

MANAGED DETECTION & RESPONSE

THREAD DEFENSE 365

THREAD DEFENSE ADVANCED

THREAD DEFENSE ULTIMATE



ThreadStone
CYBER SECURITY

MANAGED DETECTION & RESPONSE

VROEGTIJDIGE DETECTIE VAN CYBERAANVALLEN

Managed Detection & Response (MDR) is een essentiële dienst voor het veilig houden van uw IT-systemen. We bieden 24/7 monitoring en beheer door een team van cybersecurity-experts met behulp van geavanceerde tools en technologieën.

Blijf cybercriminelen een stap voor en waarborg uw cybersecurity met onze proactieve aanpak.



24/7 security monitoring van systemen met dienstverlening om snel te kunnen reageren op cyberincidenten wordt steeds belangrijker. Eén van de eisen vanuit de NIS2 wetgeving is dat binnen 24 uur aangegeven kan worden dat er een incident is opgetreden en binnen 72 uur een rapport kan worden overlegd waaruit blijkt wat de impact is en welke data en systemen zijn getroffen. In onze optiek is dit alleen mogelijk door gebruik te maken van een Managed Detection & Response dienst die vanuit een professioneel Security Operations Center (SOC) worden geleverd.

Met onze Thread Defense oplossingen leveren we een dergelijke dienstverlening. Deze brochure beschrijft de verschillende vormen die we aanbieden, namelijk Thread Defense 365, Thread Defense Advanced en Thread Defense Ultimate.

Het spreekt voor zich dat wij graag met u in gesprek gaan om samen te bepalen hoe we deze diensten bij uw organisatie kunnen inzetten.

Neem gerust vrijblijvend contact met ons op, wij helpen u graag op weg naar een digitaal veiliger en weerbaarder organisatie.

ThreadStone Cyber Security

THREAD DEFENSE 365 EN THREAD DEFENSE ADVANCED / ULTIMATE

WIJ BIEDEN ONZE MANAGED DETECTION & RESPONSE (MDR) AAN IN DRIE VARIANTEN:

➔ Thread Defense 365

Thread Defense 365 gericht op 24/7 security monitoring van uw Microsoft 365 omgeving inclusief darkweb monitoring en inzicht in zogenaamde shadow-IT.

➔ Thread Defense Advanced / Ultimate

Thread Defense Advanced of Ultimate gericht op 24/7 security monitoring van uw werkplekken, servers en netwerk.

		365	ADVANCED	ULTIMATE
	Managed Detection & Response service met 24/7 monitoring en geavanceerde beveiliging tegen dreigingen	Gericht op Microsoft 365 en Google Workspace	Gericht op servers, werkplekken en netwerken	Gericht op servers, werkplekken en netwerken
📊	Geavanceerde analyse en 'threat hunting'	✓	✓	✓
🛡️	Proactief onderzoek naar verdacht gedrag, forensisch onderzoek en ondersteuning/advies bij security-incidenten	✓	✓	✓
🎧	Premium support en periodieke reporting	✓	✓	✓
🔑	2FA security monitoring in in Microsoft 365 of Google Workspace	✓	Via 365	Via 365
🖥️	Darkweb monitoring	✓	Via 365	Via 365
☁️	Cloud applicatie monitoring	✓	Via 365	Via 365
🔍	Inzicht in Shadow IT	✓	Via 365	Via 365
📡	Extended Detection and Response (XDR)	✗	✓*	✓
🖨️	Geavanceerde server en werkplek beveiliging	✗	✓*	✓
💻	Moderne Endpoint protectie licentie	✗	✗*	✓
⚠️	Vulnerability Management servers en werkplekken	✗	Optioneel	✓
👁️	Vulnerability management en/of monitoring van netwerk devices zoals firewall, switches etc.	✗	Optioneel	Optioneel
🔒	Volledige disk encryptie	✗	✗**	✓
🛡️	Antispam, antiphishing, antimalware op Microsoft 365 en Google Workspace (mail security)	✗	✗**	✓
🔑	Gebruik van MFA op VPN, RDP, OWA en Radius gebaseerde services	✗	✗**	✓

* Op basis van aanwezige Endpoint protectie oplossing.

