IPS 5.x und höher: Optimieren der Signatur mit dem Ereignisreaktionsfilter mithilfe von CLI und IDM

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Ereignisreaktionsfilter Ereignisaktionssfilter Konfiguration von Ereignisreaktionsfiltern mithilfe der CLI Konfiguration der Ereignisreaktionsfilter mithilfe von IDM Ereignisvariable-Konfiguration Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie die Signatur mit dem Event Action Filter im Cisco Intrusion Prevention System (IPS) mit der Befehlszeilenschnittstelle (CLI) und dem IDS Device Manager (IDM) abstimmen.

Voraussetzungen

<u>Anforderungen</u>

In diesem Dokument wird davon ausgegangen, dass Cisco IPS installiert ist und ordnungsgemäß funktioniert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco IDS/IPS-Gerät der Serie 4200, auf dem die Softwareversion 5.0 und höher ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Ereignisreaktionsfilter

Ereignisaktionssfilter

Ereignisaktivitätsfilter werden als geordnete Liste verarbeitet, und Sie können Filter in der Liste nach oben oder unten verschieben.

Mithilfe von Filtern kann der Sensor bestimmte Aktionen als Reaktion auf das Ereignis ausführen, ohne dass der Sensor alle Aktionen durchführen oder das gesamte Ereignis entfernen muss. Filter können durch das Entfernen von Aktionen aus einem Ereignis verwendet werden. Ein Filter, der alle Aktionen aus einem Ereignis entfernt, verbraucht das Ereignis effektiv.

Hinweis: Wenn Sie Sweep-Signaturen filtern, empfiehlt Cisco, die Zieladressen nicht zu filtern. Wenn es mehrere Zieladressen gibt, wird nur die letzte Adresse verwendet, um mit dem Filter übereinzustimmen.

Sie können Ereignisreaktionsfilter so konfigurieren, dass bestimmte Aktionen aus einem Ereignis entfernt oder ein gesamtes Ereignis verworfen und eine weitere Verarbeitung durch den Sensor verhindert wird. Sie können Ereignisreaktionsvariablen verwenden, die Sie für die Filter in Gruppenadressen definiert haben. Informationen zum Konfigurieren von Ereignisreaktionsvariablen finden Sie im Abschnitt <u>Variablen für das Hinzufügen, Bearbeiten und Löschen von Ereignisaktionen</u>.

Hinweis: Sie müssen der Variablen ein Dollarzeichen (\$) vorstellen, um anzugeben, dass Sie eine Variable anstelle einer Zeichenfolge verwenden. Andernfalls wird der Fehler für guelle und ziel angezeigt.

Konfiguration von Ereignisreaktionsfiltern mithilfe der CLI

Gehen Sie wie folgt vor, um Ereignisaktivitätsfilter zu konfigurieren:

- 1. Melden Sie sich bei der CLI mit einem Konto an, das über Administratorrechte verfügt.
- 2. Teilmodus Ereignisaktionsregeln eingeben:
 sensor#configure terminal
 sensor(config)#service event-action-rules rules1
 sensor(config-eve)#
- 3. Erstellen Sie den Filternamen: sensor(config-eve)#filters insert name1 begin

Verwenden Sie **name1, name2** usw., um die Ereignisaktivitätsfilter zu benennen. Verwenden Sie den **Anfang. | Ende | Inaktiv | vor | nach** Schlüsselwörtern, um anzugeben, wo Sie den Filter einfügen möchten.

