ThreadStone CYBER SECURITY

ThreadScan ONLINE SECURITY

Dienstenbeschrijving

ThreadStone Cyber Security b.v. | HSD Campus | Wilhelmina van Pruisenweg 104
2595 AN | Den Haag | The Netherlands | info@threadstone.eu | www.threadstone.eu
T +31 (0) 85 060 7000 | KVK 61426202 | IBAN NL34 RABO 0192 0442 14 | BIC RABONL2U | BTW NL854336631.B01

Dienstenbeschrijving ThreadScan

Elke maand worden er zo'n 500 tot 1.000 nieuwe kwetsbaarheden gevonden waar misbruik van kan worden gemaakt. Door periodiek te scannen, analyseren en aanpassen bent én blijft u beschermd tegen aanvallen van buitenaf. Dit is de reden dat de ThreadScan diensten in abonnementvorm worden aangeboden.

ThreadStone heeft haar abonnementen zo opgezet, dat u een abonnement kunt kiezen dat past bij úw situatie. Doordat de frequentie en grondigheid van scannen instelbaar is, kunt u voor elk apparaat of website die gescand moet worden een passend abonnement vinden. Vraag uw Reseller naar het juiste abonnement.

Welke scan past bij mijn situatie?

ThreadStone levert in basis een drietal scans, welke zijn gericht op de IT infrastructuur, de websites of een combinatie. Om te bepalen welk type abonnement het beste kan worden gekozen, volgt hier een tabel:

Wat wil ik scannen?	Infra scan (Infra)	Web scan (Web)	Infra & Web scan (Infraweb)
• Router • Firewall • Mail server • Infrastructuur webserver			
• Website (op een shared webserver omgeving)			
• Dedicated webservers met website • Portal etc.			

Frequentie en 'diepte' van scannen

Uiteraard is het belangrijk om te bepalen wat de impact is als een onbevoegde een kwetsbaarheid vindt, waarmee hij op uw website of bedrijfsnetwerk kan komen en daar schade kan aanrichten. Afhankelijk van deze impact adviseren we de juiste frequentie en zgn. 'diepte' van scannen te kiezen. Vraag uw Reseller naar het juiste abonnement.

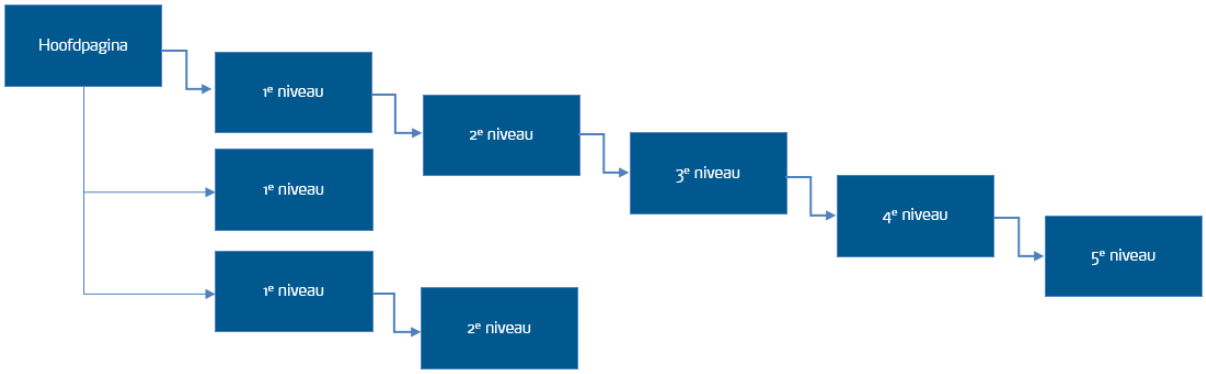
Frequenties

De abonnementen kunnen met een verschillende frequentie van scannen worden afgesloten. Er worden abonnementen met de volgende frequenties aangeboden:

- Scan per kwartaal
- Scan per maand
- Scan per week

'Diepte' van scannen

De kwaliteit van een web scan en infraweb scan is mede afhankelijk van de 'diepte' waarop gescand wordt. De 'diepte' staat niet gelijk aan het aantal pagina's dat wordt gescand; deze is onbeperkt. In feite geeft de 'diepte' de grondigheid van de scan aan. De diepte staat voor het aantal links dat vanaf de eerste webpagina 'gevolgd' wordt door onze scanners tijdens het uitvoeren van een scan. Alle pagina's die gevolgd worden, worden gescand. Om e.e.a. visueel te maken:



In bovenstaande voorbeeld zullen bij een abonnement met een diepte tot 3 pagina's het 4e en 5e niveau dus niet opgenomen worden in de scan.

