Quand les bleus se prennent pour des chercheurs de vulnérabilités

Recherche d'événements ETW (Event Tracing for Windows)

AIRBUS CERT

Sylvain Peyrefitte -- cert@airbus.com

AIRBUS

Un problème de mesure

- Comment mesure-t-on l’état d’un système ?
- Avons-nous toutes les informations nécessaires?
- N’avons-nous pas trop d’informations?

AIRBUS

Le sysadmin de Schrödinger

AIRBUS

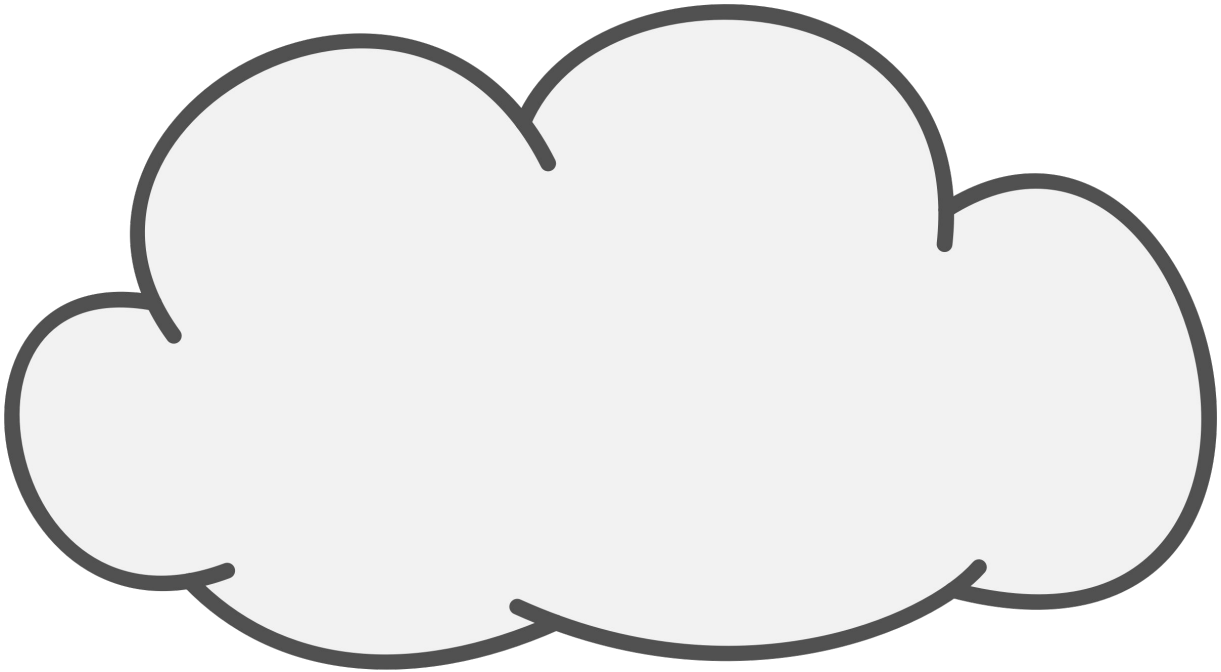
Le sysadmin de Schrödinger

AIRBUS

Le sysadmin de Schrödinger

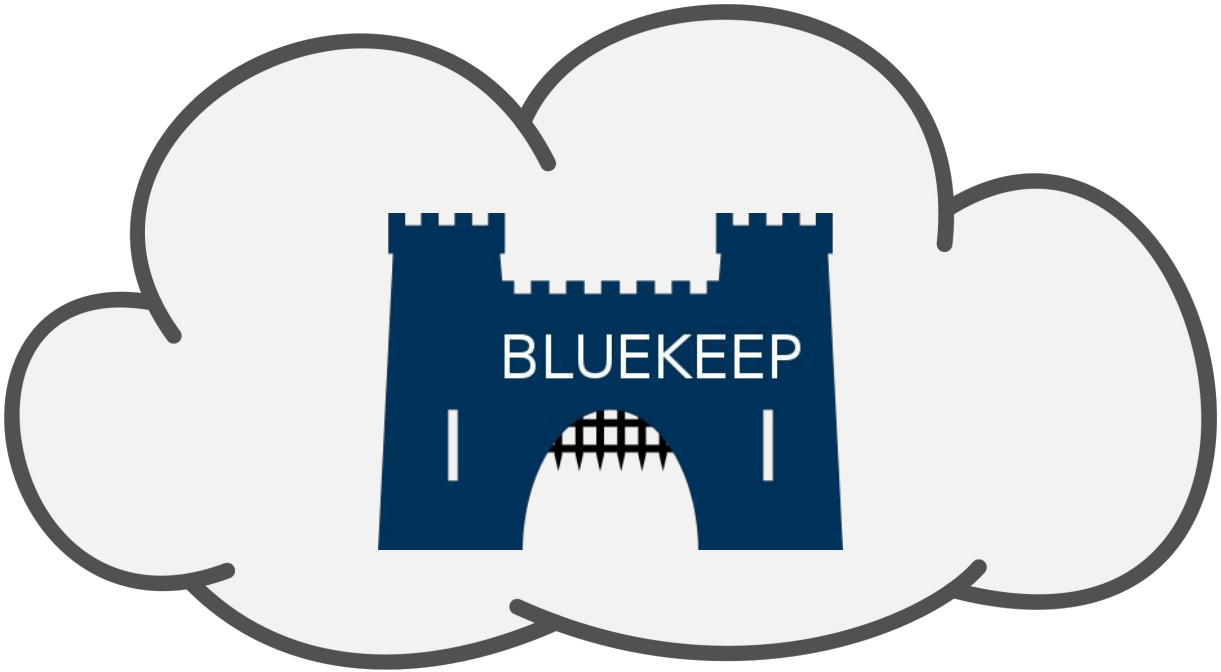
AIRBUS

Le sysadmin de Schrödinger



AIRBUS

Le sysadmin de Schrödinger



AIRBUS

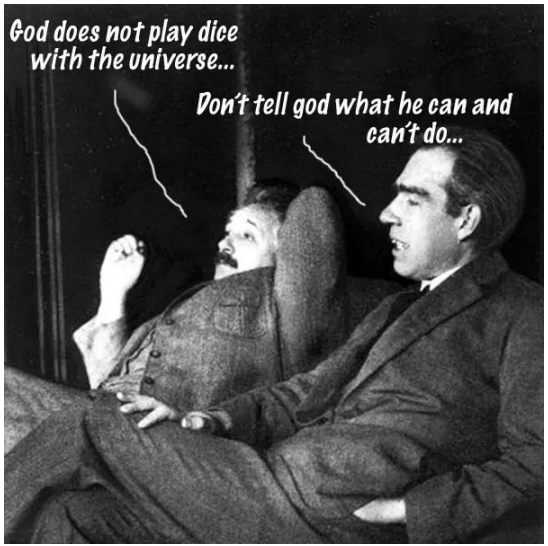
Le sysadmin de Schrödinger

$$|\ \text{  }\ \rangle + |\ \text{  }\ \rangle$$

L’état de notre sysadmin est à la fois content et pas content tant que nous ne pouvons mesurer

