

# HANDLEIDING CYBERALARM



## Gebruikershandleiding

---

### SecureMe2 B.V.

- Gieterijstraat 40, 2984 AB  
Ridderkerk
- Tel: +31 (0)85 0605424
  - [www.secureme2.eu](http://www.secureme2.eu)
  - [info@secureme2.eu](mailto:info@secureme2.eu)
- K.V.K. nummer: 68838557
- BTW: NL857613698B01

## INHOUD

1 Inloggen Mijn SAM.....	3
2 Overzichtspagina .....	4
2.1 Alarmeringen.....	5
2.2 Actie buttons.....	6
2.3 Whitelisting .....	7
2.4 Notificaties .....	7
2.5 Uitloggen.....	8
3 Contact .....	8

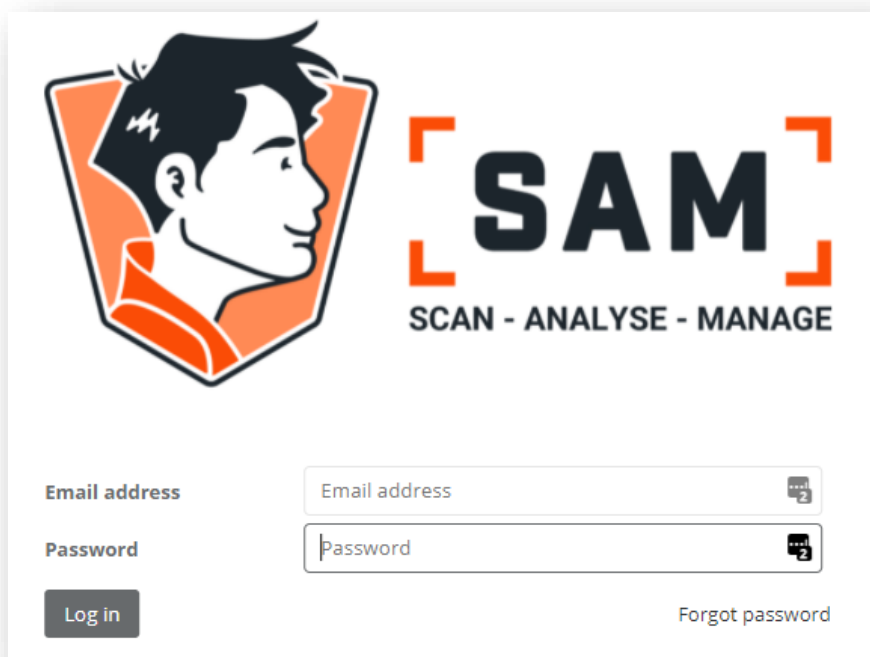
Bewerkdatum: 03-09-2021

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar worden gemaakt in enige vorm of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Secureme2

## 1 INLOGGEN MY CYBERALARM

Om uw instellingen voor My CyberAlarm aan te passen, of instellingen rondom het gebruik en het aanpassen van meldingen, kunt u inloggen in uw eigen CyberAlarm portaal. Ga hiervoor naar [www.cyberalarm.eu](http://www.cyberalarm.eu).

Middels de inlogpagina komt u vervolgens op uw eigen overzichtspagina.



