Cyber Essentials dans l'éducation

jamf

La cybersécurité dans l'éducation n'est pas la matière la plus facile, mais elle n'a pas à être un problème d'algèbre insurmontable. Avec Cyber Essentials, le Royaume-Uni et le National Cyber Security Centre ont mis au point un parcours de certification destiné aux établissements scolaires. Il vise à les aider à protéger leurs élèves, leurs enseignants, leurs appareils et leurs données contre les criminels et les cyberattaques.

Dans cet e-book, vous découvrirez :

- L'impact de l'évolution de l'éducation sur les menaces de cybersécurité
- Les dix contrôles de sécurité de base à mettre en œuvre dans l'éducation
- Le programme Cyber Essentials et son fonctionnement
- Comment cette certification peut aider votre institution à atténuer les nombreux défis de la cybersécurité.

La cybersécurité a pour mission d'assurer la sécurité de vos étudiants, de vos enseignants et de leurs appareils, et elle est moins une pratique spécifique ou la mise en œuvre d'un produit qu'un mode de vie. En d'autres termes, « ce n'est pas la destination qui compte, c'est le voyage », pour citer Ralph Waldo Emerson. Mieux encore, c'est la route sans fin que doivent suivre les équipes informatiques et de sécurité pour renforcer les ressources des réseaux éducatifs. En effet, il faut sans cesse préserver la sécurité des données et la vie privée des utilisateurs contre les menaces et les accès non autorisés.

La tâche peut sembler intimidante. Et honnêtement, pour ceux qui ne sont pas au fait des dernières cybermenaces, le parcours peut être difficile… mais pas impossible. Pour y parvenir, les écoles peuvent compter sur des organisations de référence, expertes dans le domaine de la sécurisation des ressources informatiques comme les appareils macOS et iOS. Avec la bonne équipe à leurs côtés, les enseignants deviennent entièrement autonomes et peuvent aider leurs élèves à réussir avec Apple, en toute confiance. Ils ont l'assurance que l'essentiel de l'effort de cybersécurité est pris en charge par l'appui combiné de leurs partenaires.

> **Ce n'est pas la destination, c'est le voyage. »**
>
> **– Ralph Waldo Emerson**

Mais qui sont ces partenaires ?

Excellente question ! C'est d'abord vous, l'enseignant, et votre équipe de professionnels de l'informatique et/ou de la sécurité, si votre établissement en a une. Passons maintenant au choix évident : Apple. Les Macbook Pro et les iPads offrent une approche inégalée de la sécurité et du respect de la vie privée. De plus, Apple incorpore cette démarche au cœur de la conception de macOS, iOS et iPadOS, plutôt que comme une couche supplémentaire.

Le partenaire suivant est Jamf, leader du secteur des solutions de gestion des appareils et de sécurité, qui se consacre exclusivement à Apple. Les puissantes solutions Jamf telles que Jamf School sont conçues pour gérer les appareils et configurer leurs réglages de sécurité. Elles s'intègrent à un large éventail de services logiciels tiers souvent utilisés par les enseignants – comme Google – pour gérer les salles de classe numériques et assurer l'interface avec leurs élèves. Pour autant, Jamf School est facile à apprendre : la solution a été développée dans un souci de simplicité pour aider les administrateurs à gérer les problèmes quotidiens.

Enfin, il y a les partenaires de certification. La certification Cyber Essentials, qui fait l'objet de cet e-book, vous aide à protéger votre organisation contre les cyberattaques et les menaces les plus courantes. Surtout, elle démontre l'engagement de votre établissement en matière de cybersécurité.

Avant de nous plonger dans la certification Cyber Essentials, voyons d'abord comment les développements de la cybersécurité ont influencé l'éducation, l'évolution des environnements d'apprentissage et l'adoption des appareils mobiles.

Le vent du changement

Si vous ne l'avez pas encore compris, la cybersécurité est dynamique : elle évolue et se déplace constamment. Certes, il fut un temps où aucun logiciel malveillant ou presque n'était créé pour la plateforme Mac. Non pas parce qu'elle était impénétrable, mais bien parce que cette cible n'était pas aussi populaire que les autres systèmes d'exploitation.

Mais les produits Apple ont connu une croissance exponentielle et une popularité fulgurante auprès des consommateurs et de tous les types d'organisations. Les auteurs de logiciels malveillants ont pris conscience du terrain fertile et inexploité qui s'étendait devant eux : les centaines de millions d'utilisateurs Apple dans le monde.

