事件操作改写故障排除

简介

本文在思科入侵防御系统(IPS)描述事件操作导致的可能的问题改写并且提供建议调整和排除故障您的安装。

> **注意**：事件操作改写是在签名采取的全局行动根据风险等级。如同所有全局配置，请保重与配置更改和新增内容的十分注意。

事件操作覆盖问题

说明

当该事件属于一个指定的风险等级范围时，事件操作改写添加另外的操作到签名事件。使用事件操作仔细改写。Iif您创建与一个宽风险等级范围的一覆盖频繁地被触发的事件的(特别特定，昂贵操作，例如IP记录日志操作)，您也许引起问题。

影响

额外写入到事件存储典型地关联与高CPU利用率和传感器的一般无感应性对管理访问工具的例如命令行界面(CLI)和Cisco IPS Device Manager (IDM)。

IP记录日志操作和文件描述符

文件描述符是程序用于的数据结构为了获得在文件的一个把柄;著名的描述符是0,1,2标准，标准输出和标准错误的。当进程打开一个新的文件或socket时，文件描述符创建。

如果创建一IP记录日志操作的一事件操作覆盖例如LOG攻击者数据包、LOG对数据包或者LOG受害者数据包，这也许用尽文件描述符的池;整体传感器性能也许负受影响，并且传感器可能不正常运行。

SNMP陷阱操作和事件操作改写

也有请求SNMP陷阱仅单个操作的签名生成写入到事件存储的一个提醒的事件。因此，简单网络管理协议(SNMP)陷阱操作的额外的生火也许也触发在额外看到的同样问题引起提醒的操作。

规整器引擎签名的操作

请勿添加导致事件存储写入的任何操作(例如请引起警报、请求SNMP陷阱或者LOG操作)对规整器

签名。这适用于所有1200-1330范围签名ID。

除了简要故障排除情况，您不应该使用事件操作为规整器引擎签名改写。这可以是特别有问题的在：

- 高度被分段的IP方案(由于1200范围签名)
- 大量地故障中(ooo) TCP方案(1300范围签名)

例如，事件操作覆盖导致一写入每ooo TCP数据包的事件存储能导致资源和利用率问题。

事件操作改写与风险等级0-100

一般来说，在某些情况下，因为低规定值能放置您的传感器冒险失败请避免事件操作改写与风险等级0-100。

表面上良性(和共同性)流量类型的经常阶组分签名火。阶签名寻找一个或更多阶组分签名的组合在parent阶签名前触发射击警报。默认情况下，阶组分签名没有操作关联与他们;因为他们在普通的流量，频繁地配比这是故意的。阶组分签名有默认基础风险等级15。为了排除这些签名匹配捕获在事件操作覆盖的，思科建议您比25不使用一风险等级更低，当您创建事件操作覆盖时;即风险等级不应该在25-100以下。

