



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 26 octobre 2016

N° DAT-NT-27/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 18

NOTE TECHNIQUE

DÉPLOIEMENT ET CONFIGURATION CENTRALISÉS D'EMET POUR LE DURCISSEMENT DES POSTES DE TRAVAIL ET DES SERVEURS MICROSOFT WINDOWS



Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

INFORMATIONS

Avertissement

Ce document rédigé par l'ANSSI présente les « **Déploiement et configuration centralisés d'EMET pour le durcissement des postes de travail et des serveurs Microsoft Windows** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
BSS, DTO	BSS	SDE	26 octobre 2016

Évolutions du document :

Version	Date	Nature des modifications
1.0	11 septembre 2015	Version initiale
2.0	25 février 2016	Mise à jour pour EMET 5.5
2.1	26 octobre 2016	Correction mineure d'un lien mort

Pour toute question :

Contact	Adresse	@mél
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr

Table des matières

1	EMET	3
2	Bénéfices et limites	3
3	Mécanismes de protection	4
3.1	Mécanisme spécifiques à certains processus de Microsoft	4
3.1.1	ASR (<i>Attack Surface Reduction</i>)	4
3.1.2	Certificate pinning (épinglage de certificats) pour Microsoft Internet Explorer	5
3.2	Mécanismes applicables à tous les processus	5
3.2.1	DEP (<i>Data Execution Prevention</i>)	6
3.2.2	SEHOP (<i>Structured Execution Handling Overwrite Protection</i>)	7
3.2.3	NullPage	8
3.2.4	Allocation Heapspray	8
3.2.5	ASLR (<i>Address Space Layout Randomization</i>)	8
3.2.6	ROP (<i>Return-Oriented Programming</i>)	9
3.2.7	EAF/EAF+ (<i>Export Address Table Filtering</i>)	9
3.2.8	Windows 10 untrusted fonts mitigation	10
3.3	Déploiement et configuration	10
3.3.1	Sur postes de travail	11
3.3.2	Sur systèmes serveurs	11
3.3.3	Remarques concernant la configuration d'EMET par GPO	12
3.4	Efficacité des mécanismes de protection	12
3.5	Journalisation et exploitation des journaux	12
Annexe : Déploiement et configuration centralisés d'EMET par GPO dans un domaine Active Directory		14

1 EMET

EMET (*Enhanced Mitigation Experience Toolkit*) est un outil permettant de se protéger contre certaines techniques communément utilisées pour l'exploitation de vulnérabilités, et que l'on pourrait qualifier d'HIPS (*Host-based Intrusion Prevention System*). Le déploiement de ce type d'outils s'inscrit dans une démarche de durcissement système et de défense en profondeur. Aujourd'hui disponible en version 5.5, il est mis à disposition gratuitement par Microsoft (<https://technet.microsoft.com/fr-fr/security/jj653751>) et est officiellement supporté pour les postes de travail à partir de Microsoft Windows de Vista SP2 et les serveurs à partir de Windows Server 2008 SP2. D'anciennes versions d'EMET moins complètes sont toutefois compatibles avec les postes de travail Windows XP et 2000 ainsi que Windows Server 2003¹.

2 Bénéfices et limites

EMET est doté de mécanismes de protection particulièrement utiles à la sécurisation de tous les processus (ceux du système ainsi que des applications tierces) amenés à manipuler du contenu potentiellement malveillant (fichiers, commandes, courriels, pages Web, saisies utilisateurs, etc.), notamment ceux faisant l'objet de tentatives régulières d'exploitation de vulnérabilités :

- sur les postes de travail : navigateurs et modules complémentaires associés (Flash, Java, etc.), clients de courriel, visionneuses de fichiers PDF, suites bureautique, etc. ;
- sur les systèmes serveurs : services web, de messagerie, d'accès distant, de déport d'affichage et de mises à jour parmi tant d'autres.

Le déploiement d'EMET sur un parc Microsoft est relativement simple. Sa configuration centralisée est également simplifiée en environnement Active Directory par les modèles de GPO fournis par Microsoft. Elle doit néanmoins être réalisée avec précaution sur les systèmes d'exploitation serveurs dont la disponibilité revêt un caractère souvent critique. Certaines protections peuvent être incompatibles avec les applications et services utilisés au sein du système d'information, qu'elles soient relativement courantes, ou bien développées spécifiquement pour les besoins métier de l'entité. De fait, la mise en œuvre d'EMET doit s'accompagner de tous les tests nécessaires permettant d'établir une configuration adaptée aux systèmes et aux applications utilisées.



Il est conseillé de commencer par utiliser EMET en mode « Audit » de manière à simplifier l'élaboration d'une configuration en limitant les blocages de processus inopinés. Dans ce mode, EMET ne fera qu'alerter et n'empêchera aucune exécution de code malveillant. Par la suite, il est alors primordial de passer en mode « Stop on exploit » afin qu'EMET bloque les exploits détectés et termine les processus concernés.