**Sam**  
SCAN - ANALYSE - MANAGE

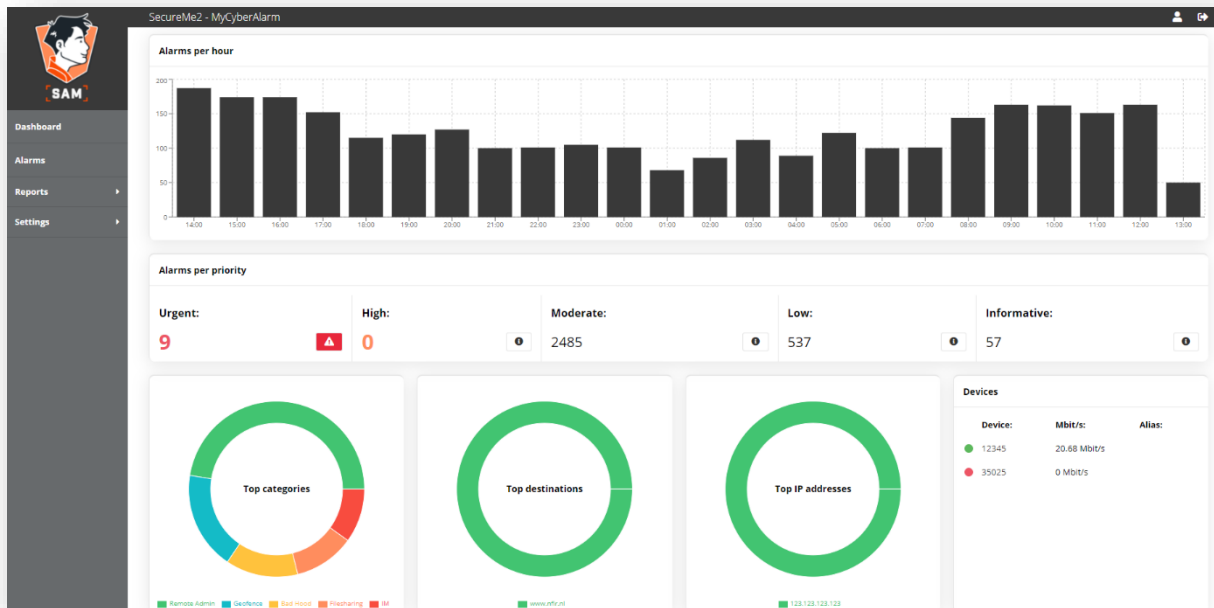
Email address

Password

Log in [Forgot password](#)

## 2 OVERZICHTSPAGINA

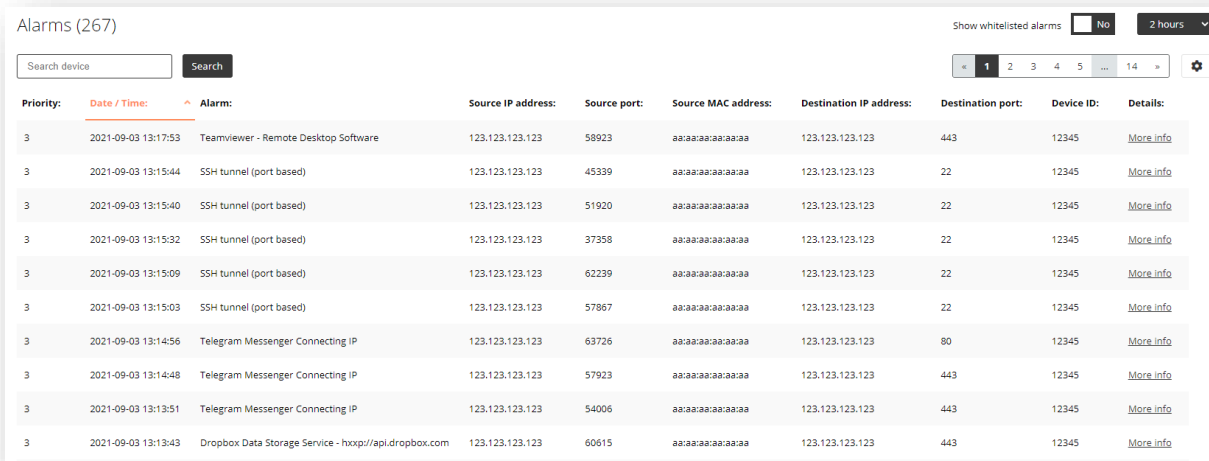
Op uw eigen overzichtspagina zijn al uw notificaties overzichtelijk samengevat. U kunt hier o.a. het aantal meldingen zien welke er in het afgelopen uur hebben plaats gevonden. Eveneens een overzicht van de eventuele meldingen gecategoriseerd per prioriteit. U kunt op deze prioriteit meldingen klikken waarna u een gedetailleerd overzicht krijgt van de melding. Mocht u tevens beschikken over meerdere SAM aansluitingen, dan kunt u deze in één oogopslag zien.



