# Secquard Applicatie Gebruikers Handleiding

# DISCLAIMER

De Secquard applicatie biedt onder voorbehoud van fouten een zo volledig mogelijk overzicht van een aantal onderwerpen van alle aangesloten systemen: Hardening, patching & vunerabilities, anti-virus en active directory. Wij willen u er op wijzen dat niet alle instellingen automatisch controleerbaar zijn en daardoor niet meegenomen worden in de applicatie.

## Uitleg

In deze handleiding bespreken wij een aantal stappen die u zo snel mogelijk op weg helpen met de Secquard applicatie. Deze handleiding sluit aan op de installatie handleiding, en gaat er daarom vanuit dat de stappen die daarin worden beschreven reeds zijn doorlopen. Voor een uitgebreid overzicht van alle pagina's van de Secquard applicatie kunt u gebruik maken van de Secquard referentie handleiding.

# 1 Het instellen van de applicatie

Voordat u de applicatie echt goed kunt gebruiken raden wij aan om de volgende stappen zorgvuldig te doorlopen.

## 1.1 Het selecteren van standaarden

De kans is aanwezig dat u Secquard gebruikt om uw compliance met een of meerdere standaarden wilt aantonen. Om de compliance met uw gewenste standaard(en) weer te geven, doorloopt u de volgende stappen:

Ga naar het menu: Options -> Update Standards. Hier kunt u standaarden toevoegen en updaten. Wanneer u op update klikt, zal de standaard worden toegevoegd of geüpdatet.


Om de standaard daad werkelijk te activeren gaat u via het menu: Accounts -> Clients -> EDIT activeren, en daarna terugvinden in het dashboard. Zie ook de volgende paragraaf.

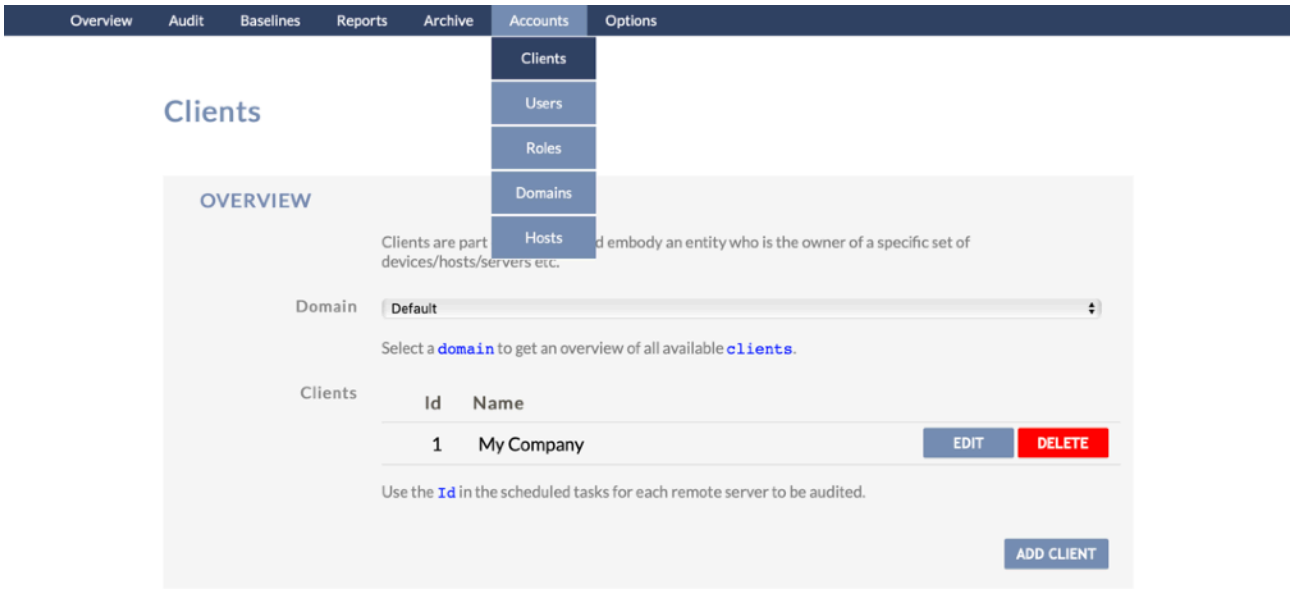
## 1.2 Client en domains

Voor veel gebruikers van de Secquard applicatie is het niet noodzakelijk om clients en/of domains aan te maken, maar voor sommige organisaties kan dit een zeer handig optie zijn. Clients zijn groepen van systemen en domains zijn groepen van clients. U kunt er bijvoorbeeld voor kiezen om uw Linux en Windows machines onder verschillende clients te verdelen en deze weer onder te brengen in een productie- en een testdomein. Voor MSP's (managed services providers) kan het handig zijn om systemen van iedere klant in

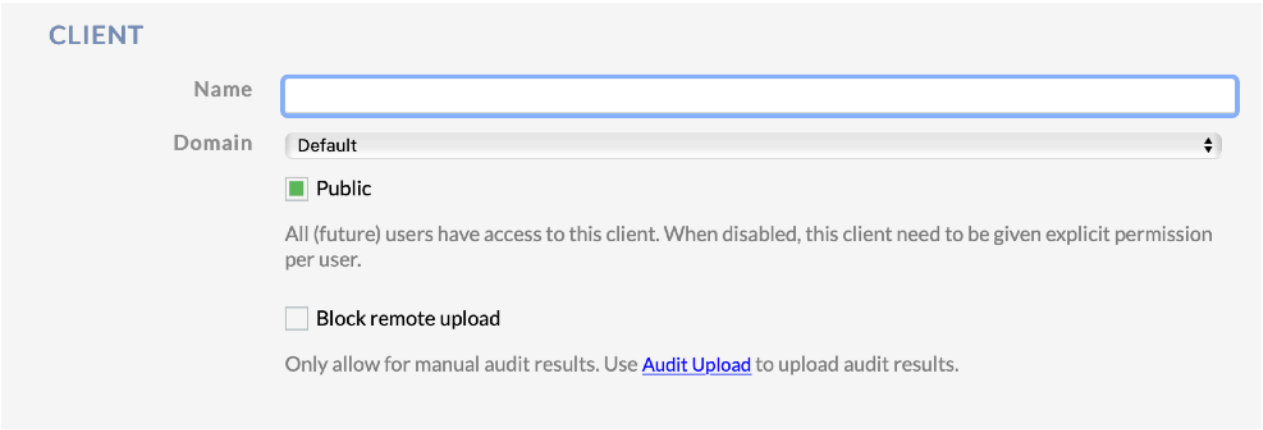
een eigen client in te delen. Of en hoe u van deze functionaliteit gebruik maakt, laten wij graag aan u over.

### 1.2.1 Clients

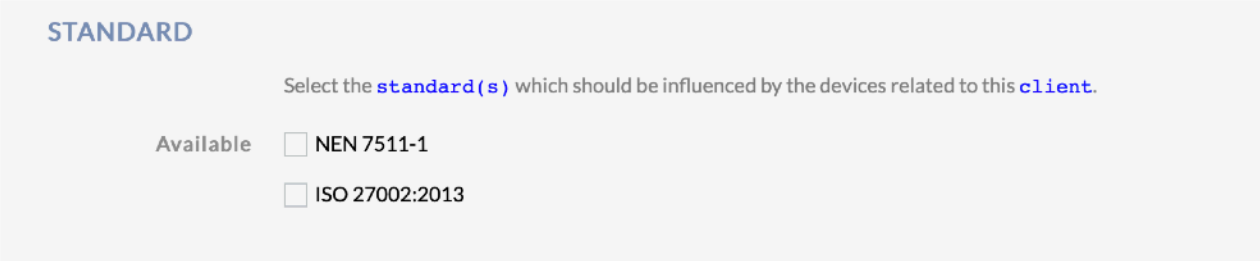
Via het menu: Accounts -> Clients krijgt u een overzicht van uw huidige clients. U kunt uw clients per domein bekijken. Daarnaast kunt u via EDIT allerlei waarden aanpassen, deze komen overeen met de instellingen voor een nieuwe client aanmaken (zie ADD CLIENT hieronder). Via DELETE kunt u de client verwijderen.