We bieden de volgende mogelijkheden in de abonnementen:
- Tot 3 pagina's diep (snel);
- Tot 5 pagina's diep (normaal);
- Tot 9 pagina's diep (grondig).

Credentialed scans

Binnen week abonnementen is het mogelijk om zogenaamde Credentialed scans uit te voeren. Een credentialed scan houdt in dat er een scan wordt uitgevoerd als ingelogde gebruiker. Hierdoor vinden onze scanners over het algemeen weer andere kwetsbaarheden dan bij een reguliere scan.

Om een credentialed scan te kunnen opstarten, moeten eerst de credentials (gebruikersnaam en wachtwoord) aangeleverd worden om in te loggen (te authenticeren). We ondersteunen de volgende mechanismen:

- Linux (via SSH);
- Windows.

Hou er bij het gebruiken van credentialed scans rekening mee dat er inlogpogingen verricht zullen worden met de aangeleverde credentials. Indien de verkeerde credentials worden ingegeven, kan het zijn dat het betreffende account geblokkeerd wordt (uiteraard is dit afhankelijk van de instellingen van uw systeem).

Credentialed scans worden alleen in overleg met ThreadStone ingeregeld.

Wat wordt er gescand?

Bij een scan die is gericht op de infrastructuur worden andere zaken gescand dan bij een website. Dit hoofdstuk beschrijft op welke onderdelen er gescand wordt bij welk type scan. In totaal scant onze engine op meer dan 90.000 bekende kwetsbaarheden, welke wij dagelijks aanvullen met de nieuwste kwetsbaarheden die bekend worden.

Scan	Infra scan (Infra)*	Web scan (Web)**	Infra & Web scan (Infraweb)*
Scan based on various vulnerability engines			
Infrastructure scanning (routers, firewalls etc.) • Full port scan • Software versions • FTP server • SSH • SSL/TLS certificates • SPF, DMARC and DKIM checks • Etc.			

Web site scanning, including:
• OWASP top 10, f.i.
  ○ (SQL) injection
  ○ Cross-site scripting (XSS)
  ○ Cross-Site Request Forgery (CSRF)
  ○ Etc.
• Payment Card Industry web audits (preparation for audit)
• Joomla scan
• WordPress scan
• Drupal scan
• SSL/TLS certificates
• DNS Sec usage
• IPv6 usage
• IPv6 possible at nameserver of provider
• Check on known malware site
• Check on known phising site
• Check on trust of websites
• Etc.
			

Basic password scan (standard user accounts)			

* All ports will be scanned
** Only port 80 and 443 will be scanned

Functionaliteit

De functionaliteit van de ThreadScan portal en -abonnementen wordt in dit hoofdstuk weergegeven.

Scan	ThreadScan Subscription
Results available via online portal	✓
Internal scanning of networks via on-premise scanner[1]	Via ThreadScan Intern
Perimeter scanning	✓
Full automatic periodic scan per week, month or quarter	✓
On-demand scanning[2]	✓
Infra or web scan	✓
Depth of web or infraweb scan	3, 5 or 9 pages[3]
IPv4 scanning	✓
IPv6 scanning	✓
Start date/time of scan[4]	✓
Number of scans on URL or IP[5]	∞
Scan history	✓
Detection on Intrusion Detection & Prevention Systems	✓
Detection on non-existing domains	✓
Credentialed scanning	Optional

[1] Internal scanning based on special pricing/quote
[2] The number of (on-demand) scans must be reasonable and primary used to confirm vulnerability
[3] Depends on the subscription
[4] Only for month and week subscriptions. Quarterly subscriptions run on the first of February, May, August and November and will be handled in queue.
[5] The number of (on-demand) scans must be reasonable and primary used to confirm vulnerability