** Veelal zijn deze oplossingen al aanwezig. Vraag uw IT-beheerder.

THREAD DEFENSE 365

VOLLEDIG BEHEERDE, PROACTIEVE SECURITY-MONITORING VAN UW MICROSOFT 365-OMGEVING

Out-of-the-box is Microsoft 365 beperkt beveiligd, terwijl er continu aanvallen plaatsvinden op Microsoft 365. Het is daarom van essentieel belang dat juist deze omgeving extra 24/7 security-monitoring krijgt. Thread Defense 365 is een managed service die uw Microsoft 365-omgeving beschermt door proactieve security-monitoring, inclusief darkweb en applicatie monitoring. Deze service omvat compliance-rapportages, real-time monitoring van verdachte activiteiten, geavanceerde dreigingsdetectie en snelle incident response.

WAAROM THREAD DEFENSE 365?

Microsoft 365 bevat veel gevoelige en vertrouwelijke informatie, zoals persoonlijke gegevens van medewerkers en klanten, financiële informatie en projectdata. Als er een inbreuk plaatsvindt op uw Microsoft 365-omgeving kan dit leiden tot datalekken, diefstal van gegevens of cyberaanvallen die de continuïteit van de bedrijfsvoering in gevaar brengen. Het is daarom essentieel om Microsoft 365 proactief te monitoren op de beveiliging en zo te bewaken tegen de nieuwste cyberdreigingen en verdachte activiteiten.

In de basis worden veel Microsoft 365-omgevingen opgeleverd en beheerd, waarbij de nadruk ligt op functioneel werken, stabiliteit van de omgeving en controle op malware. Security-monitoring en continue acties gericht op verbeteren van de beveiligingsinstellingen vindt in veel gevallen echter niet plaats. Vanuit ons Security Operations Center (SOC) bieden we Thread Defense 365, dat zorgt voor tijdige detectie en response op beveiligingsincidenten. Hiernaast ontvangt u uitgebreide compliance-rapportages waarmee uw IT-verantwoordelijke in staat is om de beveiliging verder aan te scherpen.

WAT DOEN WE?

Bij het leveren van Thread Defense 365 nemen we de volgende gestructureerde stappen om uw Microsoft 365-omgeving te beschermen:

Afstemming

We bepalen de contactpersonen en -momenten binnen uw organisatie voor incidentmeldingen en rapportages, in samenwerking met uw IT-verantwoordelijke en ThreadStone.

Koppelen van uw Microsoft 365 tenant

We sluiten uw Microsoft 365-omgeving tenant aan op ons Security Operations Center (SOC) voor uitgebreide beveiligingsmonitoring.

Monitoring

We zoeken continu naar verdachte activiteiten binnen uw omgeving en het darkweb. Daarnaast controleren we het gebruik van cloud-applicaties, zodat u zicht krijgt op zogenaamde Shadow-IT en de beveiliging daarvan.

Analyse

We beoordelen gedetecteerde incidenten om het dreigingsniveau vast te stellen.

Response

We ondernemen actie bij risico's en adviseren over preventieve maatregelen om herhaling te voorkomen.

Rapportage en overleg

We leveren periodieke rapportages over het dreigingslandschap en de beveiligingsprestaties, die we samen doornemen.

Verbetering

We gebruiken de verkregen inzichten en lessen uit incidenten om de beveiliging continu te verbeteren.

Onze aanpak garandeert een uitgebreide verdediging en optimaal beheer van uw Microsoft 365-omgeving, terwijl u zich kunt concentreren op uw kernactiviteiten.

DE DRIE GROOTSTE VOORDELEN VAN THREAD DEFENSE 365



Real-time 24/7 security-monitoring op Microsoft 365

Aanvullend op uw ICT-diensten bieden we vanuit ons Security Operations Center (SOC) 24/7 security-monitoring, geavanceerde dreigingsdetectie, en incident response. We focussen op Microsoft 365, controleren het darkweb en brengen applicatiegebruik (Shadow-IT) en beveiligingsverbeteringen in kaart.



Geschikt voor elk type organisatie

Thread Defense 365 is een betaalbare, flexibele en schaalbare security-oplossing voor alle organisaties die Microsoft 365 gebruiken.



Laat zien hoe veilig uw Microsoft 365 is

Via rapportages en periodiek overleg krijgt u inzicht in onder andere dreigingsinformatie, gebruikers met een verhoogd risico en door te voeren verbeteringen in uw Microsoft 365-omgeving.

THREAD DEFENSE ADVANCED / ULTIMATE

VROEGTIJDIGE DETECTIE VAN CYBERAANVALLEN OP UW WERKPLEKKEN, SERVERS EN CLOUD-OMGEVINGEN

Bescherm uw organisatie 24/7 met Thread Defense Advanced of Ultimate: voorkom bedreigingen van ransomware en zerodays door continue monitoring, actieve analyse en incident response. Wij waken over uw systemen, e-mail en meer met geavanceerde beveiligingstechnieken. Blijf cybercriminelen een stap voor en waarborg uw cybersecurity met onze proactieve aanpak.



