



# THREAT HUNTING

...looking (also) outside the EDR

# AGENDA



Intro



When do  
people hunt?



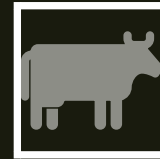
Setting up the  
(incident) scene



Let's go hunting



Better hunting



Don't get  
hunted



# Intro





# When do people hunt?

Answer: when they're hungry



A decorative L-shaped bar in the top-left corner, composed of a vertical bar and a horizontal bar meeting at a right angle.

Translating this to security talk

>>> When an incident puts pressure on a company threat hunting program get a boost (or a start, depends on the case).



# Setting up the (incident) scene

- Introduction and orientation
- First customer meeting (s)

## (a) Typical scenario for a security incident

- all (security related) logs in SIEM
- correlations in place
- EDR licensed and updated to include full command line logging and relevant intel
- ...so, we can start hunting and solve our incident!



Isn't it?

Did this ever happen  
to you?  
(or outside let's say if  
you work for the top X  
banks in the country)



# One should be happy if

- There IS a SIEM
- There IS an EDR
- The SIEM has default correlations in place and has a minima of sources like EDR alerts, firewall logs



# Typical dreams crushers

- The SIEM correlations have never been reviewed, improved or customized with one's business needs
- Quite some security logs are not (yet) in the SIEM (costs/ in-out clouds, not knowing all sources producing security logs/ shadow IT/ costs / volumes, costs/efforts in formatting and processing logs)
- The EDR is so basic that it sounds more like an AV from the 90's



# DON'T PANIC!

(And carry a towel)

Towel reasoning:  
you might need to  
spend some time on  
the incident / bring  
emergency bag.

# First meeting:

- Make sure you get access to the right contacts
- Make sure you get access to the logging in place
- When something is not clear : ASK QUESTIONS!!!
- Make sure you get the overview picture or design



AND DON'T FORGET...

WHEN  
SOMETHING IS  
NOT CLEAR


**ASK QUESTIONS YOU DO.**



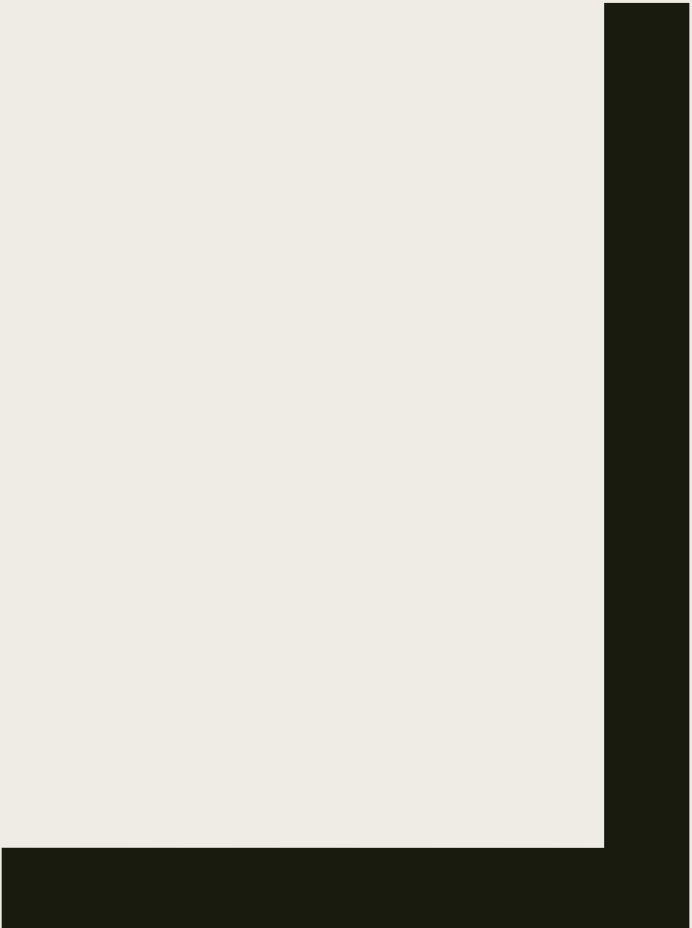

Let's see an example ...