Note : le mode audit n'est supporté que pour les mécanismes EAF, ROP, SEHOP, ASR et Fonts.

R1

Utiliser EMET en mode « Stop on exploit ».

1. La mise en œuvre d'EMET est d'ailleurs particulièrement recommandée sur ces systèmes obsolètes.

L'objectif de ce document est d'expliquer le rôle d'EMET et de clarifier les spécificités de son déploiement (dans sa version 5.2). En revanche, ce document n'a pas vocation à expliquer les différents mécanismes de protection dans le détail. Pour plus d'informations théoriques ou pratiques sur ces mécanismes, le guide utilisateur d'EMET peut être consulté et des liens vers des articles de référence sont également proposés en notes de bas de pages.

3 Mécanismes de protection

La configuration générale est visible et modifiable depuis l'interface principale d'EMET. En revanche, certains mécanismes ne s'appliquent qu'après la création de règles d'application spécifiques.

3.1 Mécanismes spécifiques à certains processus de Microsoft

3.1.1 ASR (*Attack Surface Reduction*)

L'ASR est une protection qui permet de bloquer l'exécution d'une liste prédéterminée de modules complémentaires (ou plus précisément de leurs bibliothèques) pour Microsoft Internet Explorer et Microsoft Word, Excel et Powerpoint.

Exemples :

- permettre au module Java de s'exécuter dans Microsoft Internet Explorer uniquement lorsque le processus accède à la zone « Local Intranet » ;
- bloquer le chargement du module Adobe Flash Player dans les processus Microsoft Word, Excel et Powerpoint.

Lorsqu'une entité utilise Microsoft Internet Explorer comme seul navigateur pour la navigation Internet et Intranet, EMET apporte un gain substantiel de sécurité en restreignant les modules complémentaires chargés lors de la navigation sur des sites en zone Internet. Dès lors, les modules à risque (Java, VBScript, etc.) ne sont plus utilisables qu'en navigation Intranet. La liste par défaut est à compléter des éventuels modules moins courants qu'aurait déployé l'entité.

De base, l'ASR n'est pas appliquée. Il est donc nécessaire de créer une règle pour Microsoft Internet Explorer ainsi que pour Microsoft Office Word, Excel et Powerpoint dès lors que ces logiciels sont utilisables (voir section [3.3 - Déploiement et configuration](#) pour l'importation de règles de configuration recommandées par Microsoft). La configuration de l'ASR peut ensuite être modifiée en affichant les paramètres avancés des règles d'application, comme illustré par la figure ci-après.

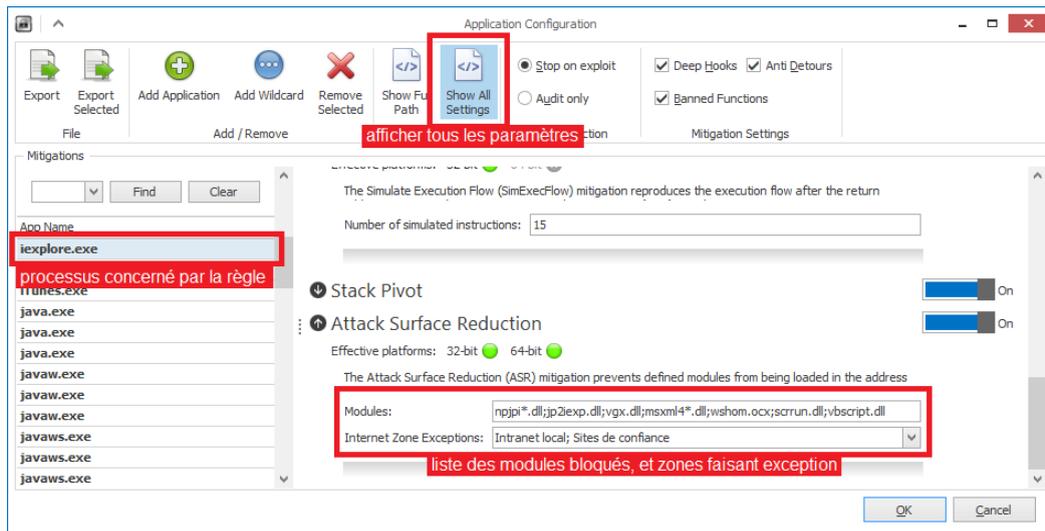


FIGURE 1 – Configuration de l’ASR dans la règle d’application pour Microsoft Internet Explorer

3.1.2 Certificate pinning (épinglage de certificats) pour Microsoft Internet Explorer

La fonctionnalité d’épinglage de certificats² apportée par EMET pour Microsoft Internet Explorer consiste en un référentiel d’associations entre des sites internet et leurs certificats respectifs. Dès lors qu’un certificat a été épinglé pour un site donné, seul ce dernier sera autorisé. Un tel mécanisme permet de s’affranchir des problèmes liés aux IGC (AC compromises, faux certificats validés car délivrés par une AC ajoutée au magasin de l’utilisateur, etc.).