Jamf Threat Labs, la branche sécurité et recherche de Jamf, surveille et étudie activement toutes sortes de menaces affectant les utilisateurs de macOS et d'iOS. Son objectif est, bien sûr, d'intégrer les dernières protections dans les solutions Jamf. Mais elle analyse également les tendances en matière d'attaques et exploite ces données pour informer le développement de nos produits et nos clients, afin de sécuriser au mieux leurs environnements.

Accéder à l'apprentissage en tout lieu et à tout moment

L'éducation a subi de grands bouleversements au cours des dernières années, mais peu ont eu un impact aussi important que l'apprentissage à distance. Il y a eu, bien sûr, les mesures de sécurité prises en réponse à la pandémie. Mais il a surtout fallu passer soudainement d'un modèle en face à face à un autre, qui imposait un changement substantiel d'infrastructure. Pensez également aux changements en matière de sécurité, nécessaires pour donner à toutes les parties prenantes un accès à distance aux ressources éducatives, ainsi qu'un appareil informatique moderne pour que chaque étudiant et enseignant puisse travailler.

Certaines institutions sont toujours aux prises avec changement radical des modes d'apprentissage. Fidèles à eux-mêmes, les acteurs malveillants ont profité de l'occasion pour moderniser leurs méthodes et attaquer les infrastructures. Ils ont modifié leurs opérations pour tirer parti du déséquilibre créé par ces transformations. Les attaquants ont commencé à cibler les utilisateurs à distance avec des campagnes d'hameçonnage agressives. Ils ont perturbé les salles de classe virtuelles avec aisance et compromis les appareils avec des logiciels malveillants. Pire encore, ils ont accédé sans autorisation à des données sensibles en exploitant les services de stockage dans le cloud.

L'adoption d'appareils mobiles comme l'iPad d'Apple est une bonne nouvelle. Cette tablette fine, légère, extrêmement puissante et polyvalente offre une autonomie exceptionnelle. Dotée de solides protections intégrées, elle est l'outil éducatif idéal pour les enseignants et les étudiants. Cette technologie moderne, dans un format abordable, prend en charge un grand nombre d'applications et de services indispensables aux enseignants. Et comme c'est en permanence un outil de communication, elle n'a pas son pareil quand il s'agit d'apprendre partout, à tout moment.

Quel avenir dessinent ces tendances ?

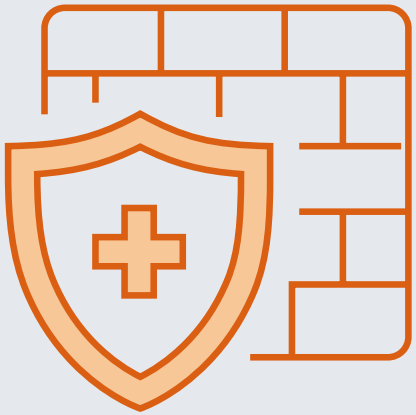
Les conclusions de Security 360, Rapport annuel sur les tendances de Jamf, mettent en évidence quelques éléments clés de l'année écoulée :

- Les installations de logiciels malveillants sur des appareils à distance **a doublé**.
- Les configurations d'appareils à risque ont eu des conséquences négatives pour **une organisation sur cinq**.
- La proportion d'appareils compromis ayant accédé à des applications de collaboration (comme Zoom et Microsoft Teams) est passée de **34 % à 64 %**.
- Près de **la moitié** des utilisateurs interrogés ont admis ne pas utiliser la technologie VPN, tout en comprenant son importance pour la sécurisation du trafic réseau.
- Les logiciels malveillants basés sur Mac **continuent de gagner** en prévalence mais aussi en sophistication : les attaquants modernisent leurs méthodes et revoient leurs ambitions à la hausse.
- Apple est la marque la plus fréquemment employée par les campagnes d'**hameçonnage** en 2021.
- Le respect de la vie privée est tout aussi **importante** pour la sécurité des appareils que pour l'utilisateur final. Il fait d'ailleurs l'objet d'une attention croissante dans les réglementations, qui en font facteur clé de conformité.

Les menaces, tout comme la mode, sont sujettes à des tendances : certaines d'entre elles s'essoufflent et disparaissent (et oui, je pense aux épaulettes des années 80). D'autres évoluent au fil du temps pour prendre une forme nouvelle – et potentiellement pire – que leur version d'origine.

Cela dit, n'oubliez pas que la cybersécurité est une voie qu'il faut sans cesse déblayer. Pour aménager une nouvelle terrasse devant votre maison, vous aurez besoin d'outils. De la même manière, vous allez vous appuyer sur des contrôles de sécurité pour renforcer votre posture contre les risques, les menaces et les attaques – celles d'aujourd'hui et de demain.

