Handleiding Mijn SAM

Gebruikershandleiding

SecureMe2 B.V.
• Ericssonstraat 2, 5121 ML Rijen
• Tel: +31 (0)85 0605424
• www.secureme2.eu •
info@secureme2.eu
• K.V.K. nummer: 68838557 • BTW: NL857613698B01

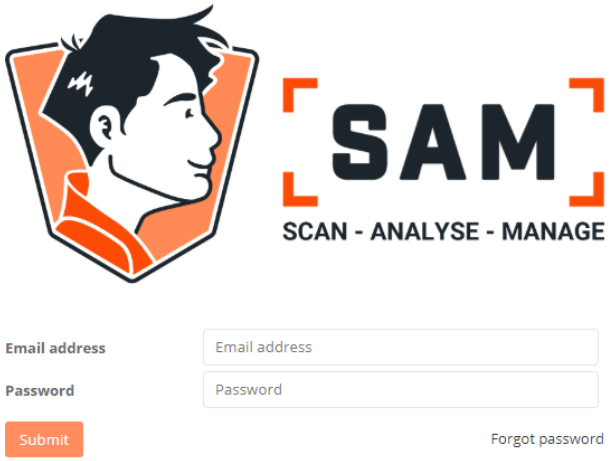
Bewerkdatum: 15-10-2018

Inhoudsopgave

Inhoudsopgave 3
1 Inloggen Mijn SAM 4
2 Overzichtspagina 4
2.1 Alarms 6
2.2 Info Buttons 6
2.2 Whitelisting 7
2.3 Notificaties 7
2.4 Uitloggen 8
3 Contact 8

1 Inloggen Mijn SAM

Om uw instellingen voor Mijn SAM aan te passen, of instellingen rondom het gebruik en het aanpassen van meldingen, kunt u inloggen in uw eigen SAM portaal. Ga hiervoor naar www.mijnsam.nl. Middels de inlogpagina komt u vervolgens op uw eigen overzichtspagina.