# What is this large data transfer?

- You see this in flow logs, firewall logs, storage logs
- Most flows nowadays are TCP 443
- Maybe a legit app usage or backup
- Maybe a 3<sup>rd</sup> party business function
- What if large transfer on port 80?
- You will not see this in the EDR logs...



WHAT ABOUT JIM IN SALES?  
WHAT ABOUT JOEL IN HR?  
WHAT DO YOU THINK THEY  
HAVE IN COMMON?





**I KNOW WHAT YOU'RE THINKING**

**BUT THIS ISN'T WHERE YOUR  
STUFF IS STORED**

# The wonders of shadow IT ! ... yet another TCP 443 flow

- Jim and Joel bought these cloud services to make their work easier
- They paid with own cc to speed up things and just declared costs
- No business impact analysis on what data goes up and down? (data classification much?)
- They agreed to the big popup informing them that data will be kept in this cloud service for an X amount of time
- They didn't setup MFA because ... well, too much effort
- They got an admin panel with security logs,  
but no one asked them  
to import these logs in the SIEM (why?)
- It will be a true adventure to correlate the large data flow we were speaking about to these services and their owners within customer realm



# What do you do as a security incident investigator?

- Add new information to your overall picture
- Record the moments in time when these new findings took place **(use UTC!!!)**
- Try to get access to review new security relevant logs when a new source has been identified
- Include in your note when did you get access to these new category of logs
- If very dangerous findings think of next steps (known full cloud compromise / security incident log located/ no MFA/ etc)



How to process that large csv / logs from alternate sources (the excel-crash type of thing)?

For large files: **Timeline explorer** (it's free!)

<https://ericzimmerman.github.io/#!index.md>

For very large files: **SOF-ELK** (also free)

<https://github.com/philhagen/sof-elk>

Filter what you  
need and add to  
your notes >>>



UTC!!!

Why I keep pushing this?





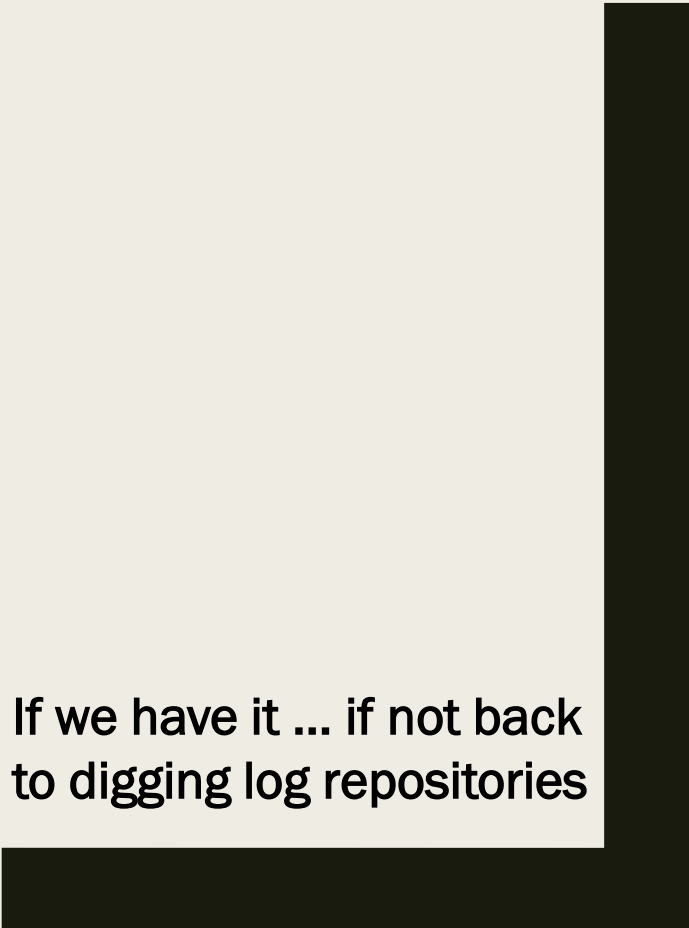
# Let's go hunting

... add a bit of time pressure as we are facing a live incident



BACK TO OUR SIEM

If we have it ... if not back  
to digging log repositories





# Few things to keep in mind

- There is a delay between live events and the SIEM log arrival (most cloud tooling has these delays published)
- SIEM will have less logs than the EDR for an endpoint, but it can point you in the right direction
- You still need to go to the EDR or host logs for more details, features, digging
- If firewall logs are too costly, try a small selection first: outgoing for example (what do you think it's more interesting: outgoing dropped or outgoing allowed?)
- If no EDR you will need to check (with the help of an admin) windows/linux server logs – and hope, there is a central logging repository



