Feasibility for EIEM

Abstract: as…

Introduction,

Background,

Feasibility

Conclusion

Require Analyze

etc

人工智能和大数据是现代SIEM的核心，SIEM上云是数字化安全转型的热门趋势。

<idea title=”骨架丰满法”>

资料堆积，

理解消化（思维工具、集合列表树图），

写架构（模板），

填充（write、draw、copy、~~code~~），

关键中间结论、总结润色；

</idea>

<copy 1>

“云中漫步”也遍布荆棘和陷阱，任何企业CSO和决策者都应该对此保持足够的警惕，成功的安全产品（例如SIEM），上云（如果合规的话）未必总是能够节省成本，弄不好还会增加成本。根据Gartner的预测，到2025年70%的企业数据都将再传统数据中心或者云计算外部处理（边缘计算），而根据IDC CloudPulse19年1季度报告，85%的企业都选择从公共云中“回迁”工作负载。未来，“上云”还是“下云”？“上哪种云”？对于企业安全主管们来说，依然是一个需要格外慎重考虑的问题。

</copy>

<copy 2>

一种“反云”模式，意即传统软件的托管、单租户、场外部署，这种模式往往也会被称为“云xx”或“ 某SaaS”。在某些情况下，这种方式对许多企业来说可能是不错的选择。但是，在某些情况下，结果不是很好。以SIEM为例，有三种产品模式：

1. SIEM软件本地部署在客户硬件上。

2. 在IaaS上部署了与本地相同的SIEM软件。

3. 原生SaaS SIEM，它是使用云技术和运营实践构建的SaaS服务。  
（请注意，我在这里避开了共同管理的模式，因为这会使今天的话题过于复杂。以上假设所有需要的维护任务都是由客户或SaaS供应商执行）

哪种模式更好？正如我的Gartner合作撰稿人所言：“这是陷阱！” 确实，这是一个很大的陷阱，因为答案取决于企业的需求和自身条件限制。

首先我们需要简要回顾一下SIEM的成本问题，因为SIEM费用将远远超过您付给SIEM供应商的许可费用。  
以下是一些最常见的SIEM的粗略成本模型（硬成本、软成本和隐性成本）：

</copy>

<copy 3>

简要回顾一下SIEM的成本问题

**首先来看硬成本：**

**1. 初始“硬”成本**

1. SIEM许可证成本：基本价格+每个用户，每个节点，每个EPS，每个CPU（和每个CPU内核）等成本

2. 对于软件SIEM，还包括所需硬件数量，服务器的OS，数据库成本

3. （如果有的话）强制性的第三方软件许可费用（有时包括代理，报告工具等）

4. 供应商或顾问的部署服务。如果未选择这些服务，则部署的人员、时间等成本将归入将在下面的软费用中！

5. 供应商培训或有关日志，日志管理，SIEM等的第三方培训

6. 额外的外部存储（大多数情况下）

**2. SIEM持续的运营“硬”成本**

1. 各种SIEM供应商服务：支持（通常是强制性的），持续的专业服务成本

2. 操作SIEM的人员：从FTE的一部分（规模非常小，SIEM的用例很少）到1 FTE（小型设备部署）到许多具有各种角色的FTE（如果实施实时监控，则SOC人员配备更多）。SIEM的0 FTE = SIEM项目失败，概率为100.00％。

**3. 定期或偶发的“硬”成本**

1. 各种SIEM供应商服务：专业服务，用于设备集成的定制开发工作（如果在内部完成，其中一些可能会变成软成本–对于高级组织或已经有SIEM经验的人员）

2. 定期对员工进行SIEM操作和调试培训

3. 专业人员：DBA，系统管理员，节点系统管理员，自定义连接器的内部开发人员，Crystal Reports管理员等，缺失的岗位则可能会变成“软”成本

4. 部署扩展成本：与初始成本相同，但是随着业务的增长，对于额外的系统、软件、硬件等，如果SIEM的授权费用基于多个维度（例如用户+ CPU +节点+服务器+其他），则这些成本漏洞将很快“溢出”。