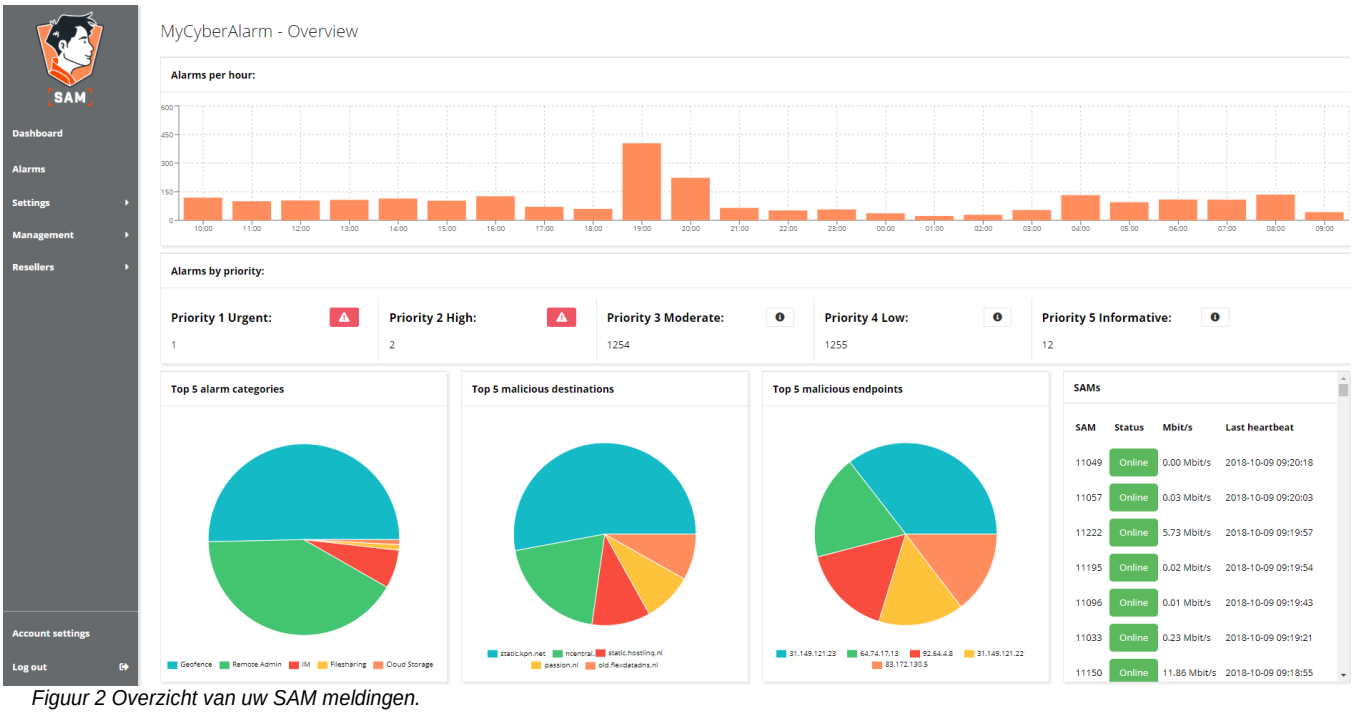


Figuur 1 Het Secureme2 Inlogportaal.

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. Evenees een overzicht van de eventuele meldingen gecategoriseerd per prio. U kunt op deze prio meldingen klikken waarna u een gedetailleerd overzicht krijgt van de melding.

Mocht u tevens beschikken over meerdere SAM aansluitingen, dan kunt u in één oogopslag zien of deze allemaal Online zijn.



Figuur 2 Overzicht van uw SAM meldingen.

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

2.1 Alarms

Het bekijken van de details van uw prio 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 prio melding aan te klikken. Het details scherm geeft u specifieke informatie over een bepaalde melding.

Priority:	Date / Time:	Alarm:	Source IP address:	Source port:	Destination IP address:	Destination port:	SAM appliance:	Details:
3	2018-10-09 09:22:20	SSH tunnel (port based)	10.34.1.121	49804	178.33.233.10	22	11193 - Spanje	
4	2018-10-09 09:22:18	location: Indonesia (ID); Asia (AS), registered: Indonesia (ID)	10.0.0.2	25	202.162.40.67	42650	11014 - Shield	
3	2018-10-09 09:21:30	Telegram Messenger	192.168.178.17	50293	149.154.167.91	443	11090	
4	2018-10-09 09:18:01	location: Ukraine (UA); Europe (EU), registered: Ukraine (UA)	192.168.11.75	20065	46.118.228.161	51413	11105 - Rosenboom	
3	2018-10-09 09:18:00	LogMeIn - Remote Desktop Software	192.168.11.93	49168	64.74.17.131	443	11105 - Rosenboom	
4	2018-10-09 09:17:33	location: Romania (RO); Europe (EU), registered: Romania (RO)	192.168.11.75	20065	5.15.33.194	36464	11105 - Rosenboom	
3	2018-10-09 09:16:55	Telegram Messenger	10.33.1.133	57379	149.154.164.224	443	11192 - Frankrijk	
3	2018-10-09 09:13:58	SSH tunnel (port based)	192.168.178.87	63524	83.172.130.54	22	11210	
4	2018-10-09 09:13:28	location: Ukraine (UA); Europe (EU), registered: Ukraine (UA)	192.168.11.75	20065	46.150.76.102	21518	11105 - Rosenboom	
4	2018-10-09 09:12:04	location: Ukraine (UA); Europe (EU), registered: Ukraine (UA)	192.168.11.75	20065	176.100.18.225	8080	11105 - Rosenboom	
4	2018-10-09 09:11:22	location: Ukraine (UA); Europe (EU), registered: Ukraine (UA)	192.168.11.75	20065	93.89.218.21	25923	11105 - Rosenboom	

Figuur 3 Gedetailleerd overzicht van uw prio meldingen.

In het Details overzicht ziet u 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. 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 houd 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 dasboard.

