Detect data exfiltration

بسم الله الرحمن الرحيم اليوم بشرح كيف تقفط الdata exfiltration

data exfiltration

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

Demo

```
"data_exif_size":600,
     "whitelist_network_processes_exif":["C:\\Users\\kira2\\AppData\\Local\\Programs\\Microsoft VS Code\\Code.exe",]
```

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

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

connections alerts

Search in table...

Rows Per Page: 10

title | id | process | pid | remote ip | remoteport | time | ip | actions

id	process	remote port	time	title	actions
1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	443	2023-03-12 23:46:15	Data exif (From config) exceed 600 byte	delete

Showing 1 to 1 of 1 rows

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