5. 外部存储扩展成本：如果您的数据容量增加，并且日志保留时间保持不变（例如，PCI DSS为1年），您将需要购买更多存储空间

**软成本主要有三大块：**

**1. 初始“软”成本**

1. SIEM项目的部署时间。如果仅使用内部人员而非供应商或顾问进行部署，则需分配更多时间

2. 日志源配置和集成。这可能比仅仅安装该工具还要多。这就是SIEM项目实施在具有多个孤岛的复杂分布式组织中需要数月时间的原因。

3. 初始调整，内容创建以及使工具匹配环境（尽管可能很轻巧）

4. 培训以及运营冷启动需要花费的其他工作人员的时间

**2. 持续的运营“软”成本**

1. 报告和其他正在进行的监控任务的审查–24/7、每天、每周

2. 告警响应和升级；SIEM意味着关联和自动告警

3. 其他“SIEM应用”任务，例如查看仪表板

4. 正常运行维护任务，即维护您的SIEM和存储、备份、更新、次要故障排除等

**3. 定期或偶尔的“软”成本**

1. SIEM规则调整，报告创建，仪表板定制，新日志源集成，其他正在进行的SIEM任务

2. 定期培训和相关人员的时间成本

3. 扩展：与初始软成本相同

隐性成本：

1. 事件响应的额外成本：可能会检测到更多事件

2. 安全事件的补救成本，包括预防性的新技术部署成本

3. 其他部门人员需要时间来处理SIEM揭示的问题。软成本确实会从安全部门蔓延到IT部门，甚至超出IT范围（法律，人力资源等）。

以我的经验，一个SIEM项目的总成本（刨除SIEM商业软件授权费之外的硬+软费用），差异极大，从SIEM许可成本的10%到令人难以置信的20倍。

因此，在第一种模式中，您支付了所有这些费用，加上硬件费用以及与在您的数据中心中托管所述硬件相关的所有费用。但是，在第二种模式，您同样需要支付所有这些成本，加上云成本（存储、计算、数据移动）。好的，表面上看，您节省了数据中心电费和制冷费用，但您将看到一笔云账单（每个月）。

我的意思是，在模式1和模式2种，所有的维护任务以及成本都是相同的。模式2是一种伪云，准确说只是租用了其他人的硬件，冷却风扇和数据中心设施。此外，最大的区别是，模式1主要是资本支出（硬件），模式2是运营支出（云），这种差异对于某些企业来说可能很重要。

云的成本到底有多高呢？在我当分析师的时候，了解过一些案例，其中一位用户在一个主流公共IaaS基础架构上部署免费日志搜索工具，结果收到来自云服务商的6-7位数（美元）的账单。如果你的供应商将数据存储在云端虚拟机上的MySQL实例中，你需要付出的代价甚至更高（您还能想象比这更“反云”的事吗？！）。这种情况下，第三种模式（原生SaaS安全应用），成本低得多，而且能够规避前两种模式的很多问题，例如：

* 收集和保留某些日志类型的合规性要求
* 监控此数据源和/或系统的合规性要求
* 易于集成日志源
* 供应商的解析器可用性
* 实际将日志数据传输到SIEM的能力

综上所述，虽然在公共IaaS中托管传统SIEM具有一些优势，例如您不必购买，管理和更新硬件，也不必购买或扩展数据中心空间。但是，你需要支付与本地部署几乎相同的SIEM成本，并且还要额外支付云成本。后者的成本有时会极为高昂。利用云原生基础架构之上的原生云计算工具（以及成熟的云运营实践）往往能够大幅降低SIEM总体成本。  
总而言之，SIEM不是省油的灯，但以反云方式在云中部署SIEM有可能会花更多的钱。

最后，需要指出的是，本文讨论的成本问题，不是SIEM独有的，也不限于“安全上云”，很多企业数字化转型IT支出都面临此类问题。

</copy>

<copy 4>

**企业中的SIEM**

全球企业的安全开销中，SIEM软件仅占很小的一部分。Gartner估测，2017年**全球企业安全开支**约在**984亿**美元左右，**SIEM软件**大概会收获**24亿**美元。Gartner预计，在SIEM技术上的开销将会平稳增长，2018年到26亿美元，**2021年**到**34亿**美元。

