CYBERSECURITY

ThreatWatcher

Continu zicht op uw digitale aanvalsoppervlak en supply chain

LRQA NETTITUDE

Inhoud

Wat is ThreatWatcher?

Wilt u onbekende bedreigingen ontdekken die op de loer liggen binnen uw aanvalsoppervlak op internet en wilt u uw managementprogramma tegen externe dreigingen versterken?

De Cyber Threat Intelligence (CTI) Service van LRQA Nettitude, ThreatWatcher, doorzoekt miljoenen digitale datapunten om risico's te identificeren en u te waarschuwen, zodat u actie kunt ondernemen voordat uw digitale activiteiten werkelijk bedreigd worden.

ThreatWatcher is een volledig op maat gemaakte, modulair opgebouwde, beheerde CTI-service, die gebruik maakt van onze geavanceerde en unieke mogelijkheden om gedetailleerde inzichten te leveren in de risico's en gevolgen van cyberbedreigingen voor uw organisatie. ThreatWatcher is een verlengstuk van uw organisatie en biedt bewustzijn van de situatie en contextuele informatie.

In combinatie met onze intelligence analysts zorgt dit ervoor dat uw organisatie weloverwogen beslissingen kan nemen, de gewenste beveiligingsgraad kan handhaven en effectief technologieën kan inzetten om aanvallen te voorkomen en op te sporen.

Waarom zou u ThreatWatcher gebruiken?

Omdat 70% van de inbreuken buiten het bedrijfsnetwerk plaatsvindt, hebben organisaties moeite om te begrijpen wat ze bezitten, waar het zich bevindt, welk risico het oplevert en hoe ze het moeten beschermen.

Aanvallen op bedrijfsmiddelen die aan het internet zijn blootgesteld, omzeilen vaak traditionele beveiligingstools en vormen een enorme belemmering voor organisaties op het gebied van informatiebeveiliging. ThreatWatcher scant meer dan een miljoen digitale kanalen, van het oppervlakteweb, deep web en dark web, en specifieke mobiele en sociale platforms om risico's te identificeren en te beoordelen, zodat u actie kunt ondernemen voordat ze invloed hebben op uw organisatie.

Krijg inzicht in uw digitale aanvalsoppervlak door het perspectief van een aanvaller

De taak om bij te blijven met het cyberdreigingslandschap, om nog maar te zwijgen van de uitdagingen van het hebben en onderhouden van een interne intelligence-capaciteit, zijn niet gemakkelijk en ook financieel niet te onderschatten.

ThreatWatcher is een service waarmee we onze expertise en inzichten met u kunnen delen door u een op informatie gebaseerde en operationele aanpak van cybersecurity te bieden die holistisch en specifiek is voor uw organisatie. Als alternatief kan ThreatWatcher uw bestaande mogelijkheden aanvullen en diepgaande expertise en beschikbaarheid bieden wanneer u die het meest nodig hebt.

Cyberaanvallen zijn geen geïsoleerde spontane gebeurtenissen

CTI is nodig om inzicht te krijgen in het cyberdreigingslandschap en wat er nodig is om uw werkomgeving en uw mensen te beschermen.

Als uw gegevens worden beschermd door uw firewalls en interne beveiliging, is het soms gemakkelijk om te weten waar ze zijn en wie er toegang toe heeft, maar als de gegevens op internet staan, is het bijna onmogelijk om een nauwkeurig beeld te krijgen. Daar komt ThreatWatcher in beeld. Het maakt gebruik van zowel bedrijfseigen als commerciële platforms voor beveiligingsinformatie die gegevens verzamelen uit de grootste verzameling bronnen van oppervlakken, gesloten en technische bronnen om zichtbaarheid en context te bieden van gegevens die gebruikt zouden kunnen worden bij een aanval tegen uw organisatie. Deze wordt geïndexeerd en ter beschikking gesteld aan ons CTI-analistenteam.

ThreatWatcher biedt u inzicht in het specifieke cyberdreigingslandschap van uw organisatie en hoe dit verband houdt met uw cruciale assets.

ThreatWatcher wordt geleverd door ons team van hooggekwalificeerde en ervaren CTI-analisten. Het levert u tijdige informatie op, die bestaat uit een combinatie van kennis, gegevens en context. Allemaal ontworpen om u te helpen cyberaanvallen te voorkomen of te beperken.

Hoe werkt ThreatWatcher?

