



Gestion des vulnérabilités

Apprenez à identifier, détecter, atténuer et signaler efficacement une vulnérabilité.

moyen

240 minutes

Démarrer AttackBox

AideSalle de sauvegarde

377

Possibilités

Room completed (100%)

Tache 1Introduction

Selon le NIST, une [vulnérabilité](#) est définie comme « *Une faiblesse dans un système d'information, des procédures de sécurité du système, des contrôles internes ou une mise en œuvre qui pourrait être exploitée ou déclenchée par une source de menace* ». Dans cette salle, nous apprendrons le processus permettant d'identifier, de détecter, d'atténuer et de signaler efficacement une vulnérabilité dans un système conformément aux cadres standards. La salle comprend un exemple pratique via un outil open source qui nous aidera à comprendre divers processus du cycle de vie de gestion des vulnérabilités.

Objectifs d'apprentissage

- Gestion des vulnérabilités vs analyse des vulnérabilités
- Comment les vulnérabilités sont-elles classées ?
- Processus du cycle de vie de gestion des vulnérabilités
- Comment pouvons-nous utiliser un cadre de gestion des vulnérabilités en cybersécurité ?

Conditions préalables

Une compréhension des sujets suivants est recommandée avant de commencer la salle :

- [Principes de sécurité](#)
- [Comprendre les bases de données de vulnérabilités](#)
- [Comment exploiter les vulnérabilités](#)

Commençons!

Répondre aux questions ci-dessous

J'ai rempli les prérequis et je suis prêt à commencer.

Complet

Tâche 2 Gestion des vulnérabilités vs analyse des vulnérabilités

Gestion des vulnérabilités

La gestion des vulnérabilités est une activité continue, proactive et fréquemment automatisée qui protège les systèmes informatiques, les réseaux et les solutions d'entreprise contre les cyberattaques et les violations de données. Il s'agit donc d'un élément essentiel d'un programme de sécurité global. En découvrant, évaluant et corrigeant les failles de sécurité potentielles, les entreprises peuvent contribuer à éviter les attaques et à atténuer leurs effets si elles se produisent.

Analyse des vulnérabilités

Étant donné que la gestion des vulnérabilités est le processus entourant l'analyse des vulnérabilités, il est essentiel de savoir comment les analyses de vulnérabilité sont effectuées et quels sont les outils disponibles. Aujourd'hui, l'utilisation d'un outil d'analyse des vulnérabilités nécessite peu de connaissances techniques. La plupart des scanners de vulnérabilités peuvent être exploités via une interface utilisateur graphique, permettant à un utilisateur d'effectuer des analyses de vulnérabilités sur l'ensemble d'un réseau en quelques clics de souris.

Les fournisseurs de sécurité proposent diverses solutions technologiques avec différents choix de déploiement, notamment des services autonomes, gérés et des logiciels en tant que service (SaaS). Certains outils commerciaux populaires d'analyse des vulnérabilités incluent Nessus,

Nexpose et Acunetix. D'un autre côté, quelques bonnes solutions open source comme Greenbone (édition communautaire), OWASP ZAP et bien d'autres.

Quelle est la différence?

Les termes gestion des vulnérabilités et analyse des vulnérabilités sont souvent mal compris. Malgré leur relation, il existe une distinction significative entre les deux. L'utilisation d'un programme informatique pour rechercher des vulnérabilités dans les réseaux, l'infrastructure informatique ou les applications constitue une analyse des vulnérabilités. Cependant, la gestion des vulnérabilités est le processus qui englobe l'analyse des vulnérabilités, ainsi que d'autres facteurs, notamment l'acceptation des risques, la correction et la création de rapports.

La gestion des vulnérabilités vise à réduire l'exposition globale aux risques d'une organisation en identifiant et en atténuant rapidement autant de vulnérabilités que possible. Cela peut s'avérer difficile, compte tenu des vulnérabilités potentielles et des ressources limitées disponibles pour y remédier. La gestion des vulnérabilités doit être un effort continu pour rester à jour face aux menaces nouvelles et émergentes.

La prévalence croissante de la cybercriminalité et les risques qui l'accompagnent obligent la plupart des entreprises à donner la priorité à la sécurité des informations. Les efforts d'une entreprise pour contrôler les menaces à la sécurité de l'information doivent inclure une procédure de gestion des vulnérabilités. Cette procédure permettra à une entreprise de recevoir un aperçu continu des vulnérabilités et des dangers associés dans son environnement informatique. Une entreprise ne peut empêcher les attaquants d'infiltrer ses réseaux et de voler des données sensibles qu'en découvrant et en atténuant les vulnérabilités de l'environnement informatique.

Répondre aux questions ci-dessous

Le processus englobant l'analyse des vulnérabilités et d'autres facteurs, tels que l'acceptation des risques, s'appelle ?

Soumettre

L'objectif global de la gestion des vulnérabilités est-il d'augmenter l'exposition aux risques d'une organisation ? (oui/non)

Soumettre

Tâche 3 Classification des vulnérabilités

Alors que les fournisseurs de sécurité préfèrent souvent développer leurs propres spécifications de vulnérabilité, la gestion des vulnérabilités est généralement considérée comme une approche ouverte et basée sur des normes utilisant la norme SCAP (Security Content

Automation Protocol) du National Institute of Standards and Technology (NIST). Les principaux composants de SCAP sont les suivants :

- **Vulnérabilités et expositions courantes (CVE)** : [MITRE](#) maintient la liste CVE des vulnérabilités et des expositions publiquement documentées. Chacun des CVE identifie une vulnérabilité qui peut être exploitée pour lancer une attaque. Avec un identifiant unique, une description et au moins une référence publique, CVE cherche à standardiser l'identification des vulnérabilités de sécurité. Tout le monde peut accéder gratuitement au système CVE, ce qui en fait une ressource précieuse pour les professionnels et les organisations de gestion de la sécurité. [CVE Details](#) est également un site Web renommé pour la recherche de CVE et leur impact.

