。
2. **定期举办培训和评估活动。**在公司内，可能有一大段时间不会发生事件。在此期间，要继续培训所有相关员工，执行评估活动，了解他们应对事件的就绪状态。此外，当发生事件时，不要忘记借此机会评估团队的实际效能。使用平均识别时间 (MTTI)、平均根本原因了解时间 (MTTK) 和平均安全问题解决时间 (MTTF) 等指标可以极大地帮助完善响应流程，同时向高级管理层证明投资回报。
3. **定期向高级管理层汇报事件响应计划的工作和成就**，确保他们为该流程给予合理的关注和资金支持，同时了解它在业务持续性中的关键作用。
4. **充分了解组织的基础设施和最重要的资产。**网络内部典型活动的可视性和外部的可靠威胁情报是事件响应的两大关键要素。
5. **制定反馈机制，确保不只是简单地清除事件**，而且要开展全面的调查。必须依法提取有关攻击者及其攻击方法的关键信息，防止类似攻击。军事战略家 John Boyd 发明了 OODA Loop（包以德循环），成为作战的决策框架（图 2）。如今，它应用在许多其他领域，且可以当作高效事件响应所需的持续流程的一个好例子。

图 2. OODA Loop（包以德循环）



技术

除了配备正确的人员和制定正确的流程外，在事件发生前部署正确的技术是另一个要点。

外部的威胁情报对于及时了解已知攻击至关重要，但若无适当的工具帮助事件响应团队深入分析其网络活动，响应工作将徒劳无功。这是因为您无法保护看不到的内容。

事件响应不仅仅是要清除恶意软件并让受感染的计算机恢复连接，还需要进一步开展调查，确定攻击的整个影响范围，是否有其他机器受影响，以及攻击者使用的战术类型。这样才能确保彻底根除您的环境所受到的攻击，并避免再次受到相同的攻击。

> “StealthWatch 使问题解决时间从几天减少到几秒。借助 StealthWatch，我们能够提前防御潜在攻击和漏洞。”
>
> – Edge Web Hosting

网络审计跟踪

了解当今大型复杂网络内的活动的最好方法就是收集和分析网络审计跟踪数据。事实上，在 Ponemon Institute 的一项调查中，有 80% 的受访者表示，对 NetFlow 和数据包捕获等来源提供的审计跟踪数据进行分析是检测安全事件和攻击最有效的方法。[5]

通过使用网络活动日志，组织可以更轻松地了解并制止攻击尝试。特别是 NetFlow，这是一项非常高效的技术，因为无需安装专用探头便可收集全网络的活动日志。而且，这些数据能够以较低的成本长时间存储。

NetFlow 的强大功能

NetFlow 由思科首创，如今已被广泛应用于各种网络基础设施设备，它通过与其他类型的网络遥测技术配合，提供来自现有路由器、交换机和防火墙的重要元数据，进而提高可视性和情境感知能力。它会提供网络上每个连接的记录，包括“来源”和“目的地”地址、端口号、传输数据量和其他信息。NetFlow 可揭示关于网络资产和行为的大量重要细节，例如谁和谁正在通信、哪些应用正在使用等等。

大多数组织已在其环境中部署 NetFlow。他们只需开始收集和分析这些数据，即可对其网络拥有更深入的洞察力。但是，并非所有 NetFlow 监控技术都一样。

随着现今网络不断发展演进，网络正在产生海量大数据。获取这些数据是重要的第一步，但是，如果事件响应团队无法理解其意义所在，未将其用于改善认知和完善决策过程，就没有任何意义。为此，就需要使用像思科® StealthWatch 这样的基于流的高级监控解决方案。