4. Geben Sie die Werte für diesen Filter an:Geben Sie den Signatur-ID-Bereich an: sensor(config-eve-fil)#signature-id-range 1000-1005

Der Standardwert ist 900 bis 65535.Geben Sie den ID-Bereich der Untersignatur an: sensor(config-eve-fil)#subsignature-id-range 1-5

Der Standardwert ist 0 bis 255.Geben Sie den Adressbereich des Angreifers an: sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23

Der Standardwert ist 0.0.0.0 bis 255.255.255.255.Geben Sie den Adressbereich des Opfers an:

sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255

Der Standardwert ist 0.0.0.0 bis 255.255.255.255.Geben Sie den Port-Bereich für das Opfer an:

sensor(config-eve-fil)#victim-port-range 0-434

Der Standardwert ist 0 bis 65535.Geben Sie die Betriebssystem-Relevanz an: sensor(config-eve-fil)#os-relevance relevant

Der Standardwert ist 0 bis 100.Geben Sie den Risikobewertungsbereich an. sensor(config-eve-fil)**#risk-rating-range 85-100**

Der Standardwert ist 0 bis 100.Angeben der zu entfernenden Aktionen: sensor(config-eve-fil)#actions-to-remove reset-tcp-connection

Wenn Sie eine deny-Aktion filtern, legen Sie den Prozentsatz der deny-Aktionen fest, die Sie ablehnen möchten: sensor(config-eve-fil)#deny-attacker-percentage 90

Der Standardwert ist 100.Geben Sie den Status des Filters entweder deaktiviert oder aktiviert an. sensor(config-eve-fil)#filter-item-status {enabled | disabled}

Die Standardeinstellung ist aktiviert.Geben Sie den Parameter stop on match (Stopp bei

Übereinstimmung) an.

sensor(config-eve-fil)#stop-on-match {true | false}

True weist den Sensor an, die Verarbeitung von Filtern zu beenden, wenn dieses Element übereinstimmt. **False** weist den Sensor an, die Filter auch dann weiter zu verarbeiten, wenn dieses Element übereinstimmt.Fügen Sie Kommentare hinzu, die Sie verwenden möchten, um diesen Filter zu erklären:

sensor(config-eve-fil)#user-comment NEW FILTER

5. Überprüfen Sie die Einstellungen für den Filter:

```
sensor(config-eve-fil)#show settings
NAME: name1
```

signature-id-range: 1000-10005 default: 900-65535

subsignature-id-range: 1-5 default: 0-255

attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255

```
victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255
attacker-port-range: 0-65535 <defaulted>
victim-port-range: 1-343 default: 0-65535
risk-rating-range: 85-100 default: 0-100
actions-to-remove: reset-tcp-connection default:
deny-attacker-percentage: 90 default: 100
filter-item-status: Enabled default: Enabled
stop-on-match: True default: False
user-comment: NEW FILTER default:
os-relevance: relevant default: relevant|not-relevant|unknown
```

```
senor(config-eve-fil)#
```

- 6. So bearbeiten Sie einen vorhandenen Filter: sensor(config-eve)#filters edit name1
- 7. Bearbeiten Sie die Parameter, und weitere Informationen finden Sie unter Schritte 4a bis 4I.
- 8. So verschieben Sie einen Filter in der Filterliste nach oben oder unten: sensor(config-eve-fil)#exit sensor(config-eve)#filters move name5 before name1
- 9. Vergewissern Sie sich, dass Sie die Filter verschoben haben:

```
sensor(config-eve-fil)#exit
sensor(config-eve)#show settings
_____
  filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)
  _____
  ACTIVE list-contents
  _____
    NAME: name5
     _____
      signature-id-range: 900-65535 <defaulted>
      subsignature-id-range: 0-255 <defaulted>
      attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 0-65535 <defaulted>
      risk-rating-range: 0-100 <defaulted>
```

actions-to-remove: <defaulted>

filter-item-status: Enabled <defaulted>

stop-on-match: False <defaulted>

user-comment: <defaulted>

NAME: name1

_____ signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> _____ _____ NAME: name2 _____ signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted>

<pre>stop-on-match: False <defaulted></defaulted></pre>
user-comment: <defaulted></defaulted>
INACTIVE list-contents

sensor(config-eve)#

- 10. So verschieben Sie einen Filter in die inaktive Liste: sensor(config-eve)#filters move name1 inactive
- 11. Überprüfen Sie, ob der Filter in die Liste inaktiv verschoben wurde: sensor(config-eve-fil)#exit sensor(config-eve)#show settings

_____ INACTIVE list-contents _____ _____ NAME: name1 signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> _____ _____

sensor(config-eve)#

- 12. Untermodus Exit event action rules (Ereignishandlungsregeln beenden):
 sensor(config-eve)#exit
 Apply Changes:?[yes]:
- 13. Drücken Sie die **Eingabetaste**, um Ihre Änderungen anzuwenden, oder geben Sie **no ein**, um sie zu verwerfen.