## Best way to know an environment is to run your hunts

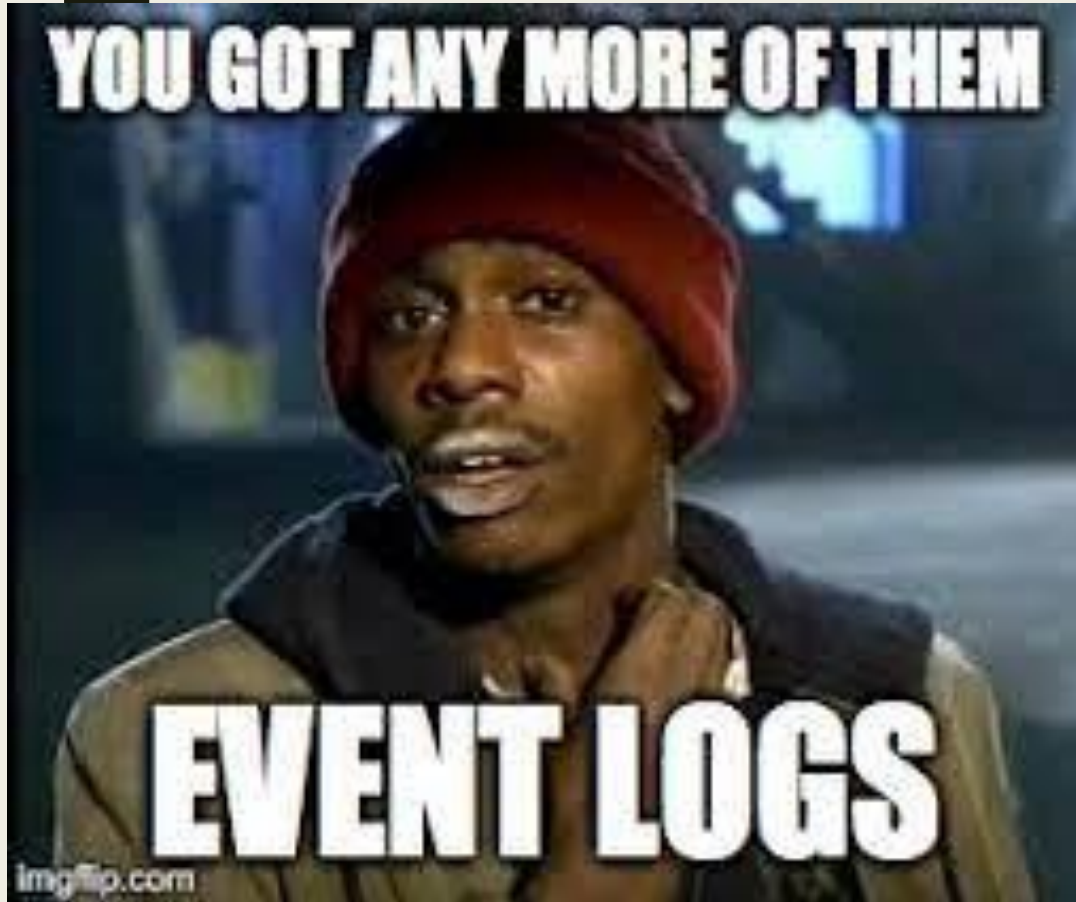
- Command history
- Scheduled tasks
- Encoded PS
- PS downloads
- New accounts
- Recon commands from LOCAL SYSTEM (netstat/whoami/at...)
- New services
- New scheduled tasks
- RDP using high privileged accounts
- Processes started from the recycle bin ....

Not all the things are bad, but at least we know who/what they are



# Syntax

... it is important to know what you are looking for/ local admin will help you get it (and if not google and experience after a while)



EDR logs are an excellent hunting ground but it can become an addiction – don't panic when it's not there.

