BODYGUARD.IO

Waarom is CDR nodig?

Analisten van Gartner identificeren CDR-technologie als bijzonder nuttig

In de nieuwste editie van Gartner's Hype Cycle-rapport over netwerkbeveiliging scoort CDR-technologie voor het opschonen van inhoud hoog op de prioriteitsmatrix voor netwerkbeveiliging, vanwege het vermogen om te beschermen tegen malware die zich 'genesteld' heeft in bijlages. CDR vereist geen langdurige dynamische analyse of traditionele inspectie (zoals signatures) voor het identificeren van malware. De analisten van Gartner identificeren CDR-technologie als bijzonder nuttig "waar bestanden de grenzen van de organisatie overschrijden".

Voordelen volgens Gartner

- Het minimaliseert het risico dat malware de organisatie binnendringt, via bijlages die via talloze kanalen binnenkomen op het apparaat van de medewerker (e-mail, web, Teams, Whatsapp, Zoom, etc.). Het verwijdert nagenoeg alle voorkomende aanvalstechnieken die op andere manieren moeilijk te bestrijden zijn.
- Het is vele malen sneller dan sandboxing en vormt daarom een goede aanvullende oplossing. Bovendien weet geavanceerde malware op eenvoudige wijze de sandbox te omzeilen.

Meer weten?

Ga naar: **bodyguard.io**

Kritische blik op de beveiligingsmethodiek van vandaag

Op signature-gebaseerde detectie

Inmiddels is bekend dat op signature-gebaseerde beveiliging eenvoudig te omzeilen is. Zodra een malware bestand minimaal wordt aangepast leidt dit al tot een andere signatu-re. Het gevolg is dat deze beveiligingstechniek gemiddeld 18 dagen achterloopt.

Dynamische analyse en sandboxing

Kent u de sjoemelsoftware bij Volkswagen nog? Moderne malware weet op een vergelijk-bare wijze onder de radar te blijven. In een sandbox wordt een momentopname gemaakt van het systeem waarbinnen de potentieel onveilige software vervolgens wordt geopend. Via een complete blauwdruk van het systeem is de sandbox in staat om minimale wijzigin-gen te herkennen en te concluderen of een bestand schadelijk is.

Helaas zijn er ontelbare mogelijkheden om de sandbox voor de gek te houden. De malware kan bijvoorbeeld voorzien zijn van een ingebouwde timer waarmee het pas schadelijk acties uitvoert na een bepaalde tijd. Stel deze timer is ingesteld op 10 minuten, dan zal vrijwel iedere sandbox het bestand vrijgeven aangezien geen enkele gebruiker zo lang op een bestand gaat wachten. Er zijn meer voorbeelden, zoals het wachten op een gebrui-kershandeling. Deze handeling zal nooit komen in een sandbox waardoor de malware onopgemerkt blijft.

Endpoint, detection and response (EDR)

Eerdere beveiligingsmethoden hebben malware niet gestopt. Hiervoor is EDR in het leven geroepen. Deze technologie analyseert de logboeken van het systeem om afwijkende gedragingen te herkennen en daarop te acteren.

Malware ontwikkelaars hebben diverse technieken waarmee zij EDR om de tuin kunnen leiden, te weten ‘unhooking’ en ‘directe systeem calls’. Dit zijn populaire methoden die zelfs werken bij de meest actuele versie van het besturingssysteem. In feite zorgt dit ervoor dat EDR geen loginformatie ontvangt over de acties van het malware proces.

Firewall en Network, detection and response (NDR)

Wanneer ook EDR gefaald heeft, dan krijgt de malware kans om aan te sluiten op de com-mand and control (C2C) infrastructuur van de cybercriminelen. Vanaf dit moment hebben zij langdurig toegang tot het apparaat en daarmee het netwerk. Door inzet van firewall en

NDR wordt ook het netwerkverkeer gemonitord om vast te stellen of er onregelmatigheden zijn. Om deze reden gebruiken criminelen steeds vaker publieke clouddiensten (OneDrive, Google Drive, AWS, etc.) aangezien deze niet als afwijkend worden beschouwd.