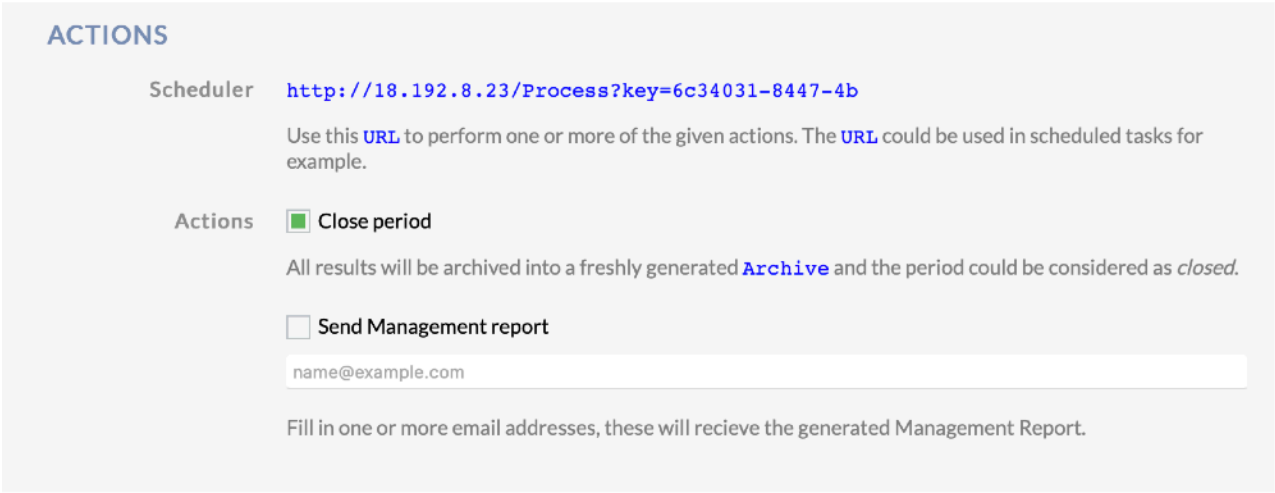

Via EDIT of ADD CLIENT kunt u een bestaande client aanpassen of een nieuwe toevoegen. Hier kunt u een flink aantal parameters instellen zoals hieronder beschreven. U kunt de client een naam geven en aangeven of deze client voor iedere user beschikbaar is.



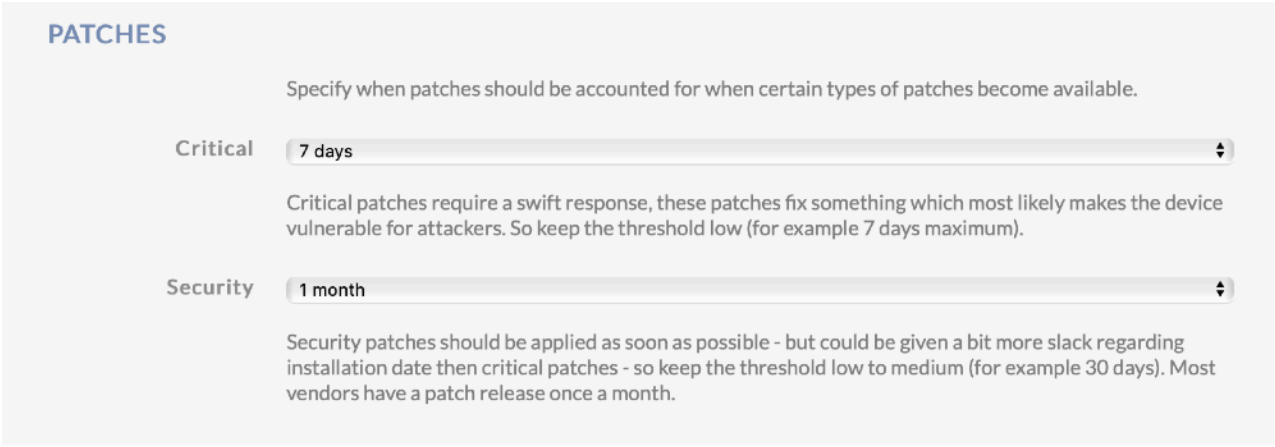
Als we verder naar onder scrollen kunnen we door middel van vinkjes aangeven welke standaarden moeten worden meegenomen voor deze client. Mist u een standaard? Zie vorige paragraaf.



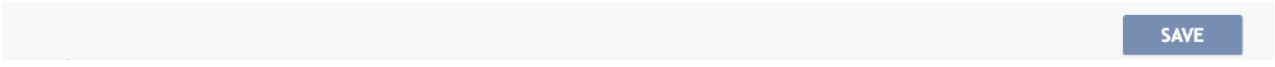

Het onderdeel actions is bij de installatie van de applicatie behandeld.




Bij patches kunt u uw patchbeleid aangeven. Vul in binnen hoeveel tijd kritische en security patches geïnstalleerd moeten zijn om als compliant beschouwd te worden.

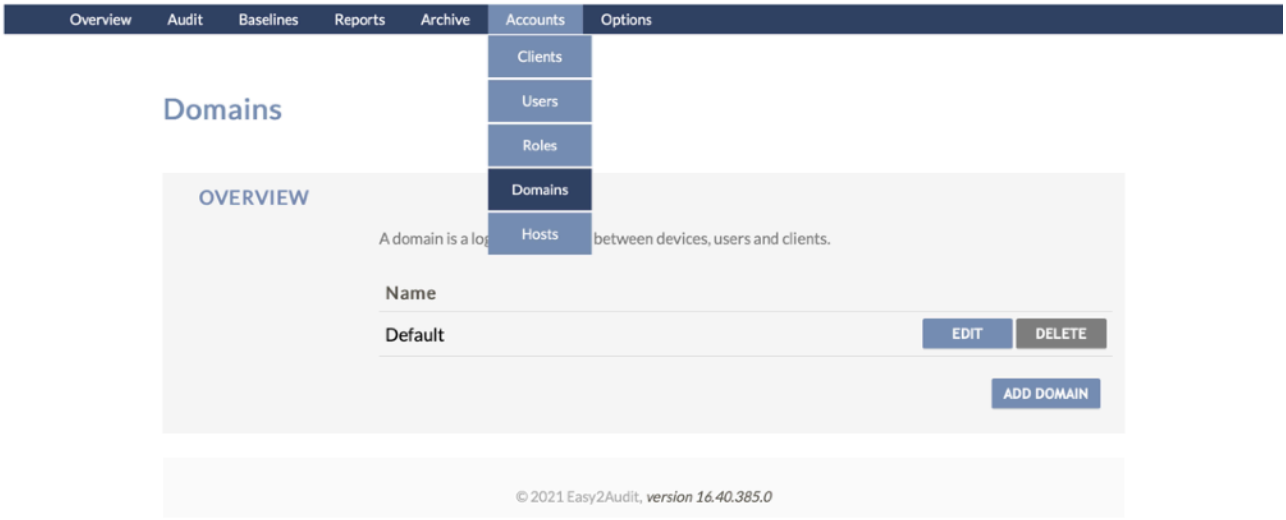



Als laatst op deze pagina: de SAVE knop. Waarmee u bovenstaande instellingen opslaat.