# Few other hunts ideas

- Create statistic hunts: top rare present process names, stats and counts on used wmi commands, top and count for 1-2 chars file names
- Event logs being cleared ("Microsoft-Windows-Eventlog", 1102 or 517/ "PowerShell log file was cleared", 104/ "System log file was cleared", 104)
- Hidden files, hidden shares (\\$)
- RDP successful login stats (logon type 10/ 4624 or 528)
- Statistics on overall file extensions and counts (interesting if encrypted/ atypical extensions or misspelled extensions are found)

# Few well-known persistence locations

Create statis and hunts for some locations:

Software\Microsoft\Windows\CurrentVersion\Run and \Runonce

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run and \Runonce

Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

Imagine you have a baseline here!





Or create a script  
to deploy and  
run autoruns on  
**EVERYTHING!**

<https://docs.microsoft.com/en-gb/sysinternals/downloads/autoruns>

A decorative L-shaped bar in the top-left corner, composed of a vertical white bar and a horizontal light gray bar.

If you have an EDR and intel feeds:

- It will be very precise to follow all persistence locations
- Intel feeds will push persistence locations typical for the threats in your domain and geography
- Or if you have a good one it will run stats and counts on ALL your files!

## Limitations -

- and need for correlations

- What about that critical alert about a connection out to a C2, identified by the EDR intel?
- Did the C2 contact really took place?
- Don't forget: (if) EDR runs ON a host, it won't go trace your packet in the network!!!





- Do you have proxy logs to correlate?
- Do you have firewall logs to correlate? (remember: which outgoing firewall logs are the most interesting?)
- Do we have intel feeds on all these devices?
- Are they DIFFERENT feeds with DIFFERENT (quality of) intel?



A decorative L-shaped bar in the top-left corner, composed of a vertical white bar and a horizontal light gray bar.

Question:

Considering the traffic path: infected host, process starts, trying to connect out to a C2.

Where is the most logical next step to have the layered approach to terminate this flow in path towards the C2? (in most cases EDR will allow a process to run first few seconds, or, if unknown as bad yet, for a longer amount of time)

Host trying to connect out to  
some\_bad\_place\_running\_malware.ru ...





- Ideally traffic should be blocked as close to the source as possible

OR

- Before leaving the enterprise domain/ infra setup

SOOOOOO....

- Ideally block right at DNS lookup/ DNS server

OR

- The latest at proxy or boundary firewall



How often did you encounter a DNS server using intel feeds? (being able to and using)

# What if you can have it all?

- Host based filter for malicious domains
- DNS server filters and intel
- Proxy filters for bad reputations assets
- Firewall filters, intel, young domains cap



**USE ALL THE LAYERS!!!**





## Better hunting

- There are a lot of potential improvements for the hunting processes which can be suggested after solving an incident
- Not many IR teams consider security improvements as an IR step



