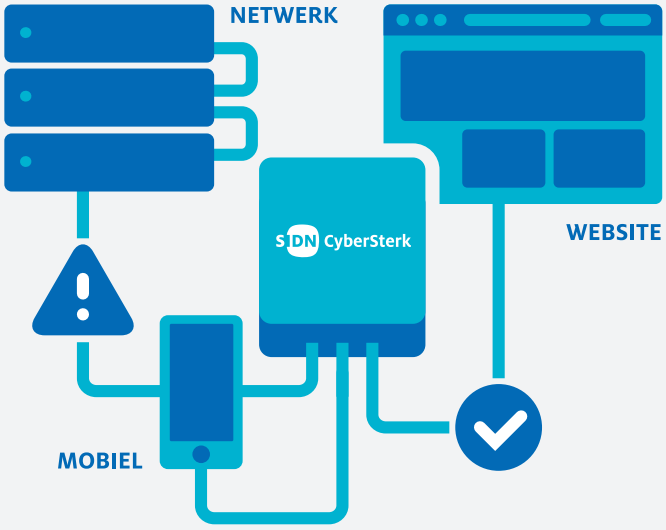
Technische informatie

SIDN CyberSterk is een begrijpelijke securitydienst die je helpt om met een gerust hart te ondernemen. Het geeft jou inzicht in de digitale veiligheid van je bedrijf, zonder je te overladen met technische details. Die technische details zijn er natuurlijk wel. Wil je er meer over weten? In dit document lees je over de precieze werking van SIDN CyberSterk.

Op cybersterk.nl/technische-informatie vind je ook nog een lijst met de meest gestelde vragen (en de antwoorden daarop) over de technische werking van SIDN CyberSterk. Vind je het antwoord op je vraag niet? Mail dan naar support@cybersterk.nl of bel naar +31 26 352 55 33.

SIDN CyberSterk bestaat uit 5 onderdelen:
1. Het Network Intrusion Detection System (NIDS);
2. De netwerkscan;
3. De websitescan;
4. Het dashboard / rapportagesysteem;
5. Phishing simulaties.

Hieronder lees je technische informatie over de eerste 3 onderdelen, de scans en data-analyse waarop ons platform opgezet is.



1. NIDS (Network Intrusion Detection System)

Met behulp van de NIDS kunnen we realtime bedreigingen en aanvallen detecteren. We sluiten de SIDN CyberSterk-box hiervoor aan op een SPAN-poort binnen het bedrijfsnetwerk, op het koppelvlak van het interne netwerk naar de buitenwereld. Hierdoor kan de box het dataverkeer monitoren en verdachte activiteiten in kaart brengen. SIDN CyberSterk kijkt hierbij niet inhoudelijk naar het dataverkeer. We slaan alleen metadata van het verkeer op (bron-ip, doel-ip, poortnummer en URL).

Deze zogenaamde IPfix-flow berichten worden vervolgens versleuteld en naar onze cloudomgeving gestuurd. Daar wordt het verkeer gecategoriseerd en geanalyseerd en tegen een uitgebreide threat-intelligence database aangehouden. Deze database maakt gebruik van een groot aantal threat-intelligence leveranciers en verwerkt meer dan 90.000 updates per 15 minuten.

De data wordt gescand op de aanwezigheid van bijvoorbeeld:
- Ransomware;
- Botnets;
- Malware/virussen;
- TOR-netwerkconnecties;
- ADware;
- Bitcoin-miners;
- File-sharing-verbindingen (torrent, emule, etc.); en andere verdachte gedragingen.

Ook kan het platform historische analyses uitvoeren. Elke nacht voert onze cloudomgeving diepgaande analyses van de meta-data van de afgelopen 6 maanden, op basis van de meest recente threat-intelligence. Zo detecteren wij ook infecties die eerder plaatsgevonden heb-ben maar waarover op dat moment nog geen informatie beschikbaar was.

