## **Detect data exfiltration**

data exfiltrationبسم الله الرحمن الرحيم اليوم بشرح كيف تقفط ال

## data exfiltration

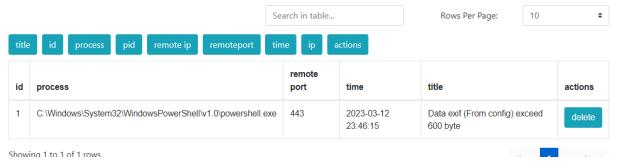
لما المخترق يوصل للجهاز الجهاز ممكن يكون فيه ملفات حساسة مثل قواعد بيانات او backup او المخترق واح يحاول ينقلها على جهازه ف اي ملفات office ممكن تحتوي على معلومات حساسه ف المخترق واح يحاول ينقلها على جهازه ف بيخليها تمر عبر الشبكة

## Demo

هنا عندنا ملف ال config يحتوي على حاجتين ال path حق اي بروسيس مسموحة انها ترفع زي ما تبي و اي agent غير متواجد راح يراقبه ال agent في الحين انا اقول لل agent غير متواجد راح يراقبه ال agent في الحين انا اقول لل Code.exe لو يرفع 10 قيقا بايت عادي الجهاز و اي عمليه ترفع فوق ال 600 بايت عطني alert طبعا alert لأنه يعتبر alert

الحين راح ارسل ويب ريقويست باستخدام powershell و راح اشوف هل راح يطلع alert او لا

## connections alerts



طلع معي بدون اي مشاكل الحين اوك كيف تشتغل الميزه هذي؟

باختصار ال agent راح يراقب ال tcp connection و بيشوف البروسيس هذي كم بايت ارسلت و بناء على الشي هذا تعطي alert او لا مثال:

لو انت حاط ان الحجم اللي المفروض ترسله البروسيس 1 كيلو بايت و البروسيس سوت 10 connections و مجموع البايتات اللي انرسلت 2 كيلو بايت راح يعطيك alert لأنه ما يراقب كل ارسال هو يراقب الاتصال كامل ف حتى لو ارسل الملف مقسم مافيه فايدة