Il convient toutefois de contrôler le certificat au préalable étant entendu que ce mécanisme peut poser problème en cas d’analyse de flux HTTPS en sortie de réseau³

Microsoft Internet Explorer n’intègre toujours pas nativement, à ce jour, de mécanisme d’épinglage de certificats. Il s’agit d’une évolution néanmoins considérée par Microsoft. Notons que les navigateurs Google Chrome et Mozilla Firefox intègrent nativement des mécanismes d’épinglage de certificats qui leurs sont propres.

3.2 Mécanismes applicables à tous les processus

Un processus présentant des vulnérabilités et amené à manipuler du contenu potentiellement malveillant expose le système à des attaques. Par différentes méthodes d’injection, les attaquants peuvent ainsi parvenir à exécuter du code malveillant sur les systèmes. Chacun des mécanismes de protection d’EMET, listés ci-après, a pour objectif de protéger contre une méthode d’attaque spécifique. Dans le cadre d’une démarche de défense en profondeur, chaque mécanisme d’EMET a son

2. Pour plus d’informations sur l’épinglage de certificats : https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning.

3. Voir les recommandations de sécurité concernant l’analyse de flux HTTPS : http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_TLS_NoteTech.pdf.

utilité propre et ces derniers sont complémentaires entre eux.

R2

Lors du déploiement d'EMET, il est recommandé d'appliquer le plus grand nombre de protections possibles au plus grand nombre de processus possibles.

3.2.1 DEP (*Data Execution Prevention*)

Cette protection permet de bloquer les instructions exécutables injectées par exploitation de vulnérabilités dans des espaces mémoires qui ne sont pas censés en contenir. Il s'agit d'un mécanisme déjà présent nativement sous Windows depuis sa version XP SP2 et activé par défaut uniquement pour les programmes et services du système d'exploitation. EMET apporte plus de flexibilité de configuration en permettant la configuration fine de DEP au niveau des applications et du système.

DEP⁴ peut être configuré de manière générale selon différents modes :

Valeur	Recommandations ANSSI	Description
<i>Always On</i>	trop strict	activé au niveau système pour tous les processus et sans possibilité de le désactiver pour une application en particulier (le paramètre DEP est alors ignoré des règles d'application). Ce paramètre peut être envisagé sur des systèmes dont le durcissement doit être maximal et dès lors qu'aucun problème de compatibilité ne se pose.
<i>Opt Out</i>	recommandé	activé au niveau système pour tous les processus à l'exception de ceux faisant l'objet d'une règle d'application spécifique stipulant de ne pas activer la DEP.
<i>Opt In</i>	non recommandé	désactivé sauf pour les processus faisant l'objet d'une règle d'application spécifique stipulant d'activer la DEP (paramètre par défaut évitant l'application de la DEP à des applications potentiellement non compatibles)
<i>Disabled</i>	non recommandé	désactivé pour tous les processus et sans exceptions possibles (le paramètre DEP est alors ignoré des règles d'application).

Certaines incompatibilités connues nécessitent la configuration d'exceptions, c'est le cas par exemple de Microsoft Office Web Components (lorsque System DEP est paramétré à « AlwaysOn »).

Note : l'activation de DEP sur un poste de travail dont le disque est chiffré avec Bitlocker est détectée comme un changement des informations de démarrage. Elle nécessitera donc la saisie de la clé de restauration au prochain démarrage (une seule fois).

3.2.2 SEHOP (*Structured Execution Handling Overwrite Protection*)

Ce mécanisme aide à se protéger contre les techniques de réécriture de SEH suivies d'une levée d'exception permettant l'exécution de code arbitraire.

SEHOP⁵ peut être configuré de manière générale selon différents modes :

Valeur	Recommandations ANSSI	Description
<i>Opt Out</i>	recommandé	activé au niveau système pour tous les processus à l'exception de ceux faisant l'objet d'une règle d'application spécifique stipulant de ne pas activer SEHOP
<i>Opt In</i>	non recommandé	désactivé sauf pour les processus faisant l'objet d'une règle d'application spécifique stipulant d'activer la SEHOP (paramètre par défaut évitant l'application de la SEHOP à des applications potentiellement non compatibles)

Certaines incompatibilités connues nécessitent la configuration d'exceptions pour par exemple : Google Chrome (sur Windows Vista), Windows Media Player (sur Windows Vista).

Note : SEHOP étant implémenté au niveau du système, les blocages de processus interviendront sans qu'EMET puisse en notifier l'utilisateur. Ces derniers seront donc visibles dans les journaux du système d'exploitation.

4. Pour plus d'informations sur la DEP : <http://blogs.technet.com/b/srd/archive/2009/06/05/understanding-dep-as-a-mitigation-technology-part-1.aspx>.

