バイアスと戦う術

Techniques to Combat Bias

Presented by mmmtzzZZ

「できてる」「やれてる」という思い込み

その１

Q.　セキュリティ対策はなにをやっていますか？
A.「マルウエア対策ソフト名をいれてます！」

Q.　他には？
A.「セキュリティ対策は、マルウエア対策ソフトでできている
　とおもっています。」

「できてる」「やれてる」という思い込み

その２

Q.　セキュリティ対策はなにをやっていますか？
A.「資産管理ソフト名をいれて、ログをとっています。」

Q.　EDRは使ってないですか。
A.　EDRってなんですか。
　　セキュリティ対策は、資産管理ソフトで全部やれてます。

「できてる」「やれてる」という思い込み

その３

Q.　セキュリティ対策はなにをやっていますか？
A.　 EPP/EDRをいれてます。

Q.　ADのログ分析はやってますか。
A.　やっていません。EDRをいれているから大丈夫。

不都合な現実

- 実際の侵害事案では、EPP/EDRでなにか疑わしいアラートがでていないということは、ふつうに起きています。

- 業界リーダーといわれているEDRでも、アカウント周りの侵害事案については、悪性のサインインということでアラートを出すことが難しいです。

- ましてや、資産管理ソフトの追加オプションで操作ログが取得できるという機能では、サイバー攻撃の検知はムリです。

積み上げ型のセキュリティ

怖いポイント：

例えば、エンドポイントセキュリティ製品が導入されているとそれで対策済みとされてしまいがち。

実際の手口に対して、検知するかどうか確認していない、導入したシステム担当は、運用として管理センターを確認するようなことがなかったとしても、「製品を導入しているからOK」と考えてしまうことがある。

確証バイアス　Confirmation Bias

- 自分の思い込みや願望を強化する情報ばかりに意識が向き、そうではない情報は軽視する。
  いわゆる、RAS※が働く。

- 正しいことを確認したいなら、仮説が間違っていないかを確認すべきだけど
  そこまでやらないで済ます。
  でも、それでOK

※ RAS（らす）は、「Reticular Activating System」の略で、脳幹網様体賦活系という脳機能の1つ。
自分の興味・関心のある情報を無意識に多くインプットする「フィルター」のような役割を果たします。