## ■ One such very brave example:

<https://github.com/WillOram/AzureAD-incident-response>

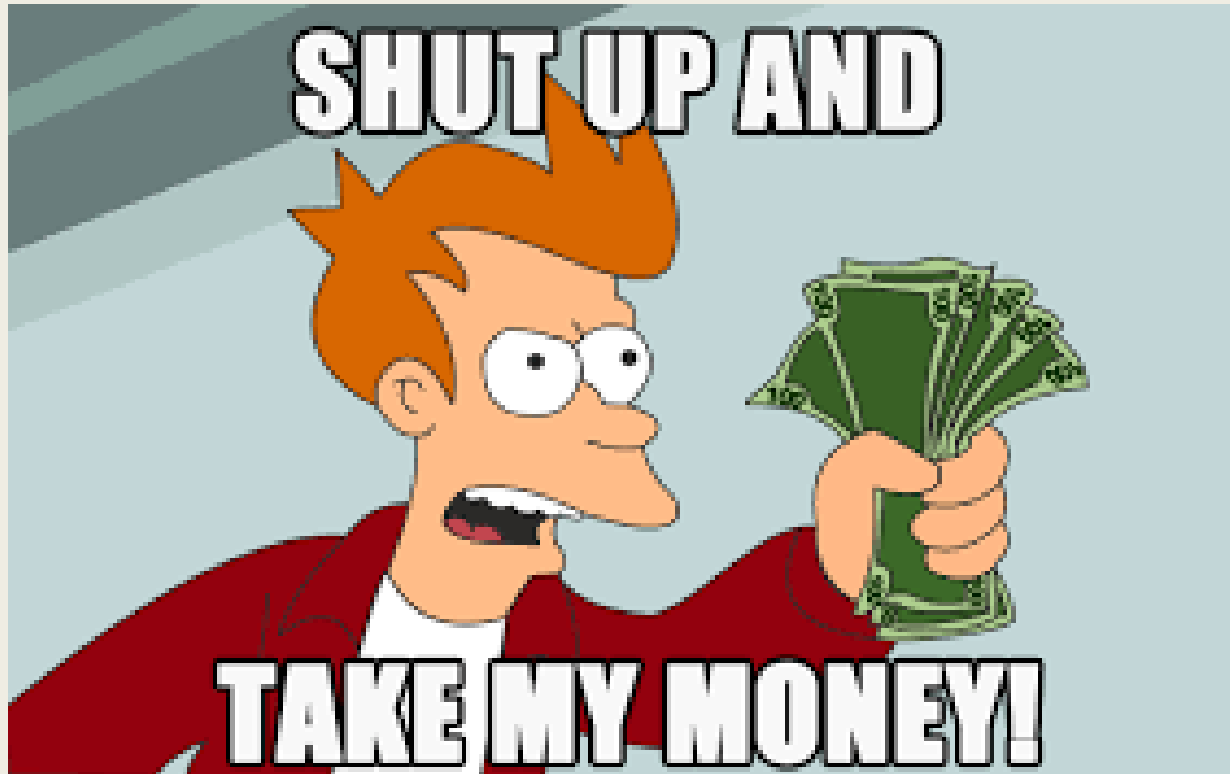
1. Mobilise the incident response team and secure their communications
2. Understand how users are authenticated, and how Azure AD and Microsoft 365 are configured
3. Identify and export available logs and configuration information
4. Investigate the extent of the attacker activity and the access the attacker has gained to the environment
5. Take immediate containment measures to remove attacker access to known compromised accounts and identities (Optional)
6. Perform a more comprehensive review to identify any persistent access the attacker has gained to accounts, systems or data
  - Hunt for modifications to the configuration of the Azure AD tenant
  - Hunt for Golden SAML Attacks
  - Hunt for the compromise of privileged accounts
  - Hunt for hijacked Azure AD Applications and Service Principals
  - Hunt for malicious modifications to mailboxes and the Exchange Online configuration
  - Hunt for illicit application consent attacks
  - Hunt for the compromise of on-premises systems and accounts
  - Hunt for the compromise of and malicious changes to Azure resources
7. Monitor for further attacker activity and prepare to rapidly respond
8. Regain administrative control and remove all attacker access
9. Assess data accessed and / or exfiltrated by the attacker
10. Improve security posture to defend against further attacks



# Worth considering

One major improvement for a lot of organizations in building an **intel sharing automation** or using an **intel sharing platform** to process all the feeds they buy from different sources