2. Netwerkscan

De SIDN CyberSterk-box scant wekelijks alle aangesloten apparaten binnen je bedrijfsnetwerk. Voor deze scans zetten wij een platform in met een uitgebreid arsenaal aan scanners dat gevoed wordt vanuit meerdere threat-intelligence leveranciers. Zo kan de SIDN CyberSterk-box laptops, desktops, netwerk-apparatuur, firewalls, servers, netwerkopslag, slimme apparaten, etc. scannen op een groot aantal beveiligingsproblemen.
Dit gebeurt over een periode van meerdere dagen zodat de scans een minimale impact hebben op het bedrijfsnetwerk.

Voorbeelden van kwetsbaarheden die de scan vindt:

- Apparatuur met missende (security)patches;
- Gebruikers met zwakke wachtwoorden;
- Open poorten;
- Ongewenste services/-diensten;
- Authenticatiekwetsbaarheden;
- Verouderde software (met beveiligingsrisico's);
- Encryptieproblemen;
- Misconfiguraties van servers en applicaties;
- Netwerkconfiguratieproblemen;
- Het netwerk is onderdeel geworden van een botnet;
- Het netwerk is vatbaar voor DDoS-aanvallen;
- Systemen die onbedoeld openstaan naar het internet.

3. Websitescan

Deze scan controleert wekelijks de website(s) op een groot aantal bekende securityproblemen. Hierbij richten we ons niet alleen op de website scannen, maar ook op de server waarop de site gehost wordt. Hierbij wordt elke link en folder op de website gescand, op zoek naar kwetsbaarheden. Daarbij maakt het niet uit of de website gebruik maakt van een standaard content management system (zoals WordPress of Joomla) of een maatwerksysteem.

Voorbeelden van kwetsbaarheden die de scan vindt:

- Injectiemogelijkheden en kwetsbaarheden;
- Foutief sessiemanagement;
- Authenticatieproblemen;
- Script-injectiemogelijkheden;
- Manipuleren en vervalsen van transacties;
- Meest misbruikte webapplicatiekwetsbaarheden;
- Niet gevalideerde verwijzingen;
- TLS/SSL-problemen;
- Server- /architectuurproblemen;
- Configuratieproblemen;
- Gevoeligheid voor DDoS-/reflectionaanvallen;
- Kwetsbaarheden in het CMS, inclusief eventuele plugins van derden.

Zo werkt SIDN CyberSterk

Security

Om de veiligheid van SIDN CyberSterk te kunnen garanderen hebben we maatregelen getroffen om het platform en de hard-ware zo goed mogelijk te beschermen.

Hardware

- De hardware is 'tamperproof' opgezet en voorzien van een unieke key/identifier.
- Elke 5 minuten stuurt de SIDN CyberSterk-box een heartbeat met daarin de ID van de box en een hash van de geïnstalleerde software. Wijzigingen aan de hardware of de software worden direct gedetecteerd.
- Upgrades en onderhoud worden volledig vanuit ons platform gemanaged en gekoppeld aan de unieke key van de SIDN CyberSterk-box.

Platform

- Het platform wordt gehost bij Nederlandse partijen die ISO 27001 en NEN 7510 gecertificeerd zijn.
- De omgeving met klantdata (administratie) en de omgeving met scanresultaten (meta-data) worden op aparte locaties gehost.
- Wij maken geen gebruik van buitenlandse partijen voor de opslag en verwerking van data. Alleen voor de hiervoor genoemde 'heartbeat' van de SIDN CyberSterk-box maken wij gebruik van AWS (Amazon Webservices) in Frankfurt, met een fallback naar AWS Ierland. Deze 'heartbeat' bevat echter geen herleidbare informatie.
- Voor het SIDN CyberSterk-platform zetten wij de technologie in van Guardian360 en SecureMe2.