Als u merkt dat een SAM device Offline is, neem dan direct contact op met uw IT verantwoordelijke. Mogelijk zijn er werkzaamheden geweest en kan de SAM de meldingen niet meer doorgeven. Als u alsnog vragen heeft, kunt u altijd contact opnemen met Secureme2.

## 2.1 ALARMERINGEN

Het bekijken van de details van uw prioriteit meldingen is mogelijk door in de taakbalk links in uw portal op 'Alarms' te klikken. Ditzelfde kunt u ook doen door in het overzicht een prioriteit melding aan te klikken. Het details scherm geeft u specifieke informatie over een bepaalde melding.



Alarms (267)

Show whitelisted alarms  No 2 hours

Search device  Search

Priority:	Date / Time:	Alarm:	Source IP address:	Source port:	Source MAC address:	Destination IP address:	Destination port:	Device ID:	Details:
3	2021-09-03 13:17:53	Teamviewer - Remote Desktop Software	123.123.123.123	58923	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	<a href="#">More info</a>
3	2021-09-03 13:15:44	SSH tunnel (port based)	123.123.123.123	45339	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	<a href="#">More info</a>
3	2021-09-03 13:15:40	SSH tunnel (port based)	123.123.123.123	51920	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	<a href="#">More info</a>
3	2021-09-03 13:15:32	SSH tunnel (port based)	123.123.123.123	37358	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	<a href="#">More info</a>
3	2021-09-03 13:15:09	SSH tunnel (port based)	123.123.123.123	62239	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	<a href="#">More info</a>
3	2021-09-03 13:15:03	SSH tunnel (port based)	123.123.123.123	57867	aa:aa:aa:aa:aa:aa	123.123.123.123	22	12345	<a href="#">More info</a>
3	2021-09-03 13:14:56	Telegram Messenger Connecting IP	123.123.123.123	63726	aa:aa:aa:aa:aa:aa	123.123.123.123	80	12345	<a href="#">More info</a>
3	2021-09-03 13:14:48	Telegram Messenger Connecting IP	123.123.123.123	57923	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	<a href="#">More info</a>
3	2021-09-03 13:13:51	Telegram Messenger Connecting IP	123.123.123.123	54006	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	<a href="#">More info</a>
3	2021-09-03 13:13:43	Dropbox Data Storage Service - hxxp://api.dropbox.com	123.123.123.123	60615	aa:aa:aa:aa:aa:aa	123.123.123.123	443	12345	<a href="#">More info</a>

U kunt per melding nog meer info zien door rechts op 'More Info' te klikken. Hier ziet u o.a. onder 'Source - details' een IP-nummer staan. Dit adres is een specifiek adres van een computer, printer of ander device dat in uw netwerk verbonden is. Eventuele bedreigingen komen dan ook van het device met dit specifieke IP-adres

U kunt hier ook externe bronnen raadplegen zoals Virustotal en MalewarePedia. Mocht u hier niet uitkomen dan kunt u ook de optie 'Support' gebruiken. U neemt dan contact op met een medewerker van Secureme2.

Het is raadzaam om zo snel mogelijk onderzoek te doen naar de oorzaak en te zorgen dat deze mogelijke dreiging niet verder verspreid kan worden.

## 2.2 ACTIE BUTTONS

Het kan in sommige gevallen een voor u bekende melding zijn. Dit houdt in dat er wel een melding ontstaat maar dat dit voor uw bedrijf een valide verbinding of applicatie is. In dat geval kunt u de melding op uw Whitelist zetten door middel van de 'Whitelist alarm' button achter de melding. Vervolgens krijgt u dergelijke meldingen niet meer in uw dashboard.

