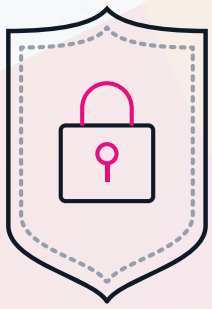
安全必备指南

使用Splunk的安全套件来应对日常挑战入门



splunk>
turn data into doing™

您的网络安全计划是什么？

您是否只是“做最坏的打算，却抱最好的希望”？

目录

那么，您怎样做才能够最好地捍卫您的组织并猎杀敌手呢？

追根究底，应对您跨整个企业的防御系统进行全方位思考。

简介

您的网络安全计划是什么？您是否只是“做最坏的打算，却抱最好的希望”？随着数字化技术的触角伸向我们生活的每个角落，新威胁每天都在爆发，在保卫您的资产、猎杀敌手的时刻来临之际，最紧要的是您的组织能够一丝不苟、消息灵通和准备充分。

高调入侵、全球勒索软件攻击和密码窃取的危害，这些都是您的组织需要收集、利用和理解正确数据的充分理由。此外，您还需要以不断增长的速度和多样化的机器数据来实施正确的过程和程序，并且通常还需要新技术、方法和需求。

那么，您怎样做才能够最好地捍卫您的组织并猎杀敌手呢？追根究底，应对您跨整个企业的防御系统进行全方位思考。这就是Splunk认为每个组织都需要一个安全神经中枢的原因所在，安全神经中枢由“六阶段安全之旅”来实现，下面我们会为您详细描述。

让我们来分析一下这意味着什么。

神经中枢模型

建立神经中枢可让组织通过优化人员、流程和技术来提高其安全性。它包括使用来自安全技术堆栈的所有数据，可帮助您以手动、半自动化或自动化的方式来调查、检测和采取快速、协同的行动来对抗威胁。当安全团队在其安全基础设施上投资时，其安全生态系统和技能将变得更加强大，从而有可能将安全实践扩展到新的领域并主动处理威胁。

Splunk数据到万物平台充当了该神经中枢，它将多个网络安全领域以及安全之外的其他领域区聚合到一起，促进协作并实现与您的数据进行交互的最佳实践。安全团队可使用Splunk解决方案来驱动统计学、视觉、行为和探索性分析，从而为决策和行动提供信息。平台在工作时可采用现代化的工作流，从收集数据到竭尽所能地采取各种措施来消除网络威胁和应对挑战。

图1：Splunk Enterprise Security

包括一个常见的框架，用于与数据进行交互和调用操作。Adaptive Operations Framework可让安全团队快速、确信地将变更应用到环境中。Splunk Enterprise Security还可使响应自动化，通过使用适合于各个域的一系列操作，从而使安全基础架构能够对付攻击者。

听上去很诱人？

是的。所以您想问，如何在真实世界中实现这一切呢？

为了让您入门，我们整理出这个简短的指南，向您介绍组织面临的顶级安全用例，并向您展示Splunk的分析驱动型平台如何帮助您应对安全性挑战。本指南划分成三部分：

1. **理解基本原理。** 在此您将看到安全之旅的介绍和安全用例的快速入门，其中每个用例均被映射到相关的Splunk解决方案。

2. **开启分析驱动型安全之旅。**在此，我们将解释数据驱动型安全之旅的六个阶段以及在各阶段您应该能够做的事情和达到的程度。

3. **借助Splunk应对常见安全性挑战。**在此我们将讨论如何应对与下列方面相关联的常见安全性挑战的例子：

    - 事件调查和取证
    - 安全性监视
    - 高级威胁检测
    - SOC自动化
    - 事件响应，合规性
    - 欺诈和分析检测
    - 内部威胁

准备好创建一个强大的安全实践了吗？我们认为应该准备好了。

理解基本原理

网络罪犯从不休息，这意味着您应该不断地寻找新的安全用例和提升洞察力，从而在您的环境中维持高水平的保护。

我们随时提供帮助。

Splunk的分析驱动型安全之旅

但凡问过诸如“我们安全吗？”之类问题的人，一定知道网络安全是一段旅程，而非终点。虽然探险可能没有终点，并且总有挑战，但您可以采取一些措施来取得旅行的成功。

首先，您必须了解您的环境并找到着手开始的位置。问自己：我要保护什么？我的关键数据是什么？我将如何应对这些威胁？

图2所示的六阶段分析驱动型安全之旅将帮助您回答这些问题，并创建一个强大的安全实践，使您能够理解您的防御中存在的差距，预见下一个挑战并采取行动迎接挑战。

图2: Splunk的分析驱动型安全之旅

Splunk的安全套件

您会在没有地图和一个装满食物与装备的背包的情况下开始徒步旅行探险吗？当然不会。正如没有合适的装备就不能成功旅行一样，没有合适的技术也不能达成成功的安全之旅。

Splunk的安全套件可以帮助安全团队在未知的领域中快速识别、调查、响应和适应动态数字业务环境中的威胁。Splunk解决方案可由一级分析师用于对时间段、关键字、IP地址或机器名进行基础研究。这些解决方案还可由资深的二级和三级分析师用于执行高级关联、构建分析模型或执行高级取证。

Splunk的安全套件

Splunk Enterprise	这是一个灵活的平台，处理了一大批安全用例，使您能够迅速从任何来源监视和分析机器数据，以提供见解从而采取行动，并提供分析驱动型基础从而加强您的整体安全性。在云中可用。
Splunk Enterprise Security	一套对从网络、端点和访问等安全技术所生成的机器数据、以及恶意软件、脆弱性和身份信息提供洞察分析的安全信息和事件管理（SIEM）解决方案。在云中可用。
Splunk User Behavior Analytics	一套由机器学习驱动的解决方案，为组织提供查找跨用户、端点设备和应用程序的未知威胁和反常行为所需的答案。
Splunk Phantom	一个与您现有的安全技术集成的安全编排、自动化和响应（SOAR）平台，在它们之间提供了一层“结缔组织”，使其更智能、更快速、更强大。
Applications	由Splunk、合作伙伴和社群开发的应用程序，用于增强和扩展Splunk平台的实力。例子如用于支付卡行业（PCI）合规的Splunk应用程序。在云中可用。
Splunk Security Essentials Application	由Splunk开发的、安装在Splunk Enterprise上的免费应用程序，向用户展示如何使用Splunk解决方案来解决不同的用例。Splunk Security Essentials展示了如何针对不同的安全用例最佳利用Splunk产品，发现安全性内容并验证成功。
Splunk Enterprise Security Content Updates	对于使用Splunk Enterprise Security (ES)的客户，它提供了被称为“分析故事”的安全性分析指南，该指南解释了如何最佳使用Splunk ES来调查和对环境中检测到的新威胁采取行动，实施何种搜索以及应该能够实现什么目标。

安全用例

下一步，您将会找到我们映射到安全之旅中的具体安全用例。继续。选择您的冒险，或称为安全性挑战。这本书的目的是教导您Splunk的分析驱动型平台是如何帮助您应对安全性挑战以及推进您的安全之旅的，包括：

将Splunk解决方案映射到安全用例

用例	Splunk解决方案
事件调查和取证	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
安全性监视	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk Phantom
高级威胁检测	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk User Behavior Analytics
SOC自动化	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
事件响应	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
合规性	Splunk Enterprise, Splunk Security Essentials App, PCI, Splunk Enterprise Security
欺诈分析和检测	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security
内部威胁检测	Splunk Enterprise, Splunk Security Essentials App, Splunk User Behavior Analytics

已定义的安全用例

最后，我们收录了针对用例的快速入门指导，以便我们能够处于同一层面上。

事件调查和取证

安全事件会在毫无预警的情况下发生，并且常常在足够长的时间内不被检测到，从而对组织造成严重威胁。通常等到安全团队意识到有问题时，损害往往已经发生了。Splunk为安全团队提供针对计算环境中所有带时间戳的机器数据的“单一数据源”。该项功能可帮助团队成员驱动效果更佳、速度更快的安全性调查，从而降低威胁长时间不被检测到的可能性。

安全性监视

安全监视使您能够分析针对威胁和其他潜在安全问题的接近实时的连续数据流。用于监视的数据源包括网络和端点系统，以及云设备、数据中心系统和应用程序。Splunk数据到万物平台使安全团队能够检测在来自这些数据源的数据流中发现的威胁并排出威胁的优先次序。

高级威胁检测

高级持续性威胁（APT）是一整套隐秘和连续的计算机黑客过程，经常由一人或多人以特定实体为目标精心策划。APT通常以民间组织和/或国家为目标，进行商业或政治图谋。Splunk Enterprise使组织能够搜索和关联数据，从而追踪高级威胁。Splunk Enterprise Security和Splunk User Behavior Analytics可提升现有能力，通过统计分析、反常检测和机器学习技术应用杀伤链方法来检测未知和高级威胁。

SOC自动化

安全运营团队采用Splunk软件来对充实和响应动作进行编排和自动化，以及进行案例管理（即事件）。这些团队使用Splunk的SOC自动化解决方案来定标操作、加速响应以及纠正威胁和其他安全问题。Splunk解决方案还可帮助组织对分析驱动型安全实践进行可操作化，并使安全团队能够跨扩展团队进行协作。