验证IPS利用率

命令

> **注意**：请使用命令查找工具(仅限注册用户)为了得到关于用于此部分的命令的更多信息

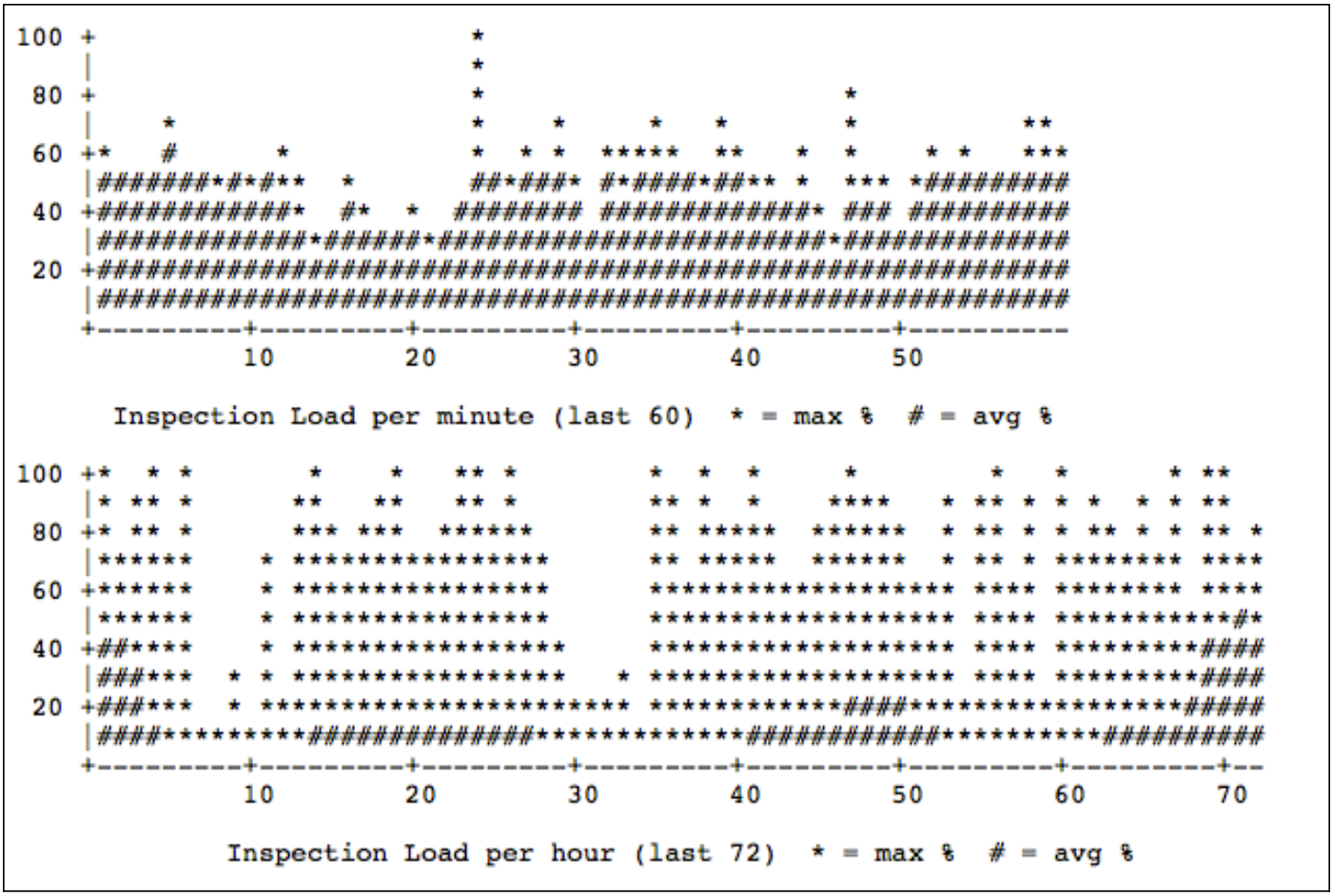
输入**show statistics虚拟传感器**on命令CLI为了寻找检查负载百分比：

```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```

在IPS版本7.0(8)E4和7.1(6)E4，**显示检查负载**命令被添加了：

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

这是从该命令的示例输出：



非常高负载百分比(90%或更加高)也许表明有事件操作触发的额外的事件改写。参考登录顺序进一步确认此可能性。

日志

额外的事件操作主要指示器改写是包裹，如在此示例main.log文件中看到的迅速事件存储：

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

一般来说，事件经常发生比的存储包裹可能每小时一次指示问题。在某些情况下，包裹是很额外的在一分钟内可能发生许多次。有许多变量，例如平台的整体功能，考虑。

故障排除

确定什么类型的事件、流量或者操作引起事件操作覆盖问题。它是否是生产警报、IP记录日志、规整器签名或者阶组件签名？

- 如果它是'话多'签名，并且确定签名创建事件的错误肯定，请写入事件操作过滤器(EAF)。
- 对于IP记录日志，思科推荐您避免EAFs或使用EAFs小心地和以对风险的完整了解。
- 规整器签名和阶组分签名不应该有一提醒的操作除了临时故障排除情况。

相关信息

- 配置事件操作改写
- IPS配置指南
- 技术支持和文档 - Cisco Systems