Konfiguration der Ereignisreaktionsfilter mithilfe von IDM

Gehen Sie wie folgt vor, um Ereignisaktivitätsfilter hinzuzufügen, zu bearbeiten, zu löschen, zu aktivieren, zu deaktivieren und zu verschieben:

- 1. Melden Sie sich bei IDM mit einem Konto an, das über Administrator- oder Operatorrechte verfügt.
- 2. Wählen Sie Configuration > Policies > Event Action Rules > rules0 > Event Action Filters (Konfiguration > Richtlinien > Event Action Rules > rules0 > Event Action Filters (Ereignisreaktionsfilter), wenn die Softwareversion 6.x ist. Wählen Sie für die Softwareversion 5.x Configuration > Event Action Rules > Event Action Filters (Konfiguration > Event-Action-Regeln > Ereignisreaktionsfilter) aus.Die Registerkarte Ereignisreaktionsfilter wird wie gezeigt

angezeigt.								
Eisco IDM 6.0 - 10.77.241.1	42	2						-02
Home Configuration	Monitoring	В	ack For	ward I	Refresh	? Help		cisco
Sensor Setup	Event Action	n Override ent Action	es Target ∨ n Fitters	alue Rating	Event Act	ion Filters	OS Identifications Event Va	riables General Settings
Sensor Key	Name	Active	Enabled	Sig ID) Sub	Sig ID	Attacker (address/port)	Select All
Trusted Hosts							(Add
Time								Edit
Subsers Interface Configuration								Move Up
Summary Interfaces								Move Down
Dinterface Pairs								Enable
VLAN Groups								Disable
A Bypass Traffic Flow Notificati								Dullete
Analysis Engine								Delete
Global Variables								
Signature Definitions								
E								
Anomaly Detections	4			1				31
Blocking						1	1	
Device Lonin Profiles					Apply		Reset	

- 3. Klicken Sie auf **Hinzufügen**, um einen Ereignisaktionsfilter hinzuzufügen.Das Dialogfeld Ereignisreaktionsfilter hinzufügen wird angezeigt.
- 4. Geben Sie im Feld Name einen Namen als name1 für den Ereignisreaktionsfilter ein. Ein

Standardname wird angegeben, Sie können ihn jedoch in einen aussagekräftigeren Namen ändern.

