Rivedere o contestare i falsi positivi IPS con Umbrella

Sommario

Introduzione

Questo documento descrive come rivedere o contestare i falsi positivi di Intrusion Prevention Service (IPS) con Cisco Umbrella.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Il Sistema di Prevenzione delle Intrusioni di Cisco Umbrella rileva (e facoltativamente blocca) i pacchetti che sono considerati associati a una minaccia nota, una vulnerabilità, ma anche

semplicemente quando il formato del pacchetto è insolito.

Gli amministratori scelgono l'elenco di firme IPS da utilizzare per rilevare le minacce in base a questi elenchi predefiniti:

- Connettività su sicurezza
- Sicurezza e connettività bilanciate
- Protezione sulla connettività
- Massima rilevazione

È importante ricordare che l'elenco di firme scelto può avere un impatto notevole sul numero di falsi positivi IPS riscontrati. Le modalità più sicure, ad esempio Rilevamento massimo e Protezione sulla connettività, dovrebbero creare rilevamenti IPS indesiderati in quanto pongono l'accento sulla sicurezza. Le modalità più sicure sono consigliate solo quando è richiesta la protezione totale e l'amministratore deve prevedere la necessità di monitorare e rivedere un numero elevato di eventi IPS.

Per ulteriori informazioni sulle diverse modalità, consultare la documentazione IPS.

Verifica rilevamenti IPS

Utilizzare Ricerca attività nel dashboard ombrello per visualizzare gli eventi IPS. Per ogni evento sono disponibili due importanti informazioni:

- Signature ID/Categoria/Nome IPS. Ricerca su https://snort.org
- Numero CVE (se applicabile). Ricerca su https://www.cve.org/

Non tutti i rilevamenti IPS indicano un attacco o un attacco noto. Molte delle firme (in particolare nella modalità di rilevamento massimo) indicano semplicemente la presenza di un determinato tipo di traffico o una violazione del protocollo. È importante esaminare le fonti di informazione menzionate in precedenza e altri dettagli sull'evento (ad esempio origine/destinazione) per determinare se l'evento richiede ulteriori indagini da parte del team di sicurezza.

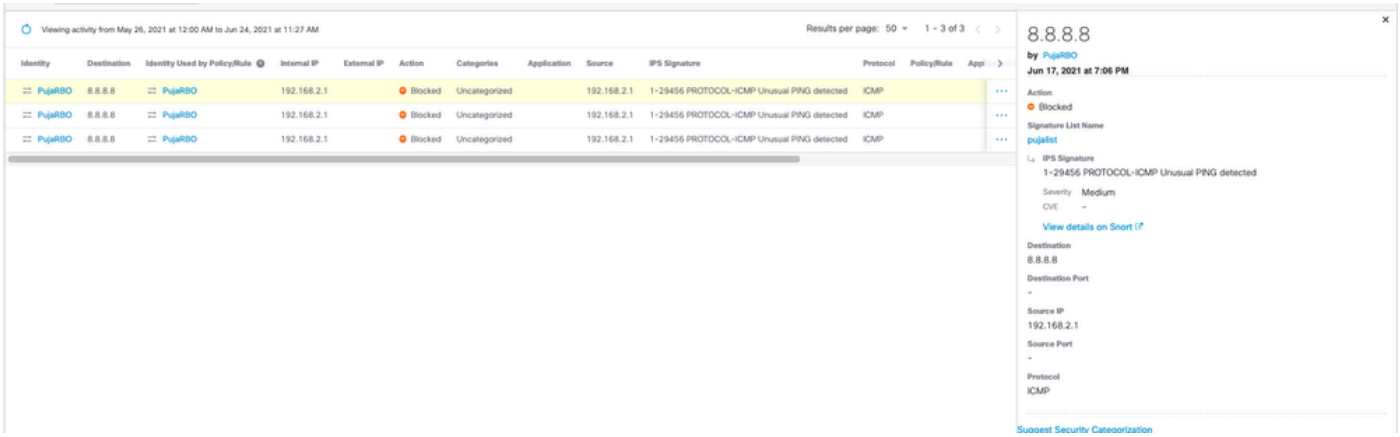
La categoria della firma può essere utile per fornire informazioni aggiuntive sul tipo di rilevamento IPS. Consulta le categorie disponibili su snort.org.