WAAROM THREAD DEFENSE ADVANCED OF ULTIMATE?

Getroffen bedrijven van ransomware krijgen naast financiële schade te maken met reputatieschade (41%) en één op de zes zelfs met faillissement. Dit betekent dat voorkomen echt beter is dan genezen. Bescherm uw bedrijf effectief tegen huidige en toekomstige cyberdreigingen met Thread Defense Advanced of Ultimate. Deze essentiële dienst zorgt ervoor dat u zich geen zorgen hoeft te maken over de constante dreiging van cyberaanvallen en het risico op dataverlies en andere schade.

Onze dienstverlening biedt continue, 24/7-monitoring van uw servers, werkplekken en cloud-omgevingen, waarbij elk teken van bedreiging direct vanuit ons Security Operations Center (SOC) wordt opgemerkt, geanalyseerd en geneutraliseerd door een team van ervaren cybersecurity-experts.

We gebruiken de meest geavanceerde tools, technologieën en de laatste threat-intelligence om uw bedrijf te beschermen.

WAT DOEN WE?

Bij het leveren van Thread Defense Advanced en Ultimate nemen we de volgende gestructureerde stappen om uw servers, werkplekken en cloud-omgevingen te beschermen:

Afstemming

We stemmen de exacte scope af voor monitoring (welke endpoints en netwerkcomponenten moeten worden opgenomen). Hierbij verwerven we inzicht over de gehele netwerk-architectuur, het applicatielandschap, de huidige beveiligingsmaatregelen, type gebruikers en wijze van gebruik van de systemen.

Activatie

Indien u al zogenaamde Endpoint Detection & Response (EDR) software zoals Microsoft Defender, SentinelOne of CrowdStrike gebruikt, dan kunnen we deze in de **Advanced** versie koppelen aan ons SOC. We installeren hiervoor dan in overleg een agent op de machines voor optimale bescherming tegen ransomware. Zo kunt u optimaal gebruik blijven maken van de licenties en software die u al gebruikt, maar dan met 24/7 security monitoring.

Indien u nog geen EDR-software heeft, dan installeren we deze in overleg op al uw servers en werkplekken en koppelen deze met ons SOC. In deze Ultimate versie zijn de EDR licenties inbegrepen, waarbij u direct extra's krijgt voor o.a. geavanceerde antispam en antiphishing. Hierdoor zijn uw mail,

cloud, servers en werkplekken direct optimaal beveiligd.

Monitoring

We monitoren uw systemen 24/7 op kwetsbaarheden en detecteren afwijkingen van normaal gedrag op uw werkplekken, servers, netwerk en cloud-omgeving.

Analyse

We beoordelen gedetecteerde incidenten om het dreigingsniveau vast te stellen.

Response

We ondernemen actie bij risico's en adviseren over preventieve maatregelen om herhaling te voorkomen.

Rapportage en overleg

We leveren periodieke rapportages over het dreigingslandschap en de beveiligingsprestaties, die we samen doornemen.

Verbetering

We gebruiken de verkregen inzichten en lessen uit incidenten om de beveiliging continu te verbeteren.

Onze aanpak garandeert een uitgebreide verdediging en 24/7-monitoring, detectie en incidentafhandeling zodat u zich kunt concentreren op uw kernactiviteiten.

DE DRIE GROOTSTE VOORDELEN VAN THREAD DEFENSE ADVANCED / ULTIMATE



Compliance

Nieuwe wetgeving zoals NIS2 en DORA vereist snelle incidentmeldingen. Een goed monitoringssysteem vergemakkelijkt het verzamelen en rapporteren van gegevens om aan deze regels te voldoen.



Volledige managed security

24/7 monitoring en Threat Hunting voor optimale beveiliging van uw bedrijfsomgeving. We detecteren verdachte activiteiten in uw netwerk, systemen en applicaties en ondernemen direct actie.



Incidentresponse

Bij een aanval minimaliseren we de impact door isolatie. U krijgt ondersteuning van Nederlandstalige experts en toonaangevende wereldwijde researchers.

ThreadStone Cyber Security

Westblaak 100
3012KM Rotterdam
The Netherlands

- ☎ +31 (0)85 060 7000
- ✉ info@threadstone.eu
- 🌐 www.threadstone.eu