AIRBUS

Théorie quantique de la mesure : L'école de Bohr

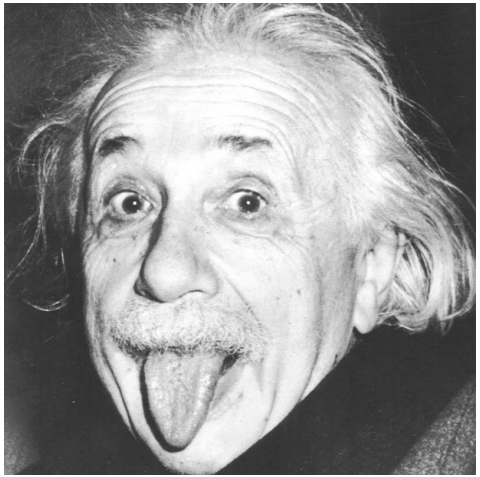


- Soit nous considérons que nous ne pouvons pas mesurer directement l'exploitation de la vulnérabilité, mais plutôt ses conséquences
  - Nous détectons les processus créés par le service
  - Nous détectons l'instabilité d'un processus via WER

AIRBUS

Théorie quantique de la mesure : L’école d’Einstein

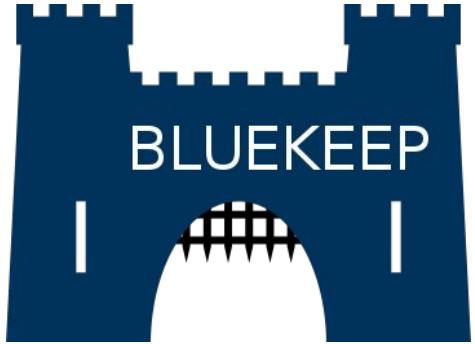
- Soit nous considérons qu’il existe une mesure qu’il faut découvrir et qui nous permettra de définir avec précision l’état de notre système



AIRBUS

Que cherchons-nous à mesurer ?

- Bluekeep
  - Affecte le service TerminalServer
  - Se base sur le mélange entre les canaux statiques et dynamiques
  - En particulier le canal principal : ms_t120



AIRBUS

Que peut-on mesurer ?

