Prüfung oder Anfechtung von IPS-Fehlalarmen mit Umbrella

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Intrusion Prevention Service (IPS) für Fehlalarme mit Cisco Umbrella überprüfen oder bekämpfen können.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Das Intrusion Prevention System von Cisco Umbrella erkennt (und blockiert optional) Pakete, die als mit einer bekannten Bedrohung oder Schwachstelle in Verbindung stehend betrachtet werden,

aber auch dann, wenn das Format des Pakets ungewöhnlich ist.

Administratoren wählen anhand der folgenden Standardlisten aus, welche IPS-Signaturliste zum Erkennen von Bedrohungen verwendet wird:

- Konnektivität über Sicherheit
- Ausgewogene Sicherheit und Anbindung
- Sicherheit über Konnektivität
- Maximale Erkennung

Beachten Sie, dass die ausgewählte Signaturliste die Anzahl der festgestellten IPS-Fehlalarme erheblich beeinflussen kann. Es wird erwartet, dass die sichersten Modi (wie Maximum Detection und Security Over Connectivity) unerwünschte IPS-Erkennungen verursachen, da sie den Schwerpunkt auf Sicherheit legen. Der sicherste Modus wird nur empfohlen, wenn umfassende Sicherheit erforderlich ist. Der Administrator muss sich daher darauf einstellen, dass eine große Anzahl von IPS-Ereignissen überwacht und überprüft werden muss.

Weitere Informationen zu den verschiedenen Modi finden Sie in der IPS-Dokumentation.

Überprüfung der IPS-Erkennung

Verwenden Sie die Aktivitätssuche auf dem Umbrella Dashboard, um IPS-Ereignisse anzuzeigen. Für jede Veranstaltung gibt es zwei wichtige Informationen:

- IPS-Signature-ID/Kategorie/Name Durchsuchbar unter https://snort.org
- CVE-Nummer (falls zutreffend) Durchsuchbar unter https://www.cve.org/

Nicht alle IPS-Erkennungen deuten auf einen bekannten Exploit/Angriff hin. Viele Signaturen (insbesondere im Modus für die maximale Erkennung) zeigen einfach das Vorhandensein einer bestimmten Art von Datenverkehr oder eine Protokollverletzung an. Es ist wichtig, die zuvor genannten Informationsquellen sowie weitere Details zum Ereignis (wie Quelle/Ziel) zu überprüfen, um festzustellen, ob das Sicherheitsteam das Ereignis weiter untersuchen muss.

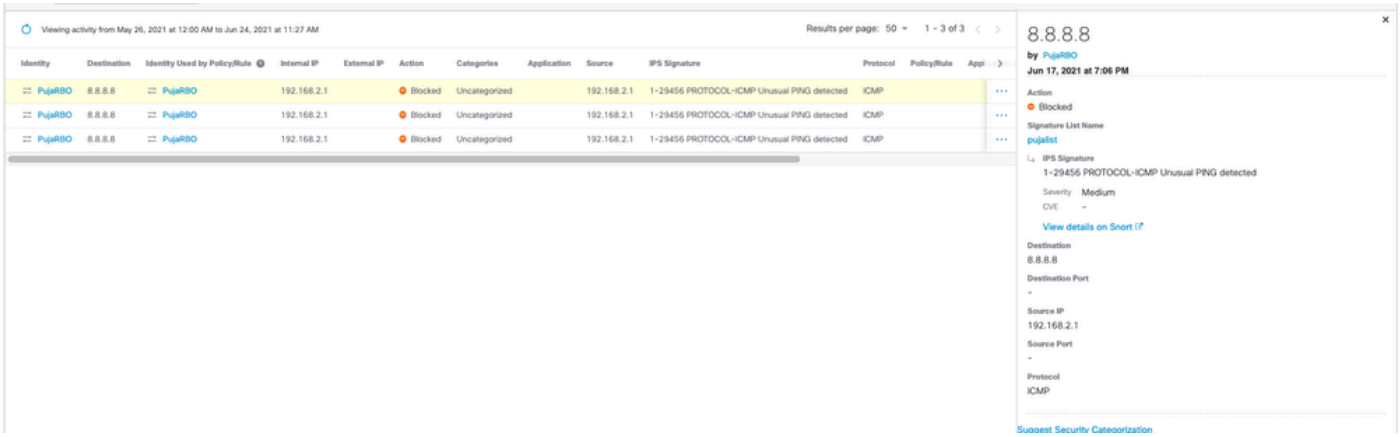
Die Signaturkategorie kann hilfreich sein, um zusätzlichen Kontext zum Typ der IPS-Erkennung bereitzustellen. Sehen Sie sich die Kategorien unter snort.org an.