思科 StealthWatch

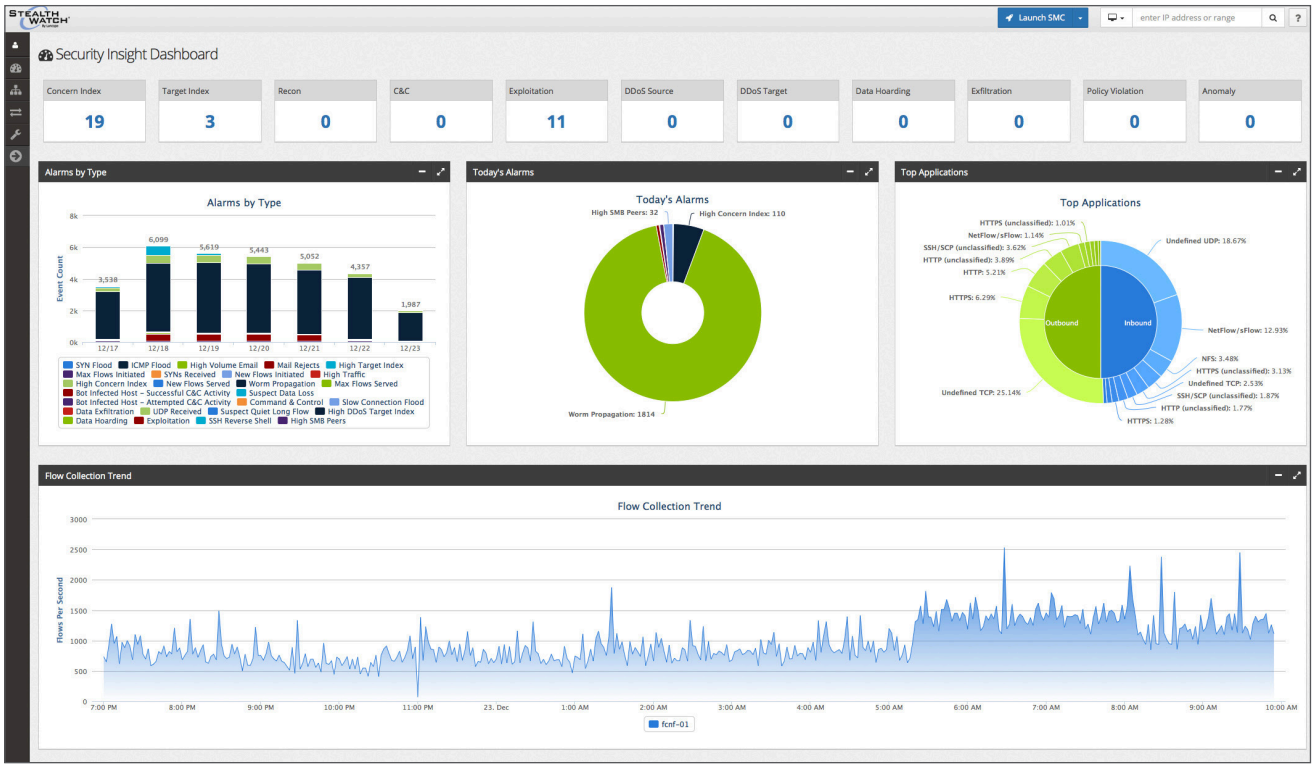
思科 StealthWatch 充当网络的耳目。它快速收集和分析大量 NetFlow 数据，为安全和响应团队提供深入的可视性和切实可行的情报。如前所述，它提供深入的网络洞察力和网络活动基准，这对于制定强大的事件响应程序至关重要。

此外，当与其他思科安全技术配合使用时，StealthWatch 可以帮助组织有效利用现有基础设施，使其网络成为一种持续运行的安全传感器，实现更无缝的威胁检测，提高成本效益。通过复杂的行为分析，StealthWatch 能够自动检测可疑行为，防止零日恶意软件、分布式拒绝服务 (DDoS) 攻击、高级持续威胁 (APT) 和内部威胁等一系列攻击。

StealthWatch 显著减少了与事件调查相关的手动分析工作。一般情况下，它能将故障排除时间从几天甚或几个月缩短到几分钟。其控制面板和报告清晰直观，安全和事件响应专业人员只需点击几下鼠标，即可快速了解所需信息，包括网络活动的整体情况、潜在问题列表或特定主机的信息（图 3）。这些信息也可以轻松与高级管理层等其他利益相关者共享。

[5] Ponemon Institute，“Cyber Security Incident Response – Are we as prepared as we think?”（网络安全事件响应 – 我们的准备是否像我们想象的那样充分？）2014 年 1 月