Vulnerability Details : [CVE-2021-23885](#)

Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.

Publish Date : 2021-02-17 Last Update Date : 2022-04-26

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	???
Gained Access	None
Vulnerability Type(s)	Execute Code Gain privileges
CWE ID	CWE id is not defined for this vulnerability

+ Products Affected By CVE-2021-23885

- Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
McAfee	Web Gateway	1

Par exemple, [CVE -2021-23885](#) illustre un identifiant CVE composé du préfixe CVE, de l'année où l'ID CVE a été attribué et du numéro de séquence. En outre, la description du CVE inclut le nom du produit concerné, les versions concernées, le fabricant du produit, la nature de la vulnérabilité, l'impact global, l'accès dont un attaquant aurait besoin pour exploiter la vulnérabilité et les entrées de code cruciales requises.

- **Énumération de configuration commune (CCE)** : une CCE donne aux problèmes de configuration du système des identifiants uniques pour relier rapidement et précisément les données de configuration provenant de différentes sources d'informations et outils. Par exemple, les identifiants CCE peuvent être utilisés pour faire correspondre les résultats de l'outil d'évaluation de la configuration avec les meilleures pratiques recommandées. Ceci est comparable à la liste CVE , qui donne les ID de vulnérabilité du système signalés publiquement.

- **Common Platform Enumeration (CPE) :** CPE est une méthode de classification et d'identification des appareils, des systèmes d'exploitation (OS) et des types d'applications au sein d'une infrastructure. Le CPE est largement utilisé dans les outils de gestion de la sécurité et des vulnérabilités pour identifier divers actifs et prendre des décisions automatisées précises grâce à une corrélation avec CVE et CCE.
- **Système commun de notation des vulnérabilités (CVSS) :** CVSS est un système de notation qui évalue la gravité des vulnérabilités et identifie leurs caractéristiques. Il attribue des scores de gravité à toutes les vulnérabilités définies, qui sont utilisés pour hiérarchiser les efforts d'atténuation et les ressources requises en fonction de la gravité. La plage des scores possibles va de 0 à 10, 10 représentant le plus grave.

Score CVSS (3)

Cote de gravité

0

Aucun

0,1 à 3,9

Faible

4,0 à 6,9

Moyen

7,0 à 8,9

Haut

9,0 à 10

Critique

Il existe de nombreux sites publics contenant des informations sur les vulnérabilités ; cependant, la [National Vulnerability Database](#) (NVD) administrée par le NIST est une base de données complète des vulnérabilités connues attribuées par CVE . Bien que NVD et CVE soient fréquemment utilisés de manière interchangeable, ils diffèrent à bien des égards. CVE n'est qu'une liste de toutes les entrées des vulnérabilités connues. Néanmoins, NVD est une base de données plus complète basée sur et entièrement synchronisée avec la liste CVE , garantissant que toutes les mises à jour de la liste CVE sont représentées dans NVD. Outre l'analyse des CVE, le NVD attribue également un score CVSS à chaque vulnérabilité.

Répondre aux questions ci-dessous

Qu'est-ce que le CVSS pour CVE-2013-1048 ?

Soumettre

Quelle est la complexité d'accès pour CVE-2013-1048 ?

Soumettre

Avec le CVE-2023-2022 fictif, quelle serait l'année d'attribution de l'identifiant CVE ?

Soumettre

Tâche 4 Cycle de vie de la gestion des vulnérabilités – Découvrir et prioriser

La tâche inclut une machine déployable

Démarrer la machine

Il existe six phases essentielles dans le cycle de vie de la gestion des vulnérabilités qui peuvent être cartographiées à partir du [cadre de cybersécurité du NIST](#) ; chacun comprend ses sous-processus et activités. Ces étapes peuvent être utilisées par les organisations souhaitant développer ou améliorer leur programme de gestion des vulnérabilités. Pour présenter le

processus d'exécution de la gestion des vulnérabilités, examinons une situation réelle.



Connexion à la machine

We will use Ubuntu as a test machine and Greenbone Community Edition (GCE) throughout the room. You can start the virtual machine by clicking `Start Machine`. The machine takes about 4 minutes to boot; additionally, please wait 1 - 2 minutes for OpenVAS to be configured in the background.

First, we will see a case study and then we will practically test an Ubuntu machine. In the case study, we will be scanning a Windows machine hosting a web application using `XAMPP`;

however, for the exercise part, we will be going through the scan report of an Ubuntu machine. Since this study aims to implement a vulnerability management system, the basic commands and the installation process are exempted. You can learn more about its installation in [this](#) room.

Using a practical example, let's dig deeper into various phases of vulnerability management. Open the web panel for the GCE by visiting the URL `http://MACHINE_IP:9392`. The default credentials for the platform are `admin:admin`. Ignore the unencrypted connection message on the screen, as this is for demonstration purposes only.

Step 1: Discover

The first step is to compile a list of all the environment's resources/assets, including the applications, services, operating systems, and configurations, to identify vulnerabilities. Typically, this combines both a network scan and a system scan and enables you against any potential threat to the organisation's information and critical infrastructure. For this purpose, organisation-wide scanning should be planned and conducted regularly.

Consider we are working as a Security Engineer in a cybersecurity company and have been tasked to perform vulnerability management of the company's assets. We can perform the discovery using the following steps in GCE:

Add Target: Once logged in to GCE, open the **Configuration** menu, and click on **Targets**. Once the page is opened, click the **page with a star** icon on the left side to add a new target. In the example, we will add the IP address **10.10.183.198**, which belongs to a Windows-based machine. We can scan all the subnets and networks of the company; however, for the sake of this task, we added only a single IP, as shown below:

New Target

Name: Windows

Comment:

Hosts: ☒ Manual 10.10.183.198
☐ From file Choose file No file chosen

Exclude Hosts: ☒ Manual
☐ From file Choose file No file chosen

Allow simultaneous scanning via multiple IPs: ☒ Yes ☐ No

Port List: All IANA assigned TCP [star icon]

Alive Test: Scan Config Default

Credentials for authenticated checks

SSH: -- on port 22 [star icon]

SMB: -- [star icon]

Cancel Save

Click to enlarge the image.

