ThreadStone CYBER SECURITY

Thread Scan INTERN 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 intern

Met de interne ThreadScan worden periodiek alle systemen binnen het bedrijfsnetwerk gecontroleerd op kwetsbaarheden. De resultaten worden inzichtelijk gemaakt in het online portaal van ThreadStone.

Appliances (hardware) of Virtual Machines (VM's)

De interne scan kan door een appliance (hardware) of Virtual Machine (VM) uitgevoerd worden. In dit document wordt gesproken over interne ThreadScan indien van toepassing op zowel appliance als VM.

Afhankelijk van de omvang van het netwerk van de eindklant wordt een appliance of VM geleverd.

ThreadScan intern	Aantal IP nummers dat gescand kan worden
ThreadScan Intern – 32 (alleen virtueel te verkrijgen)	32
ThreadScan Intern - 64	64
ThreadScan Intern - 128	128
ThreadScan Intern – 256	256
ThreadScan Intern – 512	512
ThreadScan Intern – 1.024	1.024

Bij de hardware appliance worden de volgende artikelen geleverd:

- Adapter;
- UTP CAT6 kabel van 1,2 meter;
- Aansluit handleiding.

De appliances zijn en blijven eigendom van ThreadStone cyber security en worden als 'managed service' geleverd. Na beëindiging van een contract dient de unit te worden geretourneerd!

Installatie

De appliances werken op basis van plug & play. De adapter moet worden aangesloten en de meegeleverde netwerkkabel moet in de appliance en in de switch van de organisatie worden aangesloten. Er dient dus een vrije aansluiting op de switch aanwezig te zijn.

De VM's worden in Open Virtualization Format (ovf) geleverd middels een beveiligd bestand. We adviseren om bij installatie minimaal 2 cores en 8GB intern geheugen toe te wijzen.

Het systeem moet een IP adres toegewezen krijgen door de in de organisatie gebruikte DHCP server. Vervolgens zal het systeem zichzelf aanmelden en wordt het zichtbaar in het portaal.

Voor een juiste werking is een verbinding naar het internet vanaf de interne ThreadScan noodzakelijk waarbij gecommuniceerd kan worden over poort 80 en 443. Vraag ThreadStone voor de mogelijkheden bij het gebruik van proxy servers.

Scan

De interne ThreadScan scant alleen de devices die door de appliance of VM benaderd kunnen worden en die reageren op verzoeken van de interne ThreadScan. Indien het netwerk gesegmenteerd is, zijn er de volgende mogelijkheden om het gehele netwerk te controleren op kwetsbaarheden:

1. Plaats in elk segment een aparte appliance;
2. Zorg er voor dat de appliance telkens in een ander segment wordt geplaatst;
3. Zorg er voor dat de appliance alle devices die gescand moeten worden op kwetsbaarheden kan benaderen (en dus dat er aanpassingen worden doorgevoerd in de segmentering).

Data

Om veiligheidsredenen wordt op de interne ThreadScan minimaal data bewaard. Nadat een scan is afgerond wordt de data over beveiligde verbindingen direct doorgestuurd naar het portaal en daar verder verwerkt. De data blijft volledig in Nederlandse datacentra.

Wat wordt er gescand?

Bij een interne ThreadScan worden alle systemen binnen de aangegeven IP-range gecontroleerd op kwetsbaarheden. De systemen moeten hiervoor 'AAN' staan en benaderbaar zijn door onze scanner (en daarmee dus ook terugkoppeling kunnen geven op de verzoeken die worden uitgestuurd vanuit de scanner).

Dit hoofdstuk beschrijft op welke onderdelen er gescand wordt. In totaal scant onze engine op meer dan 60.000 bekende kwetsbaarheden, welke wij dagelijks aanvullen met de nieuwste kwetsbaarheden die bekend worden.

Scan	Opgenomen
Scan based on various vulnerability engines	
Infrastructure scanning (routers, firewalls etc.)* • Full port scan • Software versions • FTP server • SSH • SSL/TLS certificates • Etc.	
Basic password scan (standard user accounts)	

* All ports will be scanned

Functionaliteit voor de interne ThreadScan

Scan	ThreadScan Subscription
Results available via online portal	
Full automatic periodic scan per month	
IP range adjustable	
Infra scan	
IPv4 scanning	
Start date/time of scan adjustable	
Adjustable IP-ranges to scan	
Number of IP's per scan	Depends on model
Number of scans on IP's	∞
Scan history	

Reporting in ThreadScan portal	ThreadScan
Management information	
Vulnerability Risk scoring, based on CVSS severity scoring[1]	
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.	

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

Management of vulnerabilities	ThreadScan
Overrule CVSS severity scoring on vulnerabilities[2]	
Extensive filter on vulnerabilities with status, severity etc.	
Vulnerability overview per scan (history)	
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 [3]	

Reporting in PDF's	ThreadScan Subscription
Export of Scan results in management report (Secured PDF)	

[2] Severity can be changed, but won't have effect on new scans. The adjustment is made for reporting purpose;
[3] Comments can be given, but won't have effect on new scans. The adjustment is made for reporting purpose;

Generieke functionaliteit van het portaal

Roles	ThreadScan
Portal owner, Technical user, commercial user[4]	
2-factor authentication	
Full audit trail	
Supported language	NL, UK[5]
Usage	**ThreadScan**
Number of customers	∞
Number of user accounts for distributor and partner	∞
Number of user accounts for end customers	∞
Multi tier[6]	
Attach documents like order confirmations to Reseller, End customer or subscription[7]	

[4] 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.
[5] Vulnerability information is provided in English only. ThreadPhish, ThreadGDPR en ThreadMature alleen in NL
[6] 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.
[7] Based on role

Alerting	ThreadScan
Alerting when scan is completed to list of users via E-mail[8]	
Support	**ThreadScan**
Support by E-mail and phone	Via Reseller

Dashboards[9]	Distributor	Partner	End customer
Piechart with number of vulnerabilities, based on severity of vulnerabilities			
Piechart with number of vulnerabilities, based on status of vulnerabilities			
Gauges with Cyberscore			

[8] Users must have an account in the ThreadStone portal
[9] All dashboards are exportable and adjustable