CyberAnt NetCaptain

Beheerde Kwetsbaarheidsscans

Zelfs met behoorlijke kwetsbaarheidsscanners kan het een zware en tijdrovende klus zijn om real-time inzicht te krijgen in het beveiligingsniveau van een organisatie. Het orkestreren van kwetsbaarheidsscanners kan tijd besparen en helpt de mitigatietijd te versnellen.

Alle Tools in één Box
CyberAnt combineert de toonaangevende tools, orkestreert ze en combineert ze tot de beste oplossing die momenteel op de markt te krijgen is. We hebben de scanners zorgvuldig geselecteerd en duidelijke afspraken gemaakt met alle leveranciers. Hierdoor kunnen wij één contract leveren tegen een zeer scherpe prijs.

Fysieke of Virtuele Appliance
Afhankelijk van de wensen van de klant kan er een fysiek kastje (appliance) worden geïnstalleerd of kan er software (virtueel image) worden geïnstalleerd op eigen hardware. CyberAnt regelt en/of begeleid de volledige installatie om een naadloze integratie te garanderen.

Een duidelijk verhaal
Hoewel alleen gebruik wordt gemaakt van de beste tools die er beschikbaar zijn, worden de scanners constant verbeterd door resultaten en risicobeoordelingen aan NetCaptain toe te voegen. Op basis van de output van alle scanners berekenen we een *CyberRisk* om aan te geven of een omgeving veilig is of niet.

Volledig geautomatiseerd
Om gestructureerd kwetsbaarheidsbeheer te kunnen uitvoeren en monitoren is het mogelijk om geautomatiseerd taken te plannen, zoals ook het scannen van het netwerk.

Dashboard
Het dashboard geeft inzicht in de CyberRisk geordend per netwerk.

Relevante statistieken
NetCaptain verzamelt relevante metrics met betrekking tot Cybersecurity. Met NetCaptain Insights kan er direct rapporten in PDF-formaat.

Boost het proces
Doordat NetCaptain de beveiligingsrisico's in het netwerk vindt kan alle focus worden besteed aan het oplossen van de kwetsbaarheden.

Scannen via het netwerk

Cybercriminelen gebruiken zwakke plekken in systemen en netwerken om (gevoelige) gegevens te stelen of de bedrijfscontinuïteit te verstoren. Door kwetsbaarheden zoveel mogelijk op te lossen wordt het voor hackers steeds moeilijker om het netwerk.

Netwerkbeheer
Om een netwerk te beschermen, moet bekend zijn welke systemen er in het netwerk aanwezig zijn. NetCaptain helpt om de CyberRisk van systemen in het netwerk bij te houden en om systemen te ontdekken die over het hoofd zijn gezien.

Scan elk apparaat
NetCaptain kan beveiligingslekken ontdekken in besturingssystemen zoals Windows, Linux/ Unix, FreeBSD etc., en databases zoals Oracle, SQL-server en MySQL, en netwerkapparaten zoals routers, switches en firewalls.

Inloggen met NetCaptain op bedrijfssystemen
NetCaptain kan kwetsbaarheden ontdekken zonder inloggegevens. Het is echter beter om inloggegevens aan NetCaptain mee te geven, omdat sommige kwetsbaarheden alleen gevonden kunnen worden wanneer NetCaptain kan inloggen op het systeem.

NetCaptain kan backdoors, virussen, malware-URL's en kwaadaardige inhoud detecteren. Het is de perfecte aanvulling op antivirussoftware.

Patchbeheer
NetCaptain detecteert ontbrekende en onjuist geïmplementeerde patches die uw systeem kwetsbaar maken voor cyberaanvallen.

Scan ze allemaal
NetCaptain scant en ontdekt apparaten, van werkstations tot netwerkapparaten.

In de Cloud
NetCaptain is in staat om audits uit te voeren op Cloud gebaseerde oplossingen.

Configuratiecontroles
NetCaptain controleert op zwakke configuratie om ervoor te zorgen dat systemen niet alleen up-to-date zijn, maar ook veilig geconfigureerd.

Webapplicaties

Volgens studies bevat meer dan 70% van alle websites kwetsbaarheden die kunnen leiden tot datalekken. Tegenwoordig zien we een toename van het vermogen van aanvallers om in korte tijd het hele internet te scannen. Vaak zijn organisaties zich niet bewust van de kwetsbaarheden in de eigen website, of vertrouwen volledig op ontoereikende oplossingen zoals *Web Application Firewalls*.

Testen van veel voorkomende technologieën
NetCaptain test alle veel voorkomende technologieën zoals *frameworks* en *open source Content Management Systemen (CMS)* op kwetsbaarheden, evenals de hierin aanwezige plug-ins.

Inloggen met NetCaptain op webapplicaties
De meeste webapplicaties gebruiken een vorm van authenticatie om hun gebruikers te identificeren. NetCaptain kan automatisch inloggen met door de gebruiker opgegeven inloggegevens. Deze inloggegevens worden op een veilige manier opgeslagen in NetCaptain.

Geavanceerde detectie van kwetsbaarheden
NetCaptain kan complexe en moeilijk te vinden kwetsbaarheden detecteren, zoals *DOM-based XSS* en *blind SQL-injection.*

Het ontdekken van gevoelige gegevens
Soms bevatten websites testgegevens of bestanden die niet op de productieserver hadden mogen staan. NetCaptain kan dit detecteren en rapporteren.

Beveiligde websites
Vaak wordt gedacht dat websites met een groen slotje in de adresbalk veilig zijn; het kan zijn dat SSL/TLS verkeerd geconfigureerd is. Dit kan leiden tot decodering van gevoelige informatie zoals wachtwoorden of API-sleutels. NetCaptain zal een eventuele verkeerde configuratie detecteren en rapporteren.

Scan webapplicaties
NetCaptain detecteert en rapporteert kwetsbaarheden in webapplicaties.

Testen
NetCaptain test alle veel voorkomende technologieën.

Configuratie SSL/TLS
NetCaptain zal een eventuele verkeerde configuratie detecteren en rapporteren.

Technische ondersteuning

NetCaptain ondersteunt o.a. de volgende technologieën:

Operating systemen

Windows 2003	Windows 7	Red Hat
Windows 2008	Windows 8	Solaris
Windows 2008 R2	Windows 10	AIX
Windows Server 2012	Windows 11	FreeBSD
Windows Server 2016	Mac OS	HPUX
Windows Server 2019	Ubuntu/ Debian	Solaris
Windows Vista	SUSE	Cisco IOS

Databases

MSSQL	MongoDB	IBM DB2
MySQL	Oracle 10	PostgreSQL
MariaDB	Oracle 11g	Informix

Toepassingen en technologieën

IIS	Spring framework	HTML5
Apache	Struts	Ruby on Rails
Nginx	Sharepoint	AngularJS
.PHP	Internet Explorer	Joomla
ASPX / .NET	Firefox	Drupal
Java	Safari	Wordpress
Tomcat	Microsoft Office	jQuery
JBoss	Adobe Reader	Mootools
	Adobe Flash	... en vele anderen

Netwerkapparaten

Cisco	Palo Alto	F5-netwerken
Juniper	Dell SonicWall	SCADA
Checkpoint	FireEye	Asterisk
		... en vele anderen