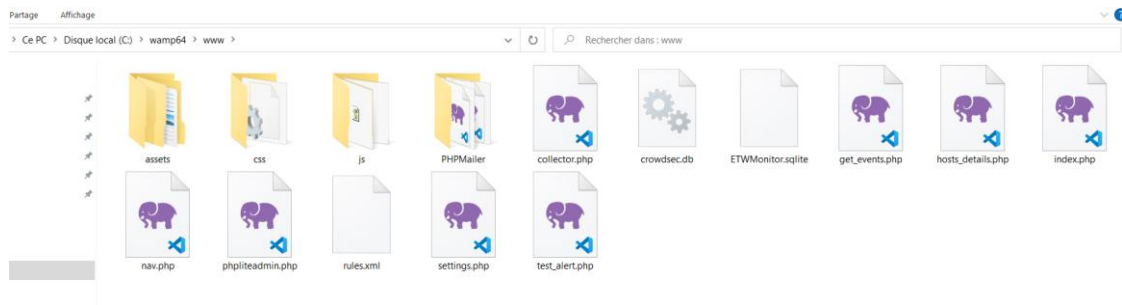




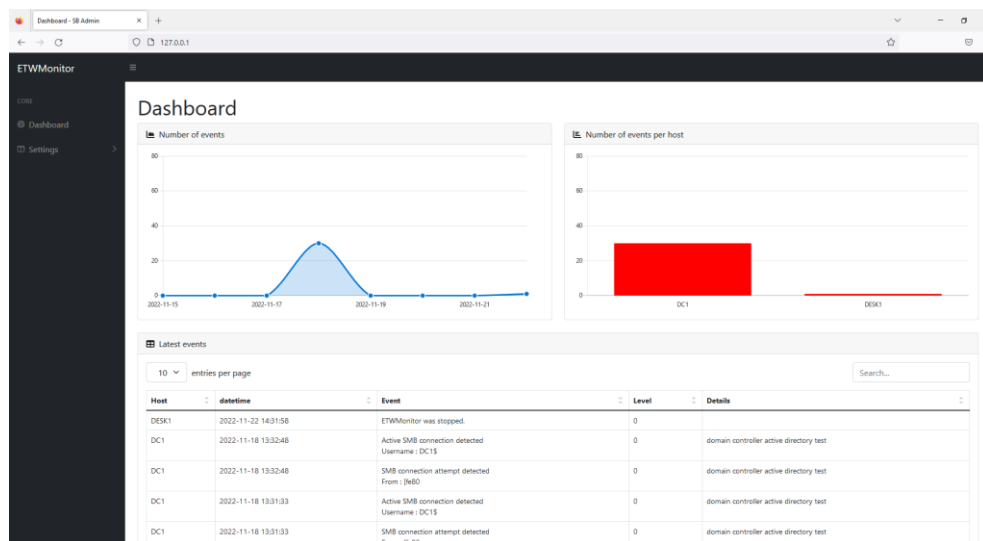
ETW Monitor

HOW TO INSTALL CLIENT-SERVER VERSION

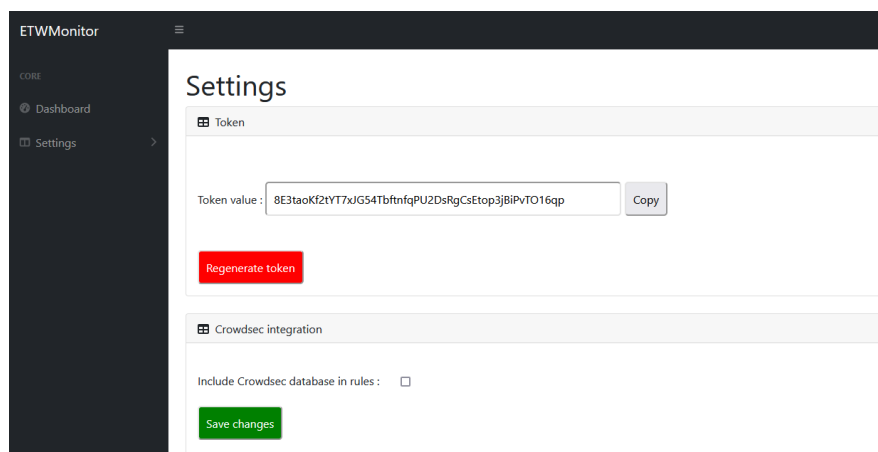
Processus Thief



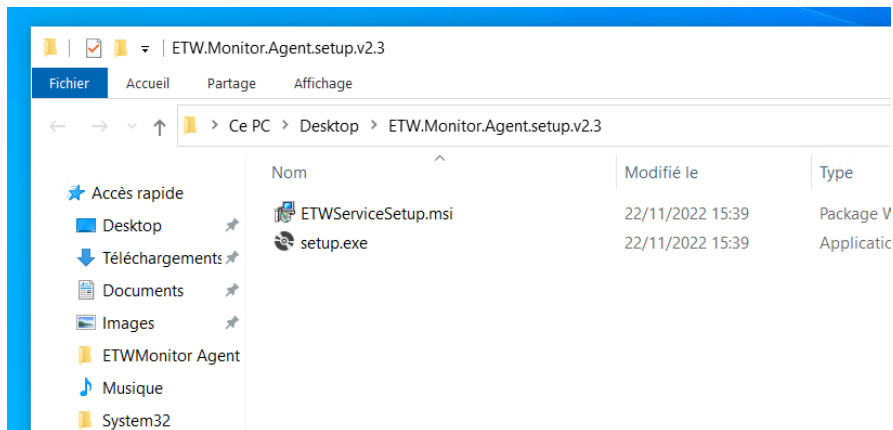