- 5. Klicken Sie im Feld Aktiv auf das Optionsfeld **Ja**, um diesen Filter der Liste hinzuzufügen, damit er bei Filterereignissen wirksam wird.
- 6. Klicken Sie im Feld Aktiviert auf das Optionsfeld Ja, um den Filter zu aktivieren. Hinweis: Sie müssen auch das Kontrollkästchen Use Event Action Filters (Ereignisreaktionsfilter verwenden) auf der Registerkarte Event Action Filters (Ereignisreaktionsfilter) aktivieren, oder keiner der Ereignisaktivitätsfilter wird aktiviert, unabhängig davon, ob Sie im Dialogfeld Ereignisreaktionsfilter hinzufügen das Kontrollkästchen Yes aktivieren.
- 7. Geben Sie im Feld Signature-ID die Signature-IDs aller Signaturen ein, auf die dieser Filter angewendet werden soll.Sie können eine Liste verwenden, z. B. 1000, 1005 oder einen Bereich, z. B. 1000-1005 oder eine der SIG-Variablen, wenn Sie diese auf der Registerkarte Ereignisvariablen definieren. Stellen Sie der Variablen mit \$ eine Vorschau vor.
- 8. Geben Sie im Feld SubSignature ID (SubSignature-ID) die Untersignatur-IDs der Untersignaturen ein, auf die dieser Filter angewendet werden soll. Beispiel: **1-5**.
- Geben Sie im Feld "Attacker Address" (Adresse des Angreifers) die IP-Adresse des Quellhosts ein.Sie können eine der Variablen verwenden, wenn Sie sie auf der Registerkarte Ereignisvariablen definiert haben. Stellen Sie der Variablen mit \$ eine Vorschau vor. Sie können auch einen Adressbereich eingeben, z. B. 10.89.10.10-10.89.10.23. Der Standardwert ist "0.0.0.0-255.255.255.255".
- 10. Geben Sie im Feld Attacker Port (Angreifer-Port) die Portnummer ein, die der Angreifer zum Senden des angreifenden Pakets verwendet.
- 11. Geben Sie im Feld "Victim Address" (Opferadresse) die IP-Adresse des Host-Empfängers ein.Sie können eine der Variablen verwenden, wenn Sie sie auf der Registerkarte Ereignisvariablen definiert haben. Stellen Sie der Variablen mit \$ eine Vorschau vor. Sie können auch einen Adressbereich eingeben, z. B. 192.56.10.1-192.56.10.255. Der Standardwert ist "0.0.0.0-255.255.255.255".
- 12. Geben Sie im Feld "Victim Port" (Victim-Port) die Portnummer ein, die der angegriffene Host verwendet, um das verletzende Paket zu empfangen. Beispiel: **0-434**.
- Geben Sie im Feld Risikoeinstufung einen RR-Bereich für diesen Filter ein. Beispiel: 85-100.Wenn der RR für ein Ereignis in den von Ihnen angegebenen Bereich fällt, wird das Ereignis anhand der Kriterien dieses Filters verarbeitet.
- 14. Wählen Sie in der Dropdown-Liste Aktionen to Subtract (Aktionen in Subtrahieren) die Aktionen aus, die dieser Filter aus dem Ereignis entfernen soll. Wählen Sie beispielsweise TCP-Verbindung zurücksetzen aus. Tipp: Halten Sie die Strg-Taste gedrückt, um mehrere Ereignisaktionen in der Liste auszuwählen.
- 15. Wählen Sie in der Dropdown-Liste Betriebssystemrelevanz aus, ob Sie wissen möchten, ob die Warnung für das Betriebssystem relevant ist, das für das Opfer identifiziert wurde. Wählen Sie beispielsweise **Relevant** aus.
- 16. Geben Sie im Feld "Prozentsatz verweigern" den Prozentsatz der Pakete ein, um Angreifer-Funktionen zu verweigern. Zum Beispiel **90**.Der Standardwert ist 100 Prozent.
- 17. Wählen Sie im Feld Stopp on Match (Auf Übereinstimmung anhalten) eine der folgenden Optionsschaltflächen: Ja - Wenn die Komponente Event Action Filters (Ereignisreaktionsfilter) die Verarbeitung beenden soll, nachdem die Aktionen dieses Filters entfernt wurdenAlle Filter, die übrig bleiben, werden nicht verarbeitet. Aus diesem Grund können keine zusätzlichen Aktionen aus dem Ereignis entfernt werden. Nein - Wenn Sie mit der Verarbeitung weiterer Filter fortfahren möchten
- 18. Geben Sie im Feld Kommentare alle Kommentare ein, die Sie mit diesem Filter speichern

möchten, z. B. den Zweck dieses Filters oder den Grund, warum Sie diesen Filter auf eine bestimmte Weise konfiguriert haben. Beispielsweise **NEUER FILTER.Tipp:** Klicken Sie auf **Abbrechen**, um die Änderungen rückgängig zu machen und das Dialogfeld Ereignisreaktionsfilter hinzufügen zu schließen.