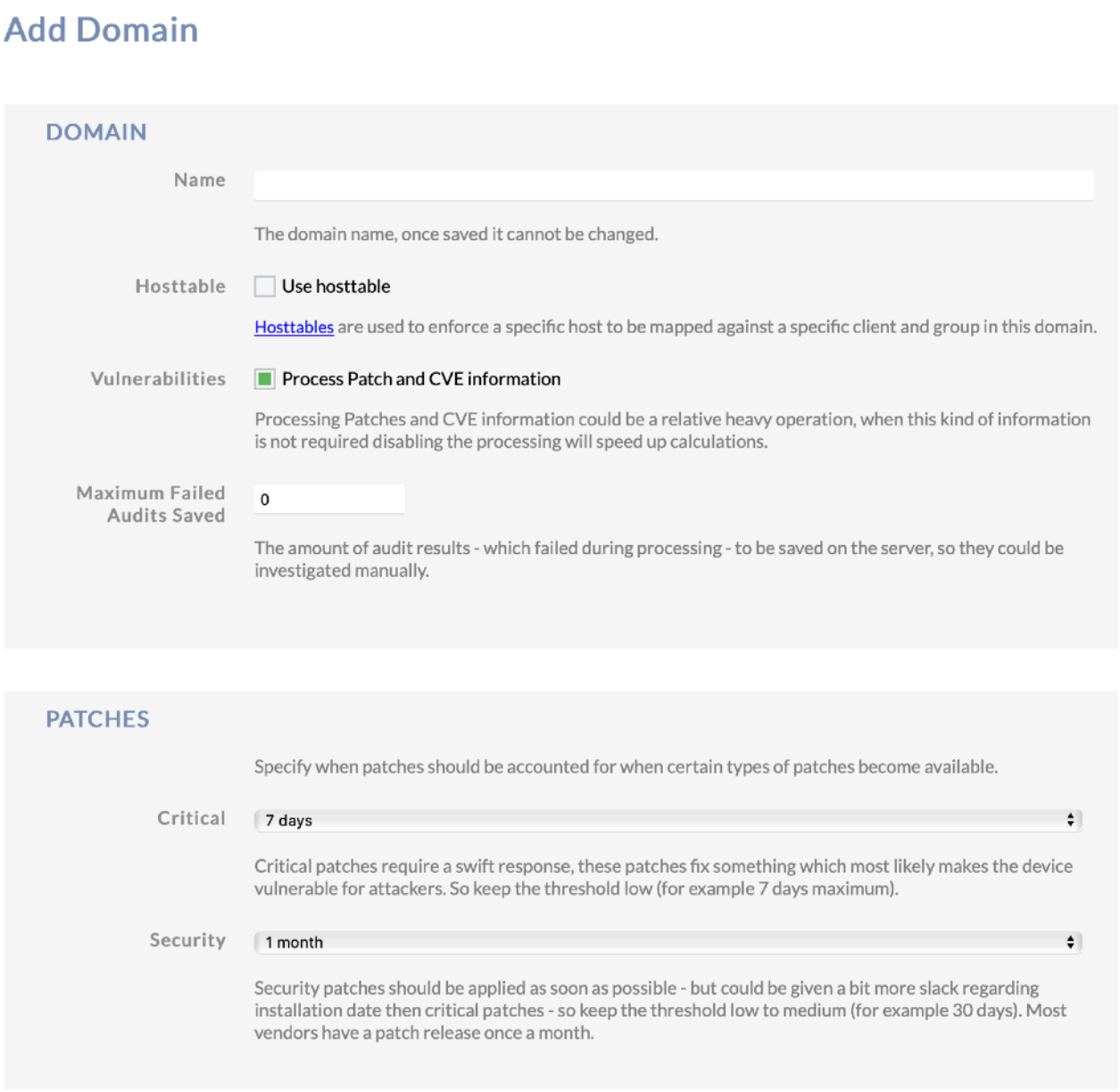
### 1.2.2 Domains

Via het menu: Accounts -> Domains kunt u domeinen toevoegen of aanpassen. Binnen een domein kunt u meerdere clients hebben, binnen die clients kun u verschillende hosts hebben (systemen).



Wanneer u op EDIT of ADD DOMAIN klikt, kunt u een naam toevoegen of wijzigen en aangeven of u gebruikt wil maken van een host table (als dit zo is, dan weet u hiervan). U kunt kiezen om vulnerabilities wel of niet mee te nemen in audits en het maximaal aantal gefaalde audits dat bewaard wordt.

Eronder kunt u voor het domein aangeven binnen hoeveel dagen uw critical en security patches geïnstalleerd dienen te zijn om als compliant beschouwd te worden. Als u zowel bij domains als clients een beleid heeft, is dat van clients leidend.

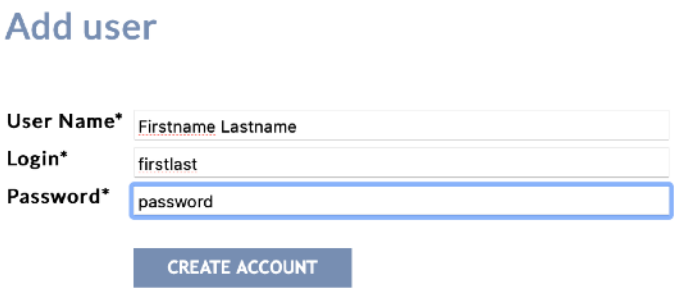


## 1.3 Het aanmaken van gebruikers

Via het menu Menu: Accounts -> Users

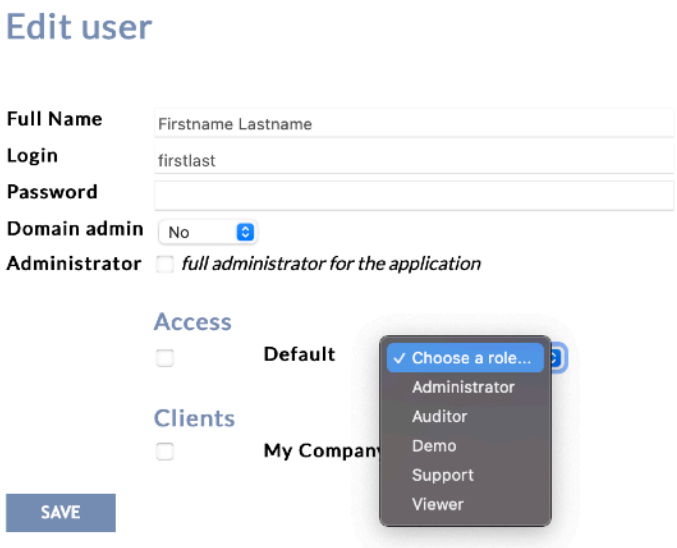
In dit onderdeel van het menu kunt u gebruikers aan de applicatie toevoegen, aanpassen en verwijderen, en hen een rol toekennen.


Het aanmaken van een gebruiker is heel eenvoudig. Klik op ADD USER… Vul een voor- en achternaam in, een gewenste gebruikersnaam en een wachtwoord. Klik op CREATE ACCOUNT.




Daarna komt u automatisch op de edit user pagina. U kunt deze pagina ook bereiken door op het potloodje naast een gebruiker te klikken in het gebruikersoverzicht (menu: Accounts -> Users).

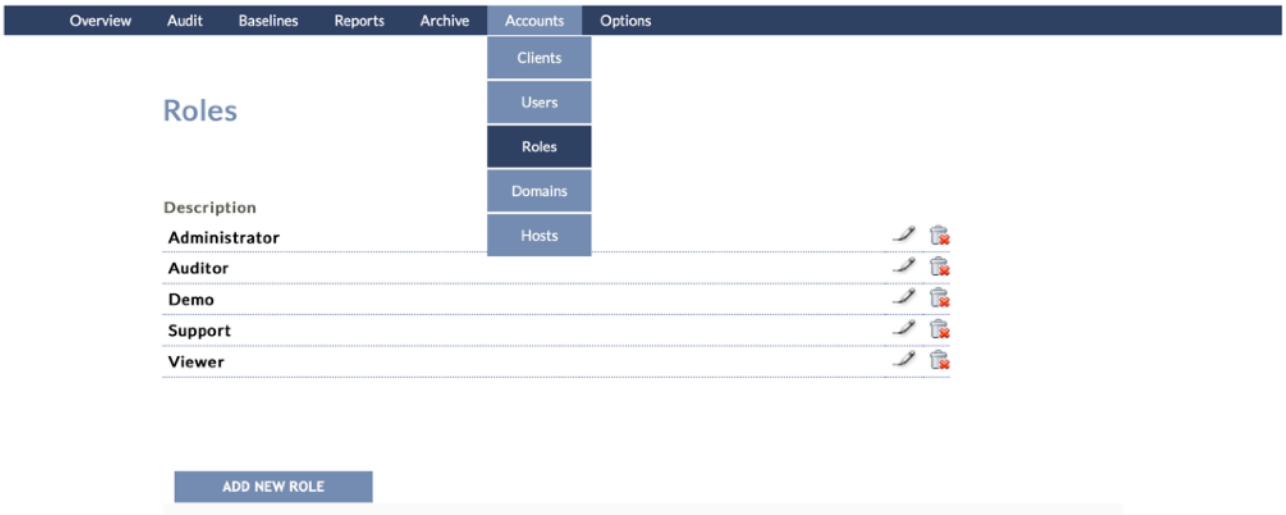
Hier kunt u aanpassingen maken aan de naam en gebruikersnaam van de user. Daarnaast kunt u aangeven of de gebruiker beheerder is van een domein of van de applicatie. Ook kunt u een rol toekennen per domein en aangeven of de gebruiker toegang heeft tot clients die niet gekenmerkt zijn als public.



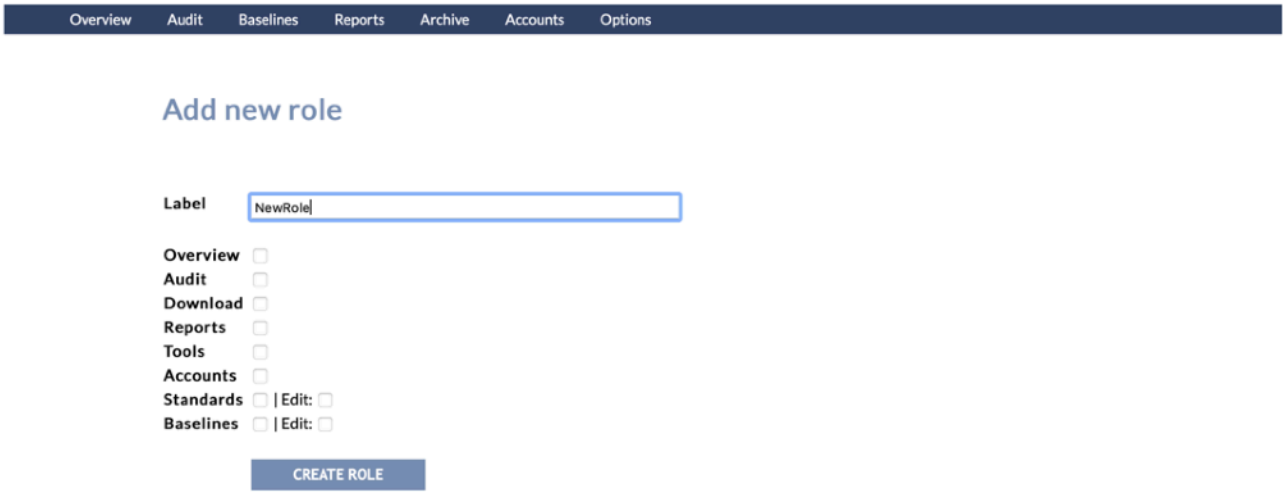

## 1.4 Het definiëren van rollen

Om zo veilig mogelijk gebruik te maken van de Secquard applicatie raden wij u aan om rollen te creëren voor (groepen van) gebruikers. Door de rechten van iedere rol te beperken tot het strikt noodzakelijke, kunt u misbruik voorkomen. Zorg er wel voor dat u per gebruiker de juiste rol toekent, zodat deze ook niet te weinig rechten heeft om zijn/ haar taken juist uit te voeren.