1. Unzip server files into web server folder



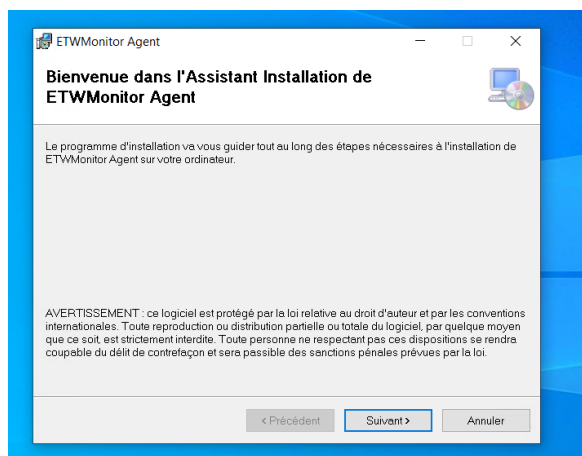
2. Go to the web dashboard



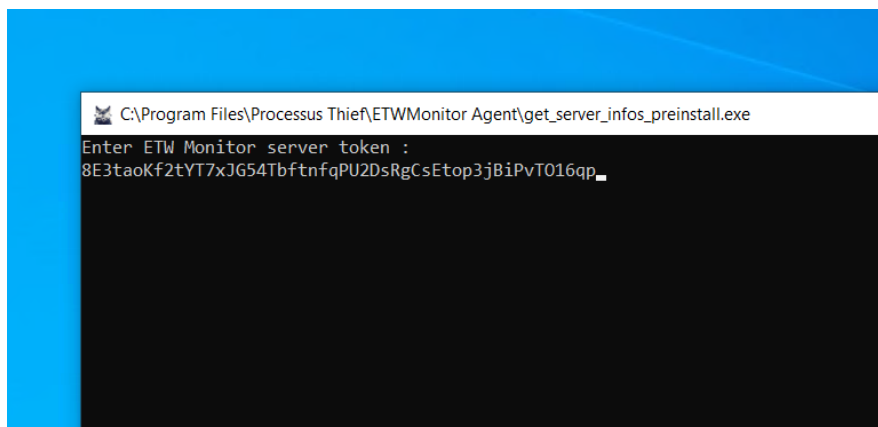
3. Go to settings and copy the token value in your clipboard