事件响应

事件响应（IR）涉及监视和检测IT系统上的安全事件，以及针对这些事件执行响应计划。IR团队有时被称为蓝队。当检测到威胁时，蓝队保卫组织的基础设施，而红队则试图发现这些系统的现有配置中的弱点。Splunk在安全产品组合中提供了各种各样的IR功能，具体取决于您所选择的产品。每个产品均提供对检测到的事件进行调查的机制。Splunk解决方案还可包括通过标准化的响应程序来指导事件响应者的能力。

合规性

在几乎所有环境中均存在种种形式的法规要求——尤其是当处理类似GDPR、HIPAA、PCI、SOC的内容，以及“**20项CIS关键安全控制**”之类的不作为真正的合规的更为常见的指导方针时。使用Splunk解决方案时，有许多应对合规挑战的方法。创建关联规则和报告用于识别对敏感数据或关键职员的威胁、以及自动证明合规性即为一个例子。

欺诈分析和检测

在数字时代，机器数据在检测欺诈活动中起着关键作用，并且处于核心地位。Splunk可搭载新数据，从而使欺诈检测团队能够更好地检测和调查反常现象。因此，公司预期能够减少财务损失、保护声誉和维持组织效率。

内部威胁检测

内部威胁来自对企业网络有访问权限、有意或无意渗漏、滥用或破坏敏感数据的现任或前职员、承包商或合作伙伴。他们通常对网络具有合法的访问权限和下载敏感资料的许可，可轻易避开传统的安全工具。通过使用Splunk解决方案，安全团队可获得一项能力，用于检测由内部人员和未被发现的被盗用的内部人员权限构成的威胁以及排出这些威胁的优先次序。

开启分析驱动型安全之旅

网络安全计划必须不断发展才能持续有效。问题是，许多组织对自己所处的位置以及如何改进缺乏清晰认识。了解您在安全之旅中所处的位置将帮助您更有效地管理时间和资源。并且有了对未来的预感，您就能更好地规划从而在后续阶段获得成功。

以下是分析驱动型安全之旅的六个阶段的分解，安全之旅使用数据为未来的攻击做好准备。让我们逐一了解每个阶段的下列方面：

- 用例的适用性
- 数据源
- 里程碑
- 挑战

第1阶段：**收集**

从您的环境中收集基本安全日志和其它机器数据。

安全用例的适用性

事件调查和取证

安全性监视

高级威胁检测

SOC自动化

事件响应

合规性

欺诈分析和检测

内部威胁

描述

第1阶段的重点是获取必要的素材，以便开始对您必须捍卫的环境获得深入了解。

数据源

第1阶段的最佳实践是捕获由安全基础设施的四个基本组件生成的机器数据：

1. **网络。**对网络流量的可见性对于任何安全团队而言均为重中之重。在此早期阶段，当务之急是查看正在进出您网络的流量类型。查看获得许可的网络流量以及被阻挡的通信尝试至关重要。

   源包括：

   - 来自供应商的防火墙流量日志，如：
     - Palo Alto Networks
     - Cisco
     - Checkpoint
     - Fortinet

2. **端点（基于主机）。**端点日志补充了网络可见性，提供了对恶意活动（例如恶意软件的执行、内部人员执行未经授权的活动或者攻击者在您的网络中驻扎）的洞察。从服务器、工作站和所有操作系统捕获这些数据非常重要。

   源包括:

   - Windows event logs
   - Linux system logs
   - Linux Auditd logs
   - MacOS system logs

3. **身份验证。**身份验证日志可告诉您用户何时从何处访问系统与应用程序。由于大多数成功的攻击最终均会涉及对合法身份证件的使用，因此该数据对于帮助区分合法登录与账户盗用至关重要。

   源包括:

   - Windows活动目录
   - 本地身份验证
   - 云身份与访问管理（IAM）
   - Linux Auditd日志
   - MacOS系统日志

4. **网络活动。**许多攻击以用户对恶意网站的访问开始，而以有价值的数据渗漏到由攻击者控制的网站告终。对谁在什么时候访问哪些网站的可视性对于调查至关重要。

源包括:

- 来自供应商的下一代防火墙（NGFW）流量过滤器或代理服务器日志，例如：
    - Palo Alto Networks
    - Cisco
    - Checkpoint
    - Fortinet
    - Bluecoat
    - Websense

里程碑

从这四个类别成功载入数据之后，您应该已达到下列里程碑：

- 关键活动日志位于一个日志不容易被攻击者篡改的单独系统中；以及
- 这四个类别的数据可用于进行基本调查。

挑战

收集不同的数据源会是一件麻烦的事情，而确保数据正确载入则会是一件乏味的事情。它经常被错误地执行，并且未能捕获足够的信息，从而导致时间损失和调查不完整。

第2阶段: **归一化**

应用标准的安全分类并添加资产和身份数据。

安全用例的适用性

事件调查和取证

安全性监视

高级威胁检测

SOC自动化

事件响应

合规性

欺诈分析和检测

内部威胁

描述

在第2阶段，您将确保您的数据与标准安全分类合规。这意味着代表常见值（例如源IP地址、端口、用户名等）的那些字段现在有了公用名称而不区分创建事件的设备。对数据归一化的这一重要的投资可让您：

- 使用来自供应商和社群的更多检测机制；

- 着手实施一个安全操作中心来跟踪您网络上的系统和用户；以及
- 开始定标您安全团队的能力。

即使您不打算维护一个正式的SOC，归一化数据也将：

- 促进交叉源相关联；
- 简化调查；以及
- 提高分析人员的效力。

数据源

在第2阶段，您应收集与下列有关的参考资料：

- IT资产（系统、网络、设备、应用程序）；以及
- 来自活动目录、LDAP和其他IAM/SSO系统的用户身份。

里程碑

第2阶段的里程碑包括：

- 数据正确映射至公用信息模型（CIM）；
- 通过使用与CIM相关联的加速后的数据模型，搜索绩效得到显著提升；并且
- 资产和用户详细信息与您安全日志平台中的事件进行了相互关联。

挑战

尽管您拥有可搜索的基本数据，但您缺乏对深入安全检测和端点可见性所需的洞察力或理解。

第3阶段: **扩展**

收集额外的高保真度数据源，例如端点行为和网元数据，以便驱动高级攻击检测。

安全用例的适用性

事件调查和取证

安全性监视

高级威胁检测

SOC自动化

事件响应

合规性

欺诈分析和检测

内部威胁

描述

域名系统（DNS）和端点数据将解锁一套丰富的检测功能，授权威胁猎杀者发现和跟踪网络中的敌手。

数据源

本阶段的数据源包括：

1. **网络。**大多数威胁猎杀者和威胁情报分析人员将告诉您如果他们只有一个数据源用于分析，那一定是DNS。

   源包括：
   - 来自Splunk Stream或Bro之类的源的特定于协议的互联数据；
   - 来自调试级日志或互联数据源的DNS查询级数据；以及
   - DHCP活动。

2. **端点。**捕捉过程创建、文件更改、注册表修改和网络连接等大量端点活动提供了在端点上发生的关键事件的异常清晰的历史。

   源包括：
   - Sysmon
   - Osquery
   - Carbon Black Defense

里程碑

通过收集高保真度数据源，您将：

- 已铺设好高级检测的基础；以及
- 已获得用以匹配盗用的某些常见指标的能力。

挑战

您正在收集的网络和端点数据细节丰富，但是却缺乏前后关系并且可能会包含您的同行组织所熟知的感染指标，并且仍然留在您的网络中而未被检测到。

第4阶段: **充实**

通过情报源来增强安全数据从而更好地了解事件的前后关系和影响。

安全用例的适用性

事件调查和取证

安全性监视

高级威胁检测

SOC自动化

事件响应

合规性

欺诈分析和检测

内部威胁

描述

除了收集重要的机器数据外，高绩效的安全团队还通过内部和外部来源的情报来丰富他们的数据。包括威胁情报馈入、开源情报（OSINT）源和内部资源信息在内的大量前后相关和调查的知识可让您的安全人员从所收集到的数据中提取更多的价值，从而尽早检测安全性活动和事件。

数据源

数据源包括:

- 本地IP/URL阻止列表
- 开源威胁情报馈入
- 商业威胁情报馈入

里程碑

通过提供前后关系的情报来丰富数据，安全人员能够:

- 理解基于资产危急程度的报警的紧急性。
- 通过将报警对照威胁情报馈入进行匹配、转向其它系统以及发起额外的前后关系收集活动，从而增强报警。

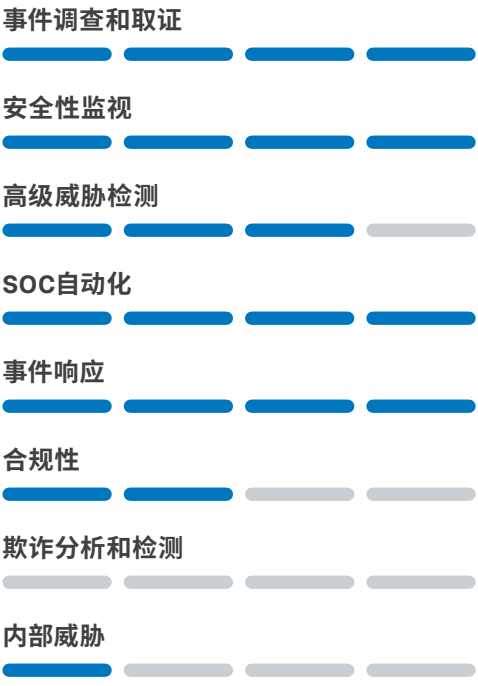
挑战

您具有重要的检测能力，但是您的团队以临时方式运营，或者未能与来自业务外部的信息进行关联来考虑他们所看见的现象的前后关系。此外，不对请求进行跟踪、不对性能进行测量、采取临时方式进行协作，并且所汲取的教训既不存储起来也不供将来利用。