Identificeren van externe dreigingen en voorkomen van een aanval

Stelt u zich eens voor dat een aanvaller uw portaal voor secundaire arbeidsvoorwaarden heeft gekloond en het heeft gehost onder een nieuw domein, ongeveer hetzelfde als het origineel. Weet u hoe u dit kunt herkennen? Wat als uw werknemers dezelfde combinatie van werkmail en wachtwoord hebben gebruikt om zich aan te melden voor webshops of online fitness services en deze services zijn gekraakt? Zou u weten om welke gebruikers het gaat?

Deze voorbeelden van externe bedreigingen zijn heel gewoon in het digitale tijdperk en veranderen voortdurend. Het is tijd om via ThreatWatcher uw organisatie vanuit het oogpunt van een aanvaller te bekijken.

Security intelligence is de combinatie van kennis, gegevens en context waarmee u cyberaanvallen kunt voorkomen of beperken. ThreatWatcher wordt geleverd door ons team van hoogopgeleide en ervaren CTI-analisten, die gebruikmaken van bedrijfseigen en commerciële beveiligingsplatforms. Deze krachtige combinatie maakt gebruik van CREST-gecertificeerde analisten en een combinatie van meer dan een miljoen databronnen die zijn geanalyseerd en gecontextualiseerd voor de volgende bedreigingscategorieën, wat resulteert in een gedetailleerd rapport met alle details van de bevindingen en aanbevelingen.

Domeinbedreigingen	Bij domeinbedreigingen gaat het om het registreren, verhandelen in of het gebruik van een internetdomeinnaam die eerder werd gebruikt of die erg lijkt op een online bedrijfsidentiteit of website van een bedrijf. Domain Squatting is vaak een voorloper van aanvallen via e-mail en kan gebruikers verleiden tot het afstaan van inloggegevens via phishingaanvallen.
Bedreigingen van inloggegevens	Inloggegevens zijn puur goud voor een aanvaller. De huidige toename van 'dumps' van inloggegevens (geldige wachtwoorden, gebruikersnamen, e-mailadressen) die online of te koop worden aangeboden, verlaagt de lat voor een mogelijke aanvaller om toegang te krijgen tot uw bedrijfssystemen.
Monitoring van het deep web en dark web	Het deep web and dark web is de plaats waar hackers en andere bedreigingen informatie over bedrijfsdoelen voor kwaadaardige doeleinden verhandelen. Dark Web Monitoring zoekt naar termen en trefwoorden die relevant zijn voor uw bedrijf en identificeert potentiële bedreigingen voor uw merk, leveranciers en medewerkers.
Bedreigingen voor sociale merken	Het monitoren van internetbronnen en het identificeren van misbruik van content en logo's helpt organisaties actie te ondernemen voor gecontroleerd gebruik van hun merk. Dit helpt kwaadwillig gebruik door derden en individuen te voorkomen, wat kan leiden tot reputatieschade en verlies van vertrouwen bij consumenten.
Beoordeling van de potentiële gevaren	Wanneer organisaties hun capaciteit voor cybersecurity opbouwen, is het essentieel om aanvallers te begrijpen. Het is essentieel voor het beheer van uw bedreigingslandschap om te weten welke bedreigingsactoren zich op uw branche richten en deze te volgen.
Bedreigingen door gegevenslekken	Paste sites en code repositories kunnen soms een schat aan details onthullen met betrekking tot uw organisatie, zoals: de manier waarop het werkt of gevoelige informatie zoals certificaten, wachtwoorden en sleutels tot uw meest kritieke bedrijfsmiddelen.

Wat zijn de voordelen van ThreatWatcher?

ThreatWatcher verkort de tijd tussen bekende en onbekende bedreigingen en helpt u de risico's van uw organisatie te identificeren en te evalueren door het perspectief van een aanvaller.

Als u onbekende bedreigingen wilt ontdekken en uw programma voor het beheer van externe bedreigingen wilt versterken, dan is ThreatWatcher de oplossing. Het biedt bewustzijn van de situatie en contextuele informatie om weloverwogen beslissingen te kunnen nemen en de beveiliging op peil te houden.

Onze intelligence analysts proberen overeenkomsten en verschillen te vinden in enorme hoeveelheden informatie en misleidingen op te sporen om nauwkeurige, tijdige en relevante informatie te leveren.