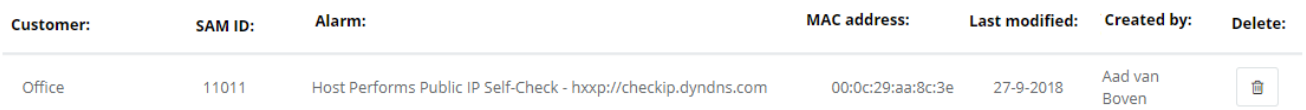
Details:

U kunt achter de melding de Details button gebruiken. Dit geeft u gedetailleerde informatie over de melding en u kunt deze opzoeken in Virustotal en MalewarePedia. Mocht u hier niet uitkomen kunt u tevens de optie 'Support' gebruiken. U neemt dan contact op met een medewerker van Secureme2.

⚠ Indien 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.



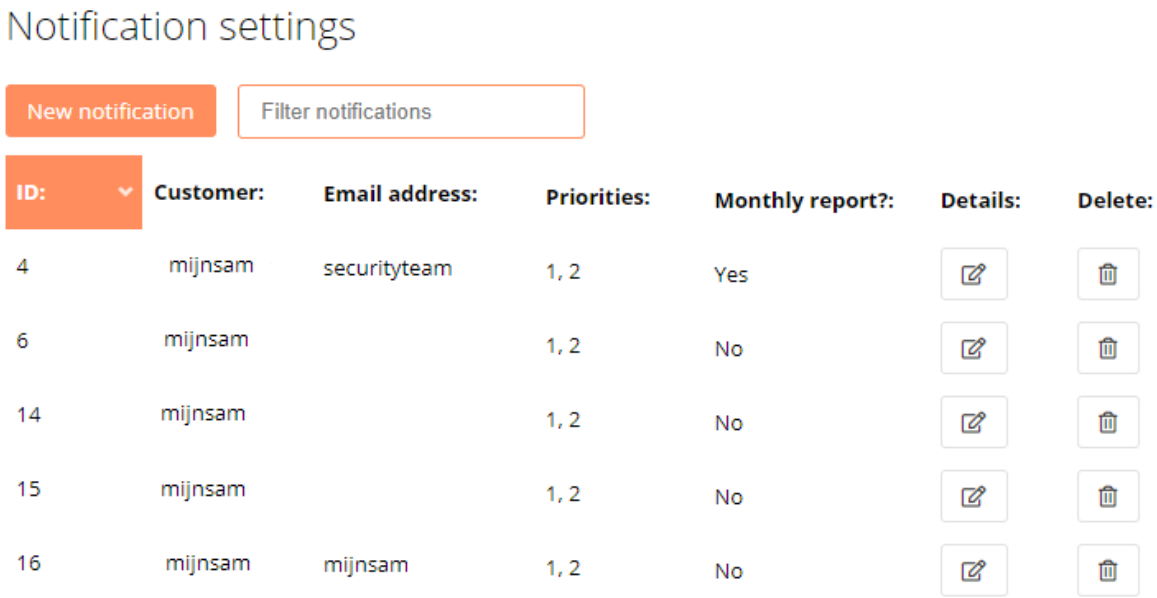
Customer:	SAM ID:	Alarm:	MAC address:	Last modified:	Created by:	Delete:
Office	11011	Host Performs Public IP Self-Check - hxxp://checkip.dyndns.com	00:0c:29:aa:8c:3e	27-9-2018	Aad van Boven	

Figuur 4 Uw Whitelisting beheren

Indien 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 prio meldingen er doorgegeven worden. Eveneens kunt u aangeven of u een maandrapportage wenst te ontvangen.



ID:	Customer:	Email address:	Priorities:	Monthly report?:	Details:	Delete:
4	mijnsam	securityteam	1, 2	Yes		
6	mijnsam		1, 2	No		
14	mijnsam		1, 2	No		
15	mijnsam		1, 2	No		
16	mijnsam	mijnsam	1, 2	No		

Figuur 5 Uw Notificaties beheren

U kunt desgewenst meerdere Email adressen opgeven waar dezelfde of andere prio 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.

2.5 Uitloggen

Zodra u uw meldingen heeft kunnen analyseren, acties uitgezet heeft of melding van prioriteiten vorm gegeven heeft, vergeet dan niet om 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.