第5阶段: **自动化和编排**

建立一贯和可重复的安全运营能力。

安全用例的适用性



描述

利用安全编排、自动化和响应 (SOAR) 解决方案可以让组织通过多种强有力的方式降低风险。实施自动化和编排的一些关键益处是，能够通过集成现有的安全工具和威胁情报源来加强防御能力，加快对安全事件的响应，简化调查过程并最大限度地减轻攻击造成的损害。成熟的组织能够持续对入站警报进行自动分类和优先级排序，从而将人力资源释放出来并集中在需要他们关注的最关键的问题上。与人工执行响应计划相

比，通过执行标准化的自动化剧本，成熟的组织还能够获得更好的一致性和可重复性。

数据源

此阶段的数据源包括由Splunk Enterprise之类的数据平台生成的高保真事件。自动化和编排系统摄取相关性搜索、值得注意的事件和其他高保真事件，以采取进一步的动作。

里程碑

第5阶段的里程碑包括进行下列工作的能力：

- 跟踪事件；
- 定期测量分析人员的效力；
- 根据上述剧本采取行动；以及
- 将简单的响应动作进行自动化，并将这些动作组合到更为复杂的编排中。

挑战

安全团队通常奋战在一线，尽可能识别、分析和减少威胁。然而，尽管他们尽了最大的努力，安全事件的积压量仍在不断增加，因为在调查和已知威胁上耗费了大量时间。（现实情况是，根本没有足够的专业人员来分析大多数组织所面临的事件数量。）

第6阶段: **高级检测**

应用包括机器学习在内的复杂检测机制。

安全用例的适用性

事件调查和取证

安全性监视

高级威胁检测

SOC自动化

事件响应

合规性

欺诈分析和检测

内部威胁

描述

通过应用机器学习、数据科学和高级统计来分析您的环境中的用户、端点设备和应用程序，您即给了自己一个检测敌手、未知威胁和内部威胁的战斗机会，即使他们只留下了细微的活动痕迹。

数据源

猎杀敌手需要从您的端点收集更多的精细数据。捕捉过程创建、文件更改、注册表修改以及网络连接的大量端点活动提供了异常清晰的在端点上发生的关键事件历史。

样本源包括：

- Microsoft Sysmon
- Osquery
- Carbon Black Defense

里程碑

在第6阶段中，您正在使用：

- 目前最先进的技术来识别未知威胁；以及
- 当新的检测机制可用时，充分利用您团队的专业知识和外部研究组织。

挑战

在此时间点，您将在不断完善您的安全组织并获得新能力方面经受挑战。您的团队还可能被要求开展新的研究。但是通过跟随旅程的指引并充分培养您的能力，您将成为这项游戏的顶尖高手。尽管您将一直处于被攻击的危险之下，但是您已将自己放在最佳的位置来检测和防止诸多对现代组织而言常见以及不太常见的威胁。

使用Splunk安全操作套件来应对常见的安全挑战

安全之旅可能会充满坎坷。如果您有一本关于您可能会遇到的挑战的手册，这样当挑战出现时，您就有工具来处理这种情况并坚持下去，这不是很好吗?

不用担心。我们会保护您的。

这里我们提供了一些示例来帮助您应对16个常见的安全挑战（您可以在**Splunk Security Essentials应用程序或Splunk Security在线演示**中找到更多）。每个示例均解释了挑战，并提供了关于数据源、用例、Splunk解决方案、编程难度、如何实现、警报量、已知误报以及如何最佳响应的信息。

示例包括：

- **事件调查和取证**
  - 使用WMI来检测横向运动
  - 识别多个未经授权的访问尝试
- **安全性监视**
  - 检测AWS中的公共S3存储段
  - 查找主机上的多重感染
- **高级威胁检测**
  - 检测到新域的连接
  - 查找与相似域的往来电子邮件

- **SOC自动化**
  - 自动化恶意软件调查
  - 自动化钓鱼调查
- **事件响应**
  - 为用户检测网络数据渗漏DLP警报
  - 识别基本的动态DNS检测
- **合规性**
  - 检测新的本地管理员账户
  - 查找登录到用户不应登录的范围内的系统的用户
- **欺诈分析和检测**
  - 检测被盗用的用户账户
  - 查找反常的医疗保健提供商
- **内部威胁检测**
  - 检测大型网页上传
  - 检测前职员账户的成功登录

事件调查和取证

使用WMI检测横向运动

第3阶段

斜角攻击战术

横向运动 | 执行

斜角攻击技术

远程服务 | Windows管理规范

数据源

Windows安全 | 端点检测和响应

安全挑战

Windows管理规范（WMI）由于其执行系统侦察、杀毒和虚拟机检测、代码执行、横向运动、持久性和数据盗窃的能力，在攻击者中越来越受欢迎。

用例

高级威胁检测

类别

横向运动

SPL 困难程度

基础

如何实施

该用例要求将sysmon安装在您想要监视的端点上，并将sysmon附加组件安装在您的转发器和搜索前端上。

报警量

Low

已知的误报

无已知的误报

如何响应

当此搜索触发时，您将希望启动事件响应过程并调查由此过程所采取的动作。

使用WMI检测横向运动的帮助

若要使用WMI来检测横向运动，我们首先需要加载我们的sysmon EDR数据。带有完整命令行的任何其他进程启动日志也足够满足要求。我们查找正在启动的Windows管理规范命令行（WMIC）的任何实例（EventCode 1表示有一个进程启动），并进行筛选以确保可疑字段位于命令行字符串中。

```
index=* sourcetype=XmlWinEventLog:Microsoft-Windows-sysmon/
Operational EventCode=1 Image=*wmic* CommandLine=*node*
CommandLine="*process call create*"
| table _time host Image CommandLine
```

识别多个未经授权的访问尝试

第1阶段

斜角攻击战术

凭证访问

斜角攻击技术

暴力破解

数据源

验证　Windows安全

安全挑战

大多数登录失败是由于密码错误。然而，到用户根本没有授权的敏感系统的多次登录失败可以表明恶意意图。在大多数组织中，除了代理日志之类的低风险情况外，用户很少会收到未经授权的消息。当在系统登录、文件共享访问等高风险活动时发生这种情况，以及当这种情况在某个用户身上持续发生时，通常有理由进行调查。

用例

内部威胁

类别

内部威胁

所需Splunk解决方案

Simple Search Assistant

SPL困难程度

中

如何实施

确保您有数据正从Universal Forwarder被摄取，并且Splunk技术附加组件存在，然后所有工作将会自动进行。

报警量

低

已知的误报

这种检测指示误报的最可能出现的情况是用户的访问打乱了。例如，昨夜发生了一个AD组更改，该用户被意外地从“dev_system_access”安全组中移除。除此之外，对于误报并没有标准模型。