10 contrôles de sécurité de base

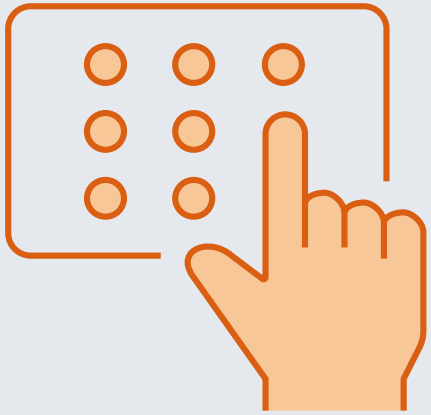


1 Pare-feux

Les pare-feux servent de barrière entre un réseau interne, qui doit rester sécurisé, et l'Internet, qui doit être traité avec prudence. Tout appareil ayant accès à Internet doit en posséder un. Ils sont particulièrement importants lorsque le personnel utilise un Wi-Fi public ou non sécurisé pour accéder à des ressources professionnelles. Et cela vaut aussi bien pour les appareils de l'école ou de l'université que pour un appareil personnel.

2 Configuration sécurisée

Les configurations par défaut des appareils et des logiciels sont souvent très souples pour faciliter la prise en main. Mais elles offrent également davantage de points d'accès aux utilisateurs non autorisés. La désactivation, voire la suppression, de fonctionnalités inutiles, ainsi que la modification des mots de passe par défaut, réduisent le risque de faille de sécurité.

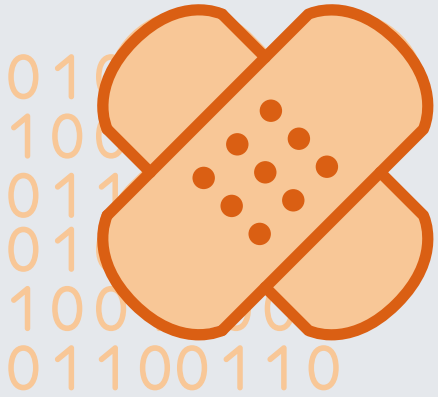


3 Contrôle d'accès

Il peut être très pratique d'accorder au plus grand nombre l'accès à vos données et services. Mais la multiplication des comptes augmente mécaniquement le risque de compromission et donc, de faille grave de sécurité. Le risque de violation involontaire, comme la suppression accidentelle de données importantes, s'en trouve aussi accru. Mais vous pouvez aussi bloquer les accès et les accorder uniquement sur la base du strict « besoin d'en connaître », pour réduire les risques de violation. En outre, tous les comptes doivent être protégés par des mots de passe forts. Lorsque le risque de violation est particulièrement élevé, comme dans le cas d'un compte admin, vous devez envisager l'authentification à deux facteurs (2FA). La cyberattaque décrite plus haut aurait pu être évitée grâce au système 2FA.

4 Protection contre les logiciels malveillants

Les logiciels malveillants – virus et rançongiciels, notamment – peuvent infecter vos systèmes lorsqu'un membre du personnel se fait piéger par un e-mail d'hameçonnage, par exemple. Mais les supports de stockage amovibles, comme les clés USB, sont aussi un vecteur courant d'infection. Vous pouvez protéger votre organisation contre les logiciels malveillants en utilisant un antivirus ou une solution contre les logiciels malveillants. D'autres techniques peuvent être utiles, comme les « listes d'autorisation » et les « bacs à sable », qui permettent d'exécuter une application dans un environnement isolé de vos réseaux afin de déterminer si elle est malveillante.



5 Gestion des correctifs

Les fabricants et les développeurs publient normalement des mises à jour régulières. Non seulement améliorent les logiciels mais elles corrigent aussi les vulnérabilités découvertes. En installant ces mises à jour dès qu'elles sont disponibles, on réduit au minimum le délai pendant lequel ces vulnérabilités peuvent être exploitées. Et si le fabricant ne propose plus de support pour le matériel/logiciel que vous utilisez, il est temps de le remplacer par une solution plus récente ou de le mettre hors service.

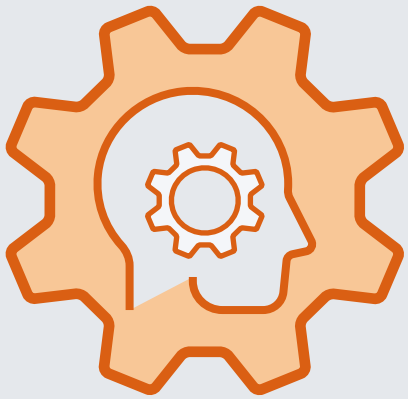
Une remarque : les cinq premiers critères suffisent à obtenir la certification Cyber Essentials (nous y reviendrons plus tard). Mais chez Jamf, nous pensons qu'une solution de sécurité complète exige d'autres éléments essentiels.

