HACKIFY

YOUR DEFENSE, OUR HACKSPERTISE

WHITEPAPER

Vulnerability Scanning

Table of

Content

Vulnerability Scanning

In een tijd waarin dagelijks nieuwe beveiligingslekken in software ontdekt worden, is het (half) jaarlijks uitvoeren van een pentest niet langer voldoende. Hoewel dit grondig inzicht geeft in het weerbaarheidsniveau, blijft het een momentopname. Organisaties moeten omgaan met een voortdurend veranderende bedreigingsomgeving, waarin elke dag nieuwe kwetsbaarheden aan het licht komen. Dit benadrukt de noodzaak voor frequente en dynamische beveiligingsmaatregelen.

Vulnerability scanning biedt een oplossing door regelmatig en systematisch het beveiligingsniveau van systemen te controleren, zodat organisaties proactief kunnen reageren op nieuwe kwetsbaarheden en hun cyberweerbaarheid kunnen versterken.

Ons Proces

Asset Discovery

We beginnen met het verkrijgen van een overzicht van alle IT-assets binnen uw organisatie. Dit omvat IP-adressen en openstaande poorten/services. Door een volledig overzicht te krijgen van alle assets, kunnen we een volledig beveiligingsbeeld schetsen, zonder assets over het hoofd te zien. Een volledige asset discovery is de basis voor het volledig in kaart krijgen van alle potentiële beveiligingsproblemen.

Vulnerability Scanning

Nadat we een volledig overzicht hebben van het IT-landschap controleren we de IT-systemen periodiek op kwetsbaarheden en misconfiguraties. Door gebruik te maken van geavanceerde tools, zowel betaald als open-source en in-house gemaakte beveiligingschecks, detecteren we snel en efficiënt mogelijke zwakke punten in uw systemen en services.

Vulnerability Assessment

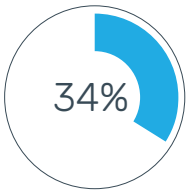
Na het identificeren van kwetsbaarheden rangschikken we deze op basis van hun realistische impact op uw organisatie. We gebruiken contextspecifieke risicoclassificaties om inzicht te geven in welke kwetsbaarheden als eerste moeten worden aangepakt. Daarnaast filteren we op eventuele false positives en aggregeren overlappende bevindingen tot één duidelijke finding. Hierdoor blijft alleen de informatie over die ertoe doet.

Vulnerability Visualization

De bevindingen worden gevisualiseerd in een interactief dashboard. Elke bevinding bevat een korte omschrijving, risicobeschrijving en een voorstel voor een oplossing. Door gebruik te maken van duidelijke grafieken en rapportages krijgt u inzicht in de kwetsbaarheden en de voortgang van het verhelpen ervan. Dit maakt het eenvoudiger om trends te herkennen, waardoor u nog meer inzicht krijgt en beter geïnformeerde beslissingen kunt nemen.

Cyberincidenten: het grootste risico voor bedrijven

Uit een enquête van Statista blijkt dat cyberaanvallen een van de grootste bedreigingen zijn voor bedrijven, gevolgd door bedrijfsonderbrekingen en macro-economische ontwikkelingen. Tussen 2018 en 2023 noemde 34% van de respondenten cyberincidenten als hun grootste zorg, waaronder malware, ransomware en cybercriminaliteit.

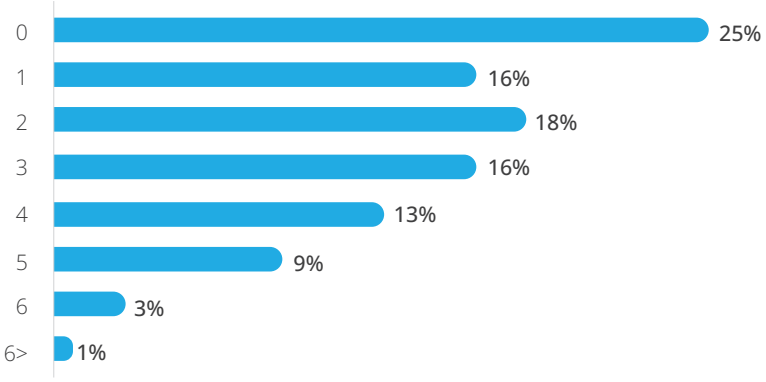


Bron: Statista

Ransomware blijft een probleem

Ransomware vormt een groeiend en verontrustend probleem. De cijfers van Veeam Insights onderstrepen deze zorgwekkende trend. Uit een onderzoek onder meer dan 1200 bedrijven blijkt dat drie op de vier organisaties het afgelopen jaar minstens één ransomware-aanval heeft ervaren.