如何响应

当该警报触发时：

1. 评估用户以前是否访问过这些想要访问的资源。
2. 查找最近的工作角色变化。
3. 查找AD组最近的更改。

在大多数组织中，下一个升级步骤是咨询资源的所有者和/或用户的经理，以确定这种行为是否是故意的。除了潜在的账户盗用外，还要留意是否有恶意的迹象。

识别多个未经授权的访问尝试帮助

若要使用实时数据来查找多个未经授权的访问尝试，我们可使用简单搜索和下面的搜索处理语言。这里我们引入了Windows安全日志，并专门寻找状态代码0xC000015B，该代码表明用户未被授予请求的登录类型。我们寻找每天有许多此类尝试的任何用户，而此类尝试可以表明试图访问敏感资源。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* source=win*security user=* EventCode=*
action=failure Logon_Type=* Failure Reason Logon Type
Status=0xC000015B
```

安全性监视

检测AWS中的公共S3存储段

第3阶段

数据源

审计跟踪　AWS

安全挑战

这是一个再普通不过的故事。人们将文件放在AWS　S3存储段上以便于快速传送，但却忘记将这些文件取下，或者将S3存储段用于敏感数据的备份但却疏忽大意将权限弄乱。由于错误配置和使公共S3存储段不必要地将敏感数据暴露于被利用的风险中，是发生破坏的常见方式，因此在将新的或现有的S3存储段设置为“公共”时进行检测非常重要。

用例

安全性监视

高级威胁检测

类别

数据渗漏分析

所需Splunk解决方案

Splunk Security Essentials

用于亚马逊网络服务的Splunk附加组件

Splunk Simple Search Assistant

SPL困难程度

中

如何实施

由规范化数据（映射到公用信息模型）促进对公共S3存储段的搜索。用于亚马逊网络服务的Splunk附加组件提供了各种AWS服务组件的可见性，包括来自CloudTrail服务和S3存储段的事件。假设您对Splunk使用AWS附加组件来将这些日志抽入，该项搜索将顺利地自动为您运行。但在实施时，请确保遵循为您的数据指定索引的最佳实践。

报警量

极低

已知的误报

在该项搜索当中，可能会发生两类不受欢迎的报警。当有人执行下列操作时，会发生这两类报警：

1. 故意创建一个公共存储段。您可能希望将定期执行该操作的营销员工列入白名单，或者希望建立一项政策来规定如何创建公共存储段，从而可以将故意创建的公共存储段排除在搜索范围之外。

2. 创建一个暂时为公共的存储段，但随后将该存储段切换为私有模式。

如何响应

当此搜索触发时，您将希望启动事件响应过程并调查由此过程所采取的动作。

使用WMI检测横向运动的帮助

若要使用WMI来检测横向运动，我们首先需要加载我们的sysmon EDR数据。带有完整命令行的任何其他进程启动日志也足够满足要求。我们查找正在启动的Windows管理规范命令行（WMIC）的任何实例（EventCode 1表示有一个进程启动），并进行筛选以确保可疑字段位于命令行字符串中。

如何响应

当一个公共S3存储段触发警报时，应该问三个问题：

1. 该S3存储段是否仍然是公共的？
2. 这些文件是否是公共的？
3. 存储段中是什么内容？

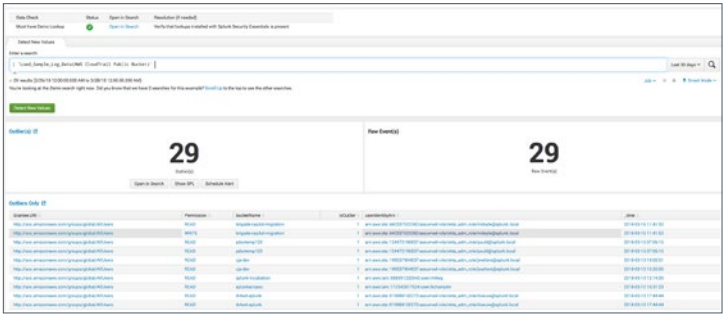
第一个问题很容易回答—只需在您的日志中搜索存储段名称和“PutBucketACL”。您将看到任何后续ACL更改。第二和第三个问题则较为棘手，需要打开服务器针对S3存储段的访问记录功能（默认情况下不打开，并且非常不方便，因此请不要押注在这上面）。

如果您有一个企业AWS环境，请按优先次序分析任何开放的S3存储段。您甚至可能希望通过AWS功能将其补救措施自动化。

检测AWS中的公共S3存储段的帮助

若要使用实时数据来对公共S3存储段进行搜索，我们可使用简单搜索和下面的搜索处理语言。实时搜索对AWS Cloudtrail日志进行操作，过滤在存储段权限更改时发生的PutBucketAcl事件，并且过滤包括AllUsers的任何事件。屏幕截图显示了对演示数据的搜索结果。

```
index=* sourcetype=aws:cloudtrail AllUsers
eventName=PutBucketAcl
| spath output=userIdentityArn
path=userIdentity.arn
| spath output=bucketName
path="requestParameters.bucketName"
| spath output=aclControlList path="requestParameters.
AccessControlPolicy.AccessControlList"
| spath input=aclControlList output=grantee path=Grant{} |
mvexpand grantee
| spath input=grantee
| search "Grantee.URI"=*AllUsers
| table _time, Permission, Grantee.URI, bucketName,
userIdentityArn | sort - _time
```



查找主机上的多重感染

第1阶段

斜角攻击战术

初始访问　执行

斜角攻击技术

由盗用驱动　Spearphishing附件

Spearphishing链接　用户执行

数据源

杀毒　反恶意软件

安全挑战

病毒出现，但多个病毒同时出现在单一主机上的情况更值得关注。此类活动可能表明利用工具包尝试若干技术，其中一些技术可能会成功，或者一个主机上有多个不相关的病毒。传统的反恶意软件产品可以有效检测已知的恶意软件，但在面对新的或不断发展的恶意软件类型时，这些产品可能会失败。由于恶意软件变种可以提供通往内部系统的后门，使得长期持久化或渗漏数据的情况发生，因此您应该立即确定优先级并调查受恶意软件感染的主机，以确定可能尚有哪些其他恶意软件未被捕获。

用例

安全性监视

类别

端点破解

所需Splunk解决方案

Splunk Security Essentials

Splunk Common Information Model Add-on

Splunk Simple Search Assistant

SPL困难程度

基础

如何实施

检测带有多重感染的主机需要从杀毒解决方案收集日志。举例而言，有了机载Symantec日志，这些搜索应能够轻松运行。如果您有一个与此不同的杀毒产品，您即可根据搜索条件来轻松调整该产品的字段名和源类型——尤其是如果您使用Splunk附加组件将其映射到公用信息模型中（在Splunkbase上搜索）。

报警量

低

已知的误报

无已知的误报。

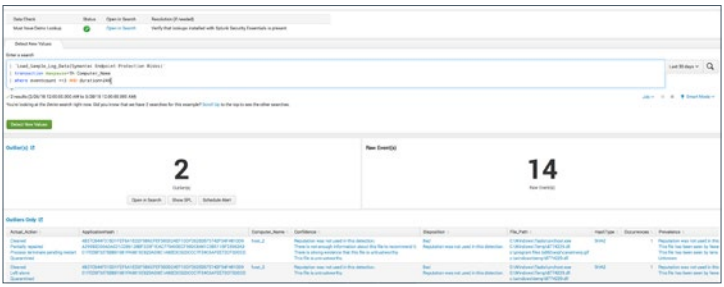
如何响应

当同一台主机上发生了多重感染时，您的响应计划应与针对任何恶意事件的响应相同，即必须是最高紧急程度。

查找主机上的多重感染的帮助

若要使用实时数据来查找在短时间内记录了多次感染的主机，我们在此举一个使用简单搜索和下面的搜索处理语言的例子。首先，我们在过去24小时内引入了我们的基本数据集，Symantec Endpoint Protection Risks（赛门铁克端点保护风险）。虽然有几种对事件进行分组的方法—其中stats命令是最快的方法—但是在这里我们使用交易，因为交易是最容易的。这样做将让我们基于Computer_Name对所有事件进行分组。最后，我们可以筛选出是否存在至少三个跨越至少几分钟的事件。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* sourcetype=symantec:* earliest=-24h
| transaction maxpause=1h Computer_Name
| where eventcount >=3 AND duration>240
```



高级威胁检测

检测到新域的连接

第2阶段

斜角攻击战术

越过封锁线　命令与控制

斜角攻击技术

经命令和控制通道发生渗漏

经替代协议发生渗漏

标准应用层协议

数据源

Web Proxy　NGFW

安全挑战

在大多数组织中，用户今天访问的域与他们昨天访问的域会有大量的重叠。但是，如若今天从您的网络请求访问的域中有很小的一部分不是您的系统以往访问的目的地，情况会如何？当然，今天会有一些合法的流量流向一些以往在网络上从未出现过的域，但它可能只占整个域集的一小部分。这些从未出现过的新域的其余部分构成了潜在的威胁。

了解用户何时浏览到新域，在各种场景中可能会与威胁息息相关，但其中最主要的是当您的系统连接到一个作为命令和控制通信中心的、受攻击者控制的域或者运行开发用服务器的域，从而发生数据渗漏或交付恶意软件。如果您相信某台主机被感染，请调查看该主机是否浏览过新域是一个需要检查的重要指标。

用例

高级威胁检测

类别

命令与控制、数据渗漏

所需Splunk解决方案

Splunk Enterprise

Splunk Security Essentials

Splunk URL Toolbox

Splunk Simple Search Assistant

SPL困难程度

中

如何实施

该匿名检测方法跟踪任何任意值集的最早和最晚时间（例如每个用户第一次登录 + 服务器组合，或者每个代码库的第一次查看 + 用户组合，或者每个系统表明USB关键使用的第一个Windows事件ID）。在正常使用情况下，您应该检查看最晚的值是否在过去24小时内，如果是这样，就应该发出警报。这是市场上许多能够轻松与Splunk Enterprise一起使用的安全数据科学工具（虽然不是Splunk UBA）的主要特征。

实施该搜索相对简单，因为该搜索需要CIM合规数据。从摄入您的代理数据（或者其它网络浏览可见性，例如stream:http或Bro）着手，并且确保有一个uri字段。还有唯一的一个其他步骤是确保您已安装URL Toolbox应用程序，该应用程序可让我们解析这些域。当缩放该搜索的规模以用于更大量的数据（或者更频繁的运行）时，我们建议使用加速功能。

报警量

很高

已知的误报

在大多数组织中，新域的百分比很小。 但是，如果您将所有这些警报均发送给分析人员进行调查，那么工作量将无法承受，因为大多数“新域警报”将由合法的流量触发。虽然没有已知的误报，但本质上，任何给定的“新域”警报的值都非常小，因此您希望将这些警报与大多数相关搜索区别对待。这些措施对于前后相关数据或者与其它指标进行关联最为合适。