Ga naar het menu: Accounts -> Roles om de rollen te definiëren. U kunt nieuwe rollen toevoegen via de ADD NEW ROLE knop, of bestaande rollen wijzigen (potloodje) of verwijderen (prullenbakje).

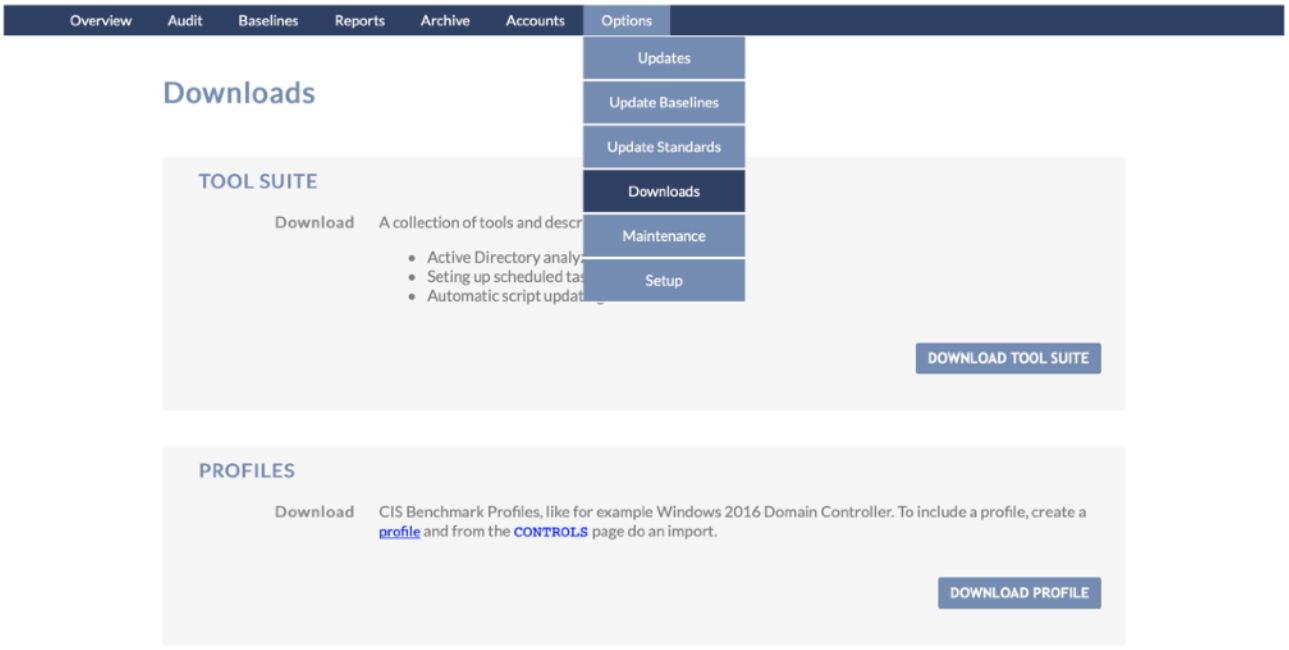


Als we een nieuwe rol aanmaken (of een bestaande rol wijzigen), kunnen we deze een naam geven, en aanvinken welke elementen van de applicatie in het menu getoond worden aan gebruikers met deze rol.

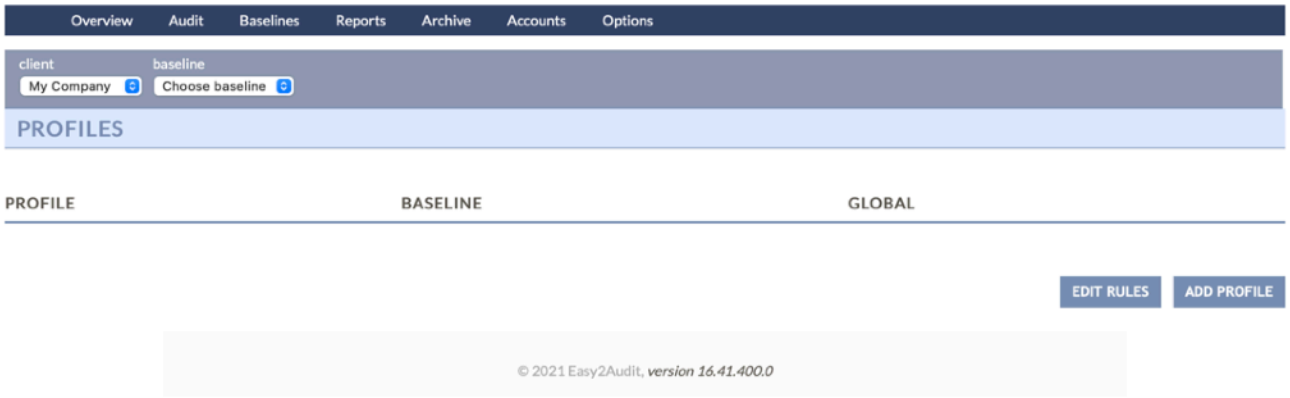



## 1.5 Het selecteren en/of aanpassen van profielen

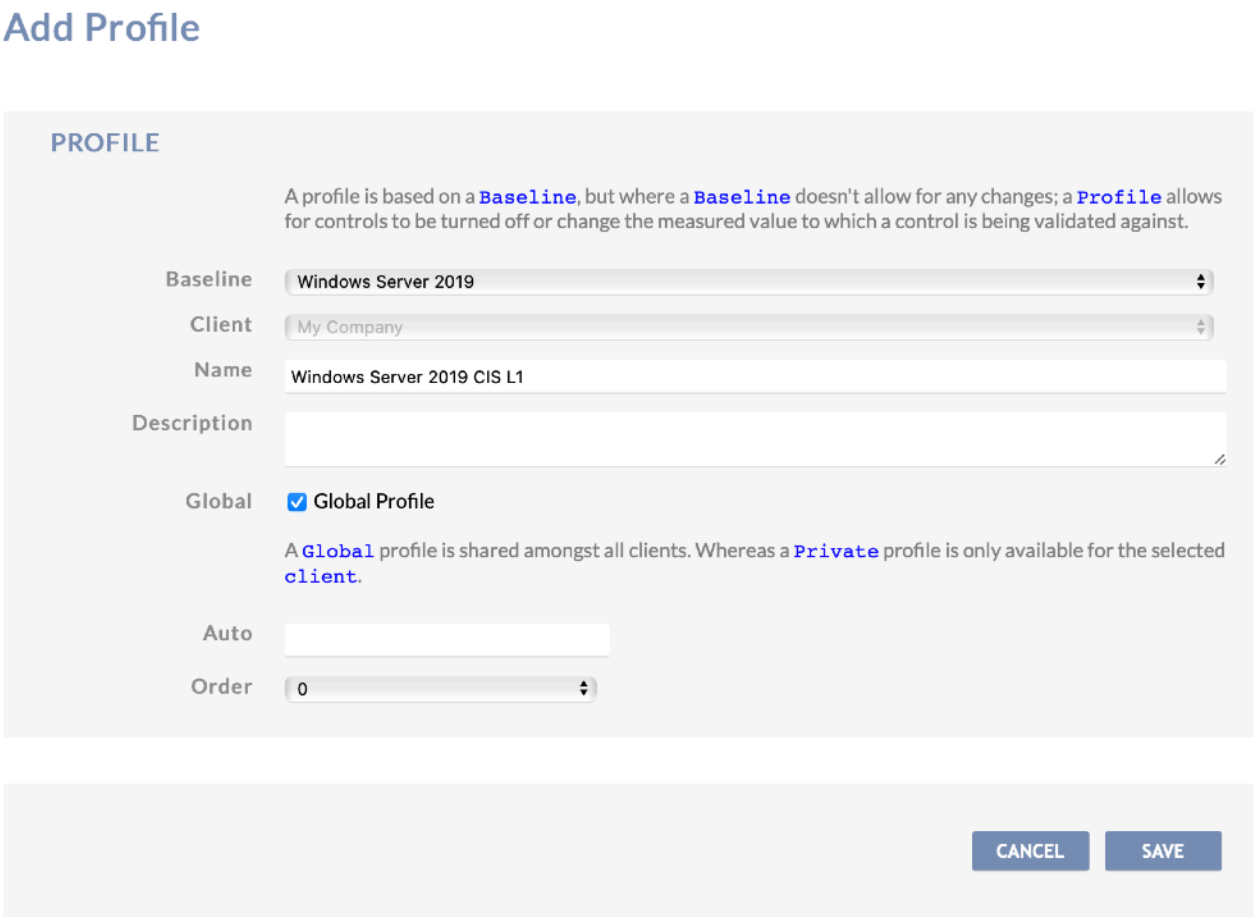
In de Secquard applicatie kunt u ervoor kiezen om profielen te gebruiken. Een profiel is een set met regels die ervoor zorgen dat bepaalde controls wel of niet worden meegenomen in een audit. Standaard worden in de Secquard applicatie alle beschikbare controls van een systeem meegenomen in audits. Met een CIS L1 (level 1) profiel bijvoorbeeld worden minder controls meegenomen dan met een CIS L2 profiel. Dit kan voor een hogere score zorgen met dezelfde instellingen. Het is belangrijk dat u de juiste profielen kiest voor de juiste systemen. Ga naar het menu: Options -> Downloads en klik op DOWNLOAD PROFILE om de profielen te downloaden.