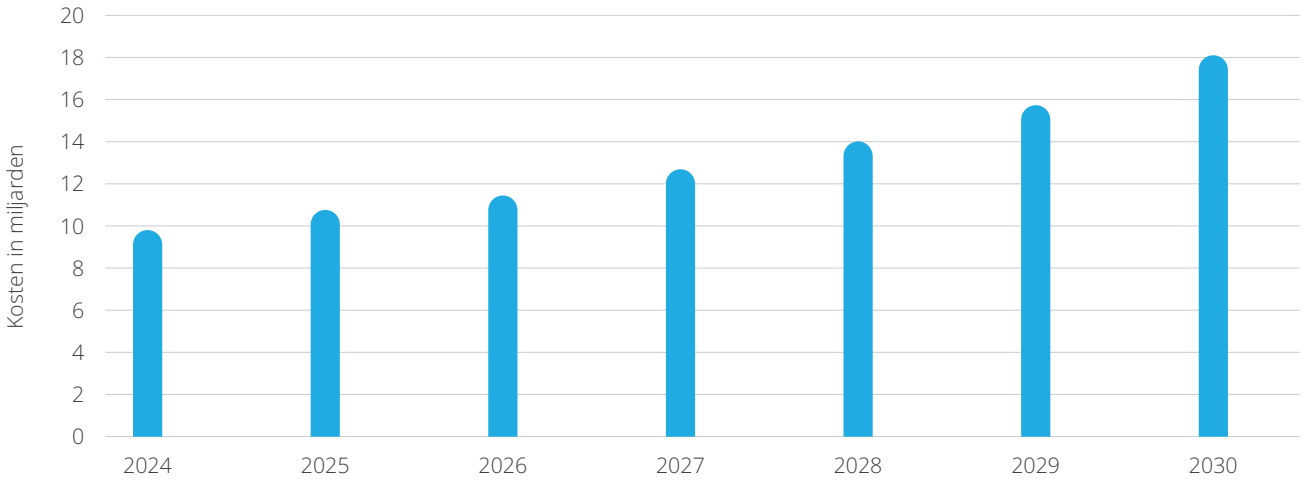
Bovendien rapporteert 26% van de bedrijven zelfs vier of meer ransomware-aanvallen binnen dezelfde periode.



Kosten van cyberaanvallen stijgen

Hoewel de totale kosten van cyberaanvallen moeilijk te voorspellen zijn door de dynamische aard van digitale bedreigingen, bieden inzichten van Cybersecurity Ventures een kader voor toekomstprojecties. Deze cijfers houden rekening met technologische ontwikkelingen, sectortrends en wereldwijde gebeurtenissen. Zowel aanvallers als verdedigers ontwikkelen voortdurend nieuwe technieken, wat invloed heeft op de kosten en effectiviteit van aanvallen en schadebeperking. Geopolitieke situaties en economische omstandigheden beïnvloeden de frequentie en aard van cyberaanvallen, wat de kostenramingen nog complexer maakt.