5. Pour plus d'informations sur la SEHOP : <http://blogs.technet.com/b/srd/archive/2009/02/02/preventing-the-exploitation-of-seh-overwrites-with-sehop.aspx>.

3.2.3 NullPage

Ce mécanisme protège la page mémoire en zéro en empêchant le déréférencement de pointeurs NULL et en pré-allouant cette première page mémoire qui pourrait être utilisée pour de l'injection de code. Il peut à priori être appliqué sans crainte à tout processus.

Cette protection n'est appliquée qu'après avoir créé des règles de configuration spécifiques aux processus à protéger.

Note : la page en zero est protégée sans EMET et par défaut à partir de Windows 8.

3.2.4 Allocation Heapspray

Ce mécanisme protège le tas contre un remplissage arbitraire (de contenu malveillant généralement répété) qui pourrait être utilisé dans le cadre d'exploitations de vulnérabilités.

Cette protection n'est appliquée qu'après avoir créé des règles de configuration spécifiques aux processus à protéger.

Note : certaines incompatibilités connues nécessitent la configuration d'exceptions, par exemple : Oracle Java (lorsque la JVM est spécifiquement configurée avec l'option `-Xms` pour réserver une large portion de mémoire).

3.2.5 ASLR (*Address Space Layout Randomization*)

En distribuant aléatoirement l'espace d'adressage mémoire, EMET permet le placement aléatoire des zones de données dans la mémoire virtuelle. Ce procédé limite les effets des attaques de type débordement de tampon qui ne peuvent ainsi pas en déduire les positions de certains espaces clés (pile, librairies, etc.). L'ASLR est un mécanisme présent nativement sous Windows depuis Vista, EMET apporte toutefois une ASLR améliorée par rapport à ce dernier et permet également le *Mandatory-ASLR* par application.

L'ASLR⁶ peut être configuré de manière générale selon différents modes :

Valeur	Recommandations ANSSI	Description
<i>Opt In</i>	recommandé	désactivé sauf pour les processus faisant l'objet d'une règle d'application spécifique stipulant d'activer la Mandatory-ASLR (paramètre par défaut évitant l'application de l'ASLR à des applications potentiellement non compatibles)
<i>Disabled</i>	déconseillé	désactivé dans tous les cas et sans exceptions possibles (le paramètre ASLR est alors ignoré des règles d'application)

Cela signifie qu'avec ces deux modes, l'ASLR d'EMET ne sera jamais actif au niveau système pour toutes les applications. En conséquence, ce mécanisme de protection ne sera appliqué qu'aux processus ayant fait l'objet d'une règle spécifiquement configurée. Il s'agit d'un détail très important

6. Pour plus d'informations sur l'ASLR d'EMET : <http://technet.microsoft.com/en-us/security/gg524265.aspx>.

à bien prendre en compte pour exploiter au mieux l'outil.

Exemple : une entité déploie EMET avec la configuration par défaut et le profil « Maximum Security Settings ». Les processus des navigateurs Internet Mozilla Firefox et Google Chrome ne bénéficient pas de l'ASLR puisqu'aucune règle n'indique à EMET de le faire. Il s'agit pourtant de processus critiques dans la démarche de durcissement des postes utilisateurs.

Certaines applications sont incompatibles avec l'ASLR, comme par exemple Windows Media Player et quelques pilotes vidéo AMD/ATI (System ASLR).

Note : il existe un paramètre « **Always On** » pour l'ASLR (ie. System-ASLR), mais ce dernier est invisible depuis l'interface graphique (configurable via le paramètre « **EnableUnsafeSettings** » en base de registres), car jugé dangereux pour la stabilité du système. En effet, le système d'exploitation pourrait s'arrêter inopinément au démarrage si un pilote n'est pas compatible avec l'ASLR au niveau système. Il paraît donc difficile d'activer ce paramètre au sein d'un système d'information pourvu de matériel et de pilotes hétérogènes.

3.2.6 ROP (*Return-Oriented Programming*)

Cette protection apporte une solution contre certaines techniques de ROP⁷ (LoadLibrary, MemProt, Caller (32 bits), SimExecFlow (32 bits) et StackPivot) en rendant ainsi plus compliquées les exploitations des séquences de codes terminées par une instruction de retour, utilisées par les attaquants lorsque les débordements de tampon simples ne sont pas possibles (du fait de l'ASLR et du DEP).

Ces protections ne sont appliquées qu'après avoir créé des règles de configuration spécifiques aux processus à protéger.

3.2.7 EAF/EAF+ (*Export Address Table Filtering*)

Ce mécanisme aide à lutter contre les techniques de découverte ROP (*Return Object Programming*) permettant l'exécution de code lorsqu'une vulnérabilité est trouvée.