🐔 Add Event Actio	n Filter
Name:	name1
Active:	⊙ Yes C No
Enabled:	⊙ Yes C No
Signature ID:	1000-1005
Subsignature ID:	1-5
Attacker Address:	10.89.10.10-10.89.10.23
Attacker Port:	0-65535
Victim Address:	0.0.0.0-255.255.255.255
Victim Port:	0-434
Risk Rating:	Minimum Maximum 85 - 100
Actions to Subtract:	Request Block Connection Request Block Host Request Rate Limit Request Snmp Trap Reset Tcp Connection
OS Relevance:	Not Relevant Relevant Unknown
Deny Percentage:	90
Stop on Match:	O Yes 💿 No
Comments:	NEVV FILTER
	OK Cancel Help

19. Klicken Sie auf **OK**.Der neue Ereignisreaktionsfilter wird nun in der Liste auf der Registerkarte Ereignisreaktionsfilter angezeigt, wie

dargestellt.								
Cisco IDM 6.0 - 10.77.241.1	42							
File Help								
Home Configuration	Monitoring	Ba	ck For	ward Ref	🔊 🤗 resh Help			cisco
🍓 Sensor Setup 📃	rules0							
Allowed Hosts	Event Actio	in Override:	s Target \	/alue Rating E	vent Action Filte	rs OS Identifications Ever	nt Variables	General Settings
Authorized Keys	I Use Ev	vent Action	Filters					
Sensor Key	Nome	Active	Enabled	Sig ID	SubSig ID	Attacker (address/port)		Select All
Trusted Hosts	name1	Yes	Yes	1000-1005	1-5	10.89.10.10-10.89.10.23 0-65535	0.0.0	Add
Time								Edit
Interface Configuration								Move Lip
								Move Down
VLAN Pairs								Enable
								Disable
Analysis Engine								Delete

20. Aktivieren Sie das Kontrollkästchen **Use Event Action Overrides** (Ereignisreaktionsüberschreibungen verwenden) wie

gezeigt	t.							
🕼 Cisco II	DM 6.0 - 10.77.241.14	2						
File Help								
Home	Configuration	Monitoring Ba	ck Forward	Refresh	? Help			cisco
Sensor	Setup	rules0						
Allo	work wed Hosts	Event Action Override:	S Target Value Ra	ting Event Ad	tion Filters	S Identifications	Event Variables	General Settings
B-9 59	H) Authorized Keys) Known Host Key:	An Event Action Over RR value for that even select Use Event Acti	rride lets you assign nt falls within the de on Overrides to use	a Risk Rating fined range fo any override	(RR) range to r a particular that is current	each event action action, that action by enabled.	type. If an event is added to the ev	occurs and the vent. You must
E Q Cer	tificates Trusted Hosts	Use Event Action	Overrides					
A	Server Certificate	Even	t Action		Enabled		Risk Rating	Select All
Use Use	e ers	Deny Packet Inline			Yes	90-10	0	
+ Interfac	e Configuration							Add

Hinweis: Sie müssen das Kontrollkästchen Use Event Action Overrides

(Ereignisreaktionsüberschreibungen **verwenden**) auf der Registerkarte Event Action Overrides (Ereignisreaktionsüberschreibungen überschreiben) aktivieren, oder keines der Ereignisreaktionsüberschreibungen wird aktiviert, unabhängig von dem Wert, den Sie im Dialogfeld Ereignisreaktionsfilter hinzufügen festgelegt haben.

21. Wählen Sie in der Liste einen vorhandenen Ereignisaktionsfilter aus, um ihn zu bearbeiten, und klicken Sie dann auf **Bearbeiten**.Das Dialogfeld "Ereignisreaktionsfilter bearbeiten" wird

Name:	name1
Active:	
Enabled:	Yes ⊂ No No
Signature ID:	1000-1005
Subsignature ID:	1-5
Attacker Address:	10.89.10.10-10.89.10.23
Attacker Port:	0-65535
victim Address:	192.56.10.1-192.56.10.255
victim Port:	0-434
≀isk Rating:	Minimum Maximum 85 - 100
Actions to Subtract	Request Block Connection Request Block Host Request Rate Limit Request Snmp Trap Reset Top Connection
OS Relevance:	Not Relevant Relevant Unknown
Deny Percentage:	100
	China China
Stop on Match:	Yes (* NO

angezeigt.