Reporting in ThreadScan portal	ThreadScan Subscription
Management information	✓
Vulnerability Risk scoring, based on CVSS severity scoring[6]	✓
Severity en scoring details per vulnerability	✓
Detailed information per vulnerability	✓
Mitigation details per vulnerability	✓
Links to external sources with more information, f.i. Wikipedia, NIST, BID, CVE etc.	✓
Management of vulnerabilities	**ThreadScan Subscription**
Set status on vulnerabilities (New, Open, Parked, Not applicable, Solved)	✓
Overrule CVSS severity scoring on vulnerabilities	✓
Extensive filter on vulnerabilities with status, severity etc.	✓
Vulnerability overview per URL or IP address	✓
Vulnerability overview over all subscriptions of distributor, partner or customer	✓
Commenting by Technical users for each vulnerability, including timestamp and logging	✓
Reporting in PDF's	**ThreadScan Subscription**
Export of Scan results in management report (Secured PDF)	✓
Export of Scan results in detailed report, including comments (Secured PDF)	✓

[6] Vulnerabilities are being categorized in Critical, high, medium, low and informational, based on CVSS scoring, only if available

Roles	ThreadScan Subscription
Portal owner, Technical user, commercial user[7]	
2-factor authentication	
Full audit trail	
Supported language[8]	NL, UK
Usage	**ThreadScan Subscription**
Number of customers	∞
Number of user accounts for distributor and partner	∞
Number of user accounts for end customers	∞
Blacklisting of certain domains by distributor	
Multi tier[9]	
Attach documents like orderconfirmations to Reseller, End customer or subscription[10]	
API	**ThreadScan Subscription**
API for automatic ordering	
API for automatic information exchange	

[7] Partners and Distributors have three roles, portal owner (all Rights), Commercial user (ordering) and Technical users (vulnerabilities and scans). End users only have portal owners and technical users; direct ordering by end customers is not supported.
[8] Vulnerability information is provided in English only
[9] Distributor, Partner and Customer roles are fully supported. A distributor has rights to support all partners and the customers of those partners. A partner has rights to support all his customers and a customer can support his vulnerabilities etc.
[10] Based on role

Alerting	ThreadScan Subscription
Alerting when scan is completed to list of users via E-mail[11]	

Support	ThreadScan Subscription
Support by E-mail and phone	Via Reseller

Dashboards[12]	Distributor	Partner	End customer
Piechart with number of subscriptions, based on status of subscription			
Piechart with number of subscriptions, based on type of subscription			
Piechart with number of vulnerabilities, based on severity of vulnerabilities			
Piechart with number of vulnerabilities, based on status of vulnerabilities			
Timeline and table with number of vulnerabilities, based on severity of vulnerabilities[13]			
Timeline and table with number of vulnerabilities, based on status of vulnerabilities[14]			
Gauges with Cyberscore			

[11] Users must have an account in the ThreadStone portal
[12] All dashboards are exportable and adjustable
[13] In timelines, on-demand scans are not taken into account
[14] In timelines, on-demand scans are not taken into account

Firewalls

Indien u (of uw hoster/IT leverancier) gebruik maakt van een geavanceerd Intrusion Detection & Prevention systeem, kan het zijn dat deze de scans van ThreadScan voortijdig afbreekt. Het afbreken van een zogenaamde portscan vindt over het algemeen plaats nadat er een aantal poorten van de firewall door onze scanners zijn gecontroleerd, waarbij de firewall dit netjes detecteert en vervolgens de verbinding verbreekt (voor uw firewall probeert er blijkbaar een onbevoegde in te breken). Dit is dus het gewenste gedrag van de firewall.

Op het moment dat een kwaadwillende echter handmatig probeert in te breken op specifieke poorten, zal de firewall dit niet detecteren. Wij adviseren daarom om onze scanners op de whitelist van uw firewall te plaatsen en vervolgens opnieuw een scan uit te voeren. De firewall zal in dat geval de verbinding niet automatisch verbreken en onze scanner kan eventuele andere kwetsbaarheden alsnog in kaart brengen. De IP nummers die op de whitelist moeten worden geplaatst zijn: 78.46.19.149 en 5.9.17.13.

Voorbeelden voor keuze van het juiste abonnement

Regelmatig krijgen we vragen welk abonnementen het beste ingezet kan worden. Dit document geeft 3 voorbeelden weer, waaruit duidelijk wordt wat er nodig is.

De diepte (grondigheid) en frequentie van scannen is volledig afhankelijk van de klantsituatie. Aangezien er maandelijks 500 nieuwe kwetsbaarheden worden gevonden adviseren we om minimaal 1x per maand een scan uit te voeren.