- Event Tracing for Windows
  - *Provider*, ceux qui vont émettre des événements
  - *Session*, afin de grouper les providers
  - *Consumer*, ceux qui vont consommer et manipuler les événements depuis une session

AIRBUS

Recherche d’un événement

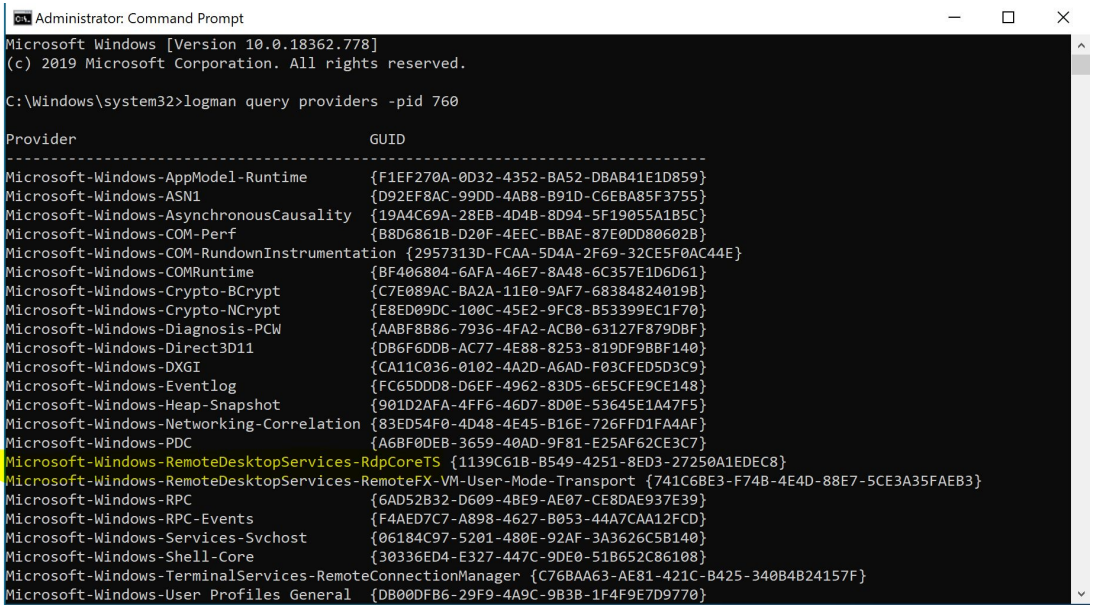
- Lister les providers émis par le service

AIRBUS

Recherche d’un événement

- Lister les providers émis par le service

```
logman query providers -pid 123
```



AIRBUS

Recherche d’un événement

- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants

AIRBUS

Recherche d’un événement

- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants

```
logman start RDP -p Microsoft-Windows-RemoteDesktopServices-RdpCoreTS -ets -rt
```

AIRBUS

Recherche d’un événement

- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants
- Visualiser les événements, les comparer, les analyser

AIRBUS

Recherche d’un événement

- Lister les providers émis par le service
- Créer une session regroupant les providers qui nous semblent intéressants
- Visualiser les événements, les comparer, les analyser

