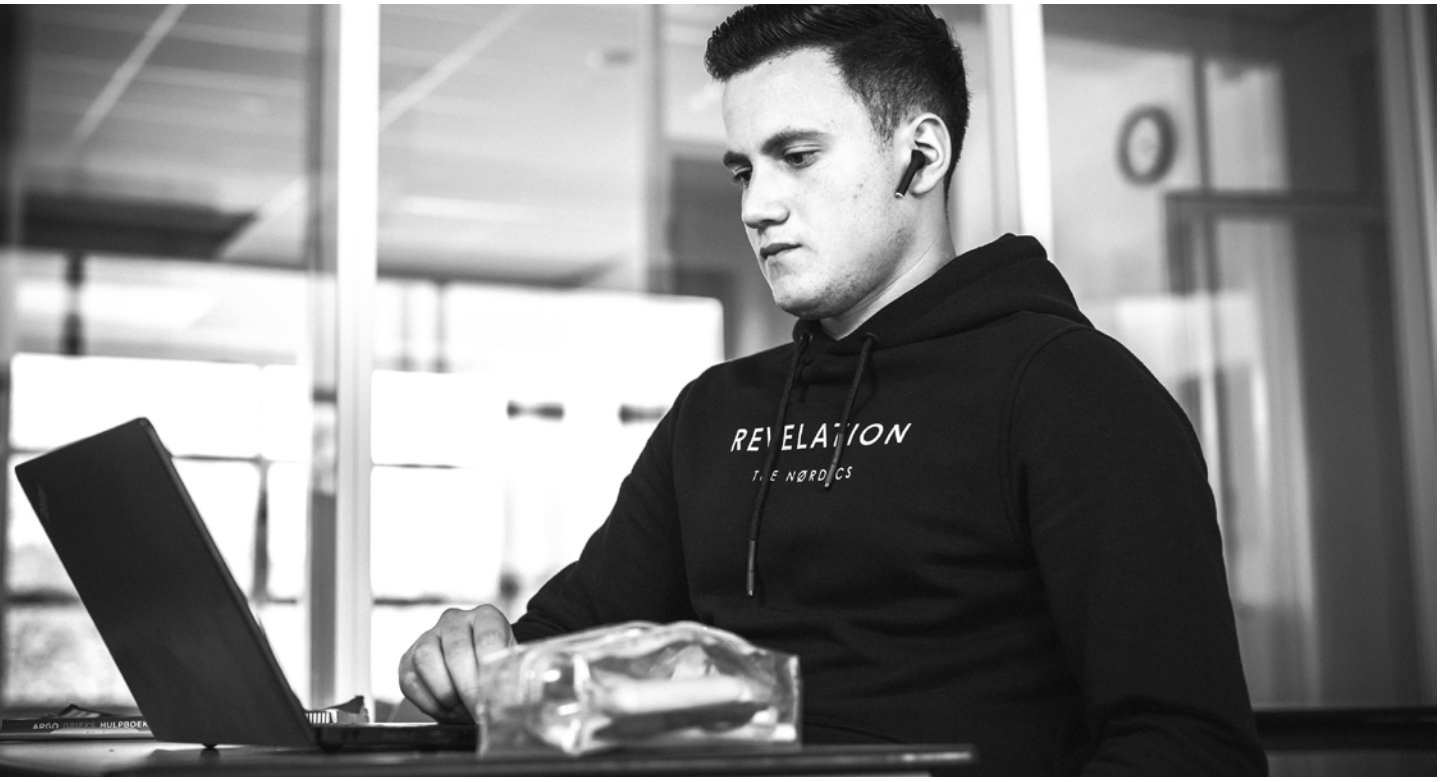
Veelgestelde vragen

Onderwijs ICT Security Scan



Onderwijs ICT Security Scan (OIS Scan) is ontstaan vanuit de groter wordende behoefte om inzicht te krijgen in de huidige situatie onder de IT-motorkap. Parallel aan deze ontwikkeling hebben we gezien dat de berichtgeving in de media over cyberaanvallen toeneemt en dat deze tot grote gevolgen kunnen leiden. Sinds 01-07-2020 biedt Breens Network de OIS Scan aan. Dit doen zij door gebruik te maken van de CSAT-software, die is ontwikkeld door haar partner QS Solutions. Uniek aan het partnership is dat Breens Network de enige partij op de Nederlandse markt is die deze software mag inzetten. Alleen al om die reden is de Onderwijs ICT Security uniek en ongeëvenaard. Wil je meer weten over de OIS Scan? Lees hier dan de antwoorden op veelgestelde vragen.

Waarom zou ik een OIS Scan willen?

Als onderwijsinstelling wil je eenvoudig en snel de status van jouw beveiliging toetsen. Je wilt inzicht in je kwetsbaarheden, die gebaseerd zijn op gegevens uit jouw bedrijfsnetwerk. De Onderwijs ICT Security Scan geeft dit door middel van een geautomatiseerde scan en de analyse van de opgehaalde gegevens. Op basis hiervan geven wij aanbevelingen en (waar noodzakelijk) een actieplan om jouw cybersecurity te verbeteren.