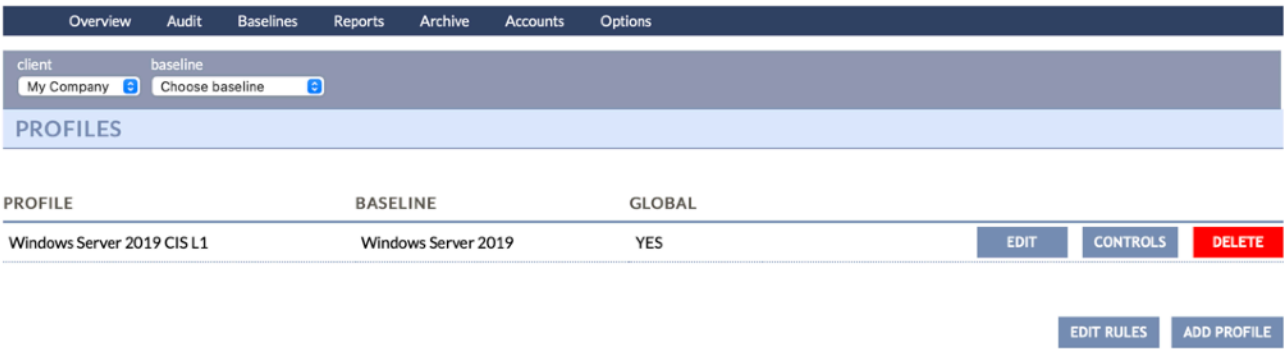
Ga vervolgens naar het menu: Baselines -> My profiles. Klik op ADD PROFILE om een profiel toe te voegen.




Kies een baseline uit voor het profiel dat u wilt gebruiken en geef het een herkenbare naam, bijvoorbeeld: Windows Server 2019 CIS L1. Geef aan of u het profiel wilt delen onder alle clients. Druk op SAVE om de instellingen op te slaan.

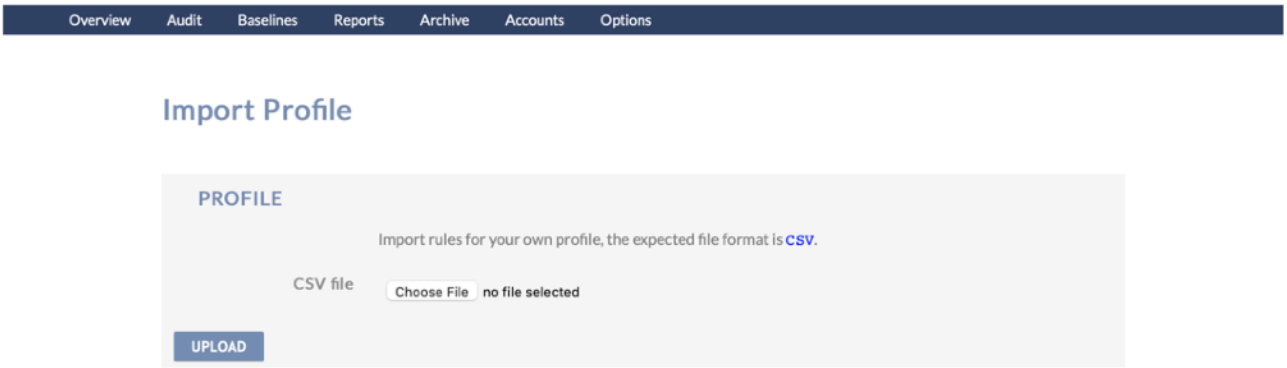


U keert nu terug naar het overzicht My profiles.

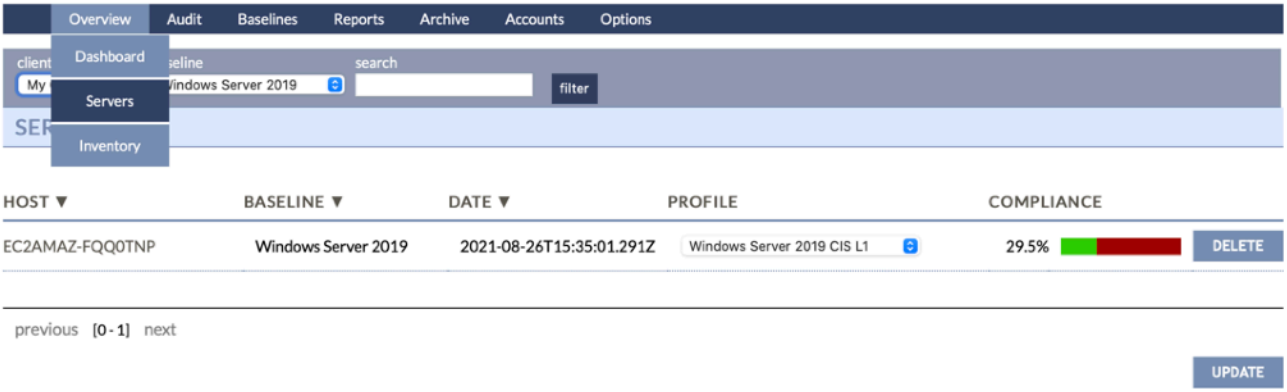



Klik op CONTROLS. U vindt u een overzicht van alle opgenomen controls van het profiel. Zoals u hieronder kunt zien, kunt u op de plusjes klikken om de hoofdstukken uit te klappen. Importeer hier het juiste profiel via IMPORT.

Klik op Choose File en navigeer naar uw downloads folder. Navigeer nu naar profiles en naar de map die het juiste OS weergeeft. In ons geval is dit Windows Server 2019. Hier kiest u het gewenste profiel. Wij kiezen voor een CIS L1 (level 1) MS (member server). Klik vervolgens op UPLOAD en daarna op CONTINUE en daarna op RECALC om compliance scores opnieuw te berekenen.




Als u nu naar het menu: Overview -> Servers gaat kunt u bij uw gekozen baseline het geïnstalleerde profiel selecteren. Klik daarna op UPDATE. En navigeer terug naar het algemeen dashboard. Hier zult u zien dat uw coulance score is aangepast aan het profiel dat u heeft geïnstalleerd.