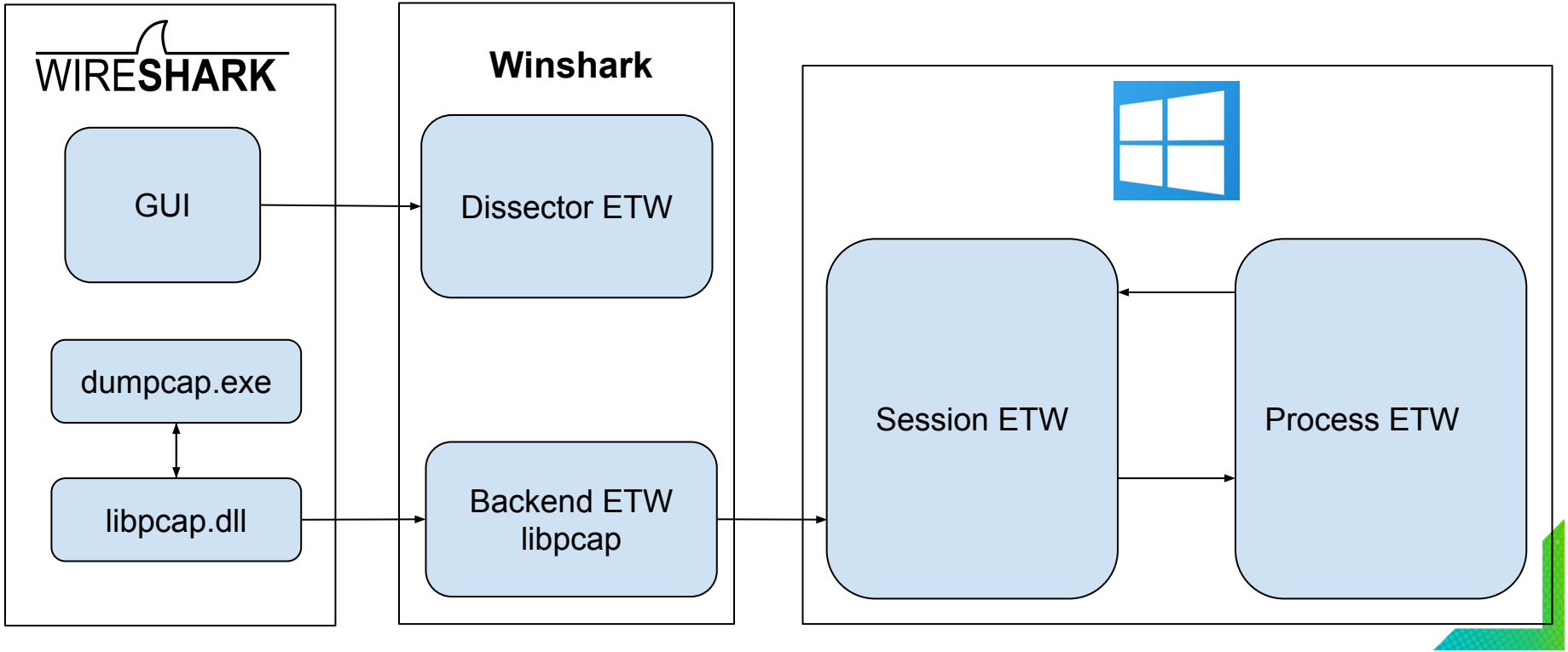
AIRBUS

Winshark

- Wireshark pour capturer des ETW
- *Dissectors* pour analyser les ETW
- Provider *Microsoft-Windows-NDIS-PacketCapture*
  (éviter d'installer un driver *NDIS* pour la capture réseau)
- Analyser les ETW de type *Tracelogging*
- Sauvegarder les ETW dans un fichier *pcap*

AIRBUS

Winshark -- structure



AIRBUS

Winshark : Demo détection bluekeep

AIRBUS

Comprendre l'événement 148

- Attribuer cet événement **seulement** à la détection de l'exploit ?
- Sous quelle condition est-il émis ?

- Analyse statique et dynamique du module en charge de cet événement
- *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers*

Analyse avec ETWBreaker

AIRBUS

Analyse avec ETWBreaker

```
ntdll!EtwEventWrite
rdpcorets!CRDPEventLogSessionBase::LogEvent+0xdd
rdpcorets!CRDPEventLogSession::ChannelClose+0x47
RDPSERVERBASE!CRdpDynVC::OnClose+0x281
RDPSERVERBASE!CRdpDynVCMgr::CloseChannels+0x6a
RDPSERVERBASE!CRdpDynVCMgr::TerminateInstance+0x373
RDPSERVERBASE!CRDPWDUMXStack::TerminateInstance+0xf6
RDPSERVERBASE!CRDPENCConnection::Abort+0x77
RDPSERVERBASE!CRDPENCConnection::Terminate+0x1c
RDPSERVERBASE!CRDPCoreConnection::TerminateInstance+0x201
rdpcorets!CUMRDPConnection::TerminateInstance+0x210
rdpcorets!CUMRDPConnection::OnDisconnected+0x2b3
RDPSERVERBASE!CRDPCoreConnection::SMAPI_Decoupled_OnRDPStackDisconnected+0x241
RDPBASE!CTSMsg::Invoke+0xfb
RDPBASE!CTSThread::RunQueueEvent+0x130
RDPBASE!CTSThread::RunAllQueueEvents+0x111
RDPBASE!CTSThread::internalMsgPump+0xc9
RDPBASE!CTSThread::internalThreadMsgLoop+0xe9
RDPBASE!CTSThread::ThreadMsgLoop+0x1c
RDPBASE!CRDPENCPlatformContext::STATIC_STAThreadProc+0x56
```

Comprendre l’événement 148

- RdpCoreTS_Event_ChannelClose
- ChannelName = ms_t120
- CRdpDynVC : Dynamic Virtual Channel

AIRBUS

To be continued...

- Ajouter des providers
  - Exemple de l'AMSI
- Exploiter les WPP
- Winshark : https://github.com/airbus-cert/Winshark
- ETWBreaker : https://github.com/airbus-cert/etwbreaker

AIRBUS

AIRBUS CERT

Merci

On recrute !

Questions : cert@airbus.com

AIRBUS