Is CSAT een cloudapplicatie?

Nee, CSAT wordt geïnstalleerd op een Windows Server in het IT-netwerk van de onderwijsinstelling. Alle verzamelde gegevens blijven dus ook binnen het netwerk van de onderwijsinstelling.

Wie heeft toegang tot de gegevens die CSAT verzamelt?

Alleen de onderwijsinstelling zelf en de OIS Scan consultant die de CSAT-applicatie installeert en configureert, hebben toegang tot de gegevens die worden verzameld. CSAT is on-premise geïnstalleerd bij de onderwijsinstelling, er worden nooit gegevens verzonden naar een derde partij of een cloudlocatie. De CSAT-installatie wordt na de beoordeling, in overleg met de onderwijsinstelling verwijderd.

Gebruikt CSAT mijn bedrijfsgegevens voor andere doeleinden dan een cybersecurity-beoordeling?

CSAT gebruikt de gegevens alleen om uw cyberbeveiligingsstatus te beoordelen en een op feiten en risico's gebaseerd actieplan te genereren om uw cyberbeveiliging te verbeteren. Er is een breed perspectief voor nodig om ervoor te zorgen dat alle relevante beveiligingsonderwerpen in de beoordeling worden behandeld. Dit gebeurt met behulp van vragen die zijn afgeleid van het internationaal erkende CIS-framework (Center for Internet Security). Voor meer informatie over het CIS-framework zie hier.

Installeert CSAT iets op de endpoints?

CSAT installeert geen permanente agent op de endpoints. CSAT implementeert een zogenaamde 'dissolvable agent' op de beoogde endpoints. Dit kleine uitvoerbare bestand verwijdert zichzelf van de endpoint nadat de relevante gegevens zijn teruggestuurd naar de CSAT-server in het netwerk van de onderwijsinstelling.

Hoe zit het met netwerkverkeer? Veroorzaakt CSAT-prestatieproblemen op het netwerk?

CSAT veroorzaakt geen prestatieproblemen. CSAT implementeert de agent slechts op 20 endpoints tegelijk. Zo zorgen wij ervoor dat de netwerkbelasting tot een minimum wordt beperkt.

Is CSAT een monitoringtool?

Nee, CSAT maakt een momentopname van de huidige status van uw cyberbeveiliging. Het verzamelt relevante informatie door gegevens uit endpoints (Windows-laptops/ desktops en Windows-servers), Office 365-services, Azure AD en lokale Active Directory te extraheren. Bovendien gebruikt CSAT een vragenlijst om inzicht te krijgen in organisatiebeleid en -procedures rond cybersecurity.

CSAT biedt u een op feiten gebaseerde weergave van de huidige cyberbeveiligingsstatus en beveelt actiepunten aan die uw beveiliging verbeteren. Het presenteren van deze feiten aan directie-/managementafvaardiging moet de follow-up beveiligingsprojecten verbeteren.

We hebben al een pentesttool (of andere beveiligingstools). Heb ik CSAT nodig?

Deze tools zijn zeer waardevol voor uw organisatie en u moet deze tools zeker blijven gebruiken. Monitoring- en pentesttools zijn reactief, ze stellen acties voor op basis van gedetecteerde incidenten door bepaalde elementen van uw systemen voortdurend te bewaken. CSAT hanteert een andere aanpak dan beveiligingspentest- of bewakingstools. CSAT biedt u een actieplan om de beveiliging te verbeteren, het is een holistische beoordelingstool die helpt bij het definiëren van de juiste beveiligingsverbeteringsprojecten. Naast het controleren op Windows-updates en enkele beveiligingsinstellingen, verzamelt CSAT enkele Identity Access Management-gerelateerde items, zoals (verouderde) accounts en machtigingen.

Ik heb al antivirus(tools). Heb ik CSAT nodig?

Antivirustools zijn zeer waardevol voor uw organisatie en u moet deze tools blijven gebruiken. Antivirusprogramma's werken op basis van gedetecteerde incidenten door voortdurend bepaalde elementen van uw systemen te controleren. CSAT hanteert een andere aanpak dan antivirus tools. CSAT biedt u een actieplan om de beveiliging te verbeteren, het is een holistische beoordelingstool die helpt bij het definiëren van de juiste beveiligingsverbeteringsprojecten. CSAT identificeert de AV die op een systeem wordt gebruikt en kan de updatestatus van de AV controleren.

We hebben al een pentesttool (of andere beveiligingstools). Heb ik CSAT nodig?

