L'action d'événement ignore le dépannage

Introduction

Ce document décrit les questions possibles provoquées par action d'événement ignore sur le Système de protection contre les intrusions Cisco (IPS) et offre des recommandations d'accorder et dépanner votre installation.

> **Note**: L'action d'événement ignore sont des mesures globales prises aux signatures basées sur une évaluation du risque. Comme avec n'importe quelle configuration globale, prenez le grand soin avec des modifications et des ajouts de configuration.

Problèmes de priorité d'action d'événement

Description

L'action d'événement ignore ajoutent des actions supplémentaires à un événement de signature quand cet événement fait partie d'une marge spécifiée d'évaluation du risque. L'action d'événement d'utilisation ignore soigneusement. Iif vous créez un dépassement avec un grand choix d'évaluation du risque pour un événement qui est déclenché fréquemment (des actions particulièrement spécifiques et chères, telles que l'IP se connectant des actions), vous pourriez poser des problèmes.

Incidence

Excessif écrit à la mémoire d'événement sont typiquement associés avec l'utilisation du CPU élevé et l'insensibilité de général du capteur aux outils d'accès de Gestion tels que l'interface de ligne de commande (CLI) et le Gestionnaire de périphériques Cisco IPS (IDM).

IP se connectant des actions et des descripteurs de fichier

Un descripteur de fichier est une structure de données utilisée par un programme afin d'obtenir un traitement sur un fichier ; les descripteurs réputés sont 0,1,2 pour la norme dedans, la norme, et l'erreur standard. Un descripteur de fichier est créé quand un processus ouvre un nouveau fichier ou un socket.

Si vous créez un dépassement d'action d'événement pour un IP se connectant l'action telle que des log-attaquant-paquets, des log-paire-paquets, ou des log-victime-paquets, ceci pourrait épuiser le groupe de descripteurs de fichier ; la représentation globale de capteur pourrait être négativement affectée et le capteur peut ne pas fonctionner correctement.

Les actions de déroutement SNMP et l'action d'événement ignore

Une signature qui a seulement l'action simple du demande-SNMP-déroutement également génère un événement vigilant qui est écrit à la mémoire d'événement. Ainsi, la mise à feu excessive de l'action de déroutement de Protocole SNMP (Simple Network Management Protocol) pourrait également déclencher les mêmes problèmes vus avec des actions d'alerte excessives de produit.

Actions pour des signatures d'engine de normalisateur

N'ajoutez aucune action qui entraîne la mémoire d'événement écrit (comme l'alerte, le demande-SNMP-déroutement, ou les log-actions de produit) aux signatures de normalisateur. Ceci s'applique à chacun des 1200-1330 id de signature de plage.

Excepté de brefs scénarios de dépannage, vous ne devriez pas utiliser l'action d'événement ignore pour les signatures d'engine de normalisateur. Ceci peut être particulièrement problématique dans :

- scénarios fortement fragmentés IP (dus aux signatures 1200-range)
- scénarios fortement en panne de TCP (d'ooo) (signatures 1300-range)

Par exemple, un dépassement d'action d'événement qui entraîne une inscription à la mémoire d'événement pour chaque paquet TCP d'ooo peut entraîner des questions de ressource et d'utilisation.

L'action d'événement ignore avec l'évaluation du risque de 0-100

Évitez généralement l'action d'événement ignore avec une évaluation du risque de 0-100 parce que la basse évaluation peut mettre votre capteur en danger de panne dans certaines circonstances.

Les signatures composantes de méta se déclenchent souvent pour les types de trafic apparemment bénins (et terrain communal). Les signatures de méta recherchent une combinaison d'un ou plusieurs signatures composantes de méta pour déclencher avant que la signature de méta de parent se déclenche une alerte. Les signatures composantes de méta, par défaut, n'ont aucune action associée avec elles ; c'est intentionnel parce qu'ils s'assortissent fréquemment sur le trafic commun. Les signatures composantes de méta ont une évaluation du risque de base par défaut de 15. Afin d'exclure la capture de ces correspondances de signature dans un dépassement d'action d'événement, Cisco recommande que vous n'utilisiez pas une évaluation du risque inférieure que 25 quand vous créez un dépassement d'action d'événement ; c'est-à-dire, l'évaluation du risque ne devrait pas être en-dessous de 25-100.

Vérifiez l'utilisation IPS

Commandes

> **Note**: Utilisez le Command Lookup Tool (clients enregistrés seulement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section

Sélectionnez la commande de virtuel-**capteur de statistiques d'exposition** sur le CLI afin de