如何响应

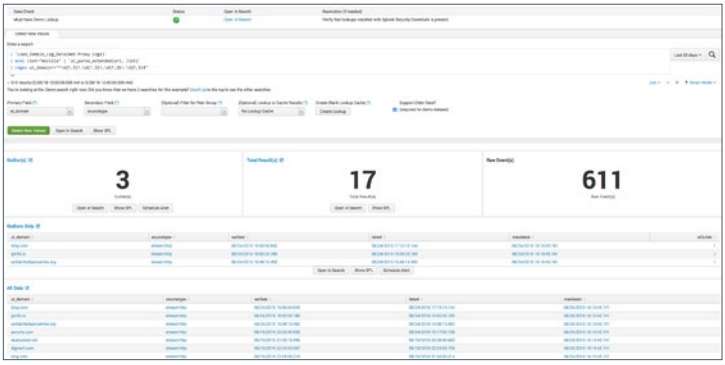
新域事件通常被视为另一事件的前后相关数据；例如未被清理的恶意软件、新服务或者不寻常的登录。完成响应的最容易的方法是将事件记录到摘要索引中，然后将对作为您调查活动一部分的索引的搜索纳入其中。Splunk Enterprise Security客户可以通过风险管理框架轻松做到这一点。通过在保存该搜索时创建风险指标适应性响应活动，该活动随后将调节所涉及资产的风险评分，并在您分析资产时显示在调查员工作台上。最后，若要在此分析任何给定警报的效力，我们建议在VirusTotal、ThreatCrowd之类的开源情报源中查看域。

检测到新域的连接的帮助

若要使用实时数据来检测到新域的连接，我们可使用简单搜索和下面的搜索处理语言。首先，我们引入代理数据集，利用公用信息模型字段并过滤出实际有URI的事件。

接下来，我们使用URL Toolbox从URL解析出域。最后，我们使用regex过滤命令将IP地址从搜索中排除。这是一个可选的步骤，但是我们发现，考虑到一些应用程序将连接到许多临时AWS实例IP进行正常操作，包含IP地址时的噪声比值可能相会当高。最后，我们使用stats命令来计算我们所看到的字段组合的最早和最晚时间，并检查看我们看到该事件的最早时间是否在最后一天（即全新的一天）。下面的屏幕截图显示了对演示数据的搜索结果。

```
tag=web url=*
| eval list="mozilla" | `ut_parse_extended(url,list)`
| regex ut_domain!="^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$"
| stats earliest(_time) as earliest latest(_time) as latest
by ut_domain, sourcetype
| where earliest >= relative_time(now(), "-1d@d")
```



查找与相似域的往来电子邮件

第4阶段

斜角攻击战术

初始访问

斜角攻击技术

Spearphishing链接

Data Sources

电子邮件

安全挑战

拥有相似域名的电子邮件是一种常见的网络钓鱼战术。一些攻击者会切换容易出错的字母，比如splunk.com收到来自spiunk.com的电子邮件。或者，他们可能会使用一个可信的子域（例如.help.com、.support等）。问题是，当人们认为电子邮件是由合法来源发送时，他们更有可能打开电子邮件。对于伪造的电子邮件，这种区别几乎是难以察觉的。

用例

高级威胁检测

类别

端点破解，SaaS

所需Splunk解决方案

Splunk Search Assistant

First Time Seen Assistant

UTL Toolbox应用程序

SPL困难程度

高级

如何实施

实施此类搜索通常相当简单。如果您有机载CIM合规数据，那么该搜索应该是开箱即用的。然而，您最好指定您电子邮件数据的索引和源类型——特别是当您有多个电子邮件日志源时，比如外围电子邮件安全设备和核心交换环境。如果您已经安装了URL Toolbox，并且具有正确的索引、源类型和src_user字段，那么它应该会像魔咒一样有效。

报警量

极低

已知的误报

该搜索动作将通过在任何名称与您的组织通常请求的域相似的域中搜索发来的电子邮件来进行搜索，与在域名上运行dnstwist十分相似。如果有任何来自与源域名相似（但不相同）的电子邮件，这些邮件通常在每天都能看到，搜索有可能会创建可能会是误报的警报。您可以想象一个场景：某家生产用于海盗船上的木板的公司（域名为plank.com）将其销售报告通过电子邮件发送给splunk.com。这将创建一个值为2的编辑距离（在这里，plank中的a变成了u，并且还有一个多余的s）并且会被标记（Arrrr!）。若要减少误报警报的数量，您可从搜索中过滤掉已知的示例，或者您也可将其送至First Time Seen检测，从而自动移除以往的示例。

如何响应

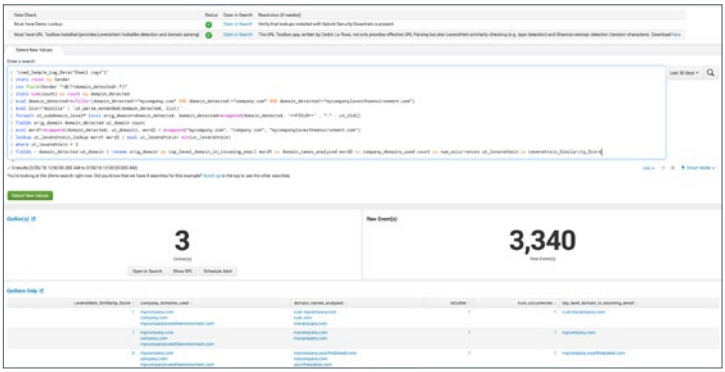
当该搜索动作返回值时，请发起您的事件响应过程并捕捉事件的时间、发送者、接收者、主题或邮件和任何附件。联系发送者。如果这是经授权的行为，则将经授权的事实及授权人记录在案。如果不是，则说明用户凭据可能已被另一方使用，因此需要进行额外的调查。

查找与相似域的往来电子邮件的帮助

为了在实时数据中查找具有相似域的电子邮件，我们使用Simple Search Assistant、URL Toolbox和下面的搜索处理语言。我们从提取电子邮件日志着手，在日志中我们有一个源地址，并且每个源地址总计一次。接下来，我们提取域并对我们将要分析的每个实际的域总计一次。我们还过滤掉我们拥有的任何域和期望从中接收电子邮件的域。使用免费的URL Toolbox应用程序，我们可从顶级域解析出子域。因为我们要传递给Levenshtein算法的字段是domain_ detected，所以我们将每个子域添加到多值字段domain_ detected。为URL Toolbox提供了两个多值字段，URL Toolbox会执行交叉检查来计算每个组合的Levenshtein分数。我们从该组中找出最低的分数。最后，我们过滤出Levenshtein分数小于3的情况。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* sourcetype=cisco:esa* OR
sourcetype=ms:o365:*:messagetrace OR
sourcetype=MSExchange*:MessageTracking OR tag=email src_
user=*
| stats count by src_user
| rex field=src_user "\@(?.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!="mycompany.
com" AND domain_detected!="company.com" AND domain_
detected!="mycompanylovestheenvironment.com")
| eval list="mozilla" | `ut_parse_extended(domain_detected,
list)`
| foreach ut_subdomain_level* [eval orig_domain=domain_
```