- 22. Ändern Sie die Werte in den Feldern, die Sie ändern müssen. Informationen zum Ausfüllen der Felder finden Sie in den Schritten 4 bis 18. Tipp: Klicken Sie auf Abbrechen, um die Änderungen rückgängig zu machen und das Dialogfeld "Edit Event Action Filter" (Ereignisreaktionsfilter bearbeiten) zu schließen.
- 23. Klicken Sie auf **OK**.Der Filter für bearbeitete Ereignisaktionen wird jetzt in der Liste auf der Registerkarte Ereignisreaktionsfilter angezeigt.
- 24. Aktivieren Sie das Kontrollkästchen **Use Event Action Overrides** (Ereignishandleraktionen überschreiben). **Hinweis:** Sie müssen das Kontrollkästchen **Use Event Action Overrides** (Ereignisreaktionsüberschreibungen **verwenden**) auf der Registerkarte Event Action Overrides (Ereignisreaktionsüberschreibungen überschreiben) aktivieren, oder es ist keine der Ereignisaktivitäts-Überschreibungen aktiviert, unabhängig von dem Wert, den Sie im Dialogfeld Edit Event Action Filter (Ereignisreaktionsfilter bearbeiten) festgelegt haben.

- 25. Wählen Sie einen Ereignisaktionsfilter in der Liste aus, um ihn zu löschen, und klicken Sie dann auf **Löschen**.Der Ereignisreaktionsfilter wird nicht mehr in der Liste auf der Registerkarte Ereignisreaktionsfilter angezeigt.
- 26. Filtern Sie in der Liste nach oben oder unten, um eine Ereignisaktion zu verschieben, wählen Sie sie aus, und klicken Sie dann auf **Nach oben** oder **Nach unten**.**Tipp:** Klicken Sie auf **Zurücksetzen**, um die Änderungen zu entfernen.
- 27. Klicken Sie auf **Apply**, um Ihre Änderungen anzuwenden und die überarbeitete Konfiguration zu speichern.

Ereignisvariable-Konfiguration

Gehen Sie wie folgt vor, um Ereignisvariablen hinzuzufügen, zu bearbeiten und zu löschen:

- 1. Melden Sie sich an. Verwenden Sie z. B. ein Konto mit Administrator- oder Operatorberechtigungen.
- 2. Wählen Sie Configuration > Policies > Event Action Rules > rules0 > Event Variables (Konfiguration > Richtlinien > Ereignisreaktionsregeln > Regeln > Ereignisvariablen), wenn die Softwareversion 6.x ist. Wählen Sie für die Softwareversion 5.x Configuration > Event Action Rules > Event Variables (Konfiguration > Ereignisreaktionsregeln > Ereignisvariablen).Die Registerkarte Ereignisvariablen wird angezeigt

angeleigi	-						_					
🕵 Cisco IDM	6.0 - 10.77.241.1	42						1	in .			_10
File Help												
Marcel	Configuration				O	Economic	Refresh	He	?			alada
rioine -	Conniguration		normoring		DOCK	Forward	heirean	1.8	ab.			cisco
Sensor Set	up 🐴	ruk	esO									
- Networ	*	F	went Antion	Over	rides Te	arnat Value R	ting Event 4	Iction F	iters or	S Identification	· Event Variables	General Settings
Allowed	d Hosts		Terit Acade	(Over	nues [14	arger value ru	any Leven A	scool i i	mers I o	5 Meriunication	6 Laron ronnero	1 oreiner ar Settings
Sol Sol	Incrimed Keye	1	Event Varia	ibles le	t you use	e the same va	lue within mut	tiple filte	ers. When	n you change i	the value of a varial	ble, all filters that
- S Kor	own Host Kev		use that var	riable :	are updat	ted with the n	ew value. If y	ou use	a variable	e in a filter, be	sure to preface the	variable with a
Ser	nsor Key	1	dollar sign ((\$) to i	ndicate th	ve value is a v	ariable and no	t a liter	al string.			
E Q Certifica	ates					1		1		1 Autor		
- 🔁 Tru	sted Hosts			Nam	e		Туре			Value		Add
Ser 🖓 Ser	rver Certificate											
Time Time												Edit .
Users												1
Pinterface Co	onfiguration											Delete
Summa	ry											
- Shtertoc	va Dairo											
VLAN F	Pairs											
- D VLAN	Groups											
Bypass												
- 🔊 Traffic	Flow Notificati											
🖳 Analysis En	igine											
Virtual S	Sensors											
Global V	Variables											
Policies	D.C.F.											
Signatu	re Definitions											
E Event A	otion Rules											
T B LIGHT	VIN 11000		1									