Add Task: Next, open the **Scans** menu, and click on **Tasks** to configure the tool to scan all the assets running on the specified target (**10.10.183.198**). Once the page is opened, click the **page with a star** icon on the left side to add a new task, as shown below. We can run the task by clicking the **start** button next to the respective task.

New Task

Name

Windows-Task

Comment

Scan Targets

Windows

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes
☐ No

Apply Overrides

☒ Yes
☐ No

Min QoD

70

%

Alterable Task

☐ Yes
☒ No

Auto Delete Reports

☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest

5

 reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Cancel

Save

Click to enlarge the image.

Nous avons lancé le processus d'analyse pour découvrir tous les atouts et vulnérabilités de la cible. L'état de toutes les tâches d'analyse est disponible via le `Scan > Reports` menu de l'outil. Dès que l'analyse est terminée, nous pouvons cliquer sur l'analyse correspondante sur la même page pour voir tous les actifs identifiés et les détails de la vulnérabilité. Vous pouvez ignorer les vulnérabilités liées à GCE .

Greenbone Security Assistant

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report

Wed, May 3, 2023 12:35 PM UTC

Done

008b5e66-5c8e-4136-abfe-9c3dc3c00c83

Created: Wed, May 3, 2023 12:35 PM UTC

Modified: Wed, May 3, 2023 1:00 PM UTC

Owner: admin

Information

Results (239 of 341)

Hosts (1 of 1)

Ports (4 of 9)

Applications (7 of 7)

Operating Systems (1 of 1)

CVEs (107 of 107)

Closed CVEs (7 of 7)

TLS Certificates (2 of 2)

Error Messages (0 of 0)

User Tags (0)

Vulnerability

Severity

QoD

Host IP

Name

Location

Created

OpenSSL End of Life (EOL) Detection (Windows)

10.0 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

443/tcp

Wed, May 3, 2023 12:43 PM UTC

PHP End of Life Detection (Windows)

10.0 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

443/tcp

Wed, May 3, 2023 12:43 PM UTC

PHP End of Life Detection (Windows)

10.0 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

80/tcp

Wed, May 3, 2023 12:43 PM UTC

Report outdated / end-of-life Scan Engine / Environment (local)

10.0 (High)

97 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

general/tcp

Wed, May 3, 2023 12:37 PM UTC

OpenSSL End of Life (EOL) Detection (Windows)

10.0 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

80/tcp

Wed, May 3, 2023 12:43 PM UTC

jQuery End of Life (EOL) Detection (Windows)

9.9 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

80/tcp

Wed, May 3, 2023 12:44 PM UTC

PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)

9.8 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

443/tcp

Wed, May 3, 2023 12:43 PM UTC

PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)

9.8 (High)

80 %

10.10.183.198

ip-10-10-183-198.eu-west-1.compute.inter...

443/tcp

Wed, May 3, 2023 12:43 PM UTC

Cliquez pour agrandir l'image.

Étape 2 : prioriser

La deuxième étape consiste à regrouper et à attribuer une priorité basée sur les risques aux actifs (identifiés lors de la phase de découverte) en fonction de leur importance pour l'entreprise. Cela peut aider considérablement l'organisation à déterminer quels groupes nécessitent une attention particulière et facilitera ainsi le processus de prise de décision lors de la distribution des ressources.

Une fois les résultats identifiés, nous prioriserons les vulnérabilités identifiées dans différents actifs en fonction de leur importance opérationnelle. Les vulnérabilités des actifs conduisant à des violations de données et à l'accès à la base de données sont classées comme risque **prioritaire**, car la violation des enregistrements sensibles de l'organisation nuirait à la réputation de l'organisation et pourrait également avoir des conséquences juridiques ou réglementaires.

Répondre aux questions ci-dessous

Nous avons déjà scanné une machine Ubuntu ; par conséquent, répondez aux questions suivantes en vous basant sur le rapport d'analyse de la tâche **LinuxAppTask**.

Complet

Après analyse, quel est le nombre total de vulnérabilités de niveau moyen ?

Soumettre

Quel est le score de gravité de la vulnérabilité « **ICMP Timestamp Reply Information Disclosure** » ?

Soumettre

Quel est le système d'exploitation et le numéro de version de la machine cible ?

