# مادختساب (PCAP فلم) ةمزحلا تانايب ليزنت بيولا مدختسم ةهجاو

# المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>خطوات لتنزيل ملف PCAP</u>

## المقدمة

باستخدام واجهة مستخدم الويب، يمكنك تنزيل الحزمة (الحزم) التي أدت إلى تشغيل قاعدة snort.يوفر المقال الخطوات اللازمة لتنزيل بيانات التقاط الحزمة (ملف PCAP) باستخدام واجهة مستخدم الويب الخاصة بنظام إدارة Sourcefire FireSIGHT.

# المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بجهاز Sourcefire FirePOWER ونماذج الأجهزة الظاهرية.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Sourcefire FireSIGHT Management Center، المعروف أيضا باسم Defense Center، الذي يشغل الإصدار 5.2 من البرنامج أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# خطوات لتنزيل ملف PCAP

الخطوة 1: تسجيل الدخول إلى مركز حماية Sourcefire أو مركز إدارة، والتنقل إلى صفحة أحداث التسلل كما يلي:

Overview	Analysis	Policies	Devices	6 Objects	Fir	eAMP
FireSIGHT Viewer Connection E		vents I	Intrusion 🔻 Fire		AMP Events	
			1	Events		
				Reviewed Ev	ents	
				Clipboard		
			1	ncidents		

**الخطوة 2:** باستخدام خانة الاختيار، حدد الحدث (الأحداث) الذي تريد تنزيل بيانات التقاط الحزمة (ملف PCAP).

Connection Events		on Events	Intrusion Events	FireAMP Events	Hosts	Applications		
		Message						
4	<b>V</b>	SERVER-WEBAPP /cgi-bin/ access (1:1668)						
4		SERVER-IIS Directory transversal attempt (1:974)						
4	V	SERVER-IIS iissamples access (1:1402)						

**الخطوة 3:** انزلاق إلى أسفل الصفحة وإما:

- انقر فوق تنزيل الحزمة لتنزيل الحزم التي أدت إلى تشغيل حدث (أحداث) الاقتحام المحددة
- انقر فوق تنزيل جميع الحزم لتنزيل جميع الحزم التي أدت إلى أحداث التطفل في طريقة العرض المقيدة الحالية

**ملاحظة**: سيتم حفظ الحزم التي تم تنزيلها على هيئة PCAP. إذا كنت تريد تحليل التقاط الحزمة، ستحتاج إلى تنزيل وتثبيت برنامج قادر على قراءة ملف PCAP.

الخطوة 4: عندما يطلب منك، احفظ ملف PCAP إلى قرصك الصلب.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيم عيف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل اقيفارت حال قمجرت لعم لاحل وه يل إم العاد عوجرل اب يصوُتو تامجرت لا مذه ققد نع امتي لوئسم Systems ال ين الم الم الي الم الم العال الم الم العال الم