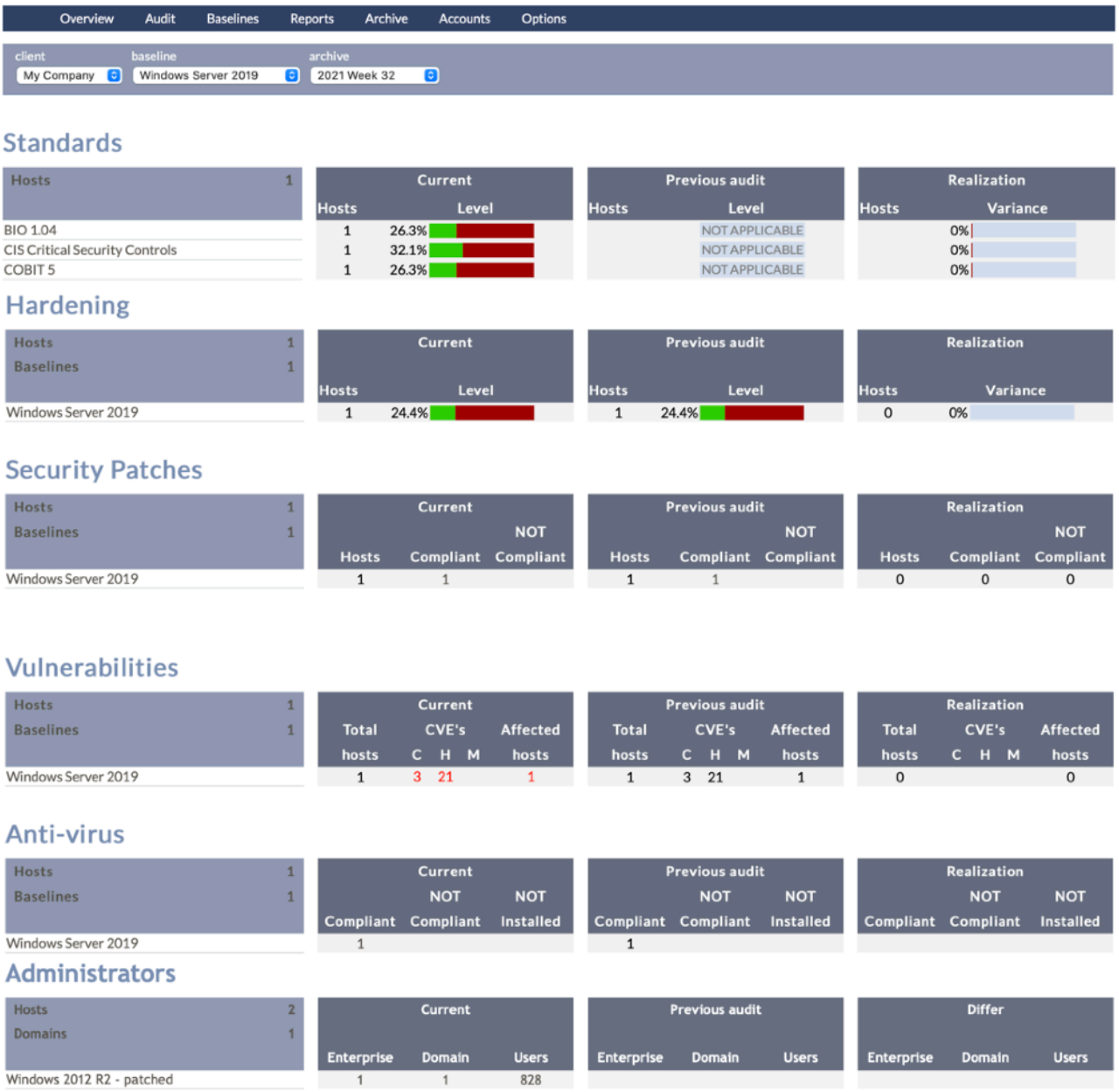


# 2 Het gebruik van de applicatie

Als u bovenstaande hoofdstukken heeft doorlopen is alles gereed voor gebruik. Daarover in dit hoofdstuk wat meer informatie. Een uitgebreid overzicht van alle pagina's van de Secquard applicatie kunt u vinden in de Secquard referentie handleiding. In het huidige hoofdstuk bieden wij u een snel overzicht van belangrijke overzichten.

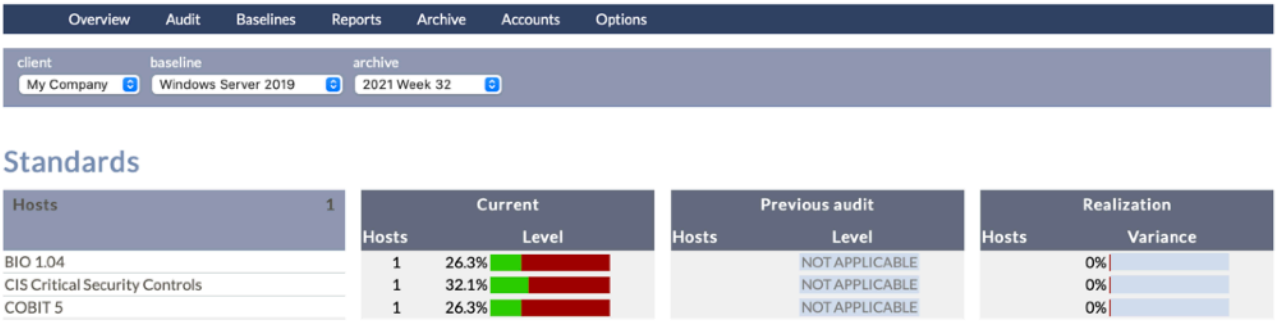
## 2.1 Dashboard

Het dashboard is de hoofdpagina van de Secquard applicatie. Hier vindt u een overzicht van de hoofdstukken: Standards, hardening, security patches, vulnerabilities, antivirus en administrators. Ook kunt u bovenaan de pagina filters instellen voor clients en baselines, en een archief selecteren om de huidige audit scores mee te vergelijken.

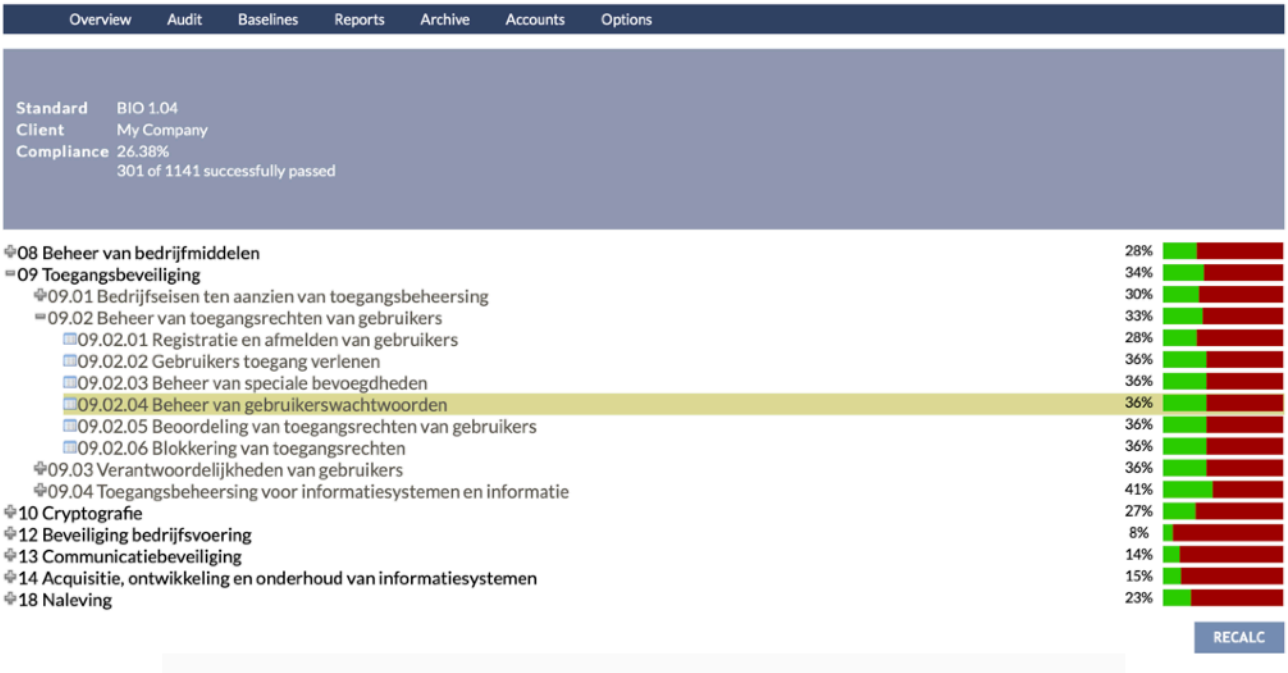


### 2.1.1 Standards

Onder standards staan standaards die u zelf heeft uitgekozen. De scores laten u zien in hoeverre uw technische maatregelen compliant zijn voor de genoemde standaard. Sommige standaarden, zoals de BIO, bestaan uit meer dan alleen technische maatregelen. Vanzelfsprekend kunnen wij deze niet automatisch auditen, daarom blijven deze buiten beschouwing in onze applicatie.

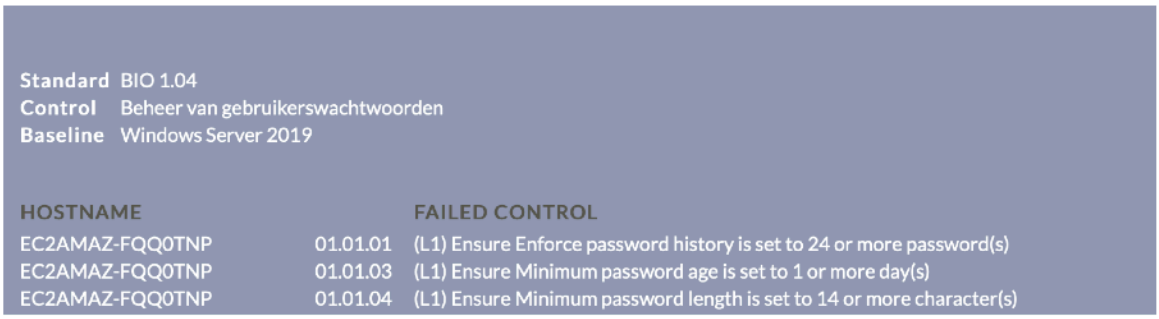



Voor dit voorbeeld klikken we op BIO 1.04 om in onderstaand scherm te komen. Door op de plusjes te drukken, klapt u de subhoofdstukken steeds uit. U kunt van de RECALC knop gebruik maken om alle scores direct opnieuw uit te rekenen. We klikken op paragraaf 09.02.04.