Geschatte kosten cyberaanvallen



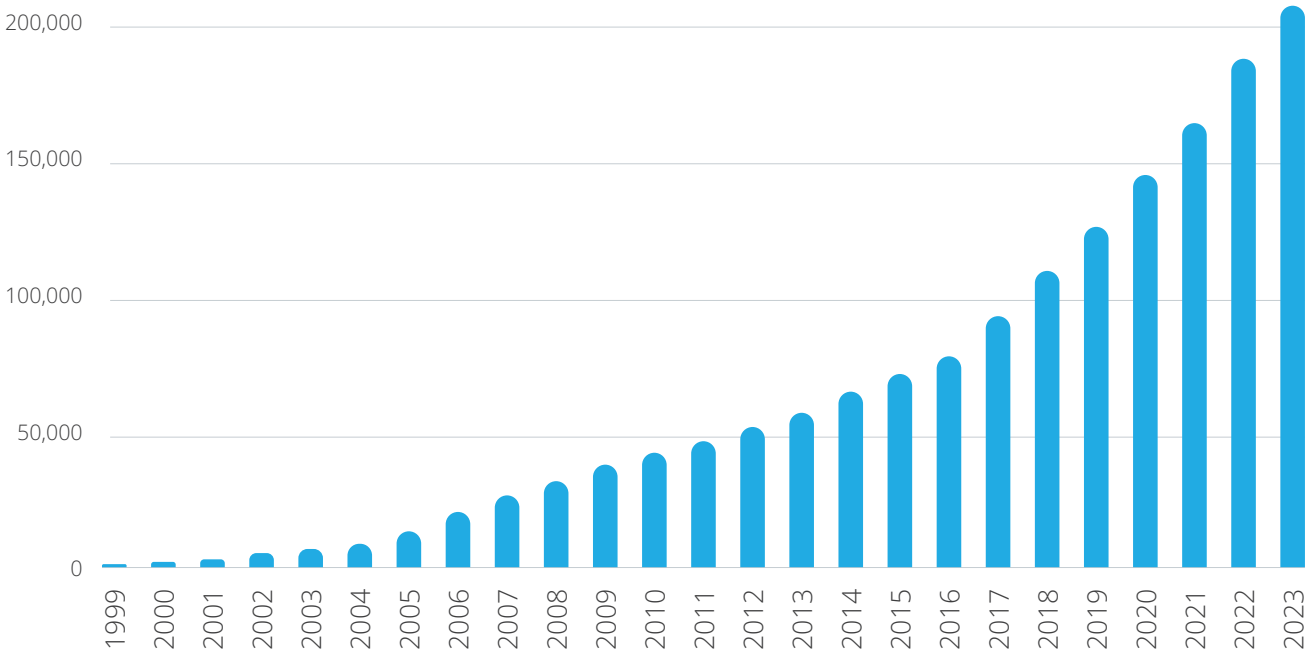
[1] https://www.expressvpn.com/nl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/
[2] https://go.veeam.com/wp-data-protection-trends-2024

Steeds meer nieuwe kwetsbaarheden ontdekt

In 2023 werden wereldwijd meer dan 28.000 nieuwe kwetsbaarheden ontdekt. Dit groeiende aantal vergroot aanzienlijk de kans dat een kwetsbaarheid over het hoofd wordt gezien en niet tijdig wordt verholpen. Volgens het Security Navigator 2023-rapport blijft gemiddeld zelfs 72% van de kwetsbaarheden binnen 30 dagen onopgelost.

Hetzelfde onderzoek toont aan dat grote bedrijven, met meer dan 10.000 medewerkers, het grootste aantal middelgrote en kritieke kwetsbaarheden hebben. Middelgrote organisaties, met 101 tot 1.000 medewerkers, worden echter het vaakst geconfronteerd met hoogrisico-kwetsbaarheden.

Met zoveel kwetsbaarheden neemt de kans toe dat sommige onopgemerkt blijven. Dit vergroot het risico op beveiligingsincidenten, datalekken en systeemuitval. Onopgemerkte kwetsbaarheden kunnen door kwaadwillenden worden misbruikt, wat kan leiden tot ernstige financiële en operationele gevolgen voor organisaties.



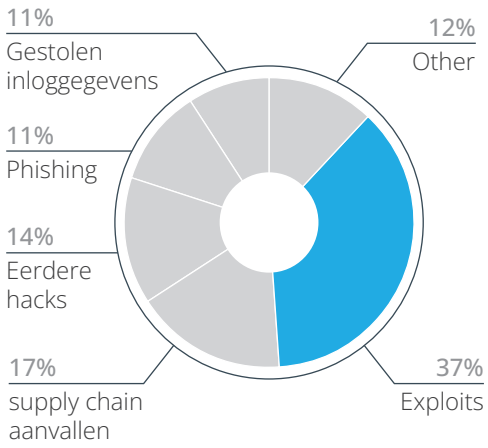
Totaal aantal kwetsbaarheden

Bron: NIST National Vulnerability Database

Hackers misbruiken bekende kwetsbaarheden

Zoals eerder vermeld, blijft het aantal nieuwe kwetsbaarheden elk jaar toenemen, wat het tijdig uitvoeren van beveiligingsupdates steeds moeilijker maakt. Dit vergroot de kans dat kwetsbaarheden over het hoofd worden gezien of te laat worden verholpen, wat kan leiden tot misbruik van deze kwetsbaarheden.