SIEM软件主要被大型企业和上市公司采用，此类公司中合规要求是采纳该技术的重要原因。

**虽然有些中型企业也用SIEM软件，小公司却既没必要也没意愿往SIEM里投钱。**分析师称，他们通常无力购买自已的解决方案，因为其年度开销可达数万到十几万美元。而且，小公司也没能力雇佣持续维护SIEM所需的人才。

也就是说，有些**中小企业(SMB)**通过**软件即服务**的方式，从足以售卖该服务的外包供应商处，获得了SIEM。

**鉴于流经SIEM系统的部分数据比较敏感，目前大型企业用户习惯在本地运行SIEM软件。**GlaxoSmithKline美国SOC首席分析师兼SANS研究所导师约翰·哈巴德说：“你在记录敏感的东西，这种东西可不是人人都敢冒在互联网上发送的风险的。”

不过，随着机器学习和人工智能在SIEM产品中的增多，一些分析师也预计，SIEM提供商会拿出一个混合选项，部分分析在云端执行。

**云端收集、整理和产出情报正在兴起，因为提供商可以比公司收集并梳理更多数据。**

</copy>

<copy 5>

**SIEM工具和提供商选择**

**基于全球销售额**，SIEM市场有几家居于统治性地位的供应商，尤其是**IBM、Splunk和HPE**（惠普企业）。还有更多一些的主流玩家，比如 Alert Logic、Intel、LogRhythm、ManageEngine、Micro Focus、Solar Winds 和Trustwave。

**鉴于SIEM选择背后两大驱动力导致的功能需求各不相同，很多企业会选取2套不同系统，一套关注合规，但这会减慢威胁检测。另一套则是战术性的SIEM，用于威胁检测。**

**最大化SIEM价值**

大多数公司仍主要将SIEM软件用于追踪和调查已发生过什么。这一用例的驱动因素，是数据泄露威胁的升级，以及此类事件中安全主管和公司企业所面临后果的不断加码。可以想象，如果公司被黑，没有任何一位CIO，会在接受董事会问询时说“我特么要是知道就好了。”他们最应该想说的是“我们会梳理日志数据，查明发生了什么。”

**不过，现在也有很多公司不满足于SIEM的这一用例，开始将该技术更多地用在检测和近实时响应上。**现在的玩法是：你的检测速度有多快？不断发展的机器学习，正帮助SIEM系统更加准确地识别异常活动和潜在恶意活动。

尽管了有了这些发展，公司企业还是面临最大化工具效果，甚至最大限度榨取已有系统价值的挑战。其中原因多种多样。

**首先，SIEM技术是资源密集型工具，需要经验丰富的人员来实现、维护和调整——这种员工不是所有企业都能完全投入的。**

很多企业因为知道这是自己需要的东西而买下了该技术，但他们并没有能够搞定该技术的人员，或者他们没对员工进行所需的培训。

**想要最大化SIEM软件产出，就需要拥有高品质的数据。数据源越大，该工具产出越好，越能识别出异常值。然而，公司企业在定义和提供正确数据方面苦苦挣扎。**

且即便有了强大的数据和高端团队来运营SIEM技术，该软件自身也有局限。**在检测可接受活动和合法潜在威胁上，SIEM并非完全准确，正是这种差异，导致了很多SIEM部署中出现了大量误报。该情况需要企业内有强力监管和有效规程，避免安全团队被警报过载拖垮。**

**安全人员往往从追逐大量误报开始。成熟的公司会学着调整工具，让该软件理解什么是正常事件，以此来降低误报数量。但另一方面，一些安全团队会跳过该步骤，习惯性直接无视太多误报——有可能错过真正威胁的一种操作。**

**更为高端的公司还会编写脚本来自动化更多常规功能。**比如从不同数据源拉取上下文数据以建立更完整的警报视图，加速对真正威胁的调查和识别。这需要良好的过程和安全运营成熟度。也就是说，**不仅仅将SIEM作为一个单独的工具，而是将之与其他技术整合，有个整体的过程来引导各种行动。**

如此，可以减少员工花费在低端动作上的时间，让他们可以将自己的精力放在高价值任务上，以提升公司的整体安全态势。

</copy>

Conclusion