### Create whitelisting ×

**Whitelist information:**

Alarm to whitelist	Telegram Messenger Connecting IP
Source MAC address	aa:aa:aa:aa:aa:aa
Source IP address	123.123.123.123
External IP address	123.123.123.123
Whitelist for MAC address	<input type="checkbox"/> No
Whitelist for source IP	<input type="checkbox"/> No
Whitelist for external IP	<input type="checkbox"/> No
Comment	<input type="text"/>
Whitelist expires	Never <span>▼</span>



Als u niet zeker weet of een dergelijke melding valide is, neemt u dan contact op met uw IT verantwoordelijke of met Secureme2. Zij kunnen u adviseren of het verstandig is deze melding(en) te accepteren. Het is sterk aan te raden om zorgvuldig om te gaan met Whitelisting.

## 2.3 WHITELISTING

Het bekijken van uw Uitgeschakelde meldingen, ook wel Whitelisting genoemd, is te vinden in uw taakbalk op uw overzichtspagina onder 'Settings'. Alle meldingen die volgens u of uw IT-partner, valide zijn voor uw organisatie, kunt u opnemen in deze lijst. Eventuele meldingen die in deze lijst zijn opgenomen, zullen niet meer als melding in uw portaal verschijnen

ID:	Created by:	Customer:	Device ID:	Alarm:	MAC address:	Source IP:	Destination IP:	Expires at:	Edit:	Delete:
2	user_32	SecureMe2	12345	location: Iran (IR); Asia (AS), registered: Iran (IR)	All	All	All	2021-09-03 17:26:26		
1	user_32	SecureMe2	12345	location: Indonesia (ID); Asia (AS), registered: Indonesia (ID)	All	All	All	Never		

Als het toch wenselijk is om een bepaalde melding wel te ontvangen, kunt u uitgeschakelde meldingen te allen tijde weer inschakelen door deze regels simpelweg te verwijderen. Dit kunt u eenvoudig doen door aan het eind van de betreffende regel, onder Acties, de prullenbak button te gebruiken. Vanaf dat moment is de regel niet meer in de Whitelist opgenomen en ontvangt u voor deze specifieke melding weer notificaties.

## 2.4 NOTIFICATIES

In uw portaal is het mogelijk om de door SAM gevonden meldingen te beheren. In de taakbalk op uw overzichtspagina kunt u onder 'Settings' de optie 'Notifications' aanklikken. In het overzicht van de Actieve notificaties ziet u op welk Email adres de notificaties ontvangen worden en welke prioriteit meldingen er doorgegeven worden. Eveneens kunt u aangeven of u een maandrapportage wenst te ontvangen.

### Edit notification

**Notification information:**

Email address \*

Customer \*

Priorities  1  2  3  4  5

Send monthly report notification  No

Notify when a device goes offline  Yes

Notify when a device stops processing data  Yes

Notification language \*

Created by

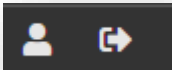
U kunt desgewenst meerdere Email adressen opgeven waar dezelfde of andere prioriteit meldingen naartoe gestuurd dienen te worden. Ook kunt u hier aangeven of er een maandrapportage ontvangen dient te worden. Middels 'New notification' kunt u vrij eenvoudig zelf deze notificatieregels aanmaken. Het is eveneens mogelijk om bestaande notificaties aan te passen of deze te verwijderen.



Het wordt sterk aanbevolen om minimaal op 1 Email adres alle notificaties binnen te laten komen.

## 2.5 UITLOGGEN

Zodra u uw meldingen heeft kunnen analyseren, acties uitgezet heeft of melding van prioriteitriten vorm gegeven heeft, vergeet dan niet om rechts bovenaan netjes uit te loggen.



## 3 CONTACT

Indien u nog vragen en/of opmerkingen heeft aangaande deze handleiding, kunt u te allen tijde contact opnemen met Securme2. Hoewel de handleiding met zorg is samengesteld kan het altijd voorkomen dat u toch specifiekere vragen heeft bij het instellen of beoordelen van uw meldingen. In dat geval kunt u te allen tijde contact opnemen met uw IT verantwoordelijke of met één van de collega's van Secureme2.