Soumettre

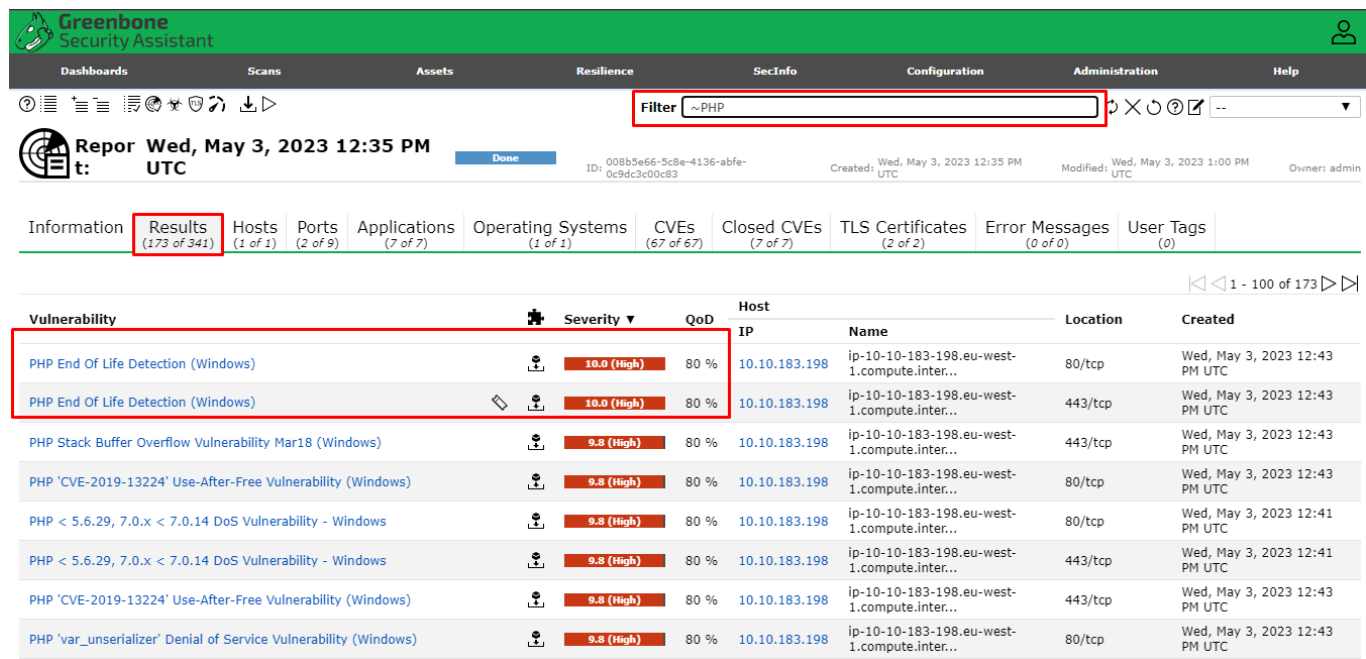
Tâche 5 Cycle de vie de la gestion des vulnérabilités – Évaluer et signaler

Étape 3 : Évaluer

La troisième phase consiste à créer une base de référence en matière de risques en évaluant vos actifs pour déterminer la gravité de chacun. Le processus permet aux organisations de décider quels risques éliminer en fonction de facteurs tels que leur classification, leur niveau de

criticité et leur niveau de vulnérabilité. À long terme, les évaluations aident les organisations à établir une base de référence cohérente.

À cette fin, nous avons examiné les actifs **les plus** risqués et avons remarqué que la plupart d'entre eux sont associés à (un langage de script côté serveur) ; c'est pourquoi nous avons décidé d'examiner d'abord les vulnérabilités de cet actif. Une liste des vulnérabilités identifiées filtrées est présentée ci-dessous. On peut constater qu'un total de **173 vulnérabilités** sont associées à cet actif par le scanner GVM OpenVAS. La plupart d'entre eux sont classés comme étant de gravité **élevée**, tandis que d'autres ont été classés comme étant de gravité **moyenne**. Seules deux des vulnérabilités associées sont classées comme étant de **faible** gravité. PHP `` PHP `` PHP



The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo', 'Configuration', 'Administration', and 'Help'. A search filter 'Filter ~PHP' is applied. The main content area shows a report for 'Wed, May 3, 2023 12:35 PM UTC'. Below the report, there are tabs for 'Information', 'Results (173 of 341)', 'Hosts (1 of 1)', 'Ports (2 of 9)', 'Applications (7 of 7)', 'Operating Systems (1 of 1)', 'CVEs (67 of 67)', 'Closed CVEs (7 of 7)', 'TLS Certificates (2 of 2)', 'Error Messages (0 of 0)', and 'User Tags (0)'. The 'Results' tab is selected, showing a table of vulnerabilities. The table has columns for 'Vulnerability', 'Severity', 'QoD', 'Host IP', 'Name', 'Location', and 'Created'. Two vulnerabilities are highlighted with a red box: 'PHP End Of Life Detection (Windows)' with a severity of 10.0 (High) and a QoD of 80%.

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
PHP End Of Life Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP End Of Life Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:41 PM UTC
PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:41 PM UTC
PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP 'var_unserializer' Denial of Service Vulnerability (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:43 PM UTC