De nombreuses incompatibilités logicielles empêchent son application avec par exemple : Excel Power Query, Power view, Power Map and PowerPivot, 7Zip, Dropbox, Skype, Immidio Flex+, SolarWinds Syslogd Manager, Windows Media Player. Plus généralement, l'EAF devrait être désactivé pour tout produit de sécurité (antivirus, parefeu, bac à sable), logiciel intégrant des protections contre le debugging (programmes de gestion de DRM ou de licences par exemple) ou bien encore exécutable empaqueté.

Ces protections ne sont appliquées qu'après avoir créé des règles de configuration spécifiques aux processus à protéger.

7. Pour plus d'informations sur le ROP : <http://en.wikipedia.org/wiki/Return-oriented-programming>.

3.2.8 Windows 10 untrusted fonts mitigation

EMET 5.5 apporte la prise en charge de Windows 10 ainsi qu'un mécanisme de protection contre les polices de caractères non approuvées (*Windows 10 untrusted fonts mitigation*)⁸ pour ce système d'exploitation spécifique. Ce mécanisme consiste à prévenir les élévations de privilèges locales qui pourraient se produire lors du traitement d'un fichier de polices de caractères malveillant et présent en dehors du dossier de confiance %windir%/Fonts.

Ce mécanisme peut être configuré de manière générale selon différents modes :

Valeur	Recommandations ANSSI	Description
<i>Always On</i>	recommandé	activé au niveau système pour tous les processus à l'exception de ceux faisant l'objet d'une règle d'application spécifique stipulant de ne pas activer bloquer les polices de caractère non approuvées
<i>Opt In</i>	non recommandé	désactivé sauf pour les processus faisant l'objet d'une règle d'application spécifique stipulant d'activer la SEHOP (paramètre par défaut évitant l'application de la SEHOP à des applications potentiellement non compatibles)
<i>Disabled</i>	non recommandé	complètement désactivé
<i>Audit</i>	recommandé en mode audit	à utiliser en mode audit pour simplement journaliser sans bloquer

Des exceptions peuvent ensuite être configurées pour ce mécanisme dans chaque règle applicative.

3.3 Déploiement et configuration

Du fait que certains mécanismes sont configurés en *Opt In* et que d'autres ne s'appliquent qu'après la création manuelle de règles de configuration, le simple déploiement d'EMET dans sa configuration par défaut est loin d'être optimal puisqu'elle a pour objectif de ne pas apporter d'incompatibilités potentielles difficiles à résoudre par des utilisateurs néophytes. Des règles pertinentes et adaptées aux applicatifs utilisés doivent alors être ajoutées pour tirer partie des mécanismes de protection apportés par l'outil, via le menu « Apps » prévu à cet effet et comme illustré par les figures ci-après.

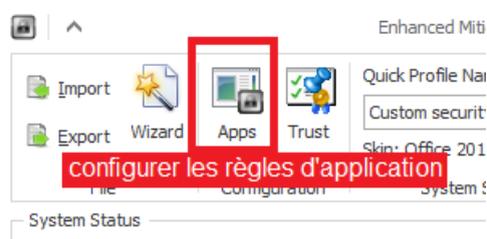


FIGURE 2 – Menu de création de règles d'application

8. Pour plus d'informations sur ce sujet, lire l'article *Block untrusted fonts in an enterprise* sur le site Technet à l'adresse [https://technet.microsoft.com/en-us/library/dn985836\(v=vs.85\).aspx](https://technet.microsoft.com/en-us/library/dn985836(v=vs.85).aspx).

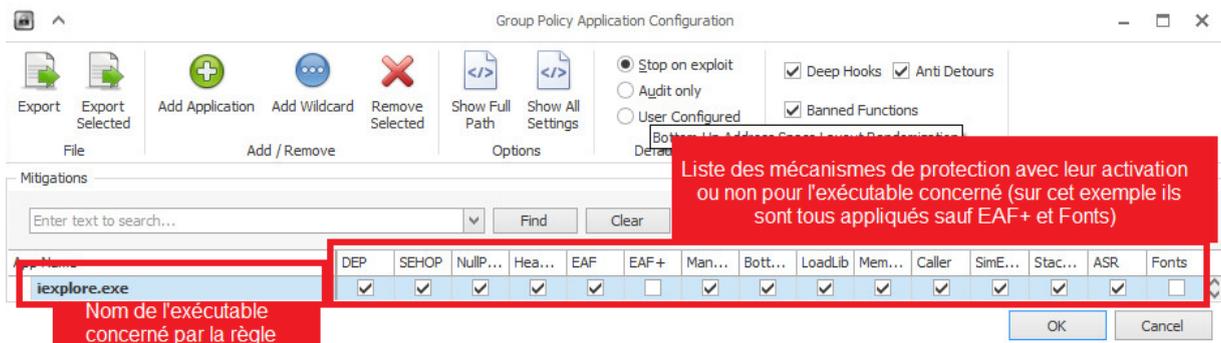


FIGURE 3 – Exemple de règle d'application pour l'exécutable iexplore.exe (Microsoft Internet Explorer)

3.3.1 Sur postes de travail

Deux jeux de règles facultatifs sont fournis avec EMET et adaptés aux postes de travail :

- un jeu *Popular Software* contenant des règles pour une cinquantaine de logiciels populaires, parmi lesquels on retrouve Google Chrome, Mozilla Firefox, Adobe Acrobat Reader, Oracle Java, etc. ;
- un jeu *Recommended Software* contenant les règles recommandées pour quelques produits Microsoft (la suite Office entre autres) mais également pour Adobe Acrobat Reader et Oracle Java.
- un jeu *CertTrust* contenant quelques règles d'épinglage de certificats considérés comme majeurs par Microsoft.