```
detected, domain_detected=mvappend(domain_detected, '<>'
. "." . ut_tld)]
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain),
word2 = mvappend("mycompany.com", "company.com",
"mycompanylovestheenvironment.com")
| lookup ut_levenshtein_lookup word1 word2 | eval ut_
levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename orig_
domain as top_level_domain_in_incoming_email word1 as
domain_names_analyzed word2 as company_domains_used
count as num_occurrences ut_levenshtein as Levenshtein_
Similarity_Score
```



SOC 自动化

自动化恶意软件调查

第5阶段

数据源

验证　Windows安全

安全挑战

当同一恶意软件出现在多个系统上时，您可能即将面临重大事件（通常与蠕虫、勒索软件和普遍的网络钓鱼活动一起出现）。调查和响应每个恶意软件警报可能需要30分钟甚至更长时间。通过使该调查和响应自动化，Splunk Phantom可验证进程是恶意的，并立即采取行动来阻止受感染端点上的散列。

用例

安全性监视

高级威胁检测

SOC自动化

类别

端点破解，横向运动

所需Splunk解决方案

Splunk Phantom

SPL困难程度

不适用

如何实施

从您的数据源将恶意软件事件摄入到您的SOAR平台。执行调查行动，例如在适用的IP、url和文件上检索声誉情报，从而帮助您更迅速地做出决策。这些前后关系收集动作是实现自动化的最佳选择。根据您的决策而定，可手动或使用自动化剧本来执行遏制和/或补救步骤。

报警量

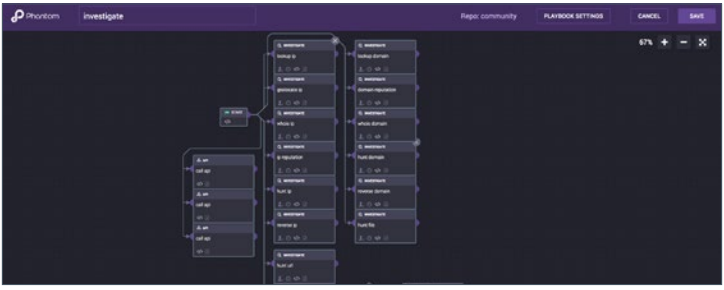
极低

已知的误报

不适用

如何响应

剧本将调查和补救端点上的恶意软件感染。通过使这些响应自动化，您将节省自己进行响应的时间，并将采取更即时的行动来阻止受感染的端点。您将开始使围绕用例的调查和检测自动化，例如隐藏文件和目录、创建带有多个扩展名的文件的垫片数据库文件执行、某个端点上的单个字母处理等等。



警报前后关系浓缩帮助

自动化钓鱼调查和响应

第5阶段

数据源

审计跟踪　AWS

安全挑战

钓鱼邮件如果未被发现，可能会对组织造成损害。调查每封电子邮件很耗时，因为分析人员可能不仅需要调查电子邮件的正文内容，还需要调查附件以及任何可能收到该电子邮件的用户。通过使调查自动化，分析人员即可更快地响应这些攻击。

用例

安全性监视

高级威胁检测

SOC自动化

类别

钓鱼，敌手战术，账户破解

所需Splunk解决方案

Splunk Phantom

SPL困难程度

不适用

如何实施

将可疑的电子邮件摄入到SOAR平台。执行调查行动，例如在适用的IP、url和文件上检索声誉情报，从而帮助您更迅速地做出决策。这些前后关系收集动作是实现自动化的最佳选择。根据您的决策而定，可使用自动化剧本采取动作从您的邮件系统中删除钓鱼电子邮件的任何副本。

报警量

极低

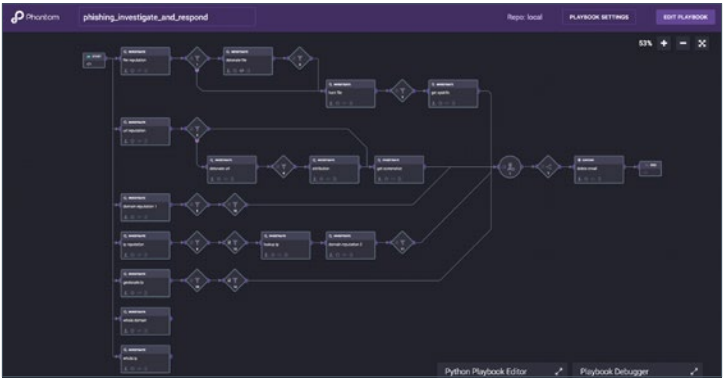
已知的误报

不适用

如何响应

在构建剧本时实施正确的调查并使之自动化，可以使您能够限制执行动作所需的人工响应数量，因为您希望在剧本中实施的响应将有助于简化钓鱼调查，从而能够更快地进行补救和采取行动。

自动化钓鱼调查



事件响应

为用户检测新数据渗漏DLP警报

第3阶段

斜角攻击战术

越过封锁线

斜角攻击技术

越过封锁线

数据源

DLP

安全挑战

当通常不生成数据渗漏DLP警报的用户突然启动时，它比传统警报更值得注意。对于关键规则或高权限用户，请调查这些事件，以确定敏感的公司情报是否正从组织泄漏出去。

用例

内部威胁

类别

内部威胁

所需Splunk解决方案

Simple Search Assistant

SPL困难程度

中

如何实施

此规则的实现非常简单——惟一的要求是能够记录哪个DLP警报代表数据渗漏。不同组织之间的术语或配置可能有很大差异，因此这需要与您的DLP团队进行协调。除此之外，只要定义了用户字段和签名字段，搜索就可发挥作用。

报警量

高

已知的误报

这是一个严格的行为搜索，所以我们对“误报”的定义略有不同。每次触发误报时，它将准确反映您正在搜索的时间段内的第一次出现（或对于查找缓存功能，无论您所构建的查找时间段是什么，均为第一次出现）。但是，虽然在传统意义上确实没有“误报”，但肯定有很多噪音。

如何响应

因为这是一个行为警告，您通常不应该单独使用它，除非：

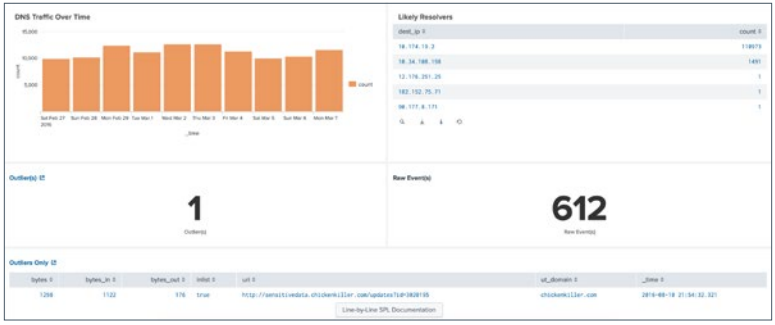
- 警报的严重程度或用户的优先级决定了该警报是如此重要，必须单独查看，或者
- 您的DLP进行了非常仔细的调优，因此很少出现警报。

对于其他所有人来说，应该通过Splunk ES中的风险聚合机制或Splunk UBA中的威胁模型，将大多数警报与其他警报结合在一起加以考虑。

为用户检测新数据渗漏DLP警报的帮助

本示例使用Simple Search Assistant功能。我们的数据集是DLP事件的基本数据集。为进行此分析，我们现正在过滤出数据渗漏警报。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* tag=dlp tag=incident
| stats earliest(_time) as earliest latest(_time) as latest by
user, signature
| where earliest >= relative_time(now(), "-1d@d")
```



识别基本的动态DNS检测

第1阶段

斜角攻击战术

命令与控制 | 敌手OPSEC | 建立和维护基础设施

斜角攻击技术

动态DNS | 标准应用层协议

数据源

Web Proxy网络代理 | NGFW | DNS

安全挑战

攻击者希望他们的命令和控制能力具有灵活性，而动态DNS可以提供这种灵活性。虽然动态DNS的使用是合法的（许多IT专业人员使用它来访问家庭网络），但不监控这种做法的风险可能是巨大的。幸运的是，在Splunk和恶意软件域提供的列表之间，很容易在您的环境中找到动态DNS。

用例

安全性监视、高级威胁检测

类别

命令与控制

所需Splunk解决方案

Simple Search Assistant
URL Toolbox

SPL困难程度

基础

如何实施

实施此检测的第一步是获取dyndns提供者列表。下载列表之后，您将需要将其格式化以适应Splunk查找格式。一旦文件就位，其余工作即会顺利进行。

报警量

中

已知的误报

使用动态DNS的生产服务虽然罕见，但确实会发生。这些将导致一些基本级别的误报，尽管它们绝不应该是业务关键型服务。动态DNS最常见的场景是用户通过网络摄像头之类方式到家里看他们的狗。究竟是允许（从而排除）这些用户，还是禁止这些活动，最终取决于政策决定。

如何响应

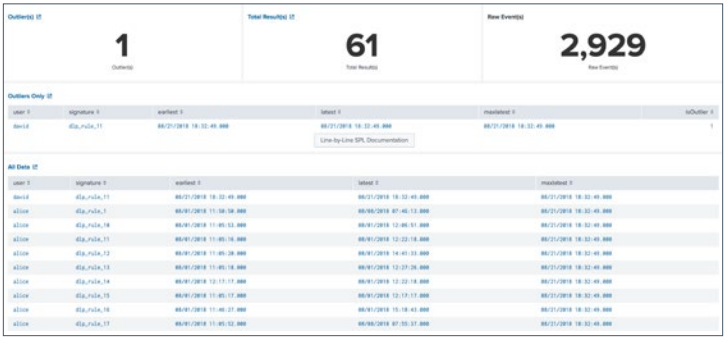
当此警报触发时，请查找常见的可允许场景，特别是那些正在访问其家庭网络的用户。如果情况似乎并非如此：

1. 请参考来自Splunk Stream或您的包捕获的数据，以确定所发送数据的类型。
2. 查看开放源情报中的DNS名称和IP，看是否有任何值得注意之处（尽管这对于本场景通常比较困难）。
3. 如果这是一个关键的主机，可以考虑通过Microsoft sysmon或其他端点响应机制进行端点日志记录，以识别创建这些连接的进程。