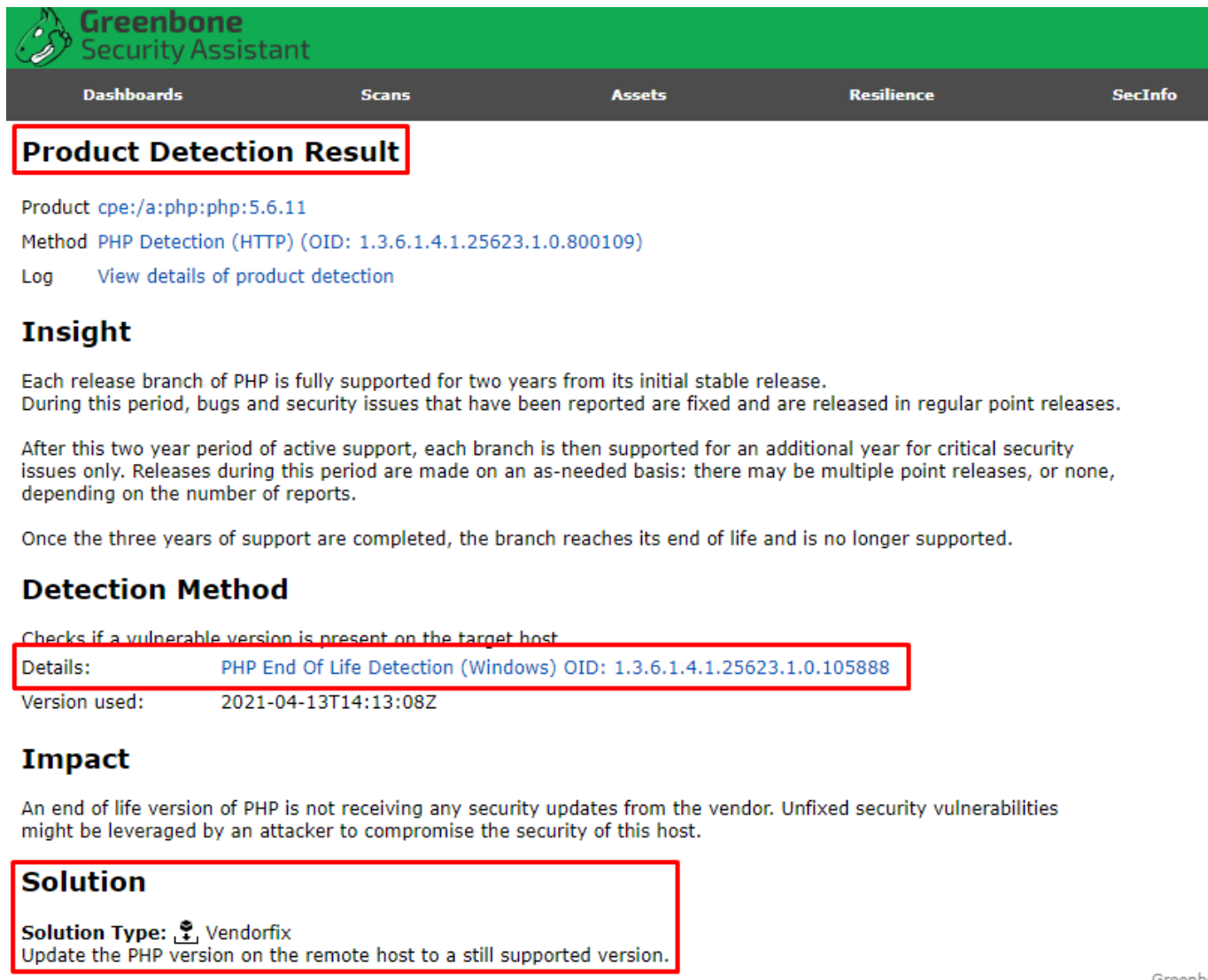
Cliquez pour agrandir l'image.

Étape 4 : Rapport

L'étape suivante consiste à utiliser les résultats de l'évaluation pour déterminer les niveaux de risque associés à chaque vulnérabilité. **Documenter et signaler** les vulnérabilités connues est crucial. Il permet aux ingénieurs de sécurité de surveiller plus facilement la dynamique des vulnérabilités sur l'ensemble de leurs réseaux et garantit que les entreprises continuent de respecter toutes les exigences et réglementations de sécurité applicables.

À cette fin, nous avons inspecté la principale vulnérabilité de gravité **élevée** avec un score CVSS de 10,0. Nous pouvons le faire en cliquant sur la vulnérabilité correspondante depuis l'interface graphique pour obtenir plus de détails sur la vulnérabilité et l'impact possible. L'image suivante montre que le GVM a fourni des informations sur la vulnérabilité et **suggéré des mesures correctives pour la corriger**. De même, nous avons inspecté la « vulnérabilité de

débordement de tampon » et plusieurs autres vulnérabilités critiques associées PHP dans les résultats de l'analyse et avons constaté qu'elles pouvaient toutes être corrigées en mettant à niveau PHP vers sa dernière version.



The screenshot shows the Greenbone Security Assistant interface. At the top is a green header with the logo and name. Below it is a dark navigation bar with tabs: Dashboards, Scans, Assets, Resilience, and SecInfo. The main content area is titled 'Product Detection Result' in a red-bordered box. It lists the product as 'cpe:/a:php:php:5.6.11' and the method as 'PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)'. There is a 'Log' link and a 'View details of product detection' link. Below this is an 'Insight' section with text explaining the support lifecycle of PHP releases. This is followed by a 'Detection Method' section, which includes a red-bordered box containing 'Details: PHP End Of Life Detection (Windows) OID: 1.3.6.1.4.1.25623.1.0.105888' and 'Version used: 2021-04-13T14:13:08Z'. The 'Impact' section describes the security risks of an end-of-life version. Finally, a 'Solution' section, also in a red-bordered box, provides a 'Vendorfix' solution to update the PHP version. The Greenbone logo is visible in the bottom right corner.

Product Detection Result

Product [cpe:/a:php:php:5.6.11](#)

Method [PHP Detection \(HTTP\) \(OID: 1.3.6.1.4.1.25623.1.0.800109\)](#)

Log [View details of product detection](#)

Insight

Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.

After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.

Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Detection Method

[Checks if a vulnerable version is present on the target host](#)


Details: [PHP End Of Life Detection \(Windows\) OID: 1.3.6.1.4.1.25623.1.0.105888](#)

Version used: 2021-04-13T14:13:08Z

Impact

An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution Type:  Vendorfix
Update the PHP version on the remote host to a still supported version.

Greenb

Cliquez pour agrandir l'image.

Avant de signaler une vulnérabilité pour correction, il est fortement conseillé de confirmer qu'il ne s'agit pas d'un faux positif, car les scanners de vulnérabilités sont sujets à de telles erreurs. Même si certaines vulnérabilités peuvent être simples à confirmer, comme celles identifiées avec des informations d'identification par défaut qui peuvent être facilement vérifiées à distance, d'autres peuvent nécessiter des efforts à distance ou de la part du client. Dans tous les cas, lorsqu'une vulnérabilité est identifiée comme un faux positif, il est recommandé de la signaler dans le rapport de l'outil pour référence future.

Répondre aux questions ci-dessous

Téléchargez le rapport **LinuxAppTask** au format PDF. Quel est l'indice de gravité de la vulnérabilité dans le rapport, où le type de solution est « **Solution de contournement** » ?