Ces jeux de règles ne sont pas appliqués par défaut et doivent être importés manuellement (voir figure 4) depuis le sous-dossier « \Deployment\Protection Profiles », ou bien appliqués par configuration centralisée au sein d'un système d'information. Les règles concernant tout autre application ne figurant pas dans ces deux jeux de règles pré-définis doivent être créées et testées.

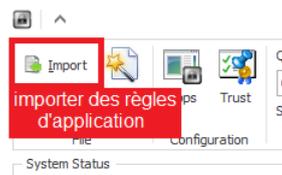


FIGURE 4 – Importer des règles d'application

Une procédure de déploiement et de configuration centralisés d'EMET en environnement Active Directory est détaillée en annexe I.

3.3.2 Sur systèmes serveurs

Aucun jeu de règles pour les systèmes serveurs n'est fourni avec EMET. Microsoft n'a à ce jour publié aucune indication de configuration pour les différents rôles et fonctionnalités qui peuvent être nativement ajoutés sous Windows Server. L'usage d'EMET reste néanmoins recommandé par Microsoft sur ces systèmes, notamment pour protéger des services exposés tels sur Microsoft Internet Information Servers (IIS) aussi bien lorsque le système n'exécute que des services intégrés nativement par Microsoft (DHCP, DNS, IIS, etc.) que lorsqu'il exécute des applications d'éditeurs tiers.

La configuration d'EMET sur les systèmes serveurs doit être réalisée avec précaution. La disponibilité des services revêtant un caractère critique, il est fortement conseillé de mettre en œuvre EMET en environnement de test et de valider le bon fonctionnement des services concernés avant tout passage en production.

3.3.3 Remarques concernant la configuration d'EMET par GPO

La version 5.5 d'EMET apporte la complète prise en charge de la configuration par GPO. Il n'est donc plus nécessaire de recourir à des scripts et lignes de commandes d'importation de fichiers de configuration en XML pour maîtriser la configuration d'EMET au sein du système d'information. Après installation des outils RSAT (*Remote Server Administration Tools*) sur un poste d'administration, et moyennant l'utilisation d'un compte du domaine disposant des privilèges adéquats, le bouton *Group Policy* de l'interface graphique d'EMET permet d'exporter la configuration locale vers une GPO et inversement. La GPO de configuration d'EMET se modifie ainsi très facilement via l'interface graphique du produit sans qu'il soit nécessaire d'utiliser la console de gestion de stratégie de groupe.

Notons toutefois que l'utilisateur du système peut ajouter des règles applicatives et d'épinglage de certificats, quels que soient ses privilèges et sans que cela puisse être interdit par GPO. Néanmoins, les règles configurées par GPO sont prioritaires et s'appliquent dans tous les cas. Il peut toutefois être problématique qu'un utilisateur ajoute ses propres règles EMET.

3.4 Efficacité des mécanismes de protection



Les différentes protections apportées par EMET ne sont pas infaillibles et il reste possible de les contourner.

Au gré des versions, les protections d'EMET gagnent en efficacité. Aujourd'hui, et à défaut d'être une barrière infranchissable, EMET rend beaucoup plus complexe l'exploitation des vulnérabilités et demande des moyens bien plus importants aux attaquants. L'outil apporte ainsi une protection supplémentaire face aux vulnérabilités *0-day*⁹ en attente de correctifs des éditeurs, ce qui représente un gain de sécurité non négligeable.

3.5 Journalisation et exploitation des journaux

EMET présente l'avantage de journaliser ses alertes de sécurité dans les journaux Windows. Si l'entité centralise ces journaux, et les analyse au sein d'un SIEM (*Security Information and Event Management*, les alertes d'EMET apportent des informations très utiles pour la détection et la traçabilité des événements de sécurité au niveau global.

Pour aller plus loin, et étant donné qu'EMET est susceptible d'interrompre les processus faisant l'objet d'un incident de sécurité, il peut être intéressant de collecter et centraliser les *User-Mode dumps* (clichés mémoire) des rapports d'erreurs Windows¹⁰, qui se révèlent être une source d'informations importante lors des analyses post-mortem. Les entités qui sont la cible d'attaques avancées ont donc

9. Pour plus d'information sur les vulnérabilités *0-day* : https://fr.wikipedia.org/wiki/Vulnérabilité_Zero_day.

10. Pour plus d'informations sur la collecte des *User-Mode dumps* : <https://msdn.microsoft.com/fr-fr/library/windows/desktop/bb787181.aspx>.

tout intérêt à centraliser les clichés mémoire des postes utilisateurs.