- 3. Klicken Sie auf **Hinzufügen**, um eine Variable zu erstellen.Das Dialogfeld Variable hinzufügen wird angezeigt.
- Geben Sie im Feld Name einen Namen f
 ür diese Variable ein. Hinweis: Der g
 ültige Name darf nur Zahlen oder Buchstaben enthalten. Sie k
 önnen auch einen Bindestrich (-) oder einen Unterstrich (_) verwenden.

5. Geben Sie im Feld Wert die Werte für diese Variable ein.Geben Sie die vollständige IP-Adresse bzw. die vollständigen IP-Adressbereiche bzw. Bereiche oder einen Satz von Bereichen an. Beispiel:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255Hinweis: Sie können Kommas als Trennzeichen verwenden. Stellen Sie sicher, dass nach dem Komma keine Leerzeichen folgen. Andernfalls wird die Fehlermeldung validation failed (Validierungsfehler) angezeigt.Tipp: Klicken Sie auf Abbrechen, um die Änderungen rückgängig zu machen und das Dialogfeld Ereignisvariable

	c ···		
hin	71 171 10	ien	711
1 111 12	Larag		20

😥 Add Event Variable	×
Name: variable1	1
Type: address	
Value: 10.89.10.10-10.89.10.23 10.90.1.1 192.168.10.1-192.168 10.255	
OK Cancel Help	

schließen.

6. Klicken Sie auf **OK**.Die neue Variable wird in der Liste auf der Registerkarte Ereignisvariablen

angezeigt. 🕵 Cisco IDM 6.0 - 10.77.241.142 - 0 File Help սիսիս О 0 2 Configuration CISCO Home Monitoring Back Forward Refresh Help rules0 Sensor Setup Network Event Action Overrides Target Value Rating Event Action Filters OS Identifications Event Variables General Settings Allowed Hosts 🖻 🔍 SSH Event Variables let you use the same value within multiple filters. When you change the value of a variable, all filters that Authorized Keys use that variable are updated with the new value. If you use a variable in a filter, be sure to preface the variable with a Known Host Key: dollar sign (\$) to indicate the value is a variable and not a literal string. Sensor Key Q. Certificates Name Type Value Add Trusted Hosts 10.89.10.10-10.89.10.23 variable1 address 10.90.1.1 Edit Time 192.168.10.1-192.168.10.255 Users Users Interface Configuration Delete Summary

- 7. Wählen Sie die vorhandene Variable in der Liste aus, um sie zu bearbeiten, und klicken Sie dann auf **Bearbeiten**.Das Dialogfeld Ereignisvariable bearbeiten wird angezeigt.
- 8. Geben Sie im Feld Wert Ihre Änderungen am Wert ein.
- 9. Klicken Sie auf OK. Die bearbeitete Ereignisvariable wird nun in der Liste auf der

Registerkarte Ereignisvariablen angezeigt. **Tipp:** Wählen Sie **Reset (Zurücksetzen)** aus, um die Änderungen zu entfernen.

10. Klicken Sie auf **Apply**, um Ihre Änderungen anzuwenden und die überarbeitete Konfiguration zu speichern.

Zugehörige Informationen

- Support-Seite für das Cisco Intrusion Prevention System
- <u>Technischer Support und Dokumentation Cisco Systems</u>