elastic

从您的 SIEM 中获得更多运营价值

elastic.co/cn →

目录

简介

随着组织开始采用数字转型举措来应对市场变化，许多组织不得不对自己的安全方法进行重新评估。新推出的网络产品和服务、移动应用以及支持远程办公的需求，这些都给了新型网络攻击更多的可乘之机。**安全团队需要快速演进，与时俱进，才能应对这些攻击**。

与时俱进的核心挑战在于避免效率低下，不然安全团队极尽所能也难使业务遭受威胁。SaaS 采用的爆炸式增长、持续的隐私要求以及整合安全功能的指令，只会徒增运营的复杂性。

在保持运营效率的同时做到掌控一切，这关键在于，您要能够在安全信息和事件管理 (SIEM) 平台中随时获得可用的数据。安全团队需要的数据量和种类呈爆炸式增长，例如云、物联网 (IoT)、移动源和可观测性数据等等，在此不一一列举。结果，事件活动大量增加，这对于发现保护业务所需的见解至关重要。

由于 SIEM 的限制，这种数据爆炸往往会带来诸多运营挑战。因此，建议您**审查使用的 SIEM 方法**，确保为迎接这些新挑战做好准备。

175 ZB

IDC 预测，到 2025 年，全球数据将增长到 175 ZB

41.6 B

到 2025 年，416 亿台联网设备将产生 79.4 ZB 的数据

42 B

据普华永道《2020 年全球经济犯罪和欺诈调查》，受访者报告的欺诈损失总额达 420 亿美元

安全需求在不断演进

随着组织采用更加以云为中心的业务模型，安全团队肩上的担子越来越重，必须确保业务中最有价值的资产（用户、应用程序、终端和数据）得到有效保护。请关注以下几个趋势，这些都会让安全团队在实现他们 KPI 和指标的道路上困难重重。

员工

领先于新的和更复杂的攻击方法至关重要。

- 安全技能紧缺
- 负担沉重的安全团队正在努力更好、更快、更高效地协同工作

流程

随着各种云举措的激增，保持运营效率和速度的压力越来越大。

- 大量的数据正在向云迁移
- 远程工作者和合作伙伴需要为更多的云解决方案提供支持

技术

对于提供对规避活动的可见性以及厘清威胁关系所需的详细信息来说，支持高容量数据源至关重要。

- 难以跨本地部署和云来执行响应迅速的查询和分析
- 在许多系统中，访问高容量数据源的成本可能过高

安全团队痛苦地意识到，数字转型增加了更多的受攻击面。每一个新的互联设备或云服务都可能为敌手带来一个可以利用的新潜在载体，并可能导致严重的安全威胁或资产暴露，致使业务风险增加。**最基本的要求是，能够在正确的时间拥有正确的背景信息，以便更好、更快地做出决策。**

以数据为框架重新考虑安全策略

对不断增长的动态攻击面保持可见性通常是不切实际的。按采集或按事件的许可模型和/或无法满足云扩展需求的架构，都可能会迫使客户进行权衡。团队经常需要费时劳力，决定在日常运营中要包含和排除哪些数据，这就使得组织在 SIEM 中的可见性非常有限，并导致多个运营孤岛，例如数据孤岛、团队孤岛和流程孤岛。

安全团队不是通过权衡和一次性的方法来保存难以纳入 SIEM 的数据（如高容量数据源或历史数据），而是越来越多地采用以数据需求为中心的各种方法。现代 SIEM 的基础必须容纳任何类型及所有的数据，这样安全团队才能打破孤岛。**通过现代 SIEM，安全团队能够在多层生态系统中快速准确地大规模搜索**任何类型的海量数据（无论是传统、非传统还是高容量数据源）。

打下坚实基础后，安全团队便可获得巨大的益处，不仅能够**大规模实施任何安全用例**（监测与合规性、威胁检测和防御、猎捕和事件响应），还能解决欺诈、隐私泄露以及其他可能使企业面临风险的重点问题。关键在于，安全运营团队能**够以一体化的方式收集、分析、可视化数据，并根据安全见解采取行动**。

您的 SOC 如何从一体化方法中受益

一体化方法为安全团队提供了许多优势。单一数据存储具有强大的数据安全性、数据处理和数据可视化功能，可跨分布式环境提供必要的背景信息，进而基于全面的数据提取有价值的安全见解。通过正确的安全分析，包括高准确度的检测、经过验证的Machine Learning 作业，以及其他跨本地部署和云的开箱即用型方法，安全团队可以有效改善安全状况，检测已知和未知的攻击，并快速响应以避免损害并防止未来发生事故。从战略上讲，**随着动态更改的发生，安全团队可以实现快速发展**。从业人员可以在如下过程中掌握更广泛的技能：

利用更多的背景信息更好地操纵数据和分析谍报技术

合作发现新的研究或实施新的检测方法

开发新的可视化和操作规程

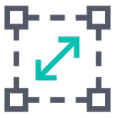
分析威胁参与者并模拟对抗行为

更多的团队可以承担猎捕职责。强大的平台级集成能力，可以实现高效的操作规程，简化对新型威胁和新兴监管要求的适应过程。

利用一体化的方法，您的 SOC 可以解决涉及多种安全功能的复杂安全问题，包括威胁猎捕、SIEM、威胁研究、合规性、安全监测和调查、数字取证和事件响应、终端保护、反欺诈等。

整体可见性

收集安全见解，并纳入所需的任何数据源，以推动实现与业务相一致的结果。



云可扩展性

从整个组织中获取必要的背景信息，以核实威胁，包括多年的历史背景信息。

高效率的 SOC

快速找到优先级最高的问题，并轻松地与其他工具和技术集成，以更快地进行调查和响应。

对整个安全团队的价值

安全工程师和管理员

- 无论数据源有多么分散，您都可以集中分析整个环境中的日志、流和背景信息数据
- 借助快速的联合搜索，在复杂的分布式环境中快速访问和搜索
- 索引并轻松访问高容量数据源，无需支付高昂费用

安全分析人员

- 更快地检测复杂威胁的准确性
- 加快响应速度和提高效率
- 执行自动威胁检测并最大限度缩短 MTTD

SOC 经理

- 高度保持对整个环境的洞察力，以改善安全状况
- 既要发现未知问题，又要避免已知问题再次发生
- 在不产生高额成本的情况下实现安全 KPI

elastic

您的 SIEM 是否阻碍了您的发展?

今天，与安全相关的数据可能来自云服务、网络和用户活动、终端、应用程序、互联设备和许多其他来源。许多试图访问所有这些数据源的 SIEM 解决方案，都导致了分析时间卡顿变慢或部署成本过高。

有些 SIEM 建立在用于不同类型安全分析的独立数据存储上，例如，一个用于 Machine Learning，一个用于基于事件的关联性，让团队将数据归档到另一个独立的数据存储中，用于获取威胁猎捕背景信息或取证证据，等等。前面已经提到，这些孤岛会导致团队在共享背景信息、协作、管理案例和应对威胁等方面效率低下。

SIEM 应该有助于您的 SOC 发展得更快，但许多 SIEM 产品并不具备可扩展性或灵活性来帮助安全团队打破数据孤岛或任务孤岛，这会导致调查工作流受到这些孤岛的限制。因此，产生了运营孤岛，致使安全团队无法更快、更智能、更高效地采取行动。

传统 SIEM 解决方案在运营效率方面的常见挑战包括：

- 安全数据源并未整合在一起，而是驻留在企业的不同数据存储中，因此很难获得整体可见性。
- 保留时间太短，迫使客户需要在检测、调查背景信息和威胁猎捕方面进行权衡。难以对停留时间较长的攻击确定入侵范围。
- 对于可能不会表明存在高级持续威胁，但在很大程度上仍然会对业务产生真正威胁的活动，安全分析人员缺乏足够的数据源来获取这类活动的背景信息。
- SOC 团队无法利用 Machine Learning 工具，除非他们拥有内部数据科学家来开发模型，并有熟练的威胁猎手来解释背景信息。
- 当安全工程师需要添加背景信息丰富的新数据源（如高容量数据）时，他们必须对数据规范化项目投入大量精力，和/或不断重新构建 SIEM 的底层数据结构。他们必须清楚了解自己的数据才可做到。
- 研究团队需要花费大量时间来开发 SIEM 规则，而这些规则很脆弱，对规避技术没有弹性，并且缺乏来自正确数据的高准确度的背景信息。
- 1-2 级分析师花费太多时间追踪告警，结果不是走到死胡同，就是需要从其他数据存储中检索额外的背景信息，从而导致延迟和效率低下。
- 开发人员将大部分时间花在解决集成问题上，或疲于跟上供应商的最新进展。

使用现代 SIEM 获得更好保护

无论数据的规模、大小或位置如何，现代 SIEM 可以访问所有的安全数据。借助对整个环境的可见性，安全团队可以访问丰富的背景信息和历史回溯周期，以便更好、更快地检测和响应威胁，并更准确地确定威胁的优先级。

访问任何类型及所有的数据

实时和历史见解

实现 SOC 极限速度

将 Elastic 安全作为 SIEM，提高运营效率

安全团队管理的数据量越来越多，需要能够快速准确地搜索、分析所有数据并执行自动化的检测。应对现代威胁需要即时关联，以便在传统安全数据、云基础架构、应用程序数据和多年历史数据之间进行有效的调查工作、猎捕、威胁分析等。

安全团队使用 Elastic 安全可访问整合后的数据，将发现的问题与威胁和业务背景信息联系起来，并使用历史数据快速找到最佳的解决路径。Elastic 安全解决了 SIEM、Endpoint Security、威胁猎捕、云监测、欺诈检测和许多其他用例，因此您的 SOC 可以利用搜索和可视化的强大力量，通过一体化的威胁检测、预防和响应方法来保护组织。

使用 Elastic 安全更智能地工作

获得整体可见性

使用 Beats 收集 Elastic Common Schema 规范化数据并索引所有与安全相关的数据，将整个组织的数据孤岛消除殆尽。使用直观的开箱即用型仪表板进行交互，并使用 Kibana、Lens 和 Canvas 开发定制符合自身需求的拖放式可视化效果。

快速获取安全见解

兼用写时模式和读时模式格式采集数据，以获得最佳查询性能，并在采集后灵活添加或更改字段。Elastic Stack 的速度众所周知，几秒钟内便可将结果显示在仪表板上。使用已确定优先级的关联彻底消除告警疲劳。

纳入多年的历史数据

利用可搜索快照，经济高效地充分利用您所需的安全数据，将其纳入检测、调查背景信息、威胁猎捕、云监测等内容中。确定停留数月甚至数年时间的入侵的范围。

缩短停留时间

要实现检测自动化，既可以使用由 Elastic 内部安全研究团队开发的 MITRE 映射的开箱即用型检测方法，也可以使用定制检测方法，利用强大而直观的事件查询语言 (EQL) 执行关联，以检测高级威胁的工具、策略和过程。

发现恶意异常活动

将无监督 Machine Learning 作业应用于任何带有时间戳的数据源，以识别构成潜在威胁的独立异常或相关异常。结合有监督和无监督的 Machine Learning 来检测具有低误报率的域生成算法 (DGA) 等方法。

简化安全运维 (SecOps) 工作流

使用 Elastic 安全的交互式工作区来检测和响应威胁、分流事件，并在直观的交互式时间线上收集证据。利用内置案例管理以及与主要安全编排、自动化和响应 (SOAR) 和工作流供应商的集成，加快响应和解决速度。

实施现代 SOC

Elastic 安全是各地现代安全团队所依赖的技术基础。Elastic 开放式安全平台的方法，能够让您轻松实现集成，灵活扩展，并利用社区驱动的贡献和协作，帮助 SOC 团队快速发展并更好、更快地做出决策。

结论

面对组织不断扩大的安全环境，安全团队在保护组织安全无虞的同时，一定不能忽视保持运营效率的必要性。通过访问所有与安全相关的数据，并以经济高效的方法来访问历史数据，您可以将 Elastic 安全部署为 SIEM，从而解决更多用例，并从整体上提高 SIEM 部署的运营价值。领先的**安全团队都选择 Elastic 安全作为他们的 SIEM，因为他们需要一种一体化的检测、防御和响应方法**。

Elastic 以快速和高效的方式提供整个环境的整体可见性，以发现和解决问题，在整个混合环境中提供云可扩展性，不管 SOC 团队目前如何分散或者在多少孤岛中操作，他们都可以实现最高的效率。使用 Elastic 安全的新 SIEM 方法保护您的业务。

想亲自试用 Elastic 安全?

请在 Elastic Cloud 上试用 Elastic 安全（14 天免费，无需信用卡）。
或者，也可以随时免费进行本地部署。

开始免费试用 Elastic 安全 →

Search. Observe. Protect.

Elastic 能让您在企业搜索、可观测性和安全领域大规模地实时利用数据。Elastic 解决方案基于免费且开放的单一技术栈构建而成，可在任何地方部署，让您从任何类型的数据中都能立即获得可付诸实践的见解 — 从查找文档，到监测基础架构，再到威胁猎捕，无一不能胜任。全球范围内有数以千计的公司/组织使用 Elastic 来为任务关键型系统提供支持，例如，思科、高盛、微软、Mayo 医学中心、美国国家航空航天局 (NASA)、纽约时报、维基百科和 Verizon 等等。Elastic 成立于 2012 年，为 NYSE（纽约证券交易所）上市公司，股票代码为 ESTC。更多详情，请参见 elastic.co/cn。

美洲总部
800 West El Camino Real, Suite 350, Mountain View, California 94040
常规业务 +1 650 458 2620，销售 +1 650 458 2625

info@elastic.co