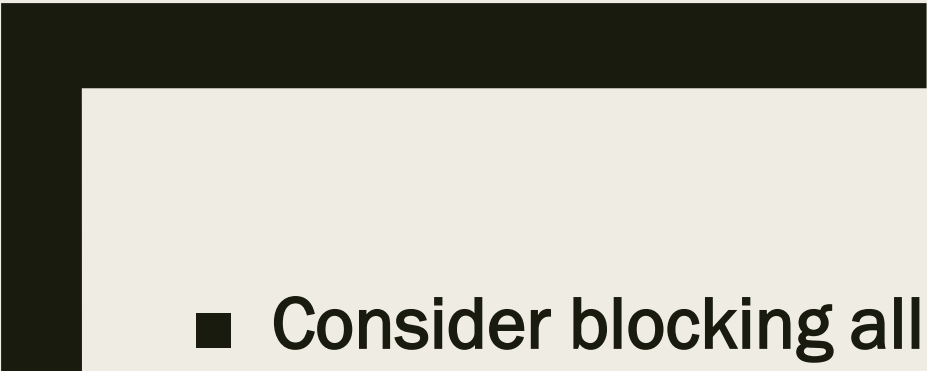
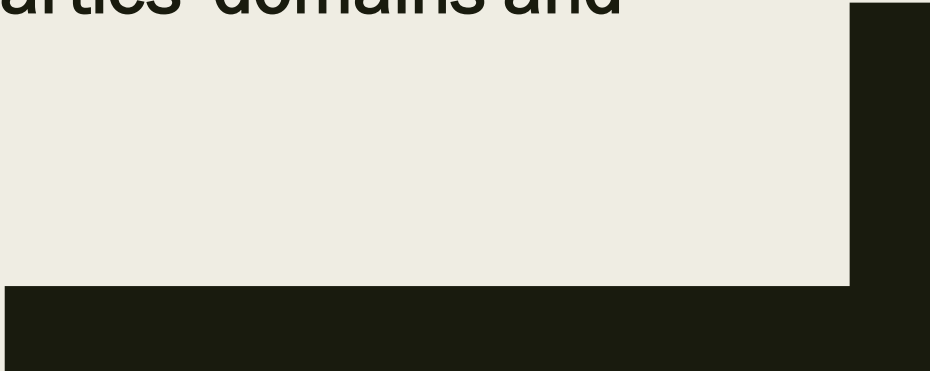
MANY EVEN BUY THE  
SAME INTEL TWICE !!!

**Advice: investigate before you decide to buy an intel feed (EXPENSIVE!!!) for overlap with intel you already use and plan to use the intel in every project able to consume.**

# Also... SEGMENTATION!

You can buy a top-of-the-line EDR, click on a spear phishing and still face risks if every project you are running runs happily together in vlan 1.



- 
- Consider blocking all domains which are newer than few weeks (1 – 4 weeks, most common choices)
  - Feature present in many proxy and firewall tooling: USE IT!!!
  - You can always exclude own and 3<sup>rd</sup> parties' domains and subdomains.
- 

Quick win!



Question:

Which one is the **best intel** you can have?

# Remember this slide?

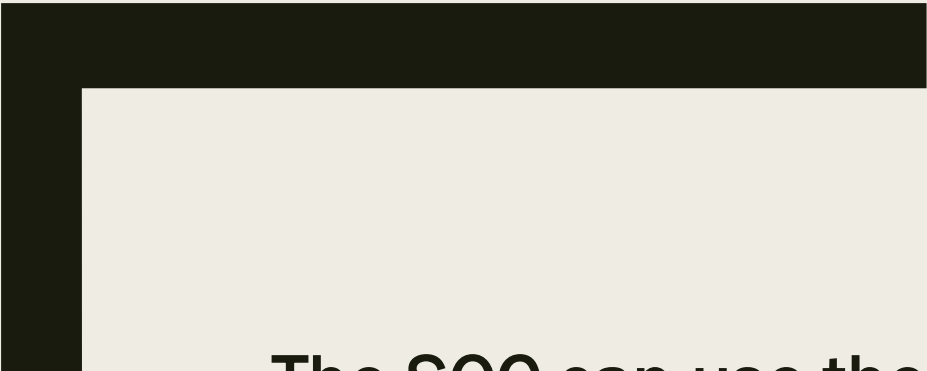

Best way to know an environment is to run your hunts

- Command history
- Scheduled tasks
- Encoded PS
- PS downloads
- New accounts
- Recon commands from LOCAL SYSTEM (netstat/whoami/at...)
- New services
- New scheduled tasks
- RDP using high privileged accounts
- Processes started from the recycle bin ....

Not all the things are bad, but at least we know who/what they are



**Well, this is intel which is created in your own context.  
This is the non degraded by time or external setup.**

- 
- The SOC can use the hunts to create alerts once the query is adapted to identify the outliers
  - It should be a process where hunting feeds SOC intel for their alerts even outside an incident situation
- 

**BONUS!**





# Don't get hunted

- Don't forget smart adversaries ALSO hunt during incidents (aka they might setup automations to alert on security response activities)
- Beware of where from you run your hunts, under what account, what queries and where the results get stored – so the intruder doesn't notice your activities, or even worse ... starts influencing your results