Soumettre

Quel est le type de solution pour la vulnérabilité « **horodatage TCP** » ?

Soumettre

Qu'est-ce que le CVE pour « **Divulgarion d'informations de réponse à l'horodatage ICMP** » ?

Soumettre

Tâche 6 Cycle de vie de la gestion des vulnérabilités – Corriger et vérifier

Étape 5 : Correction

Cette phase consiste à corriger les vulnérabilités découvertes précédemment, en commençant par les plus graves. Les vulnérabilités identifiées doivent être signalées aux parties prenantes concernées pour y être corrigées. Quelques approches sont à la disposition des organisations pour gérer les vulnérabilités connues et les erreurs de configuration. **Les mesures correctives, telles que la résolution approfondie ou la correction des vulnérabilités, constituent la meilleure solution** . Si une réparation complète n'est pas réalisable, les entreprises pourraient atténuer les dégâts, ce qui implique de réduire le risque d'exploitation ou de minimiser les dommages potentiels. Enfin, les ingénieurs en sécurité peuvent reconnaître leur vulnérabilité, par exemple lorsque le risque encouru est faible, et choisir de ne rien faire.

Maintenant que nous connaissons les vulnérabilités les plus critiques de l'organisation, il est temps de les signaler aux parties prenantes pour y remédier. À cette fin, nous créerons un ticket pour la `PHP` vulnérabilité et l'attribuerons à l'équipe responsable. Les tickets dans le GVM peuvent être créés à partir de l' `Detail View` interface graphique de la vulnérabilité correspondante, comme indiqué ci-dessous.

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

Filter

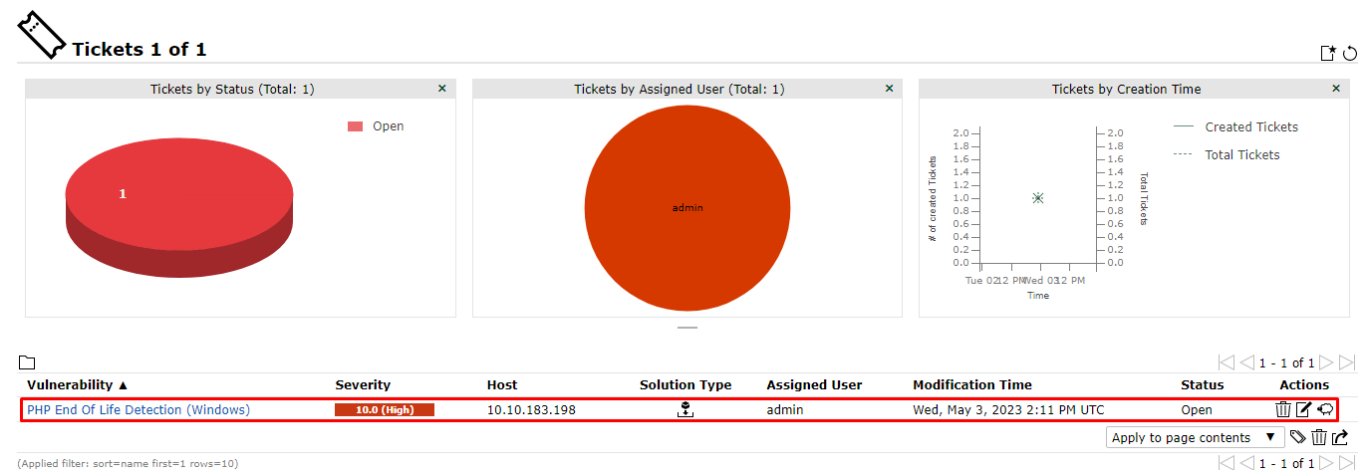
Report Wed, May 3, 2023 12:35 PM UTC Done ID: 008b5e66-5c9e-4136-abfe-0c9dc3c00c83 Created: Wed, May 3, 2023 12:35 PM UTC Modified: Wed, May 3, 2023 1:00 PM UTC Owner: admin

Information Results (259 of 341) Hosts (1 of 1) Ports (4 of 9) Applications (7 of 7) Operating Systems (1 of 1) CVEs (107 of 107) Closed CVEs (7 of 7) TLS Certificates (2 of 2) Error Messages (0 of 0) User Tags (0)

Task Name: Windows-Task
 Scan Time: Wed, May 3, 2023 12:36 PM UTC - Wed, May 3, 2023 1:00 PM UTC
 Scan Duration: 0:23 h
 Scan Status: Done
 Hosts scanned: 1
 Filter: apply_overrides=0 levels=hml min_qod=70
 Timezone: Coordinated Universal Time (UTC)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

L' équipe responsable a reçu le ticket et résoudra le problème en effectuant une mise à niveau PHP vers la dernière version. Une fois le problème résolu, ils changeront le statut en **Corrigé**. Le statut du ticket de correction peut être suivi à partir du **Resilience > Remediation Tickets** menu, comme indiqué ci-dessous.



Cliquez pour agrandir l'image.

Étape 6 : Vérification et surveillance

Lors de la dernière étape de la gestion des vulnérabilités, des audits réguliers et une surveillance des processus sont utilisés pour garantir que toutes les menaces ont été éradiquées.

À cette fin, nous analyserons à nouveau la cible après avoir appliqué le correctif. Si les résultats sont satisfaisants, nous clôturerons le ticket de remédiation.

Répondre aux questions ci-dessous

Créez un ticket pour résoudre la vulnérabilité « **Transmission en texte clair d'informations sensibles via HTTP** ».

Complet

En tant qu'ingénieur de sécurité, la priorité d'un ticket de remédiation pour une vulnérabilité critique doit être (élevée/moyenne/faible) ?