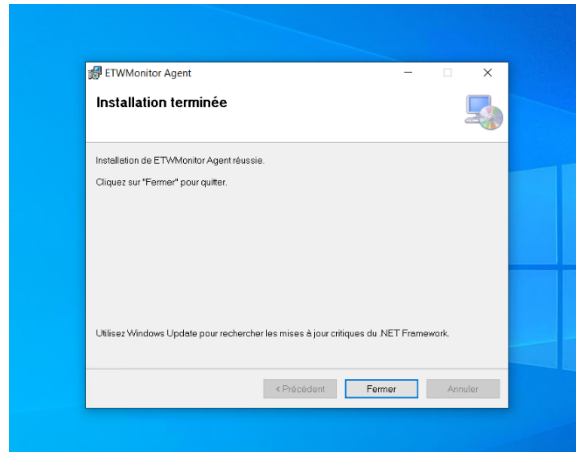
4. On your endpoint, unzip agent folder



5. Launch setup and follow default configuration



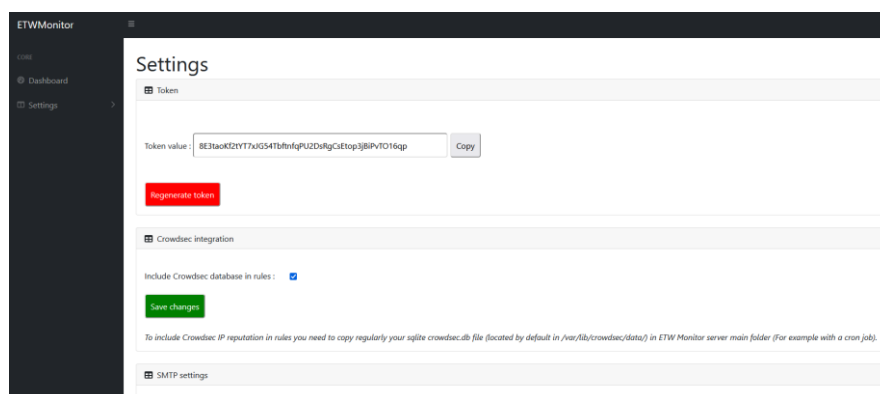
6. Write server IP address and paste token in preinstallation console



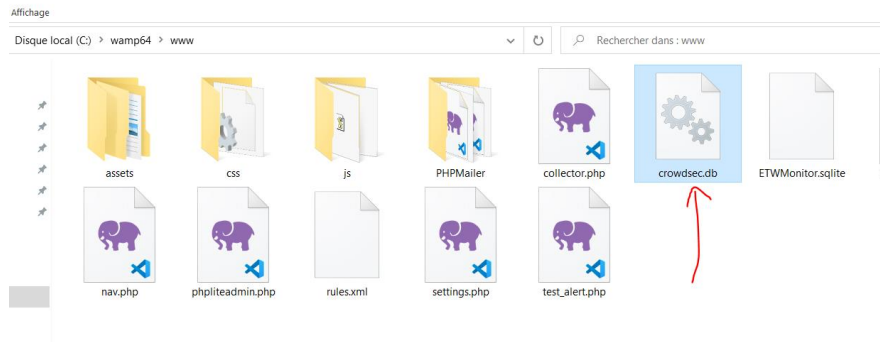
7. Wait until the end of the installation

Latest events			
<div>10 entries per page</div>			
Host	datetime	Event	Level
DESK1	2022-11-22 14:40:49	ETWMonitor was started !	0