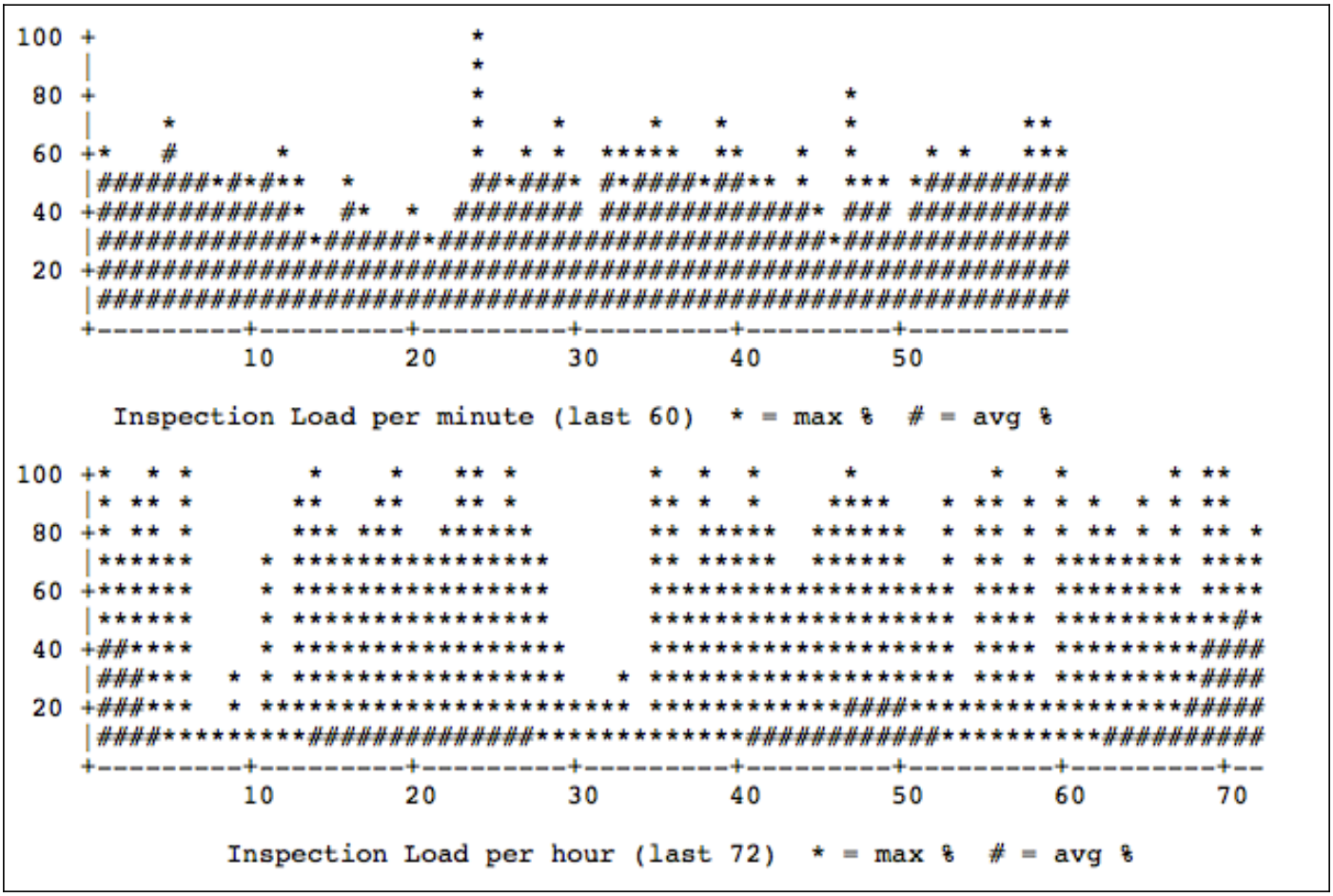
rechercher le pourcentage de chargement d'inspection :

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

Dans des versions 7.0(8)E4 et 7.1(6)E4 IPS, la commande d'inspection-**chargement d'exposition** a été ajoutée :

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

C'est exemple de sortie de cette commande :



Très un pourcentage de charge élevée (90% ou plus élevé) pourrait indiquer qu'il y a des événements excessifs déclenchés par action d'événement ignore. Référez-vous à la commande de logins pour confirmer plus loin cette possibilité.

Logs

L'indicateur principal de l'action excessive d'événement ignore est mémoire rapide d'événement s'enveloppant, comme vu dans ce fichier de main.log d'exemple :

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

Généralement l'emballage de mémoire d'événement qui se produit plus souvent qu'une fois par heure peut indiquer un problème. Dans quelques scénarios, l'emballage est si excessif qu'il puisse se produire beaucoup de fois dans une minute. Il y a beaucoup de variables, telles que la capacité de performance globale de la plate-forme, pour considérer.

Dépanner

Déterminez quel type d'événement, de trafic, ou d'action pose le problème de priorité d'action d'événement. Est-ce une alerte de produit, se connecter IP, signature de normalisateur, ou signature de composant de méta ?

- Si c'est une signature « bavarde » et vous déterminez la signature crée des faux positifs pour des événements, écrivez un filtre d'action d'événement (EAF).
- Pour l'IP se connectant, Cisco vous recommande évitent EAFs ou utilisent EAFs avec prudence et avec une compréhension complète des risques.
- Les signatures de normalisateur et les signatures composantes de méta ne devraient pas avoir une action d'alerte excepté les scénarios provisoires de dépannage.

Informations connexes

- Configurer l'action d'événement ignore
- Guides de configuration IPS
- Support et documentation techniques - Cisco Systems