Soumettre

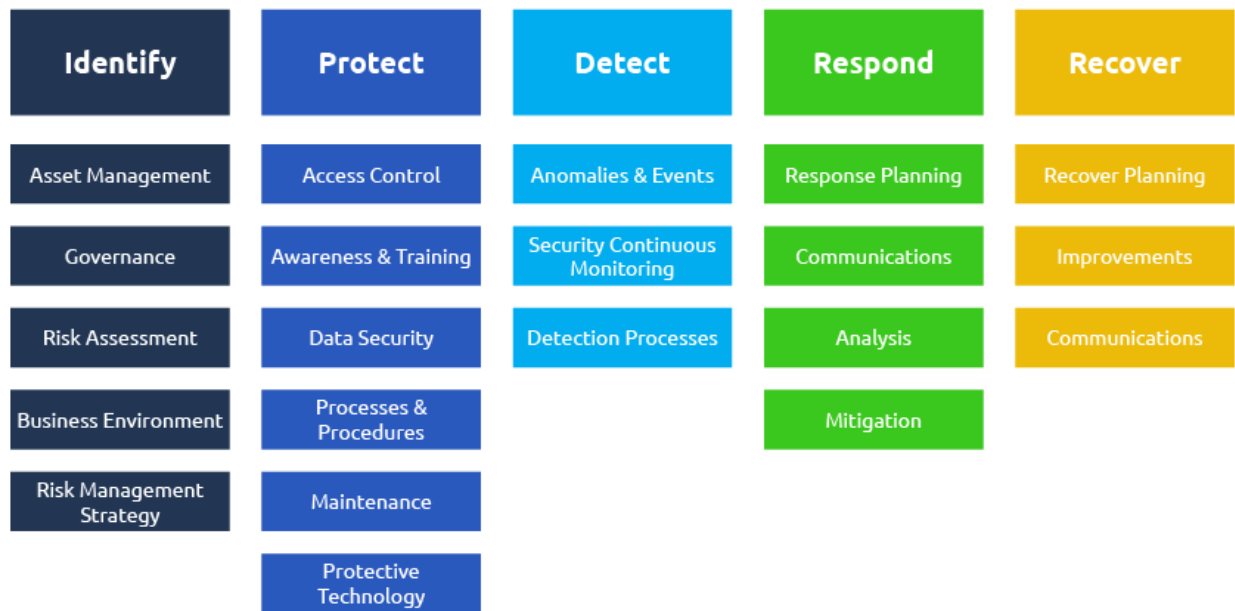
Tâche 7 Cadre de gestion des vulnérabilités

Cette tâche abordera brièvement un cadre renommé utilisé dans le monde entier pour la gestion des vulnérabilités. Le [National Institute of Standards and Technology \(NIST\)](#) a créé le [Cybersecurity Framework \(CSF\)](#) comme guide permettant aux organisations de mieux gérer et réduire leurs risques de cybersécurité. Le cadre de cybersécurité du NIST est conçu comme une stratégie de cybersécurité complète et est devenu une ressource utile de gestion des risques pour les entreprises du secteur des entreprises et les entités gouvernementales. Les composants fondamentaux du cadre de cybersécurité du NIST sont divisés en cinq domaines applicables à la gestion des vulnérabilités qui aident à atteindre les objectifs de cybersécurité d'une organisation.

- **Identifier** : Quels actifs et processus nécessitent une sécurité ?
- **Protéger** : mettre en place les mesures de sécurité appropriées pour protéger les actifs de l'organisation.
- **Détecter** : mettre en œuvre des procédures adéquates pour détecter les événements de cybersécurité.
- **Répondre** : Développer des méthodes pour atténuer les effets des incidents de cybersécurité.
- **Récupérer** : mettre en œuvre les procédures appropriées pour restaurer les capacités et les services impactés par les incidents de cybersécurité.



NIST CYBER SECURITY FRAMEWORK



The NIST CSF comprises guidelines, standards, and best practices for managing cybersecurity risk. In recent years, it gained immense popularity, and many organisations now employ the CSF to govern their cybersecurity state. Even though the NIST CSF has a broader range of applications, let's examine how to exploit its fundamental elements for vulnerability management.

Identify

The framework's first and foremost objective is to provide a solid basis for a cybersecurity program. This stage addresses the query, "**What assets require protection?**" in the context of vulnerability management. This phase may involve the following steps:

- **Develop asset discovery methodologies:** You cannot safeguard what you do not know. Implement the required tools and procedures to achieve complete insight over enterprise assets, including those on-premises and cloud assets.
- **Discover assets in real-time:** The process of discovering assets should be automated to get a near real-time picture of all the assets within the organisation.
- **Ascertain the criticality of assets:** Adding security and business relevance to the assets would assist you in prioritising their significance to your business. It's crucial to analyse as much data as possible. Unfortunately, most companies use a subjective method to estimate the importance of their assets to the business. They tend to make cybersecurity decisions based on intuition rather than data, which yields poor results.

Protect

This phase encompasses limiting or reducing the effects of a potential cyber incident and deploying the appropriate safeguards to secure the provision of IT infrastructure services. For vulnerability management, this phase addresses the query, **"Have you adopted the necessary measures to secure the assets of your organisation?"** This phase may involve the following steps:

- **Deploy security safeguards:** Make use of security systems and technology, and follow best practices, including proactive security (email security, network security, ransomware and anti-malware protection), preventative security (encryption, regular backups) and Information Security Management Systems (ISMS) (patch management solutions, Identity Access Management (IAM), Security Information and Event Management (SIEM), and Data Loss Prevention (DLP)).
- Deploy vulnerability management software.