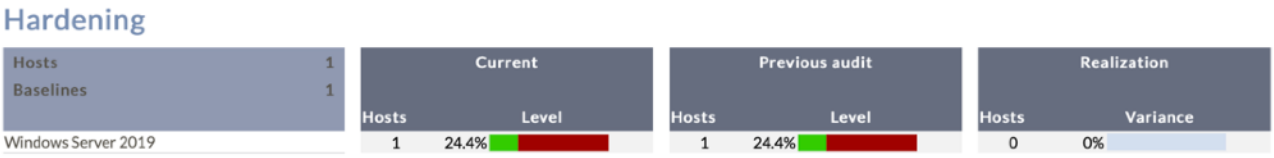
Onderstaande pop-up verschijnt. Hier ziet u informatie over de paragraaf “Beheer van gebruikerswachtwoorden”, met een beschrijving en een compliance score. Daarnaast kunt u onder FAILED zien hoeveel controls niet compliant zijn, en onder MAPPING hoe alle controls gemapped zijn naar de hoofdstukken van de standaard.


Door onder FAILED op 108 control(s) te klikken, verschijnt een nieuwe pop-up. Een deel hiervan ziet u hieronder. Hieruit blijkt bijvoorbeeld dat de minimale wachtwoord lengte van de systemen niet toereikend is, en dus lager staat ingesteld dan 14 karakters.



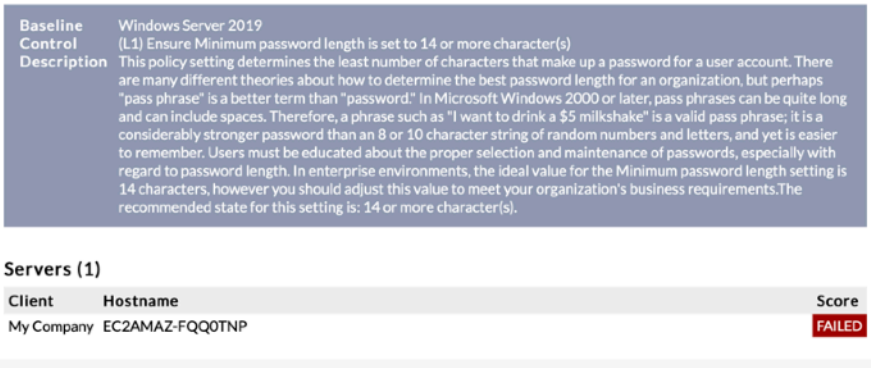
## 2.1.2 Hardening

Onder het kopje hardening vindt u een overzicht van alle systemen. In de huidige audit (current) scoort dit systeem 24.4% compliance (ten opzichte van de CIS benchmark).




Door op een baseline klikken, in dit geval Windows Server 2019, navigeert u naar een volgende pagina. Op deze pagina ziet u in hoeverre alle controls voldoen aan de CIS benchmark. Als voorbeeld zijn hier het eerste hoofdstuk en subhoofdstuk uitgeklapt door op het plusje te klikken.


Wanneer wij op een control klikken krijgen wij een pop-up, met een lijst van servers en of deze wel of niet compliant zijn.

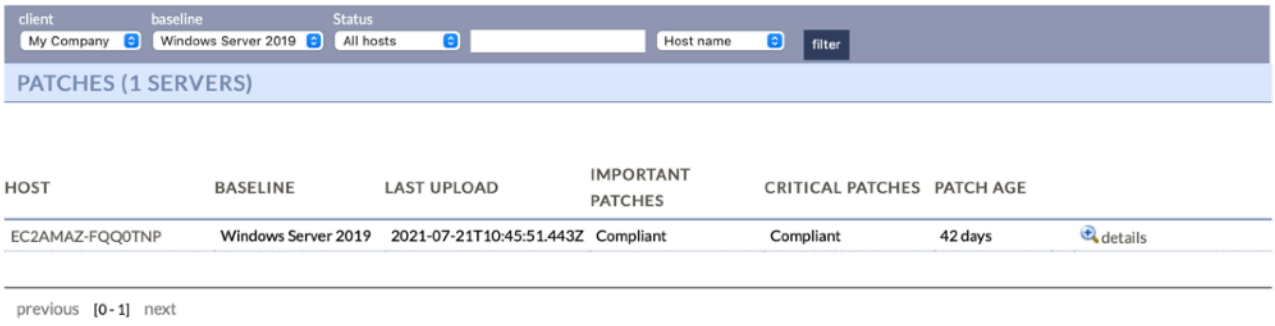


### 2.1.3 Security patches

Terug op het dashboard zien we de volgende sectie bij security patches. Hier ziet u een overzicht van alle baselines, hoeveel hosts hierbij horen en hoeveel hiervan wel en niet compliant zijn bij huidige (current) en vorige (previous) audits.


Wanneer we klikken op de baseline (Windows Server 2019), komen we bij het volgende scherm.

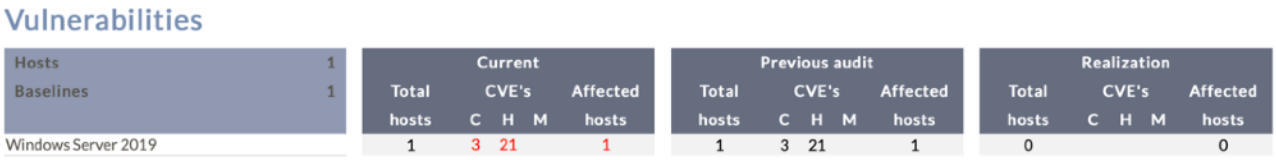
Bovenin kunt u de weergave filteren op client, baseline, status en u kunt zoeken op hostname, installed patch of missing patch.




Wanneer we op de naam van de host klikken, of op details, komen we bij het volgende scherm. Hier zien we o.a. een lijst met geïnstalleerde patches.

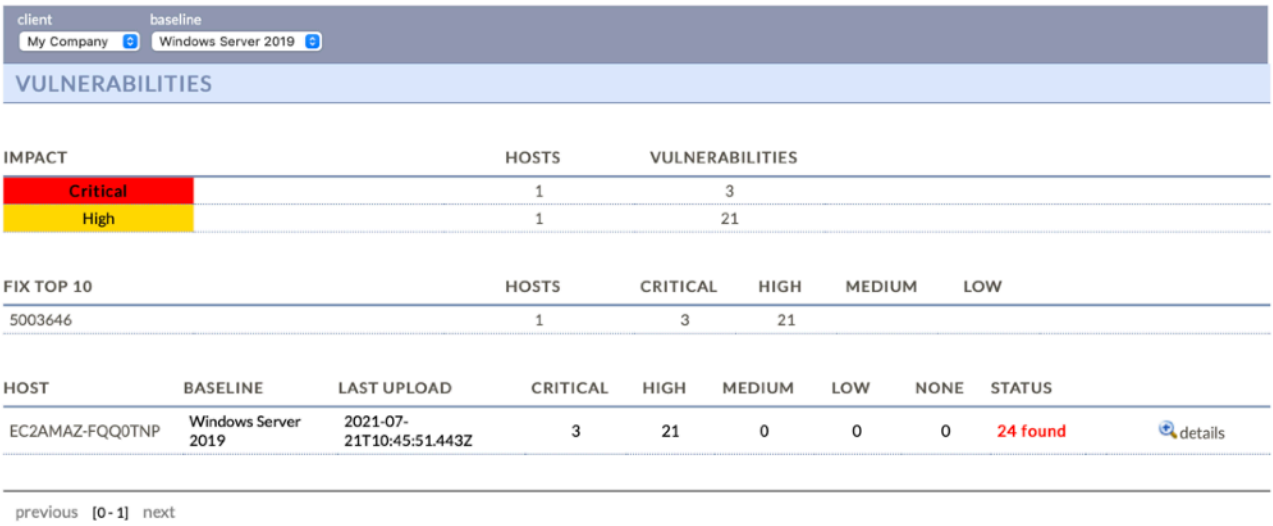
## 2.1.4 Vulnerabilities

Terug naar het dashboard, zien we bij de vulnerabilities hoeveel vulnerabilities (CVE's) er zijn gevonden op de volgende niveaus: Critical, High, en Medium.