识别基本的动态DNS检测的帮助

本例使用简单搜索和下面的搜索处理语言来检测到活动数据上的动态DNS服务器的出站通信。首先，我们引入代理日志数据集。为了定位动态DNS提供者，我们使用URL Toolbox将子域从注册域中分离出来。接下来，我们可以使用ddns域的查找功能。该功能将为任何匹配添加一个名为inlist的字段，其值为“true”。最后，我们可以查找匹配的那些记录。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* sourcetype=pan:threat OR (tag=web tag=proxy)
earliest=-20m@m earliest=-5m@m
| eval list="mozilla" | `ut_parse_extended(url,list)`
| lookup dynamic_dns_lookup domain as ut_domain OUTPUT
inlist
| search inlist=true
| table _time ut_domain inlist bytes* uri
```



合规性

为用户检测新数据渗漏DLP警报

第1阶段

斜角攻击战术

防御规避　存留

斜角攻击技术

有效账户　创建账户

数据源

审计跟踪　Windows安全

安全挑战

本地管理员账户被合法的技术人员所使用，但他们也是攻击者的圣杯。一旦攻击者进入网络，他或她很可能希望获得管理员权限，从而获得对所需账户和资产的不受检测和不受约束的访问。达到此目的的一个简单方法是破解现有账户，然后提升权限。

用例

高级威胁检测、安全性监视、合规性

类别

端点破解

所需Splunk解决方案

Splunk Security Essentials
Splunk Enterprise

SPL困难程度

中

如何实施

首先，核实您的Windows安全日志中有内容写入，并且您已实施账户变更审计。如需帮助，请参考Windows安全数据源文档。

一旦您的日志中有内容写入，您应该能够搜索“sourcetype=” WinEventLog:Security” EventCode=4720 OR EventCode=4732” 来查看账户创建或变更事件。最后，确保您的本地管理员组名为 “administrators”，从而使我们能够查找正确的组员关系变更。

报警量

中

已知的误报

该项搜索中误报的唯一真实来源将会是创建本地管理员账户的技术支持管理员。如果这是您环境中的一种惯常做法，您应该通过将其用户名排除在基础搜索之外，从而过滤掉其管理员账户创建消息。如果您的本地管理员组不包括 “管理员” 术语，则可能会潜在地生成漏报。

如何响应

当该搜索返回值时，发起您的事件响应过程并捕获：

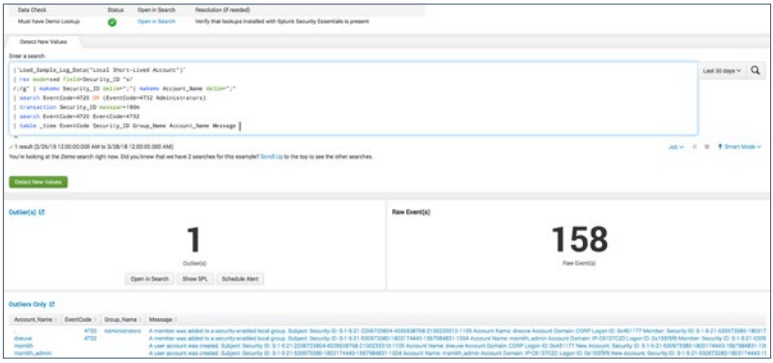
- 新的账户名称
- 创建时间
- 创建该账户的用户账户
- 发起请求的系统
- 任何其他相关信息

联系系统的所有者。如果事件是经授权的行为，则将经授权的事实及授权人记录在案。如果不是，则说明用户凭据可能已被另一方使用，因此需要进行额外的调查。除了调查之外，现在还是一个确保合法的管理员账户切实需要所分配权限、并受到复杂的长密码保护的好时机。

检测新的本地管理员账户帮助

本例使用简单搜索和下面的搜索处理语言来查找新创建的、被提升到本地管理员状态的账户。我们的数据集是一个Windows安全日志的集合，其中包含账户创建事件或账户更改以及组成员身份事件。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* source="winEventLog:Security" EventCode=4720 OR
(EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 (EventCode=4732 Administrators)
| table _time EventCode Account_Name Target_Account_Name
Message
```



查找登录到用户不应登录的范围内的系统的用户

第4阶段

斜角攻击战术

凭证访问 | 特权升级 | 收集

斜角攻击技术

有效账户 | 来自信息存储库的数据 | 账户操纵

数据源

验证 | Windows安全

安全挑战

根据《一般数据保护条例》（GDPR），机构须就员工、供应商及/或处理商获授权访问处理个人资料的系统及应用程序的情况，维护完整的审计跟踪记录。GDPR给予欧盟和欧洲经济区的公民个人向组织询问他们的数据存储在哪里，以及哪些实体正在访问这些数据的权利。

为履行该请求，组织将需要识别哪些雇员、供应商和处理商访问过相关的个人数据；并确定和报告有哪些其他服务会定期处理这些数据。在代表控制人处理个人资料时，还有一项要求，即须证明只有获授权的个人访问过有关资料。如果存在表明未经授权访问的审计跟踪，则需要将其记录下来并报告给数据隐私主管部门。

通过使用由控制加强的数据映射来检测违规，组织可以识别：

- 哪些员工、供应商和/或处理商访问了数据；
- 数据可能存储在哪里；以及
- 哪些其他服务会定期处理数据。

如果您正在代表一名控制人处理数据，该项搜索可证明仅经授权的个人有访问数据的权限。

用例

内部威胁、合规

类别

GDPR、IAM分析、横向运动、操作

所需Splunk解决方案

Splunk Enterprise

SPL困难程度

基础

如何实施

首先，使用您的数据映射结果来构建一项将系统与其GDPR分类进行关联的查询。然后针对用户执行相同的操作。此刻，只要您有机载CIM合规数据，一切就会顺利进行！

报警量

高

已知的误报

当不在记录清单中的人访问数据时，将触发此搜索。最可能出现误报的场景是，授权用户的记录清单已经过期。

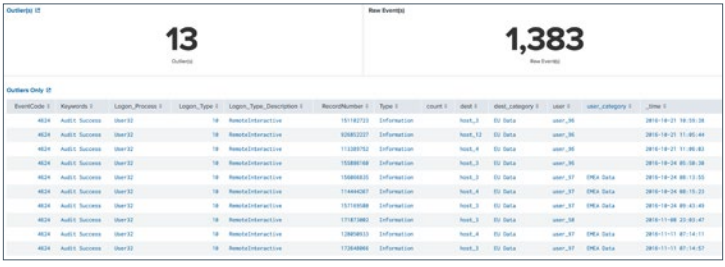
如何响应

查找应将某个人添加到文档中的指示，但在做任何更改之前，请先让您的数据保护专员员（DPO）或其团队验证您的数据。考虑使授权用户清单的更新自动化，并从您的DPO保存授权用户的最终记录的源中提取该清单。另一种选择是通过用部门名称来充实用户名，将信息归纳并充实到有访问权限的部门。

查找登录到范围内系统的用户帮助

该示例使用简单搜索和下面的搜索处理语言来查找未经授权的用户登录到实时数据的范围内系统。数据集是Windows身份验证日志的集合，其中包括来自Windows安全日志的登录。我们的搜索将在GDPR分类查找中查找主机，并且仅筛选出属于GDPR范围内的主机。接下来，我们在GDPR分类查找中查找用户，最终查找没有匹配的GDPR类别的用户或没有获得任何GDPR信息授权的用户。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* source=win*security user=* dest=* action=success
| bucket _time span=1d
| stats count by user, dest
| lookup gdpr_system_category.csv host as dest OUTPUT
category as dest_category | search dest_category=*
| lookup gdpr_user_category user OUTPUT category as user_
category
| makemv delim="|" dest_category | makemv delim="|" user_
category
| where isnull(user_category) OR user_category != dest_
category
```



欺诈分析和检测

检测被盗用的用户账户

第1阶段

数据源

应用程序日志 **网页访问日志**

安全挑战

无论是银行、信用卡、电子邮件、医疗账户，还是来自无数服务提供商的任意数量的账户，欺诈者可以在您不知情的情况下接管这些在线账户。通过利用网络钓鱼、间谍软件和/或恶意软件诈骗，攻击者获得重要的凭证信息，以获得对账户的访问权。账户接管的一些主要用途是信用卡欺诈、使用账户权利和使用账户订阅。诈骗者通过伪装成真实的客户，可以更改账户细节、购买、提取资金以及利用窃取的信息来访问其他账户甚至是更敏感的数据。根据不同的活动而定，黑客可能不会更改某个账户，并可能和账户的所有者在同一时间使用该账户。

用例

欺诈分析和检测

类别

账户接管、密码表攻击（凭证篡改）

所需Splunk解决方案

Splunk Enterprise

SPL困难程度

中到高

如何实施

确定关键用户账户数据并确认正确抽取字段。您还希望实现安全性增强，比如您可以实施阻止不良身份验证、双因素身份验证、在所有身份验证上使用验证码、机器学习或生物识别检测之类的功能。通过实施周全的增强措施，可使创建工作变得更加困难，并且添加任何摩阻力均有助于防止未经授权的访问。诸如速率限制、IP阻塞和阻塞不良请求等也有助于限制攻击的规模。

报警量

中

已知的误报

无

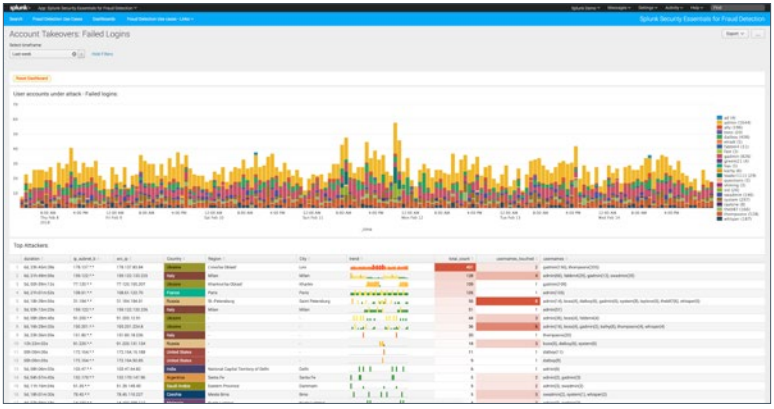
如何响应

这是试图盗用用户账户的最强力量。调查进攻的IP和子网并相应调整防火墙规则，从而最大限度地减少可能发生的账户接管事件。注意时序图上的峰值并调查正在受到大量攻击的账户。

检测被盗用的用户账户帮助

使用web日志来显示某个用户或IP地址的行为，使用身份验证日志来帮助您了解哪些账户被实际破解。该做法为查看高失败率提供了有用的信息。其他账户日志还可以帮助了解是否进行了其他更改，如电子邮件更改。数据必须包含有关登录尝试的信息以及尝试是成功了还是失败了的标志。搜索处理语言如下所示。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=web-logs action=login result=failure
| stats count, sparkline as trend by src_ip | where count>5
| sort - count
| table _time src_ip trend count
```