8. On server dashboard, a new event should appear



9. If you have Crowdsec installed on your web server, you can activate integration from settings panel



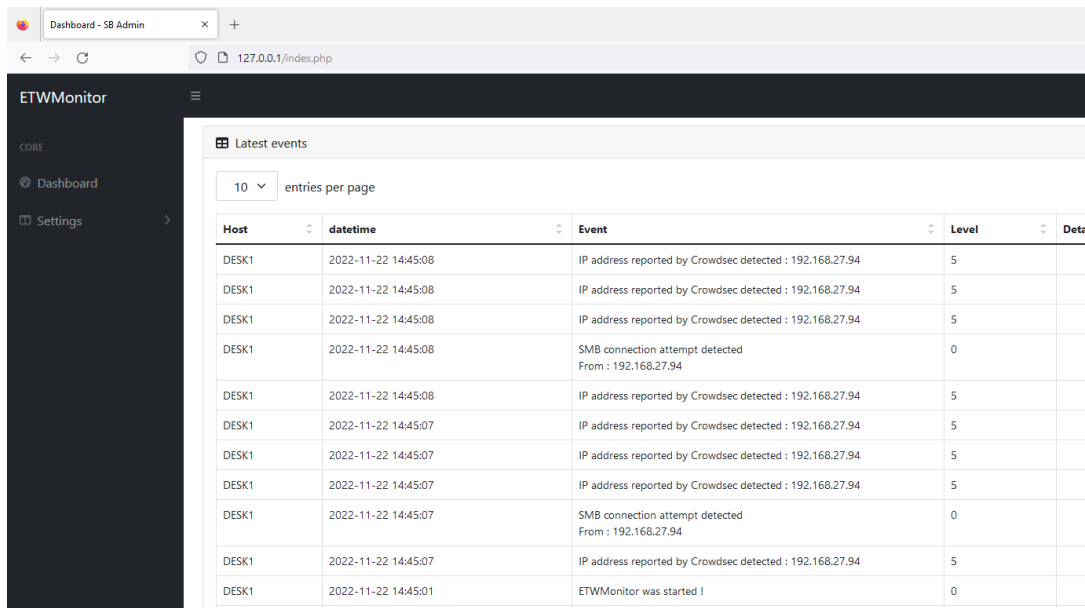
10. You have to copy and paste your crowdsec sqlite database file inside ETW Monitor server main folder

```

rules.xml
150         </match>
151         <alert>RPC connection to service manager - Potential PSEXEC attack detected</a
152         <score>5</score>
153     </detected-psexec>
154     <detected-atexec>
155         <match>
156             <string>smb2requestcreate</string>
157             <string>atsvc</string>
158         </match>
159         <alert>RPC connection to scheduled task manager - Potential ATEXEC attack dete
160         <score>5</score>
161     </detected-atexec>
162 </detections>
163 <crowdsec>
164 <crowdsec-0>
165     1.1.223.106
166 </crowdsec-0>
167
168 <crowdsec-1>
169     1.1.223.110
170 </crowdsec-1>
171
172 <crowdsec-2>
173     1.169.110.3
174 </crowdsec-2>
175
176 <crowdsec-3>
177     1.169.62.71
178 </crowdsec-3>
179
180 <crowdsec-4>

```

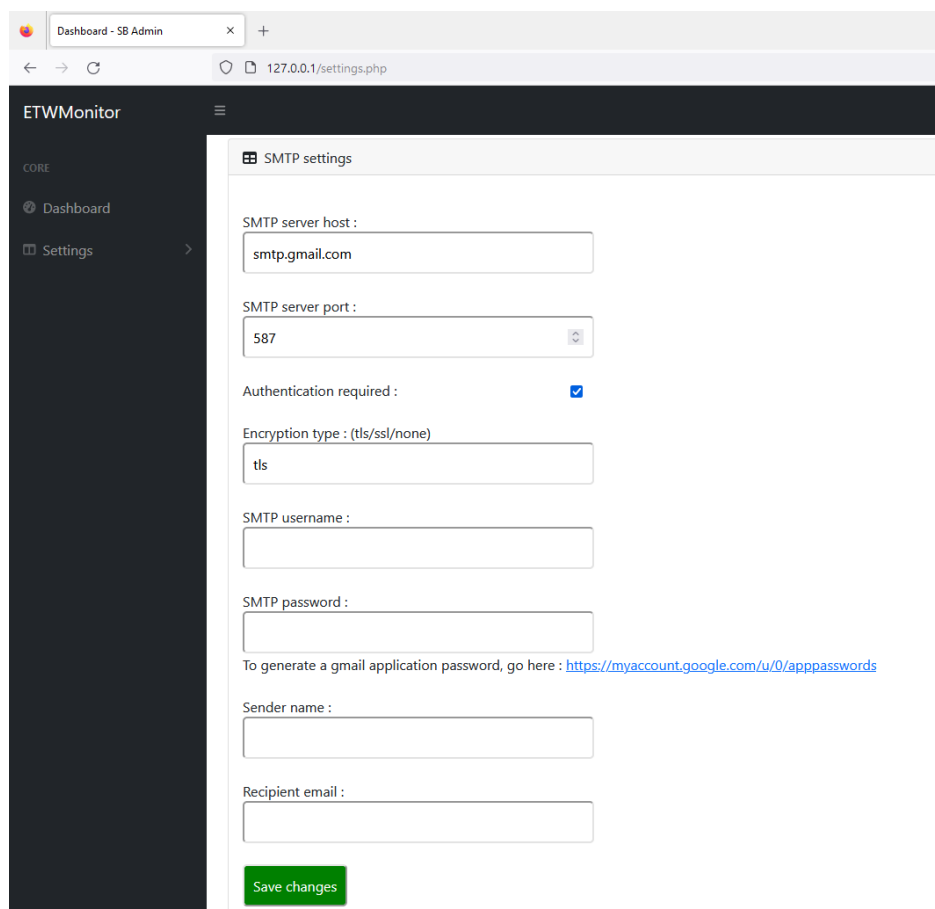
11. When collector will be called next time, it will extract all IP addresses from Crowdsec database and parse it in server rules file



The screenshot shows the ETWMonitor dashboard with the 'Latest events' section. A sidebar on the left contains 'CORE', 'Dashboard', and 'Settings'. The main content area has a 'Latest events' header with a dropdown set to '10 entries per page'. Below is a table of events.