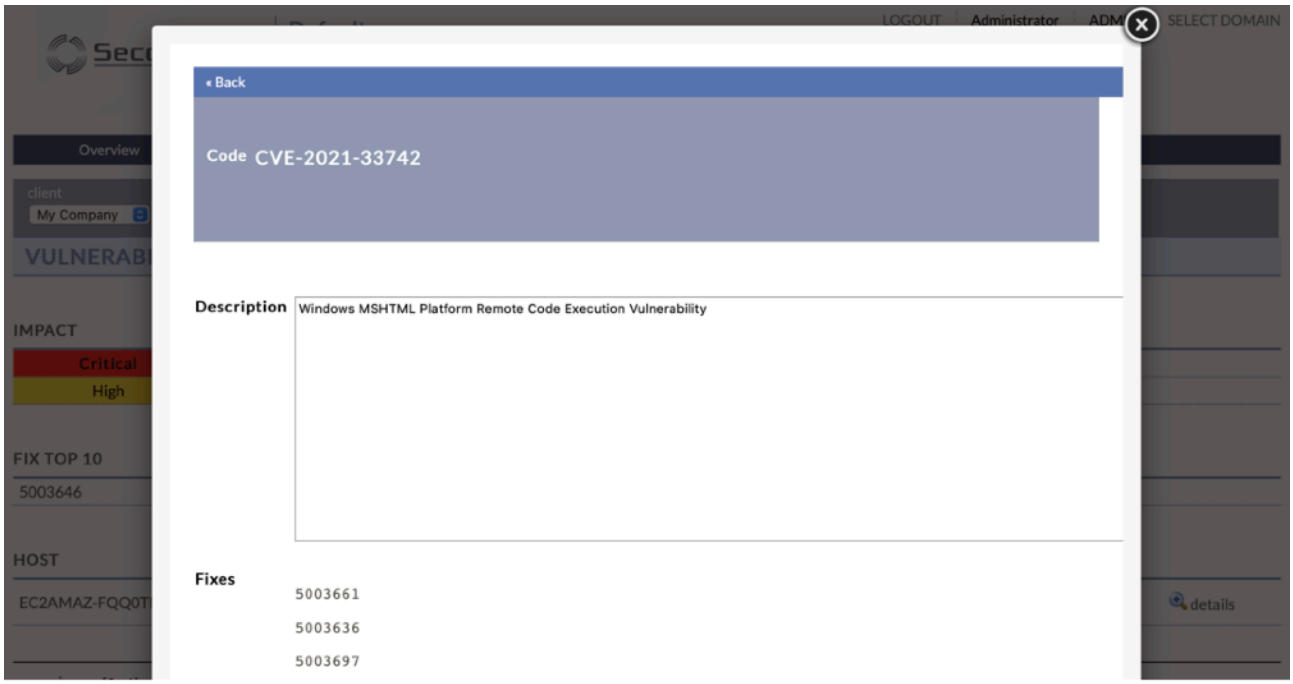

Wanneer we doorklikken door op de baseline te klikken komen we in het volgende scherm.

Wij zien in het voorbeeld nogmaals dat er voor de enkele host met de Windows Server 2019 baseline 3 critical vulnerabilities zijn gevonden, en 21 high. Wanneer we bij het kopje IMPACT op het getal klikken in de rij van critical en de kolom van hosts, krijgen we een overzicht met van alle kritische vulnerabilities per host. U krijgt voor de andere cellen in deze matrix vergelijkbare pop-ups.



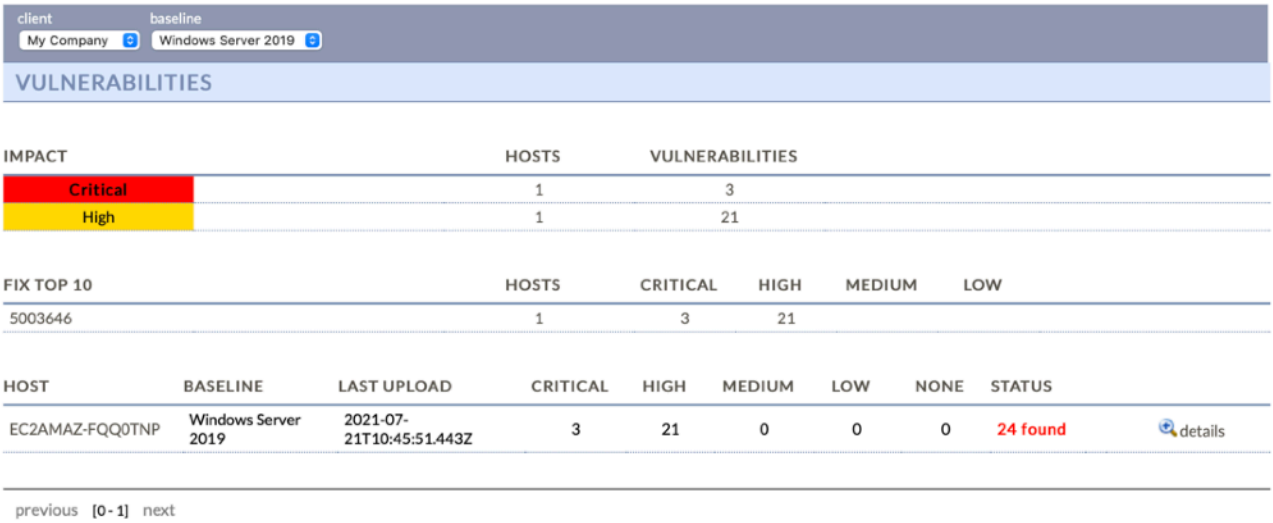

In de afbeelding hieronder vindt u het overzicht van de kritische vulnerabilities per onze enkele host. Door op info… te klikken krijgt u een pop-up met meer informatie over de specifieke vulnerability.

Hieronder ziet u de pop-up die hoort bij de bovenste vulnerability. Bovenaan de identificatie code van de vulnerability (CVE), eronder een beschrijving en daaronder een lijst met fixes die deze vulnerability verhelpen. U kunt deze fixes aanklikken, dan wordt u doorgestuurd naar de website van (in dit geval) Microsoft, waar u meer informatie kunt vinden over de fix.




Wanneer we de pop-ups wegklikken komen we terug bij vulnerabilities.

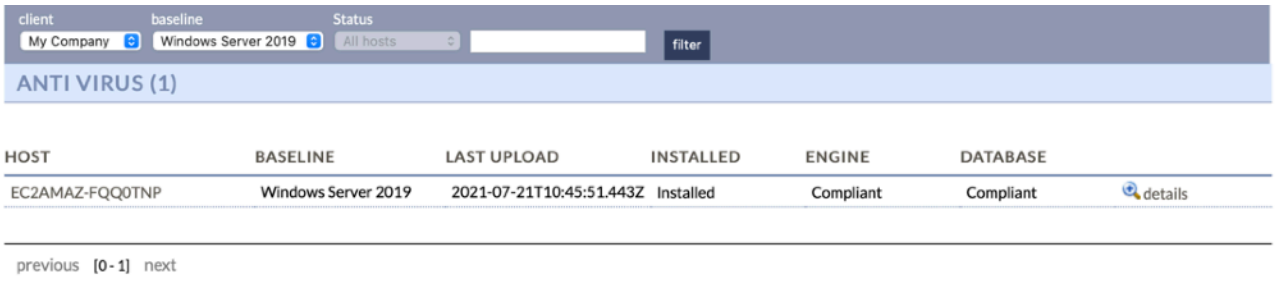
De FIX TOP 10 is een bijzonder interessante lijst. Aan de hand van een risico-analyse laat deze toptien zien welke fixes het grootste effect hebben op uw cyberweerbaarheid. In dit geval telt de lijst slechts 1 fix omdat deze fix alle gevonden vulnerabilities verhelpt. Ook hier kunt u op verschillende cellen in de matrix klikken voor pop-ups met overzichten.



### 2.1.5 Antivirus

Terug op het dashboard zien we het hoofdstuk anti-virus. Hier ziet u een overzicht van de baselines en daarbij behorende hosts, en hoeveel van deze hosts wel en niet compliant zijn.


Door op de baseline te klikken (Windows Server 2019) komen we in een volgend scherm. Hier zien we de bekende filters bovenaan en daaronder een lijst met hosts en extra informatie. We zien dat deze host compliant is omdat antivirus software is geïnstalleerd.




Klikkend op de naam van de host of op details komen we in een volgend scherm. Dit scherm toont informatie over de geïnstalleerde antivirus software en of deze momenteel draait (running).

## 2.1.6 Administrators

Onder Administrators kunt u zien welke users onder uw active directory vallen. Door op de server te klikken komt u in een volgend scherm.


Hier ziet u een overzicht van gebruikersgroepen die bepaalde kenmerken delen.


Wanneer u klikt op een kenmerk (zoals inactieve users) krijgt u een overzicht van alle daarbij behorende gebruikers.