Onze 'Gouden regel'

We hanteren een 'gouden regel' voor het aanbieden van de juiste abonnementen:

Bekijk wat er van 'buiten' zichtbaar is. ThreadScan opereert als een 'kwaadwillende' uit China, Rusland, Amerika of welk land op afstand dan ook en ziet alleen hoe het bedrijf op het internet aanwezig is. Vervolgens geldt:

1. Voor elke IP adres dat aan het internet is gekoppeld een infra abonnement;
2. Voor elke URL dat aan het internet gekoppeld is een web abonnement;
3. Voor elke IP waar 1 enkele website op draait kan gekozen worden voor een infra & web abonnement (combinatie van 1 & 2)

Let op: Een IP adres kan meerdere URL's hebben (shared webhosting).

Voorbeeld 1

Wat draait er?

1 server bij een hosting provider
op die server draaien 10 websites
www.website1.com
www.website2.com
...
www,website10.com

Wat adviseren we?

Op de server zelf een infra abonnement. Deze kan afgesloten worden op 1 van de internetsites of direct op het IP adres van de server.

Op de website1, website2..., website10 adviseren we per website een web abonnement. Dit omdat website1 andere content laat zien dan website2.

Optie: Het is ook mogelijk om 1 van de websites te voorzien van een infra & web abonnement (waarbij dus de infrastructuur en de web omgeving van deze internetsite wordt gecontroleerd) en de overige websites van een web abonnement te voorzien.

Voorbeeld 2

Wat draait er?

2 fysieke servers (hosts) met Microsoft hyper-v

Op host 1 draait het volgende:
- webserver
- database server
- ms exchange

Op host 2 draait het volgende
• fileserver
• print server
• citrix server

Daarnaast zijn er 2 firewalls die aan het internet zijn gekoppeld met de volgende DNS-namen
• Firewall 1 verwijst naar mail.mijnbedrijf.eu
• Firewall 2 verwijst naar www.mijnbedrijf.eu

Achter mail.mijnbedrijf.eu zit ms exchange en op poort 8080 draait nog een Citrix server. Achter www.mijnbedrijf.eu zit alleen de webserver.

De firewalls sturen het verkeer door naar de betreffende hosts op de fysieke hosts met Microsoft Hyper-v.

Van de buitenkant is er dus:
• 1 server met alleen website
• 1 server met exchange en citrix server

De print server, fileserver, database server zijn niet toegankelijk vanaf het internet.

Wat adviseren we?

Wij adviseren om voor www.mijnbedrijf.eu een infra & web abonnement af te sluiten. Dit omdat je de hele firewall en internetsite wilt scannen en de server dedicated is toegewezen voor de website (niet gedeeld).

Voor mail.mijnbedrijf.eu adviseren we een infra abonnement. Dit omdat er niet getest hoeft te worden op SQL injectie mogelijkheden etc. (een exchange server en citrix server zullen deze niet hebben).

Aangezien we niet vanaf het internet rechtstreeks kunnen komen bij de fileserver, print server en database server hoeven die niet gescand te worden.

Indien de servers een direct aan het internet aangesloten remote toegang voor beheer hebben (bijvoorbeeld iLO), dan adviseren we daarvoor een Infra abonnement af te sluiten.

Voorbeeld 3

Wat draait er en wat adviseren we?

De volgende URL's en IP adressen zijn bekend (waarbij xxx.yyy voor een nummer-combinatie staat uit het IP adres). Achter elke URL is het advies abonnement aangegeven:

URL	IP adres	Advies
mysql.mijnbedrijf.nl	10.0.0.14	intern, geen abonnement
www.mijnbedrijf.nl	145.xxx.yyy.123	Infra & web
testfase.mijnbedrijf.nl	178.xxx.yyy.114	Infra & web
game.mijnbedrijf.nl	178.xxx.yyy.116	Infra & web
firewall.mijnbedrijf.nl	193.xxx.yyy.10	Infra
portalextern.mijnbedrijf.nl	193.xxx.yyy.11	Infra & web
demo.mijnbedrijf.nl	193.xxx.yyy.11	Web
webservices.mijnbedrijf.nl	193.xxx.yyy.11	Web
exchange.mijnbedrijf.nl	193.xxx.yyy.12	Infra
portal.mijnbedrijf.nl	193.xxx.yyy.13	Infra & web
mail.mijnbedrijf.nl	194.xxx.yyy.8	Infra
ftp.mijnbedrijf.nl	194.xxx.yyy.21	Infra
spelletje.mijnbedrijf.nl	213.xxx.yyy.232	Infra & web