Les *User-Mode dumps* pouvant contenir des informations sensibles (clés, mdp), il est important de garantir leur confidentialité en plus de leur intégrité.

Annexe :

Déploiement et configuration centralisés d'EMET par GPO dans un domaine Active Directory

Cette annexe présente de manière synthétique une méthode de télé-déploiement reposant sur GPO.

Téléchargement du paquet MSI

EMET 5.5 est téléchargeable à l'adresse <https://www.microsoft.com/en-us/download/details.aspx?id=50766>, il a pour pré-requis le déploiement préalable du Framework .NET en version 4.0 (par exemple par WSUS ou par déploiement au format MSI).

Configuration par GPO via la console de gestion de stratégie de groupe

Pour pouvoir définir des règles de configuration d'EMET dans une GPO depuis la console de gestion de stratégie de groupe, il est nécessaire de préalablement récupérer les modèles d'administration fournis par Microsoft. Ces derniers se trouvent dans le sous-dossier « \Deployment\Group Policy Files » du répertoire d'installation d'EMET.

Ensuite, dans un scénario de déploiement en domaine Active Directory, le modèle ADMX ¹¹ doit être déposé dans un dépôt central au sein du dossier SYSVOL présent sur les contrôleurs de domaine et contenant les GPO.

Voici un exemple de GPO de configuration d'EMET :

11. Pour plus d'informations, un guide pas à pas de gestion des modèles ADM et ADMX est disponible sur le site technet de Microsoft à l'adresse <http://technet.microsoft.com/fr-fr/library/cc709647>.

GPO Configuration Manager

Données recueillies le : 18/02/2016 11:24:27 [afficher tout](#)

Configuration ordinateur (activée) [masquer](#)

Stratégies [masquer](#)

Modèles d'administration [masquer](#)

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/EMET [masquer](#)

Stratégie	Paramètre	Commentaire
Default Action and Mitigation Settings	Activé	
Deep Hooks:	Enabled	
Anti Detours:	Enabled	
Banned Functions:	Enabled	
Exploit Action:	Stop Program	
EMET Agent Custom Message	Désactivé	
EMET Agent Visibility	Activé	
Start Agent Hidden:	Enabled	
Reporting	Activé	
Event Log:	Enabled	
Tray Icon:	Enabled	
Early Warning:	Enabled	
System ASLR	Activé	
ASLR Setting:	Application Opt-In	
System DEP	Activé	
DEP Setting:	Always On	
System SEHOP	Activé	
SEHOP Setting:	Application Opt-In	

FIGURE 5 – GPO de configuration d'EMET 1/2

Autres paramètres Registre [masquer](#)

Le nom convivial de certains paramètres est introuvable. Vous pouvez peut-être résoudre ce problème en mettant à jour vos fichiers .adm utilisés par GPMC.

Paramètre	Statut
Software\Policies\Microsoft\EMET.Defaults\7-Zip\7z.exe	-EAF
Software\Policies\Microsoft\EMET.Defaults\7-Zip\7zFM.exe	-EAF
Software\Policies\Microsoft\EMET.Defaults\7-Zip\7zG.exe	-EAF
Software\Policies\Microsoft\EMET.Defaults\Adobe\Reader\AcroRd32.exe	+EAF+ eaf_modules\AcroRd32.dll;Acrofox32.dll;AcroForm.api
Software\Policies\Microsoft\EMET.Defaults\Adobe\Acrobat\Acrobat\Acrobat.exe	+EAF+ eaf_modules\AcroRd32.dll;Acrofox32.dll;AcroForm.api
Software\Policies\Microsoft\EMET.Defaults\Adobe\Adobe Photoshop CS\Photoshop.exe	
Software\Policies\Microsoft\EMET.Defaults\Foxit Reader\Foxit Reader.exe	
Software\Policies\Microsoft\EMET.Defaults\Google\Chrome\Appl\chrome.exe	+EAF+ eaf_modules\chrome_child.dll
Software\Policies\Microsoft\EMET.Defaults\Google\Google Talk\googletalk.exe	-DEP
Software\Policies\Microsoft\EMET.Defaults\Internet Explorer\iexplore.exe	+EAF+ eaf_modules\mshtml.dll;flash.ocx;jscript.dll;vbscript.dll;vgx.dll;asr_modules\npapi.dll;jp2exp.dll;vpx.dll;msxml4.dll;wshom.ocx;scrn.dll;vbscript.dll;asr_zones;1;2
Software\Policies\Microsoft\EMET.Defaults\iTunes\iTunes.exe	
Software\Policies\Microsoft\EMET.Defaults\Java\jre\bin\java.exe	-Heap Spray
Software\Policies\Microsoft\EMET.Defaults\Java\jre\bin\javaw.exe	-Heap Spray
Software\Policies\Microsoft\EMET.Defaults\Java\jre\bin\javaws.exe	-Heap Spray
Software\Policies\Microsoft\EMET.Defaults\Microsoft Lync\communicator.exe	
Software\Policies\Microsoft\EMET.Defaults\mIRC\mirc.exe	
Software\Policies\Microsoft\EMET.Defaults\Mozilla Firefox\firefox.exe	+EAF+ eaf_modules\mozjs.dll;xul.dll