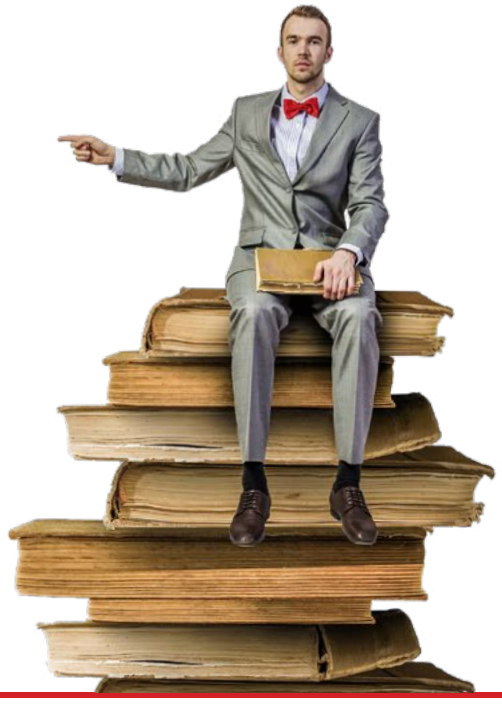
Proces

- Zowel de hardware als het softwareplatform worden regelmatig onderworpen aan security-audits en pentesten.
- SIDN CyberSterk verstrekt nooit data (klantgegevens, ruwe data of rapportages) aan derden.
- Alleen bevoegde SIDN CyberSterk-medewerkers hebben toegang tot de scanresultaten.

SIDN CyberSterk is een product van SIDN Business B.V.,
onderdeel van SIDN | KvK 75364689 | BTW NL860254252B01

SIDN Zorgeloos online

Bedankt voor uw interesse in Cybersterk!



Hopelijk heeft dit document u de benodigde informatie en inzicht gegeven waar u op zoek naar was.

Andere tools die uw organisatie weerbaarder maken

ProteQtor IT Security is niet alleen reseller partner van SIDN Cybersterk, maar biedt nog meer cybersecurity tools aan om uw organisatie zo weerbaar mogelijk te maken.

Hieronder tools die wellicht interessant zijn ter bescherming van uw organisatie:

- Bescherm uw gegevens met **SentinelOne endpoint protection**
- Liever een Europese endpoint protection & EDR tool? Kies **Reaqta**
- Beveilig uw e-mail met **Proofpoint email security**
- Train uw medewerkers met laagdrempelige **Wizer security awareness trainingen**
- Bescherm het inloggen met **Watchguard Authpoint multi-factor authenticatie**
- Voorkom bezoeken aan ongewenste websites met **NSOC360 Safeweb webfiltering**
- Krijg inzicht in de veiligheid van uw netwerk met **Guardian360 scans**
- Herstel verloren data met **NSOC360 Safedata online backup**

ProteQtor
Next-Gen IT Security

Laat hackers uw bedrijfscontinuïteit niet in gevaar brengen!

Cyberaanvallen bedreigen privacy, bedrijfskritische data, de reputatie en andere 'kroonjuwelen' die cruciaal zijn voor de continuïteit van uw organisatie. De vraag is allang niet meer 'of' uw organisatie aangevallen wordt, maar 'wanneer' uw organisatie (weer) aangevallen wordt. Het is essentieel om cyberaanvallen te voorkomen en de gevolgen van cyberaanvallen tot een minimum te beperken. Het feit dat u deze pdf leest, toont dat u dat belang inziet.

Vanwege de grootte, de complexiteit en de diversiteit van moderne cyberaanvallen is een multidisciplinaire aanpak nodig. We helpen u graag met praktische adviezen en effectieve oplossingen om deze aanpak te realiseren.

Met de juiste trainingen, tools en support helpen wij u hackers het hoofd te bieden en er voor te zorgen dat alles wat voor uw organisatie van waarde is, beschermd blijft.

Hulp nodig? Bel 088-0660770 of plan een afspraak in

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl