Elastic 隐私数据表

Security

产品摘要：Elastic Security

Elastic Security 将威胁检测分析、云原生安全和终端保护功能整合到一个一体化解决方案中。它使组织能够通过 AI 驱动的安全分析快速检测、调查和响应整个环境中的网络威胁和漏洞。借助 Elasticsearch AI 平台，Elastic Security 可帮助客户大规模应对各类威胁，有效缓解告警疲劳，并支持安全人员针对安全发现的相关性进行快速调查。

- **产品类型：**软件
- **部署模式：**
  - 本地部署（自管理）
  - 云 (SaaS) (Elastic Cloud Hosted, Elastic Cloud Serverless)
  - 混合

在 Elastic Security 中处理的数据

Elastic Security 处理客户为进行威胁检测、调查和响应而摄取的安全事件数据和其他相关信息。处理的具体数据类型取决于客户的环境和日志配置。客户可以从不同来源摄取数据，包括日志、训练数据和机器学习模型的输出内容，以进行安全分析。

访问和使用 Elastic Security 所需的个人数据类别：

- 管理员和用户标识符、凭据、权限、会话 cookie 和活动日志。处理此类数据对于产品部署、配置、治理、管理、安全访问和确保使用过程可供审计至关重要。

- 任何偶然包含在网络威胁指标中的个人数据（例如，不可信的网络标识符、样本、可疑可执行文件及其他文件的哈希值与路径），Elastic Security 须处理这些数据以实现某些安全功能。请注意，其中部分功能只有在与 Elastic 后端服务器进行通信时（例如，声誉查询和威胁情报数据库）才能运行。客户如果自行决定禁用此类功能，或阻止自管理或混合部署模式的产品与 Elastic 后端服务器之间的通信，则必须理解并承认这将导致产品功能下降和安全性能降低。

其他被处理的个人数据类别可能包括但不限于以下内容：

- 来自安全事件日志的个人标识符和网络/系统活动数据：
  - 例如：用户 ID、用户名、电子邮件地址、IP 地址、MAC 地址、主机名、目录路径、文件名、URL。

- 威胁情报数据：
  - 示例：与已知威胁相关的信息，如果与特定恶意实体或活动关联，则可能包含标识符。

- 为取证分析、合规性报告或 AI 驱动的安全分析而采集的任何数据：
  - 示例：技术文档、训练数据中的详细信息、操作日志、大型语言模型 (LLM) 提示和响应（如果使用 AI Assistant 或 Attack Discovery），以及来自完整决策管道（从输入数据到最终安全结果）的数据。

- 用于安全态势管理的云环境和端点元数据：
    - 示例：AWS、GCP 和 Azure 云资产、Kubernetes 资源和虚拟机的配置详细信息，其中可能包含可识别信息。

处理输入到 Elastic Security 中的客户数据的典型目的：

在具体部署中，客户可以自行决定其选择提供给产品的任何数据的实际处理目的。一般来说，Elastic Security 是为以下使用场景而设计的：

- 检测、调查并响应 IT 环境中的网络威胁和漏洞。
- 利用先进的检测引擎来识别各种威胁。
- 为事件分流、调查和案件管理提供一个集中的工作空间。
- 提供交互式数据可视化工具，以便获得全面的安全见解。
- 实现集成，收集多个来源的安全数据，包括终端、服务器和云服务。
- 提供云原生安全功能，如云安全态势管理 (CSPM)、Kubernetes 安全态势管理 (KSPM)、云原生漏洞管理 (CNVM) 和云工作负载保护。
- 通过 Elastic Defend 启用终端保护功能，包括事件收集和恶意活动预防。
- 通过利用内置的机器学习工具和高级行为检测来识别恶意行为。
- 通过先进的实体分析和实体风险评分，为主机和用户生成全面的风险分析。
- 使用 AI 助手支持安全分析师进行有关 Elastic Security 的查询、理解警报并生成 ES|QL 查询。
- 辅助 Attack Discovery，利用大型语言模型分析多个警报并识别潜在攻击，详细说明涉及的用户和主机，并映射到 MITRE ATT&CK 框架。
- 通过预构建和自定义检测规则及警报，实现对环境的主动监测。
- 评估训练数据的组成，识别可能影响 AI 系统性能和公平性的潜在偏差或缺失，并比较不同人口群体的结果，以防止算法歧视。

产品使用数据

Elastic Security 会自动收集与产品使用情况相关的某些信息。此类产品使用数据——与前面提到的网络威胁指标不同且无关——按照 Elastic 产品隐私声明中所述的方式进行处理。在本地部署和某些混合部署模式中，客户可以在产品的配置设置中限制或禁用产品使用数据处理（请参阅适用的产品文档）。但是，在云 (SaaS) 部署模式中，此类产品使用数据的收集和处理对于产品的正常运行是必不可少的。

访问客户数据

- **客户访问：**客户对摄入到 Elastic Security 的数据保留完全控制权。无论是在 Elastic Cloud 还是在自管理部署环境中，他们都可以通过 Kibana 中的 Elastic Security UI 访问和分析安全数据。Kibana 提供各种仪表板（例如概述、检测与响应、云安全态势），用于可视化、排序和过滤数据和告警。客户可以使用强大的查询 DSL 来探索数据集以检测偏差，并过滤数据以比较不同人口群体的结果。

Attack Discovery 提供对潜在攻击的综合见解，详细说明涉及的用户和主机。客户可以创建案件以跟踪调查进展、添加警报，并与团队协作，同时利用 AI 助手提问有关发现和修复的问题。基于角色的访问控制已内置到 Elastic Security 和 Kibana 中，允许管理员定义角色，以限制用户对特定索引、仪表板或操作的访问，从而遵循最小权限原则。

- **Elastic 的访问：**对于 Elastic Cloud 产品与服务，仅有极少数 Elastic 员工被授予生产环境的特权访问权限，且仅用于必要的平台管理、维护及支持活动目的。此类访问权限基于最小权限和按需知情原则进行配置，并且定期接受审查和调整。Elastic 在自管理部署中无法访问集群或客户内容，只有在获得客户书面授权后（例如应客户要求提供支持服务时）才会访问 Elastic Cloud 部署中的客户内容。

    - Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的访问。Elastic 的内部团队积极开发和实施针对可疑内部账户活动和未经授权访问的检测，包括文件完整性监测和账户接管指标。
    - Elastic 的原则规定，只有在法律严格强制的情况下，其才会披露客户数据或提供对客户数据的访问权限，这些原则还包括挑战此类请求以及在法律允许的情况下通知相关方的既定规程。

处理地点

我们的安全解决方案的 Elastic Cloud 部署托管在由行业领先的 IaaS 提供商管理的认证云平台上，这些提供商包括 Amazon Web Services (AWS)、Google Cloud Platform (GCP) 和 Microsoft Azure。客户可以选择他们希望托管其部署的地理区域。

子处理：Elastic 利用特定的基础架构和客户支持子处理方来提供服务。具体涉及的子处理方取决于客户选择的数据中心位置、服务和功能。这些子处理方受合同约束，必须提供至少等同于 Elastic 信息安全附录中所述水平的数据保护。Elastic 对其子处理方保持完全透明（参见内部和外部列表），并为其行为和疏忽承担责任，其责任范围与 Elastic 自行提供服务时相同。

遵守隐私法规

Elastic 将根据适用的客户《数据处理附录》收集、处理、存储并保护客户个人数据。我们的信任中心是了解我们隐私实践和合规工作相关信息的综合资源。

- **数据所有权：**客户数据仍归客户所有。Elastic 仅为客户协议中指定的目的处理这些数据，并且绝不会将客户数据出售给第三方。
- **GDPR 合规性：**Elastic Cloud 功能在设计时即致力于支持遵守《通用数据保护条例》及其他全球数据保护和隐私法律。这包括通过有效的技术和组织措施优先保障个人数据安全，提供符合 GDPR 要求的数据处理附录。在 Elastic，我们拥有专门的隐私团队来监督 GDPR 的合规工作。

- **数据隐私框架 (DPF)：**Elasticsearch, Inc. 已通过由美国商务部制定的《欧盟-美国数据隐私框架》、《欧盟-美国数据隐私框架英国扩展版本》以及《瑞士-美国数据隐私框架》认证。
- **跨境数据传输：**Elastic 依据现行的标准合同条款及参与数据隐私框架（针对向美国的传输以及从美国发出的后续传输），在开展业务的各司法管辖区之间合法进行个人数据传输。此外，我们还实施强有力的补充措施以保护传输过程中的数据，如传输中加密和静态加密、对公共机构索要数据的请求提出挑战的程序，并为客户提供选择区域服务器的选项以托管数据。

数据可移植性

客户可以轻松管理其 Elastic Security 数据的可移植性，并可以下载由 Elastic Security 生成的警报和报告。这支持客户满足“数据主体访问请求”的需求，并支持导出数据以进行进一步分析或系统集成。

保留和删除

Elastic 提供一系列工具和功能，使客户能够针对安全日志和数据，有效地管理其数据保留与删除政策。

- 客户可以为其在 Elastic 环境中收集和处理的数据定义和执行保留策略。
- Elastic 支持长期保留日志，并通过数据分层架构提供经济实惠的存储选项，确保所有数据均可即时访问以进行分析。
- Logstash 作为 Elastic 组件，可用于执行数据转换，包括匿名化和假名化，这有助于实现数据最小化目标，并降低数据安全风险。
- Elastic 的平台使组织能够更深入地分析其保留个人数据的实际使用情况，从而能够更有效地调整数据保留期限和政策。
- 针对数据主体的删除请求，Elastic 提供了相应的功能：既可对数据进行标记以作为例外情况予以保留，也可利用匿名化等合规的删除与去标识化技术对数据进行永久删除，从而协助客户在短响应时限内保持合规。

个人数据的安全性

您 Elastic Cloud 数据的安全和隐私还依赖于保持稳妥配置的部署并维护 Elastic Cloud 登录凭证的机密性（详情请参阅我们的安全常见问题解答）。Elastic 支持一套全面的纵深防御安全模型，旨在于整个生命周期中保护客户数据，无论其处于传输中、静止中还是内存，并辅以稳健的密钥管理程序。我们也使用 Elastic Security 进行内部信息安全运营。

- **加密：**客户数据在静态下使用 AES-256 加密，在传输中通过 TLS 1.2 进行加密。Elastic 实施严格的加密密钥管理程序。

- **访问控制：**Elastic 实施技术、逻辑和管理控制措施，使数据访问权限限制在授权用户范围内。这些控制措施包括多因素身份验证、强密码强度标准以及使用虚拟专用网络进行管理访问。此外，基于角色的访问控制集成到了 Elastic 部署和 Elastic Cloud 管理平台中，允许对用户权限进行细致控制。
- **日志记录和监控：**Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的访问。Elastic Security 擅长大规模地聚合、存储和分析日志，以实现实时分析与可视化。它还支持强大的告警和异常检测功能。
- **系统更新和补丁：**Elasticsearch 实例会根据最新的操作系统内核定期更新和部署。每当在任何组件软件中发现共同漏洞和暴露时，都会及时应用相应补丁。
- **事件检测与响应：**Elastic 实施并持续更新检测规则，用于识别可疑活动和未经授权的访问，包括文件完整性监测和账号接管指标。这些检测是自动化工作流的一部分，可以向威胁检测与响应团队发出警报，并触发分析调查。Elastic 在内部使用 Elastic Security，该解决方案包括终端检测和响应功能，并集成了威胁情报源以支持入侵检测。它通过与第三方 SOAR 平台的集成支持自动化响应，降低违规可能性并加快响应时间。
- **安全软件开发框架 (SSDF)：**Elastic 维护着一套基于 NIST 800-218 标准的安全软件开发框架。该框架指导着所有 Elastic 软件的安全设计、开发、部署、跟踪和维护过程，确保落实“设计即安全”和“默认安全”的原则。
- **第三方供应商审核：**Elastic 与主要 IaaS 提供商（AWS、GCP、Azure）开展合作，并按第三方风险管理计划对他们的安全与合规标准进行严格审核，包括审核其 SOC 2 审计报告和 ISO 27001 认证情况。
- **渗透测试：**Elastic Cloud 每年由独立的第三方机构进行应用程序和网络渗透测试。Elastic 还设有公开的漏洞赏金计划，供研究人员进行持续测试。
- **员工培训：**所有 Elastic 员工在入职时及之后至少每年都必须完成全面的信息安全和数据保护/隐私培训。