Uit onderzoek van Mandiant blijkt dat 37% van de cyberaanvallen begint met het uitbuiten van bekende kwetsbaarheden. Onderzoekers van Palo Alto ontdekten dat cybercriminelen soms al binnen enkele minuten na het ontdekken van een nieuwe kwetsbaarheid het internet scannen om deze kwetsbaarheid te vinden en te misbruiken.

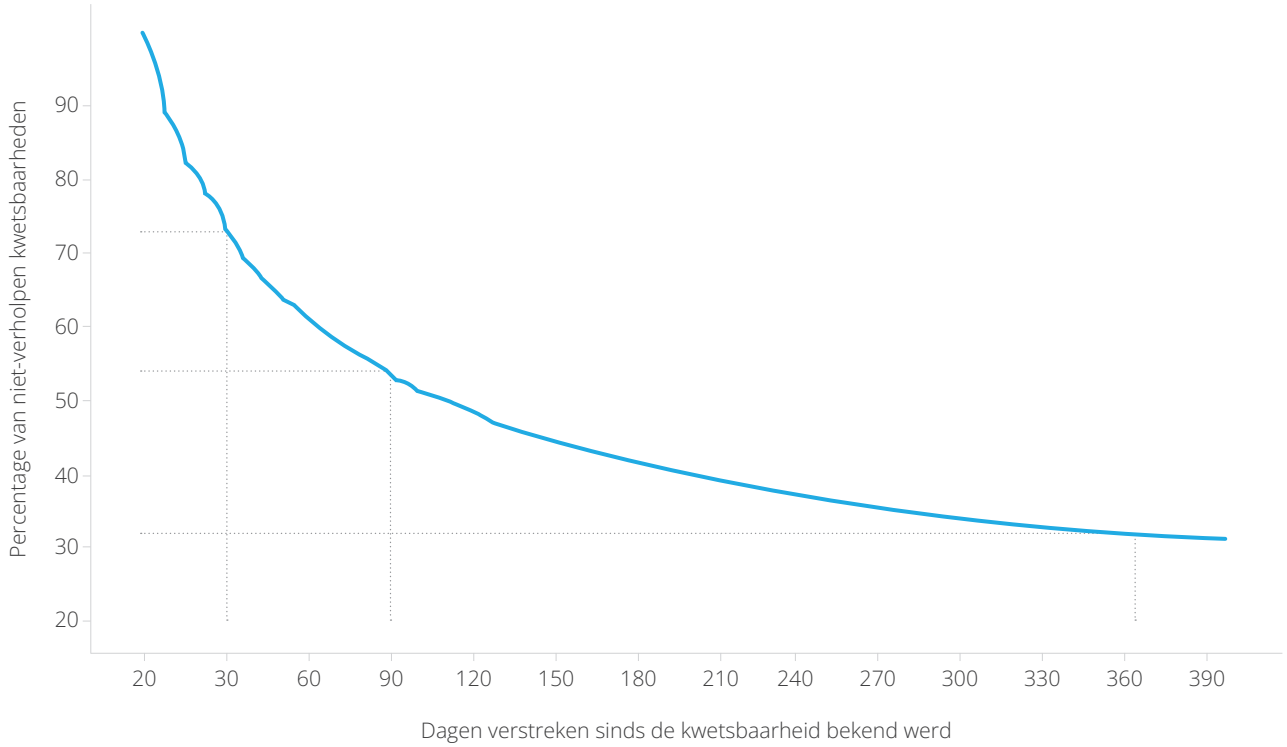


Bron: Mandiant

Levensduur van Kwetsbaarheden

Uit onderzoek van Tenable blijkt dat de levensduur van kwetsbaarheden sterk kan variëren. Gemiddeld wordt slechts 27% van de kwetsbaarheden binnen 30 dagen verholpen. Daarnaast blijkt dat 32% van de kwetsbaarheden zelfs na een jaar nog niet opgelost zijn en 26% helemaal nooit worden verholpen.