FIGURE 6 – GPO de configuration d'EMET 2/2

Configuration par GPO via l'interface graphique d'EMET 5.5

Avec la version 5.5 d'EMET, il est désormais plus simple de configurer les GPO depuis le bouton *Group Policy* de l'interface graphique d'EMET plutôt que depuis la console de gestion de stratégie de groupe :

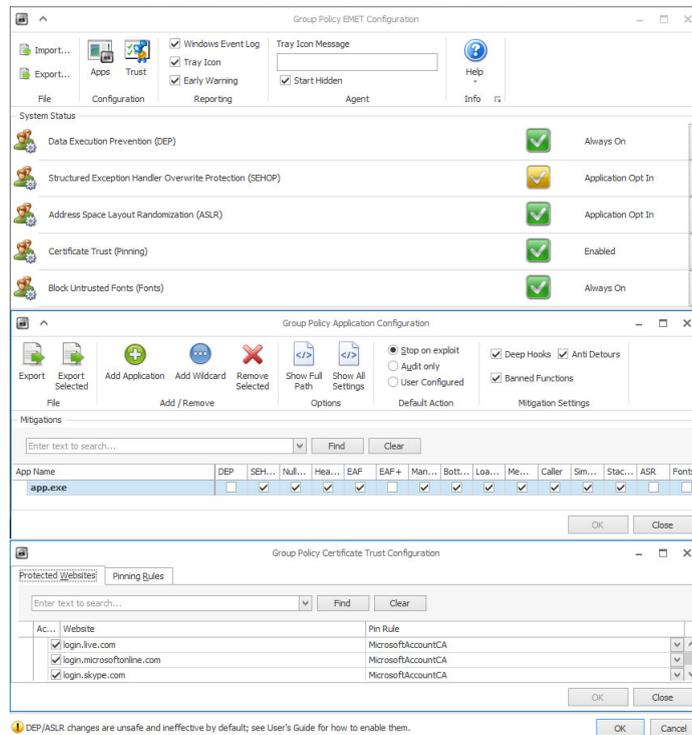


FIGURE 7 – Interface intégrée de configuration de GPO sous EMET 5.5

Déploiement

Le fichier MSI doit ensuite être déposé dans un partage de fichiers (d'un serveur de fichiers idéalement) accessible en lecture seule par tous les utilisateurs. Le chemin UNC (*Universal Naming Convention*) du partage créé sera utilisé dans la stratégie de groupe (c'est à dire par exemple « \\serveur\partage\emet55.msi » et non pas « C:\partage\emet55.msi » puisqu'il s'agit du chemin qui sera utilisé par les ordinateurs pour accéder aux fichiers d'installation). Les comptes utilisateurs (ou d'ordinateurs, en fonction de la GPO) doivent bien entendu avoir uniquement les droits de lecture sur ce partage.

Une stratégie de groupe permet de télédeployer le paquet d'installation. Cela se fait au niveau de la console de gestion des stratégies de groupe du domaine, en créant et modifiant une nouvelle GPO ayant par exemple les paramètres suivants :

GPO-C-Deploy-EMET	
Données recueillies le : 24/04/2015 10:24:38	
afficher tout	
Configuration ordinateur (activée) masquer	
Stratégies masquer	
Paramètres du logiciel masquer	
Applications attribuées masquer	
EMET 5.2 masquer	
Informations produit afficher	
Informations de déploiement masquer	
Général	Paramètre
Type de déploiement	Attribué
Source du déploiement	\\dc\Deployment\EMET.msi
Désinstaller cette application lorsqu'elle se trouve en dehors de l'étendue de la gestion	Activé

FIGURE 8 – GPO de déploiement de paquet d'installation MSI

Le déploiement peut également se faire au niveau de la stratégie utilisateur plutôt que de la stratégie ordinateur. L'étendue d'application de la stratégie de groupe peut également être restreinte à certains groupes d'ordinateurs ou d'utilisateurs. Si le déploiement se fait par stratégie utilisateur, la GPO s'applique par défaut à tous les utilisateurs authentifiés, ce périmètre pouvant être affiné au besoin à une population précise.

Une fois les GPO de déploiement et de configuration des règles d'EMET appliquées, celui-ci sera automatiquement installé et configuré selon les règles définies.