正常性バイアス　Normalcy Bias

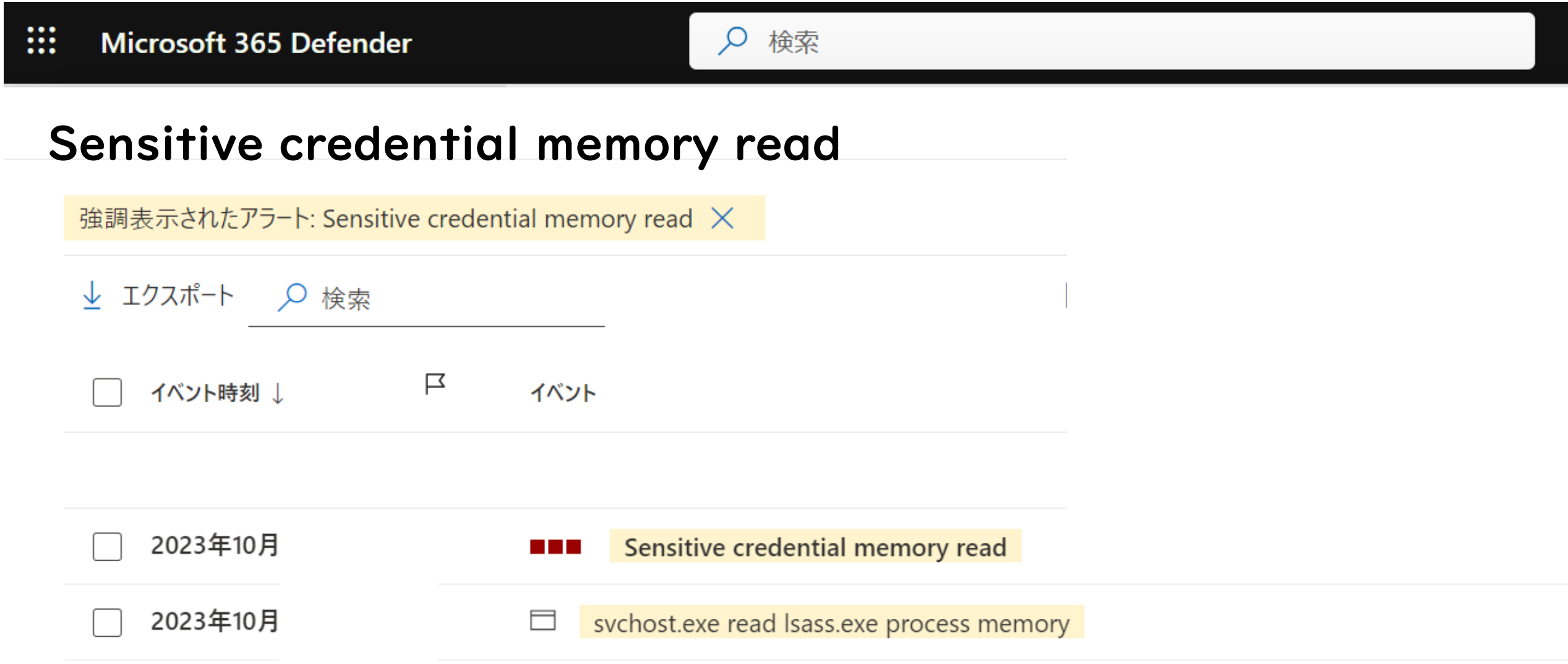
- 過去の経験（例：起きていない）から「大丈夫」と思い込む

同調性バイアス　Conformity Bias

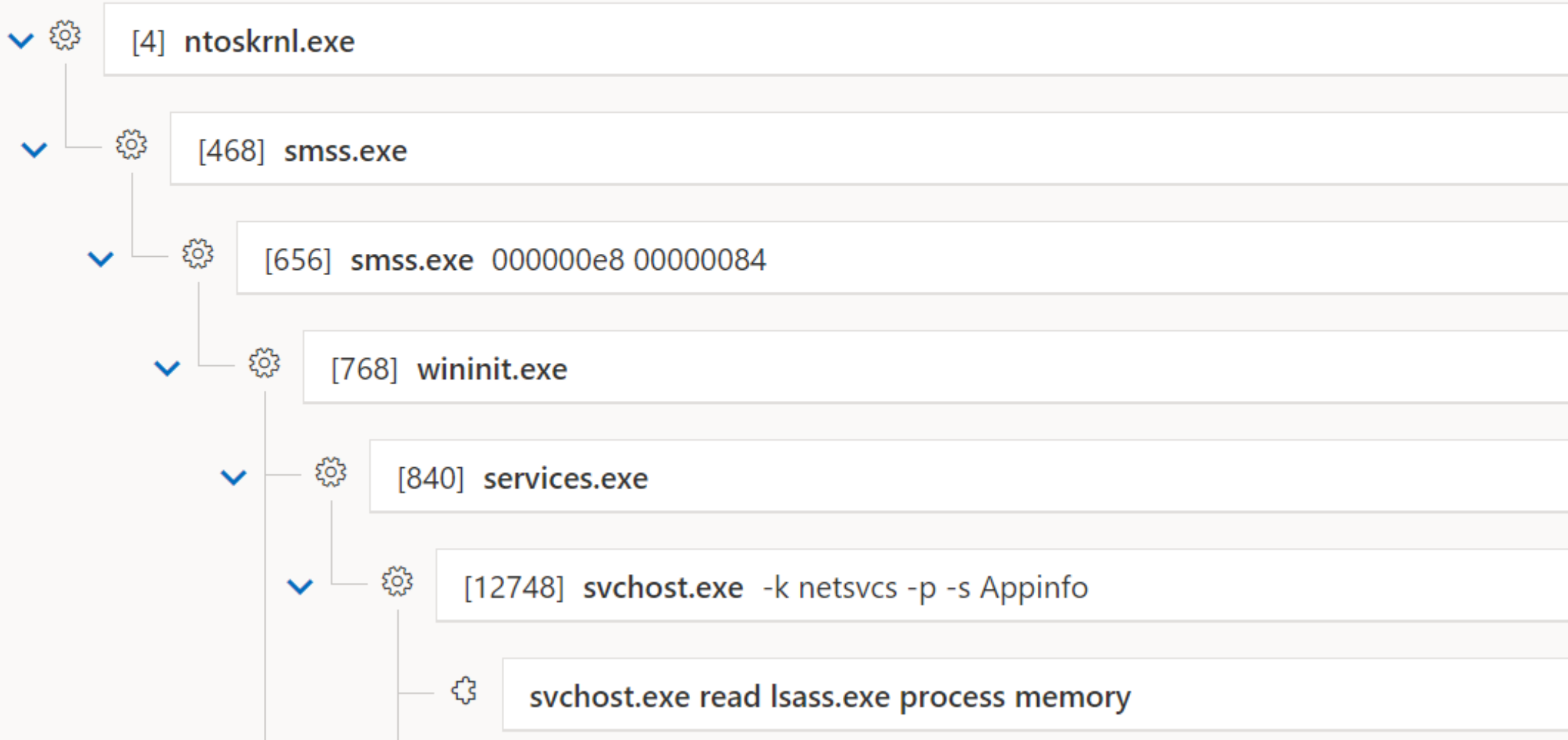
- 他の人もやっていないから、他と同じだから
  じぶんも「大丈夫」と思い込む

とある日　M365 Defenderアラート

https://www.microsoft.com/en-us/security/blog/2022/10/05/detecting-and-preventing-lsass-credential-dumping-attacks/
https://www.microsoft.com/en-us/security/blog/2019/05/09/detecting-credential-theft-through-memory-access-modelling-with-microsoft-defender-atp/



アラートのストーリー



資産管理ツール取得ログ　Lsass.exeはなし

当日の投影ONLY

どうすればシステム/セキュリティ担当者のバイアスと戦えるか？

How to combat the bias whose in charge of system/security:

① 侵害される手口（実績あり）に対して、検知できる/できないをツールの検知状況を説明する。

・動画や解説ブログ

② 製品比較などのレポートはあるが
担当者の興味を引くように、ありがちな事例での結果比較をつけてみる。

自分ひとりじゃ無理だな・・・

- 一人でやるのは到底無理だとおもうので
  防御側は協力できたらうれしいです。

- I spend days of thinking of that achieving cybersecurity is really difficult.
  I think it would be impossible to do it alone, so I would be happy if the defenders could cooperate with trusted friends.