Deze tools zijn zeer waardevol voor uw organisatie en u moet deze tools zeker blijven gebruiken. Monitoring- en pentesttools zijn reactief, ze stellen acties voor op basis van gedetecteerde incidenten door bepaalde elementen van uw systemen voortdurend te bewaken. CSAT hanteert een andere aanpak dan beveiligingspentest- of bewakingstools. CSAT biedt u een actieplan om de beveiliging te verbeteren, het is een holistische beoordelingstool die helpt bij het definiëren van de juiste beveiligingsverbeteringsprojecten. Naast het controleren op Windows-updates en enkele beveiligingsinstellingen, verzamelt CSAT enkele Identity Access Management-gerelateerde items, zoals (verouderde) accounts en machtigingen.

Ik heb al antivirus(tools). Heb ik CSAT nodig?

Antivirustools zijn zeer waardevol voor uw organisatie en u moet deze tools blijven gebruiken. Antivirusprogramma's werken op basis van gedetecteerde incidenten door voortdurend bepaalde elementen van uw systemen te controleren. CSAT hanteert een andere aanpak dan antivirus tools. CSAT biedt u een actieplan om de beveiliging te verbeteren, het is een holistische beoordelingstool die helpt bij het definiëren van de juiste beveiligingsverbeteringsprojecten. CSAT identificeert de AV die op een systeem wordt gebruikt en kan de updatestatus van de AV controleren.

Uit welke bronnen verzamelt CSAT informatie?

CSAT verzamelt relevante informatie door gegevens te extraheren uit endpoints (Windows-laptops en Windows-servers), Office 365-services, Azure AD en lokale Active Directory. Voor elke bron wordt een andere methode van gegevensverzameling gebruikt. Voor de endpoints gebruikt CSAT een 'dissolvable agent' op de beoogde endpoints. Dit kleine uitvoerbare bestand verwijdert zichzelf van het endpoint nadat de relevante gegevens naar de CSAT-server in het netwerk van de onderwijsinstelling zijn verzonden. Voor lokale Active Directory gebruikt CSAT de beheerders-credentials om de AD-informatie uit te pakken. De Microsoft-cloudservices worden aangesproken met behulp van de API's.

Hoe verzamelt CSAT gegevens van de endpoints?

CSAT verzamelt gegevens door aanvragen via WMI-poorten te verzenden (dus deze poorten moeten open staan op endpoints). Onze 'dissolvable agent' wordt vervolgens via WMI geïnstalleerd en uitgevoerd op de endpoint. Na het extraheren van de informatie en het terugsturen naar de CSAT-server, wordt de 'dissolvable agent' automatisch verwijderd van het endpoint.

Al onze IT is uitbesteed, hoe kan CSAT van waarde zijn voor ons?

CSAT kan worden gebruikt om de huidige beveiligingsstatus van de omgeving te controleren. Als u uw IT heeft uitbesteed, is het nog steeds uw verantwoordelijkheid om te controleren of de beveiliging in orde is.

We gebruiken VDI of remote desktop verbindingen/ thinclients. Is CSAT dan nog steeds nuttig voor ons?

CSAT kan een VDI-systeem en de servers scannen. Er zijn nog steeds veel beveiligingsproblemen te vinden op deze systemen. We hebben de neiging om VDI-systemen slechts eens in de 3 maanden te patchen, vanwege problemen met het bedrijf dat acceptatietests uitvoert. Samen met de vragenlijst kunnen we veel onderwerpen behandelen.

Wat voor toegangsrechten zijn nodig voor een CSAT-installatie en -scan?

CSAT moet op een nieuwe server worden geïnstalleerd, dus daarvoor zijn machtigingen nodig.

We hebben het te druk voor deze beoordeling. Hoeveel tijd neemt de CSAT-scan voor mijn team in beslag?

Uw team zal maximaal één dag besteden aan het volledig uitvoeren van het project.

- **Bijwonen van de kick-off**
- **Opleveren nieuw geïnstalleerde server**
- **De scans configureren en aanzetten**
- **Afnemen van de vragenlijst/interview door OIS Scan Consultant**
- **Bijwonen van de presentatie van de resultaten**

Voor een scan is het volgende nodig:

AD-scan
Een gebruikersaccount waarmee alle gebruikers, accounts, groepen, computers en domeinfunctionaliteitsniveaus kunnen worden opgesomd.

Endpointscan
Domeinbeheerderaccount met machtigingen voor het endpoint of een lokaal beheerdersaccount (bijvoorbeeld ingesteld via een groepsbeleid) op alle endpoints.

Office 365/Azure AD-account
Nieuw gemaakte Service-principal moet worden goedgekeurd door de globale beheerder.

SharePoint
Service-principal maken, deze goedkeuren met het SharePoint-beheerdersaccount.

Contact

Wil je weten waar je staat met de veiligheid van jouw onderwijsorganisatie? Of wil je inzicht in verbeteracties en securityprioriteiten? Wij helpen je graag.

Neem contact op met ons via sales@it-workz.nl, bel naar **088-4896700** of kijk op www.onderwijsictsecurityscan.nl