De levensduur van een kwetsbaarheid hangt af van factoren zoals de complexiteit van het probleem, de beschikbaarheid van een oplossing en de prioriteit binnen de organisatie. Eenvoudige kwetsbaarheden worden sneller opgelost, terwijl complexere problemen langer blijven bestaan.



[3] https://www.tenable.com/blog/what-is-the-lifespan-of-a-vulnerability

Onze unieke aanpak

Met de toename van kwetsbaarheden en de uitdaging om deze tijdig te verhelpen, wordt het belang van vulnerability scanning steeds duidelijker. Traditionele methoden zijn vaak traag en inefficiënt, wat leidt tot een verhoogd risico op misbruik van zwakke punten. Door continue en geautomatiseerde scans uit te voeren, kunnen organisaties potentiële risico's sneller identificeren en verhelpen, waardoor de kans op uitbuiting door cybercriminelen aanzienlijk wordt verminderd.

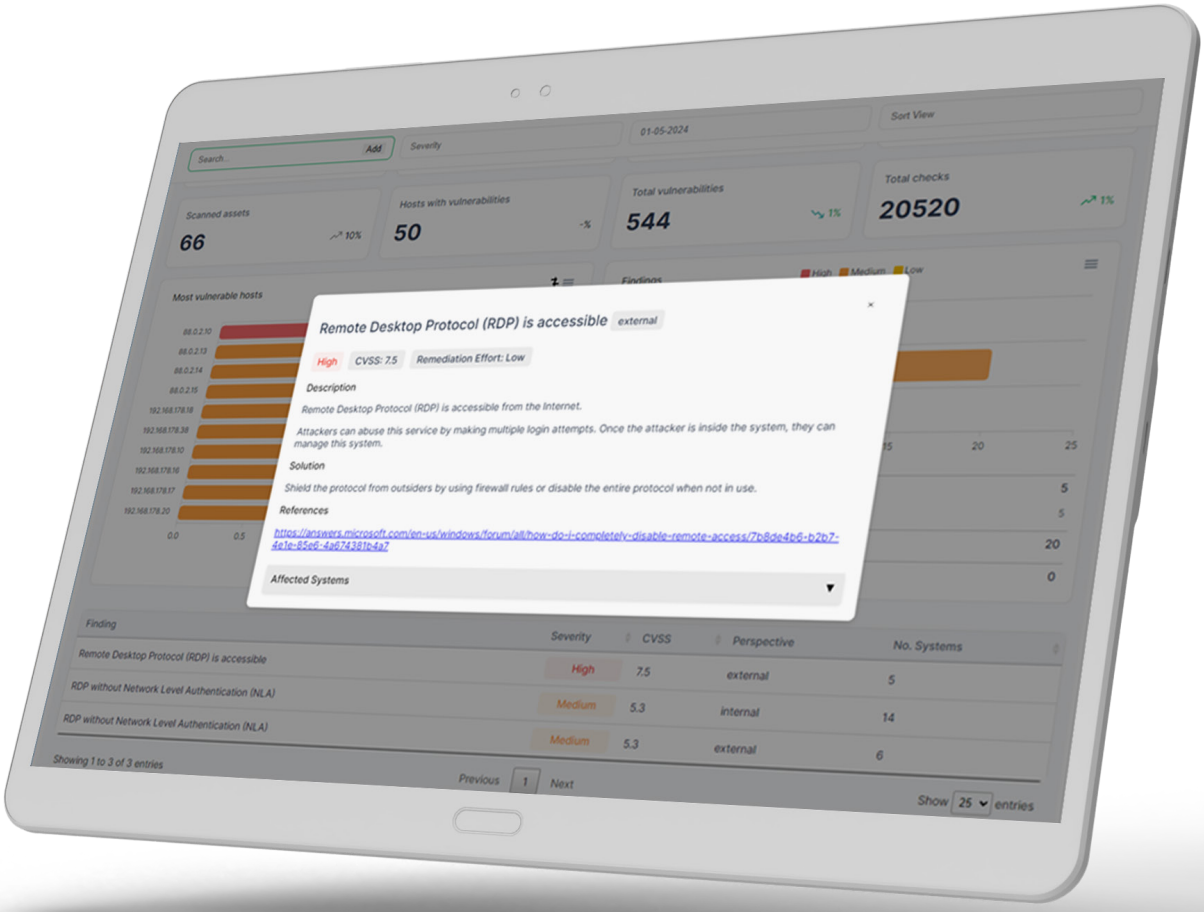
Onze unieke aanpak onderscheidt zich door het filteren en aggregeren van resultaten, zodat u niet overspoeld wordt met onnodige details. In plaats van meerdere bevindingen over specifieke SSL/TLS-aanvallen zoals Lucky13, BEAST en Crime, geven wij één duidelijke bevinding waarin staat vermeld dat uw SSL/TLS-configuratie verouderd en zwak is. We verwijderen bevindingen die alleen maar ruis veroorzaken, zodat u een helder en duidelijk overzicht krijgt van wat echt belangrijk is. Dit stelt u in staat om snel en gericht actie te ondernemen zonder tijd te verliezen aan onbelangrijke details.