6 Création des identités (IdP)

L'IdP basée sur le cloud permet de centraliser la gestion des comptes d'utilisateurs. Elle sécurise l'authentification en interrogeant une base de données à distance pour traiter les demandes d'accès aux ressources éducatives. Celles-ci peuvent être locales ou externes, et servies par des services web, des clouds publics ou privés, et des plateformes SaaS (logiciel en tant que service). Les demandes d'authentification peuvent également être approvisionnées par le biais d'un portail : les parties prenantes peuvent alors accéder en un seul endroit à toutes les ressources utiles, grâce à l'authentification unique (SSO).

7 Accès réseau Zero-Trust (ZTNA)

Cette solution moderne sécurise les connectivités, et pas seulement les communications basées sur le réseau comme le fait un VPN. C'est un énorme bond en avant qui affranchit la sécurité de la question du périmètre. Elle repose sur la création microtunnels spécifiques aux applications pour établir une connexion sécurisée aux ressources de partout, via n'importe quel standard de communication. Et lorsque le ZTNA est intégré à l'IdP, les utilisateurs peuvent accéder aux ressources à l'aide de leurs identifiants. De plus, toujours pour réduire les risques, le ZTNA peut vérifier l'état des appareils avant d'accorder son autorisation, et attendre que les appareils soient mis en conformité.



8 Machine Learning

L'automatisation est l'un des petits avantages des technologies de machine learning. Les ordinateurs savent quantifier les flux de données et y rechercher des points communs. Ils peuvent corréler les données d'attaques passées avec celles d'une application, d'un service ou d'un acteur malveillant. Et tout cela donne aux équipes informatiques et de sécurité à la fois un éclairage inégalé sur les attaques qui se sont produites, et des informations essentielles pour prévenir les attaques futures. Nous le savons, la vitesse à laquelle les ordinateurs peuvent analyser les données est bien supérieure à celle de l'être humain et à ce que permettent les processus manuels.

9 Défense contre les menaces mobiles (MTD)

Comme les solutions de sécurité pour ordinateurs de bureau, la MTD offre une prévention contre les logiciels malveillants et les menaces de sécurité qui visent les appareils mobiles, comme l'iPad et l'iPhone. Pourquoi une catégorie spécifique de logiciels pour se protéger contre ces menaces ? En termes simples, la conception des appareils mobiles diffère du fonctionnement des appareils macOS. Les acteurs malveillants mettent au point de nouveaux moyens d'attaquer les appareils mobiles. Il faut donc une solution basée sur le cloud qui protège contre une variété de menaces mobiles, des logiciels malveillants aux attaques basées sur le réseau. Ces solutions s'appuient sur des règles et des contrôles réguliers de la santé des appareils pour vérifier leur conformité.

10 Conformité réglementaire

L'éducation est un secteur réglementé. Au niveau mondial, l'enseignement est reconnu comme l'une des principales cibles des attaques de cybersécurité. Malheureusement, le secteur accuse un net retard sur les autres en matière de sécurité. En raison de cette faiblesse, combinée à un taux d'attaque élevé et aux réglementations gouvernementales, les violations de données constituent un problème majeur pour tous les acteurs impliqués. Maintenir la conformité est plus facile à dire qu'à faire. Mais ce n'est pas impossible, et c'est le moyen pour les établissements de conserver une solide posture de sécurité. Ils peuvent ainsi minimiser les risques liés aux menaces et garantir les bons niveaux de configuration des appareils. Et en cas de compromission, ils pourront rebondir plus rapidement en gardant le contrôle sur les performances de référence et les niveaux de configuration des appareils.

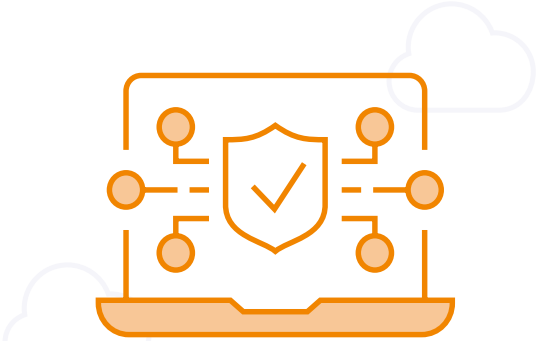
Nous avons désormais une idée plus précise du paysage de la cybersécurité dans l'éducation, et notamment de la myriade de menaces et de défis qui pèsent sur l'apprentissage moderne. Nous avons également abordé les contrôles de sécurité essentiels qui soutiennent le mieux l'objectif du secteur de l'enseignement, éduquer aujourd'hui l'avenir de demain. Revenons sur Cyber Essentials et sur l'appui qu'il peut apporter à cet objectif.