Detect

This phase outlines the operations performed to promptly recognise a cybersecurity incident's presence. To vulnerability management, this stage addresses the query, **"Have you put in place suitable measures to discover security vulnerabilities?"** This phase may involve the following steps:

- **Detect vulnerabilities:** After you have mapped the attack surface, you must implement tools and methods to detect vulnerabilities and shortcomings in the IT infrastructure. Discovering vulnerabilities is a crucial part of a program for managing vulnerabilities.
- **Prioritise vulnerabilities:** Since every enterprise has a large number of vulnerabilities, it is essential to prioritise vulnerabilities for remediation, ensuring that the responsible team takes adequate measures to fix vulnerabilities based on their priority.
- **Quantify risks:** Once vulnerabilities are prioritised, the associated risks can be quantified by assigning a score to each vulnerability, which can be customised based on the organisation's mission. Estimating cyber risk in quantified terms gives a consistent vocabulary for prioritising initiatives and tracking the efficacy of the overall cybersecurity program.
- **Monitor constantly:** Implement tools for continuous monitoring to detect newly found vulnerabilities, new assets, and other changes in your environment.

Respond

This stage emphasises the steps required once a cybersecurity vulnerability has been identified. This process addresses the query: **"Have you implemented the necessary**

techniques and mechanisms to mitigate the vulnerability's impact?" This phase may involve the following steps:

- **Define ownership:** It is essential to determine who is responsible for addressing each vulnerability. Clarity regarding ownership warrants accountability and encourages action.
- **Establish reporting:** Reports present relevant stakeholders with the extent of vulnerabilities that have been identified. Creating risk-owner-specific reports enables progress comparisons. Leaderboards, warnings, and reminders can be utilised to encourage the concerned team member to fulfil their responsibilities for the assigned duties.
- **Share status regularly:** Provide stakeholders with timely updates on the remedial queue. A further part of status sharing is the ability to provide reports that demonstrate progress on risk mitigation and the commercial value the security program is bringing.
- **Adopt a risk acceptance approach:** Swiftly eliminating all discovered vulnerabilities is impossible. There could be circumstances where business-critical assets must be taken offline to address a vulnerability. One should establish a strategy for risk acceptance based on risk threshold and business requirements.
- **Établir des mesures correctives :** pendant les opérations normales, les équipes de sécurité doivent se concentrer sur l'éradication d'un grand nombre de vulnérabilités critiques et l'élimination des failles de sécurité rapidement et efficacement. Cependant, lorsque des adversaires exploitent activement une vulnérabilité critique récemment découverte, l'équipe de sécurité doit se concentrer sur la recherche et la publication de correctifs ou d'atténuations rapides pour remédier à ces vulnérabilités graves.

Récupérer

Il s'agit de la dernière étape du NIST CSF. Cette phase implique la mise à jour et le renforcement des plans de résilience et la restauration de toutes capacités ou services compromis causés par un événement de cybersécurité. Pour la gestion des vulnérabilités, elle répond à la question « **Avez-vous mis en œuvre les processus et technologies nécessaires à la détection et à la résolution des futures vulnérabilités ?** » Cette phase peut impliquer les étapes suivantes :

- **Mettre en œuvre des capacités de recherche sophistiquées :** avoir le pouvoir de rechercher les actifs affectés est l'une des mesures préventives requises pour la remédiation de la gestion des vulnérabilités. Lors de la phase de détection, vous devez être en mesure d'identifier rapidement et précisément tous les actifs compromis. De même, vous devriez être en mesure de confirmer que les occurrences de vulnérabilité ont été corrigées pendant la phase de récupération.
- **Étendre la sécurité aux zones non gérées :** L'utilisation croissante de l'infrastructure cloud alimente l'explosion des surfaces d'attaque au sein des organisations. Lors de la

phase de reprise, il peut s'avérer nécessaire d'améliorer la compréhension des actifs conventionnels (par exemple, ordinateurs portables, ordinateurs de bureau) et des actifs non actuellement couverts par vos solutions (par exemple, appareils IoT , actifs cloud). Une solution de gestion des surfaces d'attaque des cyberactifs (CAASM) peut combler ce vide et offrir à votre organisation une image précise et presque en temps réel de ses actifs .

- **Enregistrer les enseignements** : Réviser vos procédures pour prendre en compte les enseignements des événements de sécurité et améliorer la stratégie de cybersécurité actuelle.

Répondre aux questions ci-dessous

Le processus de liste des vulnérabilités selon leur ordre de priorité est appelé ?

Soumettre

Quelle phase implique la mise à jour et le renforcement des plans de résilience et la restauration des capacités ou services compromis causés par un événement de cybersécurité ?

Soumettre

J'ai lu les détails concernant les cinq phases du NIST CSF.

Complet

Tâche 8Conclusion

Dans cette salle, nous avons appris différentes étapes du **cycle de vie de la gestion des vulnérabilités** et comment protéger vos actifs contre les vulnérabilités en suivant un cadre de gestion des vulnérabilités renommé. La direction d'une organisation risque d'ignorer les risques de sécurité potentiels associés à son infrastructure informatique si elle ne dispose pas d'une approche de gestion des vulnérabilités.

Implementing a program for vulnerability management is all about risk management. By implementing a well-defined program, a company can gain a continuous perspective of the risk posed by security vulnerabilities in its IT infrastructure. It enables **management to make well-informed decisions regarding the risk-reduction measures** that could be undertaken.

Any organisation that wishes to understand the security threats posed by the technology it employs should implement a vulnerability management program. **Implementing a new vulnerability management approach within an enterprise can be challenging for a security engineer**. Various factors must be considered to ensure the success of a vulnerability management program, like choosing a **vulnerability scanning technique** that meets the

organisation's demands or configuring and fine-tuning the vulnerability scanning technology. Finally, it is advised that early vulnerability scans be limited in scope when beginning vulnerability management. This stops initial scans from finding a large number of vulnerabilities. A preferable strategy would be only to **select a small range of vulnerabilities** (such as OWASP Top 10) or just those issues that the vulnerability scanning program identifies as **High** severity .

Stay tuned and keep finding and patching vulnerabilities.

Answer the questions below