Security operations center (SOC) en threat hunting

Indien een organisatie beschikt over een SOC, dan zijn er professionals aanwezig om securityincidenten nader te onderzoeken. Eerder benoemde oplossingen genereren een hoop meldingen waar vervolgens aanvullend onderzoek voor nodig is. Een hoop daarvan wordt inmiddels afgehandeld door kunstmatige intelligentie, maar de rol van de SOC-analist is daarbij nog altijd onmisbaar. Menselijk oordeel komt met een foutmarge en de hamvraag is uiteindelijk, wie draagt de verantwoordelijk wanneer het fout gaat? De middelen van managed SOC-diensten worden veelal gedeeld door meerdere afnemers. De term SOC mag dan wellicht de illusie wekken dat de verantwoordelijk is verlegd, maar de opdrachtgever blijft in de praktijk gewoon aansprakelijk.

Onder aanbieders van SOC-diensten zijn grote verschillen waar te nemen. Is de dienstverlening uitsluitend reactief of ook proactief. Zo ja, in welke mate? Een dedicated threat hunting team onderzoekt manueel of er sporen van dreigingen zijn die door de automatische detectiesystemen over het hoofd zijn gezien. Dit is voor de meeste organisaties onbetaalbaar en dus wordt het resterende risico voor lief genomen.

Grote organisaties hebben de middelen om een stap verder te gaan en doen dit met red- en blue-teaming. Het red-team bestaat uit ethische hackers en neemt het op tegen het verdedigende blue-team. De realiteit is als volgt, 68% van de ondervraagde organisaties geeft aan dat het aanvallende red-team altijd wint. Zeg zelf maar, zouden criminele organisaties, met miljoenen aan omzet, niet gevaarlijker zijn dan een deeltijd red-team?

Waarom is CDR-technologie anders?

In tegenstelling tot bovengenoemde detectiemethodieken, biedt CDR een nieuwe vorm van preventie zonder alleen te vertrouwen op detectie. 75% van malware zit verstopt in documenten. Cybercriminelen misbruiken functionaliteit binnen documentstructuren om

kwaad aan te richten. Denk hierbij aan elementen zoals macro's, scripts, triggers en ingesloten objecten. Nog steeds is dit dé manier waarop zij toegang krijgen om een geslaagde hackaanval uit te voeren. Waarom dit probleem nog altijd zo groot is, komt door het gemak waarmee detectie kan worden omzeild. Met behulp van CDR technologie – relatief nieuwe technologie – wordt een document proactief geschoond waardoor geavanceerde malware en onbekende malware (zero days), geen kans krijgen om op te starten. Het resultaat is een document dat AwareLess kan worden gedownload, dat visueel identiek is aan het origineel en waar de gebruiker geen nadeel – bijvoorbeeld qua snelheid – van ondervindt.

Bodyguard is de eerste CDR endpoint oplossing

Medewerkers ontvangen documenten via talloze communicatiekanalen zoals web, mail, Teams, Zoom, Slack, etc. Tot dusver was er niet één oplossing om al deze kanalen te beschermen tegen schadelijke documenten die worden verstuurd of gedeeld... Tot nu.

Conclusie

Wanneer beveiliging in grote mate afhankelijk is van detectie, is de kans groot dat cybercriminelen een manier vinden om onopgemerkt binnen te dringen. CDR maakt een einde aan het kat- en muisspel tussen malware en detectie. Zoals Gartner al aangeeft wordt CDR steeds vaker erkend als de onmisbare schakel voor een moderne security stack. Hiermee wordt een antwoord geboden op geavanceerde malware en onbekende malware (zero days). CDR-technologie schoont alle risicovolle bijlagen waardoor malware zo vroeg mogelijk wordt geneutraliseerd.

Bodyguard biedt CDR – technologie aan als complementaire endpoint oplossing – als enige in de markt - en kan schaalbaar worden uitgerold zonder verborgen kosten.

Meer weten? Bel dan direct voor een demo met
Vincent van Sas (06-25016673) of **Daniël Luthra** (06-28038610).

Meer weten?

Ga naar: **bodyguard.io**