Qu'est-ce que Cyber Essentials ?

Selon le site web du RGPD britannique, « Cyber Essentials est un programme de l'administration britannique soutenu par le NCSC (National Cyber Security Centre), et il a pour but d'aider les organisations de toute taille à démontrer leur engagement envers la cybersécurité, tout en conservant une approche simple et des coûts bas. »

Le programme requiert cinq contrôles de sécurité fondamentaux :

1. Pare-feux
2. Configuration sécurisée
3. Contrôle d'accès
4. Protection contre les logiciels malveillants
5. Gestion des correctifs



En se concentrant sur **cinq** contrôles clés de cybersécurité, le secteur de l'enseignement peut facilement mettre en production une protection « contre **80 %** environ des cyberattaques courantes », selon le NCSC.

Pourquoi Cyber Essentials ?

Les écoles et autres établissements d'éducation britannique bénéficiant des fonds de l'ESFA devaient obtenir la certification Cyber Essentials, à partir de 2021. Les acteurs de l'éducation soutiennent ainsi activement les efforts du Royaume-Uni pour l'amélioration de la cybersécurité dans l'éducation, entre autres facettes de la société.

L'obtention de la certification Cyber Essentials ne démontre pas seulement aux étudiants, aux enseignants et à tous les autres acteurs qu'un établissement prend au sérieux la cybersécurité et la protection de la vie privée. Grâce à la mise en œuvre des contrôles de sécurité décrits ci-dessous, l'éducation accroît la sensibilisation à la sécurité au sein de ses écoles. Surtout, elle protège la confidentialité et l'intégrité des données sensibles au moyen de **« mesures techniques et organisationnelles appropriées ».**

Quelle sera l'intérêt de Cyber Essentials ?

Le programme Cyber Essentials est conçu pour atténuer les risques en réduisant les menaces liées aux cyberattaques les plus courantes. Le NCSC estime qu'environ **80 % des attaques reposent sur la faiblesse, voire l'absence, de protection contre les menaces de cybersécurité. Elles sont souvent automatisées, et les criminels opèrent à distance.**

En mettant en œuvre les **cinq contrôles de sécurité** ci-dessus, il devient possible d'atténuer ces types de cybermenaces et d'arrêter les cyberattaques *si/quand* elles se produisent. Si un appareil est compromis, le niveau de protection offert par les contrôles de sécurité et le renforcement des surfaces d'attaque peut indéniablement minimiser l'impact de l'agression.

L'atténuation d'une attaque réduit son impact. D'autre part, le temps nécessaire au triage et à la correction d'un appareil compromis est raccourci : étudiants et enseignants peuvent donc reprendre leur travail plus rapidement.

Comment fonctionne la certification Cyber Essentials ?

La certification Cyber Essentials comporte deux niveaux. Chacun d'eux prévoit un questionnaire d'auto-évaluation (SAQ) à remplir pour démontrer que les cinq contrôles de sécurité de base ont bien été mis en œuvre.

Cyber Essentials : le SAQ doit être rempli.

Cyber Essentials Plus : en plus du SAQ, ce niveau exige une vérification technique pratique, comprenant les éléments suivants :

- Analyse des vulnérabilités externes
- Évaluation sur site
- Analyse des vulnérabilités du réseau

Certains établissements souhaiteront examiner de plus près leur préparation en matière de cybersécurité avant de demander la certification Cyber Essentials. Pour cela, ils peuvent effectuer une évaluation gratuite auprès d'un fournisseur de services associé au NCSC. Cette évaluation consiste en des questions conçues pour apporter aux une vision détaillée de leur flotte et de leurs réseaux informatiques. Ce contrôle de l'état de préparation fournit également des détails sur ce qui devra figurer dans le SAQ formel, afin que rien ne manque.

> Un voyage de mille lieues commence par un pas. »
>
> – Lao Tseu

Jamf + certification Cyber Essentials

Une combinaison gagnante pour vous, le secteur de l'enseignement et la cybersécurité

jamf

Pour en savoir plus sur la demande de certification Cyber Essentials, consultez le site web du National Cyber Security Centre.

Pour savoir comment Jamf peut vous aider à démontrer votre engagement en faveur de la cybersécurité et à protéger votre école contre les cybermenaces :

En savoir plus

Ou contactez votre revendeur habituel de matériel Apple.