Andere aanbieders		Wij	
Medium	*Lucky13 attack*	High	Verouderde en kwetsbare SSL/TLS configuratie
High	RC4 ciphers		
Medium	*BEAST attack*		
Medium	*Crime attack*		
High	SSL versie 2 & 3		
High	*Drown attack*		
High	*Poodle attack*		

Automatische scans detecteren snel en efficiënt kwetsbaarheden, maar kunnen soms fouten maken. Daarom nemen wij de bevindingen van onze scanners nooit zonder meer over; er vindt altijd een grondige controle op false positives plaats. Standaardconfiguraties van scanners zijn vaak suboptimaal, wat kan leiden tot gemiste beveiligingsproblemen. Met onze jarenlange ervaring configureren en voeren wij deze scans zelf uit, zodat u verzekerd bent van nauwkeurige en betrouwbare resultaten. Hierdoor kunt u zich concentreren op wat echt belangrijk is, zonder bezorgd te hoeven zijn over mogelijke fouten in de scanresultaten.

Bevindingen in context geplaatst

Dankzij onze jarenlange ervaring als ethical hackers plaatsen wij bevindingen altijd in de juiste context. Zo heeft het Remote Desktop Protocol (RDP), dat via het publieke internet bereikbaar is, een ander risicoprofiel dan wanneer het alleen via het interne netwerk toegankelijk is. We houden rekening met de specifieke omgeving en hanteren een contextspecifieke risicoclassificatie. Dit zorgt ervoor dat u een accuraat beeld krijgt van de werkelijke risico's en prioriteiten, zodat u gerichte en effectieve beveiligingsmaatregelen kunt nemen.



Voor aanvullende informatie of verduidelijking kunnen onze cybersecurity-experts u verder helpen. Onze deskundige professionals staan klaar om met u te overleggen en de meest effectieve aanpak te bepalen. Hiermee kunt u niet alleen de geïdentificeerde kwetsbaarheden aanpakken, maar ook waardevol advies ontvangen over uw algehele beveiligingsstrategie en mogelijke verbeteringen.

Interactieve resultaten met voortgang en filtering

Het presenteren van bevindingen via een rapport is vaak inefficiënt en moeilijk doorzoekbaar. Daarom hebben wij een interactief dashboard ontwikkeld dat intuïtief en gebruiksvriendelijk is. Het maakt het eenvoudiger om inzicht te krijgen in de resultaten door filtering toe te passen.

Daarnaast toont het dashboard de voortgang ten opzichte van de vorige scan. U ziet of bevindingen zijn verholpen of dat er nieuwe kwetsbaarheden zijn bijgekomen. Deze trends zijn belangrijk om inzicht en grip te krijgen op uw cyberweerbaarheid.

Verschil vulnerability scan en een pentest

Een pentest (kort voor penetratietest) en een vulnerability scan worden vaak door elkaar gehaald. Hoewel beide zwakke plekken in het bedrijfsnetwerk of kantoorautomatisering identificeren, zijn er duidelijke verschillen tussen beide diensten. Vulnerability scans zijn geautomatiseerde scans die beveiligingsrisico's op hoog niveau identificeren, terwijl penetratietests diepgaande beoordelingen zijn waarbij specialisten actief kwetsbaarheden in het netwerk opsporen en proberen uitbuiten. Samen bieden ze een grondig inzicht in de beveiligingsstatus en helpen ze bij het verbeteren van de weerbaarheid tegen cyberaanvallen zoals ransomware.

HACKIFY

YOUR DEFENSE, OUR HACKSPERTISE