Violazioni di protocollo

Nell'esempio, un evento IPS è collegato alla firma:
https://www.snort.org/rule_docs/1-29456

La descrizione della firma è:

"La regola cerca il traffico PING in entrata nella rete che non segue il formato normale di un ping."



4403885889428

In questo caso, la regola Snort non sta necessariamente rilevando un particolare attacco, ma sta rilevando un pacchetto ICMP in formato non valido che è stato bloccato. In base alle informazioni disponibili sul sito snort.org e ad altri dettagli sull'evento (ad esempio origine/destinazione), l'amministratore può decidere che l'evento non richiede ulteriori verifiche

Compatibilità delle applicazioni

Alcune applicazioni legittime non sono compatibili con le firme IPS, in particolare quando sono configurate le modalità più aggressive (rilevamento massimo). In questi scenari, l'applicazione può essere bloccata per le ragioni descritte nella sezione Violazione del protocollo. L'applicazione può utilizzare un protocollo in modo imprevisto oppure utilizzare un protocollo personalizzato su una porta normalmente riservata ad altro traffico.

Anche se l'applicazione è legittima, questi rilevamenti sono spesso validi e non possono sempre essere corretti da Cisco.

Se un'applicazione legittima viene bloccata da IPS, Umbrella consiglia di contattare il fornitore dell'applicazione con i dettagli dell'evento/firma. Le applicazioni di terze parti devono essere sottoposte a test di compatibilità con le firme IPS all'indirizzo snort.org.

Al momento non è possibile escludere una singola applicazione/destinazione dalla scansione IPS.

Disattivazione delle firme IPS

Se viene rilevato che una firma causa problemi di compatibilità con un'applicazione di terze parti, è possibile disabilitarla (temporaneamente o definitivamente). Questa operazione deve essere eseguita solo se si considera attendibile l'applicazione e si è determinato che il valore dell'applicazione supera i vantaggi di protezione della firma specifica.

Per informazioni sulla creazione di un elenco di firme personalizzato, completare i passaggi descritti nella documentazione Aggiunta di un elenco di firme personalizzato. È possibile utilizzare le impostazioni correnti come modello e quindi disattivare le regole desiderate impostandole su Solo registro o Ignora.

Supporto

Eventi storici

Umbrella Support non è in grado di fornire ulteriori dettagli sugli eventi IPS cronologici. Gli eventi IPS segnalano che il traffico non corrisponde alla firma IPS. Informazioni dettagliate sulla firma sono disponibili al pubblico sul sito snort.org. Umbrella non memorizza una copia di traffico/pacchetti non elaborati e non è quindi in grado di fornire ulteriore contesto o conferma sulla natura di un evento IPS.

Problemi IPS / falsi positivi

Se desideri contestare un problema IPS corrente (ad esempio un falso positivo), contatta l'Assistenza Umbrella.

Per indagare su questi problemi, è richiesta l'acquisizione di un pacchetto da parte del Supporto Umbrella. Il contenuto non elaborato dei pacchetti è necessario per determinare in che modo il traffico ha attivato il rilevamento IPS. Per generare l'acquisizione del pacchetto, è necessario essere in grado di replicare il problema.

Prima di generare un ticket, utilizzare uno strumento come Wireshark per generare l'acquisizione del pacchetto durante la replica del problema. Le istruzioni sono disponibili nella knowledge base.

In alternativa, il supporto Umbrella può fornire assistenza nella generazione dell'acquisizione dei pacchetti. Devono pianificare un momento in cui il problema con l'utente o l'applicazione interessata può essere ricreato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).