Wij zorgen ervoor dat de output van ThreatWatcher een oplossing op maat voor u is, zodat uw organisatie weloverwogen beslissingen kan nemen, de gewenste beveiligingsgraad kan handhaven en de technologieën effectief kan inzetten om aanvallen te voorkomen en te detecteren.

- Wie zijn mijn ware tegenstanders?
- Wat zijn hun tactieken, technieken en procedures?
- Hoe kan ik mij daartegen verdedigen?
- Waar liggen de kansen?
- Staat mijn beveiligingsgraad in verhouding tot mijn bedreigingsprofiel?
- Welke bedreigingen zijn van belang voor mijn sector?

Hoe wordt ThreatWatcher geleverd?

Of u nu een volledige CTI-service of een combinatie van modules nodig hebt, u kiest wat het beste bij u past. ThreatWatcher kan worden aangepast om ervoor te zorgen dat u het gewenste niveau van bewustzijn van de situatie en contextuele informatie krijgt.

ThreatWatcher biedt toegang tot de meest geaccrediteerde expertise, gecombineerd met toonaangevende beveiligingstechnologie, om uw informatievereisten vast te leggen. De geavanceerde onderzoeken en analyses van ThreatWatcher helpen bij het identificeren van voorheen onbekende bedreigingen die tegen uw organisatie kunnen worden gebruikt in een cyberaanval, waarbij mensen, processen en technologie betrokken zijn.

Onze CTI-mogelijkheden stellen ons in staat om brede, op intelligence gebaseerde oefeningen uit te voeren, zoals die doorgaans worden uitgevoerd door echte bedreigingsactoren terwijl ze zich voorbereiden op hun aanval. Het doel is om een beeld te krijgen van de organisatie, vanuit het perspectief van een aanvaller. Dit is essentieel om contextualisering toe te voegen.

Onze CTI biedt toegevoegde waarde door onzekerheid te verminderen en tegelijkertijd dreigingen en kansen te identificeren, waardoor het risico op een echte aanval wordt verminderd.

De output van ThreatWatcher is specifiek voor uw organisatie en kan worden gebruikt op alle niveaus van uw organisatie, van tactisch tot strategisch, zodat u zich optimaal kunt verdedigen tegen bedreigingen en risico's.

Zodra u bent begonnen met de service, werken onze analisten met u samen om de juiste watchlists op te stellen binnen ons platform voor informatie over dreigingen. Zodra deze live zijn, worden er waarschuwingen geactiveerd wanneer één van de doelentiteiten is gematcht. Onze analisten zullen deze waarschuwing vervolgens beoordelen en de correctheid ervan vaststellen voordat ze contextuele informatie zoeken om de bevinding te ondersteunen. Tot slot wordt een beoordeling gemaakt van de bevindingen alvorens deze door te sturen naar de vooraf gedefinieerde contactpersonen. Indien nodig kunnen we ook 24/7 ondersteuning bieden bij het melden van dreigingen.

Hoe ThreatWatcher wordt geleverd en wat u krijgt

De core service richt zich op het beantwoorden van belangrijke vragen die vaak voorkomen in de plannen van een organisatie voor het verzamelen van inlichtingen. Veelgestelde vragen die een waarschuwing, beoordeling en melding veroorzaken zijn:

- Zijn er vermeldingen van uw merk(en) op het dark web? En in welke context?
- Zijn de credentials van uw medewerkers online identificeerbaar?
- Is het mogelijk om potentiële typo-squatting-domeinen te identificeren van uw portalen en websites?
- Is uw website tijdens de looptijd gekloond?
- Worden uw merken of werknemers vermeld op gekopieerde websites?
- Worden uw merken of werknemers vermeld in code-repositories?

Aanvullende modules kunnen zijn:

Vulnerability intelligence module

Deze module biedt organisaties contextuele en reële bedreigingsgegevens die verband houden met hun blootstelling aan kwetsbaarheden. Het einddoel is om extra context te bieden rond kwetsbaarheden in het netwerk, zodat de patch met prioriteit kan worden hersteld.
De module wordt gevuld met een recente scan van de kwetsbaarheden (van de betreffende organisatieonderdelen) en wordt maandelijks herhaald.

Threat assessment module

Deze module biedt een maandelijkse analyse van het bedreigingslandschap dat direct relevant is voor uw organisatie, de branche waarin u opereert en strategische observaties die waarschijnlijk van belang zijn voor de organisatie.