图 3. StealthWatch 控制面板



思科 StealthWatch 可以提供高级网络可视性和安全情报，加快事件响应速度。

或许，一名内部人员正在反复尝试访问您的网络的限制区域。或者，您的网络正在发出异常大量的数据，或者内部主机正与外国某个可疑 IP 地址通信。高效的网络可视性和安全分析工具可以识别这些行为，并提醒管理员进一步调查。

> “有 80% 的受访者表示，对 NetFlow 和数据包捕获等来源提供的审计跟踪数据进行分析是检测安全事件和漏洞最有效的方法。”
>
> – Ponemon Institute

StealthWatch 的优势

不同于只能监测进出网络的流量的许多其他技术，StealthWatch 还可以监控横向（东西）流量，以检测在网络内传播的攻击和识别内部威胁。StealthWatch 通过持续监控网络上的异常行为以及使用高级安全分析、报警和报告工具，将潜在问题告知管理员，提高事件响应的速度和效率。

处理 NetFlow 所消耗的资源一般少于全数据包捕获等备选方案。但是，对于一个全球性企业来讲，全面日志记录所产生的记录量仍可能超出每秒一百万个流。有效解决方案必须能够适当扩展，降低存储和功耗。Stealthwatch 具有强大的可扩展性，能够删除重复数据和融合单向流记录，为最大、最复杂的企业网络带来具成本效益的流监控和存储。

除了改善实时威胁检测外，StealthWatch 还有助于您更快、更全面执行调查分析。它可以将流数据存储数月甚至数年，并使用其高级查询功能快速提取以前攻击的相关信息。此历史回溯功能对于调整事件响应程序以增强威胁防御至关重要。随着网络通过云、软件定义网络 (SDN) 和物联网 (IoT) 架构不断发展和演变，高效收集、分析和解译大量网络和安全数据的功能将变得越发重要。

> “在采用 StealthWatch 之前，我们手动分析和关联我们的网络活动数据。StealthWatch 通过一个简单易用的界面自动为我们提供详细的网络分析，为我们的安全、网络运营和合规性工作提供帮助。”
>
> – BlueCross BlueShield of Tennessee

增强的安全性情景和集成

研究表明，69% 的组织认为他们的安全工具未能为他们提供足够的情景来了解他们面临的风险。[6]

StealthWatch 通过自身的技术和行业协作（包括紧密集成其他思科技术），额外提供多层安全性情景，以进一步加速和改善事件响应及调查分析。

这些附加值情报层的例子包括：

- 用户和设备感知
- 云可视性
- 应用感知
- 威胁源数据
- 终端安全集成
- 代理可视性
- 数据包捕获

从单一控制台访问所有这些信息可以大幅简化威胁调查和补救工作。事实上，根据 Enterprise Strategy Group 调查，80% 的组织认为他们的事件检测和响应流程受缺乏安全技术集成的制约。[7]遗憾的是，支离破碎的解决方案减慢了威胁缓解并留下可被攻击者轻松利用的安全漏洞。增强情景层和深度集成使现今组织可更自动、顺畅和高效地应对自身所面临的各种威胁。

结论

遗憾的是，时至今日，仍没有技术能够使企业网络完全免于遭受黑客攻击。但是，如果组织利用合适的人员、流程和技术组合，定期监控其自身的环境，安全团队将能够更好地识别和阻止仍在发生的攻击，同时在发生攻击时避免灾难性后果以及与数据泄露相关的成本。

[6] Ponemon Institute，“Privileged User Abuse & The Insider Threat”（特权用户滥用和内部威胁），2014 年 5 月

[7] Enterprise Strategy Group，“Tackling Attack Detection and Incident Response”（处理攻击检测和事件响应），2015 年 4 月

相关详细信息

Stealthwatch 通过结合思科广泛的安全产品组合，跨网络、数据中心、终端、移动设备和云提供从边缘到访问的全面保护和简化的事件响应。

点击此处了解思科自身的 CSIRT 如何使用 StealthWatch 检测和分析恶意流量，以改善事件响应和调查分析。

了解详情。请求演示。
stealthwatch@cisco.com

“80% 的组织认为他们的事件检测和响应流程因缺乏安全技术集成而受到制约。”

– 企业战略组

C11-737531-00 07/16