Protokollverletzungen

In diesem Beispiel ist ein IPS-Ereignis mit dieser Signatur verknüpft:
https://www.snort.org/rule_docs/1-29456

Die Unterschrift ist wie folgt zu beschreiben:

"Die Regel sucht nach PING-Datenverkehr, der in das Netzwerk eingeht und nicht dem normalen Format eines PING entspricht."



4403885889428

In diesem Fall erkennt die Snort-Regel nicht unbedingt einen bestimmten Exploit, sondern ein falsch formatiertes, blockiertes ICMP-Paket. Auf der Grundlage der Informationen unter snort.org und anderer Informationen über das Ereignis (wie Quelle/Ziel) kann der Administrator entscheiden, dass keine weiteren Untersuchungen erforderlich sind.

Anwendungskompatibilität

Einige legitime Anwendungen sind nicht mit IPS-Signaturen kompatibel, insbesondere wenn die aggressiveren (Max-Detection-)Modi konfiguriert sind. In diesen Szenarien kann die Anwendung aus Gründen blockiert werden, die im Abschnitt "Protocol Violation" (Protokollverletzung) beschrieben werden. Die Anwendung kann ein Protokoll auf unerwartete Weise verwenden oder ein benutzerdefiniertes Protokoll über einen Port verwenden, der normalerweise für anderen Datenverkehr reserviert ist.

Auch wenn die Anwendung legitim ist, sind diese Erkennungen häufig gültig und können nicht immer von Cisco behoben werden.

Wenn eine legitime Anwendung durch IPS blockiert wird, empfiehlt Umbrella, den Anbieter der Anwendung mit Details zum Ereignis/zur Signatur zu kontaktieren. Anwendungen von Drittanbietern müssen auf Kompatibilität mit den IPS-Signaturen getestet werden: snort.org.

Es ist derzeit nicht möglich, eine einzelne Anwendung/ein einzelnes Ziel vom IPS-Scanning auszuschließen.

Deaktivieren von IPS-Signaturen

Wenn festgestellt wird, dass eine Signatur Kompatibilitätsprobleme mit einer Drittanbieteranwendung verursacht, kann die Signatur deaktiviert werden (entweder vorübergehend oder dauerhaft). Dies ist nur möglich, wenn Sie der Anwendung vertrauen und festgestellt haben, dass der Wert der Anwendung die Sicherheitsvorteile der jeweiligen Signatur überwiegt.

Führen Sie die Schritte in der Dokumentation zum Hinzufügen einer benutzerdefinierten Signaturliste aus, um Informationen zum Erstellen einer benutzerdefinierten Signaturliste zu

erhalten. Sie können Ihre aktuellen Einstellungen als Vorlage verwenden und dann die gewünschten Regeln deaktivieren, indem Sie sie auf Nur protokollieren oder Ignorieren setzen.

Support

Historische Ereignisse

Umbrella Support kann keine zusätzlichen Details zu früheren IPS-Ereignissen bereitstellen. IPS-Ereignisse informieren Sie, dass der Datenverkehr nicht mit der IPS-Signatur übereinstimmt. Einzelheiten zur Unterzeichnung sind unter snort.org öffentlich zugänglich. Umbrella speichert keine Kopie des Rohdatenverkehrs bzw. der Rohdatenpakete und kann daher keinen weiteren Kontext oder keine Bestätigung über die Art eines IPS-Ereignisses bereitstellen.

IPS-Probleme/Fehlalarme

Wenn Sie ein aktuelles IPS-Problem anfechten möchten (z. B. ein False Positive), wenden Sie sich an den Umbrella Support.

Um diese Probleme zu untersuchen, ist eine Paketerfassung durch den Umbrella Support erforderlich. Der Rohinhalt der Pakete wird benötigt, um zu bestimmen, wie der Datenverkehr die IPS-Erkennung ausgelöst hat. Sie müssen in der Lage sein, das Problem zu replizieren, um die Paketerfassung zu generieren.

Verwenden Sie vor dem Auslösen eines Tickets ein Tool wie Wireshark, um die Paketerfassung beim Replizieren des Problems zu generieren. Eine Anleitung finden Sie in unserer Wissensdatenbank.

Alternativ kann Umbrella Support Sie bei der Erstellung der Paketerfassung unterstützen. Sie müssen einen Zeitpunkt festlegen, zu dem das Problem mit dem betroffenen Benutzer oder der betroffenen Anwendung erneut auftreten kann.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.