Analyst support module

Tijdens de hele levensduur van de service kunt u een beroep doen op ons team van CTI-analisten om informatie te verschaffen over specifieke zaken of om extra context te bieden voor bedreigingen die in de service zijn ontdekt. Dit belangrijke onderdeel betekent dat u toegang heeft tot uw informatievoorziening of, als die al bestaat, tot extra capaciteit en mogelijkheden. Dit biedt u de mogelijkheid om contact op te nemen met onze analisten en hen de opdracht te geven dieper in te gaan op de bedreigingsthema's van uw keuze.

Takedown services

Voor elke infrastructuur of service waarvan wordt aangenomen dat deze uw merk belemmert of kwaadaardige content host, kan via deze service ook de verwijdering worden aangevraagd. Deze belangrijke functie zorgt ervoor dat assets die als kwaadaardig zijn geïdentificeerd, kunnen worden aangepakt met behulp van de Takedown services.

Andere aanvullende rapportagemethoden voor de service omvatten:

Wekelijkse briefings

Indien gekozen, biedt deze rapportageoptie de mogelijkheid om de meldingen van bedreigingen te ondersteunen door een wekelijkse briefing van de analisten om de belangrijkste punten van de week te bespreken. (Indien nodig) wordt dit ondersteund door extra afdelingen en expertise binnen LRQA Nettitude.

Maandelijks overzicht

Indien gekozen, biedt deze rapportageoptie een grondige output van de resultaten van de activiteit van de vorige maand en maakt gebruik van de mogelijkheid om een terugblikkende analyse te geven die op het betreffende moment nog niet kon worden ontwikkeld. Intelligence Summaries (INTSUMS) die zijn opgesteld door LRQA Nettitude zullen ook worden opgenomen, indien van toepassing.

ThreatWatcher en ISO/IEC 27001:2022

Op 25 oktober 2022 werd de nieuwe versie van ISO 27001 gepubliceerd – een nieuw tijdperk van best practices voor informatiebeveiliging.

De belangrijkste veranderingen in ISO 27001:2022 waar organisaties op moeten letten zijn de updates van Annex A, controles in overeenstemming met ISO 27002:2022, waaronder de herstructurering van de oorspronkelijke 14 beheersingsdomeinen in vier categorieën en het verminderen van het totale aantal controles van 114 naar 93 – voornamelijk vanwege de samenvoeging van 57 controles in 24 controles. 58 controles blijven grotendeels ongewijzigd, met kleine contextuele updates, en 11 controles zijn gloednieuw voor ISO 27001:2022.

ISO 27001:2022 Organisatorische controle: Threat Intelligence

Eén van de nieuwe organisatorische controlemaatregelen, A.5.7 Threat Intelligence, vereist dat organisaties informatie over bedreigingen verzamelen, analyseren en produceren met betrekking tot de informatiebeveiliging.

Het doel van deze nieuwe controle is om organisaties een dieper inzicht te geven in cyberdreigingen door gegevens over huidige en toekomstige cyberaanvallen te verzamelen, te analyseren en in context te brengen. Daarnaast is de nieuwe controle ontworpen om organisaties te helpen begrijpen hoe ze gehackt kunnen worden en om bedrijven te informeren over welk type data aanvallers zoeken.

ThreatWatcher biedt deze exacte oplossingen, zodat organisaties kunnen aantonen dat ze voldoen aan de nieuwe naleving van Threat Intelligence.

Neem contact op met onze experts voor meer informatie over ThreatWatcher en hoe dit kan helpen bij het aantonen van naleving met de nieuwe vereisten en controlemaatregelen die zijn geïntroduceerd in ISO 27001:2022.

NEEM CONTACT MET ONS OP

CREST VA PEN TEST STAR Intelligence-led PT STAR Threat intelligence CSIR SOC OVS

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council APPROVED SCANNING VENDOR

CYBER ESSENTIALS

ISO 9001 ISOQAR REGISTERED

ISO 27001 ISOQAR REGISTERED

Cert No. 23208

ISO 14001:2004 REGISTERED FIRM

Neem contact op

Ga naar **www.nettitude.com** voor meer informatie of stuur uw aanvragen per e-mail naar **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES

Americas
810 Seventh Avenue
Suite 1110
New York
NY 10019

Asia Pacific
460 Alexandra Road
#15-01
mTower
Singapore 119963

Europa
Fidiou 9
Athina
106 78
Greece

LRQA NETTITUDE