查找反常的医疗保健交易

第1阶段

数据源

应用程序日志

安全挑战

全国有超过400人被指控参与处方药索赔骗局。此类欺诈可能会影响法规和要求，使供应商难以开展日常业务，并使客户难以获得实际所需的处方。该项搜索可找到全国范围和全州范围内有关处方药索赔的反常行为。

用例

欺诈分析和检测

类别

账户接管

所需Splunk解决方案

Splunk Enterprise、Splunk Machine Learning Toolkit (MLTK)、Splunk Stream

SPL困难程度

中

如何实施

数据集可从**https://data.cms.gov/**下载。数据采用CSV格式，以便于

摄入。您可以下载该应用程序，以便查看指示板和深入了解源SPL。而APP已随封装的CMS数据集一并提供。

报警量

中

已知的误报

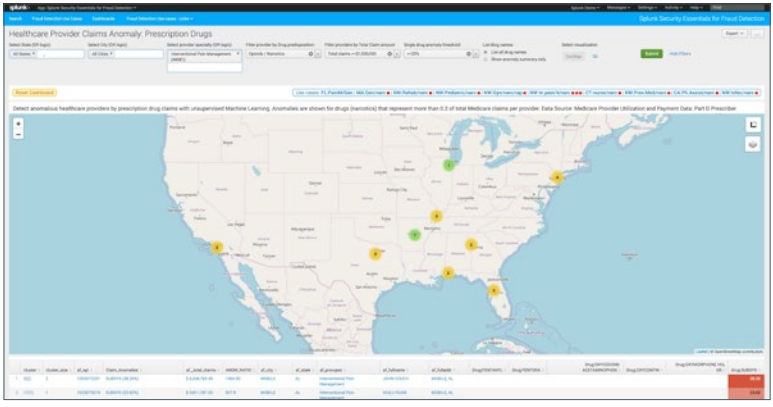
结果显示为反常值或异常值。没有明确的指示表明所显示的提供商是否是欺诈。但经过进一步的研究我们发现，在许多情况下，反常提供商（特别是开大量阿片类药剂的提供商）在我们发布数据集数年之后时不时会牵涉可疑的商业行为。

如何响应

单击某个提供商名称将打开详细的档案分析指示板。该操作可让您调查详细的处方数据并确认某个提供商的开药行为不符合其同行组在“全国范围内提供商档案与该提供商档案对比”图表中的行为。

查找反常的医疗保健提供商帮助

反常情况显示在地图上。单击黄色的圆圈将显示有关具体反常行为的摘要数据。单击某个供应商名称将打开一个详细档案分析指示板，指示板上有与给定提供商相关的具体数据。



内部威胁检测

检测大型网页上传

第1阶段

斜角攻击战术

越过封锁线

斜角攻击技术

经命令和控制通道发生渗漏

经替代协议发生渗漏

数据源

Web Proxy网络代理　NGFW

安全挑战

数据渗漏如今通常在标准通道上发生，例如经内部人员将数据上传到Google、Dropbox、Box、小文件共享站点或者甚至是未列出的回收站点。由于HTTPS始终允许数据传出，因此渗漏在大多数组织中变得相对容易。

用例

安全监视、内部威胁

类别

数据渗漏

所需Splunk解决方案

Splunk Enterprise

Splunk UBA

Splunk simple search

SPL困难程度

基础

如何实施

该项搜索应能够立即对任何Palo Alto Networks环境起作用，并且可轻松适应于代理可见性的任何其它源中。这包括专用的代理，以及网络可见性工具，如Splunk　Stream或Bro。只需调整源类型和字段进行匹配，然后即可顺利进展。

报警量

中

已知的误报

该项搜索将触发许多无辜的事件发生，比如上传假期照片等等。许多组织将通过重点关注因具有对敏感数据（高管、科学家等）的访问权限或者因雇佣原因（绩效计划、通告发布、合同终止等）而被列在观察名单上的用户，从而试图过滤掉这些事件。这些观察名单可通过使用查找操作来落实。

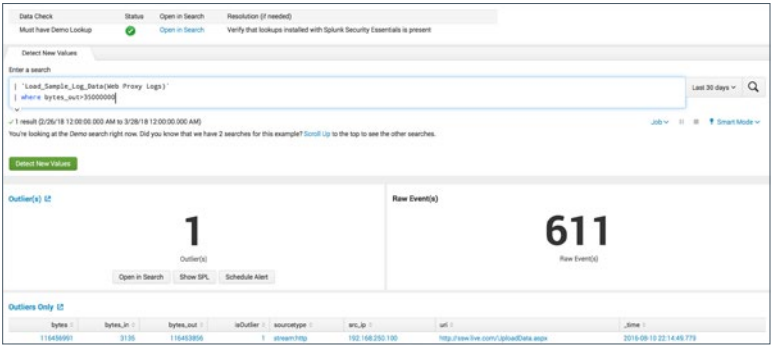
如何响应

当该警报触发时，通常是由于完全合法的原因（上传度假照片等）。作为响应，许多分析人员将查看数据发送的目的地，以及用户此前是否曾将数据上传至该站点。通常，分析人员会打电话给用户以确认活动，打电话之前最好事先了解员工在组织中的地位。例如，员工是否在执行绩效计划或即将合同期满。这两种情况均表明较大的数据渗漏风险。如果您通过针对该目的地站点的NGFW或DLP系统打开了SSL检验，有时您可以看到已传送的实际文件，从而帮助提供前后关系。

检测大型网页上传帮助

本例使用简单搜索和下面的搜索处理语言。实时搜索使用代理日志的数据集，并查找大于35MB的事件。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* sourcetype=pan:traffic OR (tag=web
tag=proxy) OR (sourcetype=opsec URL Filtering) OR
sourcetype=bluecoat:proxysg* OR sourcetype=websense*
earliest=-10m
| where bytes_out>35000000
| table _time src_ip user bytes* app uri
```



检测前职员账户的成功登录

第4阶段

斜角攻击战术

特权升级　凭证访问

斜角攻击技术

有效账户　账户操纵

数据源

验证　Windows安全

安全挑战

离开了您组织的用户通常不应登录。这可能意味着他们的凭证早前被盗用了，或者也可能意味着他们试图登录进行某些不恰当的行为。无论是哪种情况，您都希望检测到。

用例

安全监视、内部威胁

类别

账户盗用、内部威胁

所需Splunk解决方案

Splunk Simple Search Assistant

SPL困难程度

基础

如何实施

如果您遵守了Splunk Security Essentials应用程序中的数据装载指南，搜索将立即为您工作。您通常应指定存储Windows安全日志的索引（例如，index=oswinsec）。如果您使用不同于Splunk Universal Forwarder的机制来装载数据，请验证所使用的源类型和字段。剩下的就简单了！

报警量

低

已知的误报

如果您的组织并未禁用或移除账户，则该项搜索可能无法执行。如果是您，可以考虑通过指定预期会有“可接受的”离职后活动的系统来创建一些围绕该行为的边界，例如电子邮件环境。另外，将一个检测控件落实到位，以确保在员工从活动状态变为非活动状态时密码被更改。此外，尽量限制在员工离职后的账户使用。

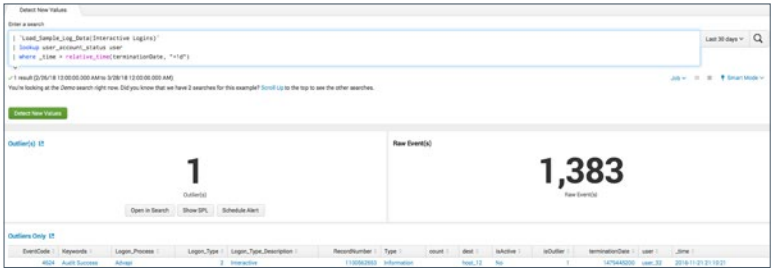
如何响应

当该警报触发时，需要了解的第一件事情是：这是正常系统运行的某些延续（例如他们办公桌底下的台式机仍处于登录状态，或者iPhone账户仍处于活动状态）还是蓄意的行为。显然，成功或失败也颇有分量。最后，尤其是对于架构简单的组织中的系统管理员类型的员工，确保在该账户下无服务或预定的作业运行，否则立即禁用该账户可能会影响运行。

检测前职员账户的成功登录帮助

本例使用简单搜索和下面的搜索处理语言通过实时数据来检测前员工账户上的身份验证活动。我们的数据集是一组匿名的、登录成功的Windows身份验证日志。通过查找可显示用户状态，查找时允许我们过滤至少一天前过期或被禁用过期的用户。下面的屏幕截图显示了对演示数据的搜索结果。

```
index=* (source=win*security OR sourcetype=linux_secure OR
tag=authentication) user=* user!="" action=success
| lookup user_account_status.csv user
| where _time > relative_time(terminationDate, "+1d")
```



学习更多内容。

准备好学习更多有关如何使用Splunk的分析驱动型安全性来改善您的安全状态了吗？从Splunkbase下载**Splunk Security Essentials**应用程序来免费了解如何应对300种不同的安全性挑战。然后与Splunk的安全性专业人员和合作伙伴协同工作，从而在您的环境中实施用例。**请联系我们**，从今天开始起航！

splunk>