Host	datetime	Event	Level	Details
DESK1	2022-11-22 14:45:08	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:08	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:08	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:08	SMB connection attempt detected From : 192.168.27.94	0	
DESK1	2022-11-22 14:45:08	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:07	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:07	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:07	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:07	SMB connection attempt detected From : 192.168.27.94	0	
DESK1	2022-11-22 14:45:07	IP address reported by Crowdsec detected : 192.168.27.94	5	
DESK1	2022-11-22 14:45:01	ETWMonitor was started !	0	

12. After rules update on endpoint, crowdsec integration will send alerts when communication with a suspect IP address is detected



The screenshot shows the 'SMTP settings' panel in ETWMonitor. The sidebar on the left has 'CORE', 'Dashboard', and 'Settings'. The main content area is titled 'SMTP settings' and contains several input fields for configuring email alerts.

SMTP server host : smtp.gmail.com

SMTP server port : 587

Authentication required : ☒

Encryption type : (tls/ssl/none)
tls

SMTP username :

SMTP password :

To generate a gmail application password, go here : <https://myaccount.google.com/u/0/apppasswords>

Sender name :

Recipient email :

13. In settings panel, you can also configure a SMTP server to send alert through email

ETW Monitor - Alert from DESK1



processus.thief@gmail.com
À Christopher THIEFIN

↩ Répondre

↩ Répondre à tous

→ 1



Traduire le message en : Français

Ne jamais traduire à partir de : Anglais

Préférences en matière de traduction

Démarrer votre réponse avec :

What does this mean?

What is this?

Seems to be working.

Commentaires

New alert from host : DESK1

IP address reported by Crowdsec detected : 192.168.27.94

14. When an alert is received with a score above 5 it will be sent by email

```
rules.xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <root>
3   <providers>
4     <guid>{d48ce617-33a2-4bc3-a5c7-11aa4f29619e}</guid>
5     <guid>{1139c61b-b549-4251-8ed3-27250a1edec8}</guid>
6     <guid>{a7975c8f-ac13-49f1-87da-5a984a4ab417}</guid>
7     <guid>{0a002690-3839-4e3a-b3b6-96d8df868d99}</guid>
8     <guid>{a0c1853b-5c40-4b15-8766-3cf1c58f985a}</guid>
9     <guid>{6AD52B32-D609-4BE9-AE07-CE8DAE937E39}</guid>
10    <guid>{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}</guid>
11  </providers>
12  <detectors>
13    <detected-dns-0>
14      <match>
15        <string>Microsoft-Windows-DNS-Client</string>
16        <string>QueryName="pastebin.fr"</string>
17        <string>Une réponse a été reçue</string>
18      </match>
19      <alert>La résolution d'un domaine malveillant a été effectuée : pastebin.fr</alert>
20      <score>3</score>
21    </detected-dns-0>
22
23    <detected-powershell-0>
24      <match>
25        <string>Nom de commande = Import-Module</string>
26        <string>ID d'interpréteur de commandes = Microsoft.PowerShell</string>
27      </match>
28      <alert>Un module powershell a été chargé en mémoire</alert>
29      <score>5</score>
30    </detected-powershell-0>
31
32    <detected-defender-0>
33      <match>
34        <string>Microsoft-Antimalware-Engine</string>
35        <string>_report::build_report</string>
36      </match>
37      <alert>Windows Defender a détecté une menace</alert>
38      <score>5</score>
39    </detected-defender-0>
40  </detectors>
41 </root>
```

15. You can also manually personalize the server rules file with your own custom rules :

- Give a new GUID provider to collect ETW events
- Give one or more matching keywords, an alert message and a score

Then restart your endpoints or just wait until they update rules (every 10 minutes by default)