



IngramMicro
FlexibleServices

INGRAM[®]
MICRO

BlackBox Penetration Test (BBPT)

Het Ingram Micro Cyber Security Center of Excellence team is opgericht met de visie om te helpen het Cyber Security potentieel te ontsluiten. Het team, dat gevestigd is in Utrecht, biedt een reeks gespecialiseerde Cyber Security consultancy- en trainingsoplossingen aan onze Business en Channel Partners.

Met een services portfolio bestaande uit technische assessments, consultancy en managed security services zijn we in een zeer sterke positie om onze channel partners te helpen om elke cyber security deal te winnen. We doen dit door onze partners volledig te ondersteunen bij complexe security vraagstukken en de

INGRAM[®]
MICRO

Cyber Security Center



mogelijkheid te bieden om zelf cyber security diensten (door) te ontwikkelen en verder te laten groeien om zo lucratieve white-labelled beveiligingsdiensten aan te bieden aan eindklanten.

Black Box Penetration Testing is een methode om het beveiligingsniveau van een organisatie te testen door een aanval te simuleren die een hacker zou kunnen ondernemen om de zwakke punten in het doelnetwerk en de applicaties uit te buiten en te doorbreken. Black Box Penetration Testing wordt uitgevoerd zonder enige voorkennis van het organisatiesysteem, het netwerk of de applicaties.

In Black Box Penetration Testing richten we ons vooral op bedrijfsinfrastructuur, bedrijfslogica, applicaties en diensten die door de klant worden geleverd. Het Ingram Micro team volgt de best practice methoden en aanpak van de industrie om Black Box Penetration Testing uit te voeren. Black Box Penetration Testing wordt uitgevoerd op alle detecteerbare toepassingen, servers en netwerkapparatuur.

De doelstellingen van de Black Box Penetration Testing service zijn:

- Het simuleren van een echt hack-scenario (d.w.z. denken als een hacker) om de kracht van de bestaande beveiliging te testen en tegenmaatregelen te nemen.
- Het valideren van de configuratie van IT-assets en het produceren van een lijst van bekende kwetsbaarheden die aanwezig zijn in systemen en applicaties en het verminderen hiervan voordat ze worden uitgebuit door tegenstanders.
- Het geven van een gedetailleerd rapport over elke beveiligingsfout en het voorstellen van betere herstelrichtlijnen voor elk van de beveiligingskwetsies.

Bij het leveren van de Black Box Penetration Testing diensten zal Ingram Micro een combinatie van geautomatiseerde en handmatige scanmethoden gebruiken en zal gebruikmaken van commerciële en publiekelijk beschikbare hulpmiddelen, evenals aangepaste scripts en toepassingen die door Ingram Micro zijn ontwikkeld.

Na afloop van de Black Box Penetration Testing zal een gedetailleerd rapport worden gestuurd, met daarin het volgende:

- Managementsamenvatting: samenvatting van het doel van deze beoordeling, evenals een korte uitleg van de bedreigingen waaraan de organisatie wordt blootgesteld vanuit een zakelijk perspectief.



IngramMicro
FlexibleServices

INGRAM^{MICRO}

- **Bevindingen:** een gedetailleerde, technische uitleg van de bevindingen van de beoordeling, samen met stappen en bewijzen van de bevindingen.
- **Conclusie & aanbevelingen:** in dit hoofdstuk vindt u de laatste aanbevelingen en een samenvatting van de kwesties die tijdens de beveiligingsbeoordeling zijn gevonden.

Meer weten over onze Cyber Security Assessment services?

Neem contact op met het Ingram Micro Cyber Security Center of Excellence (COE) via cs-coe-weur@ingrammicro.com of met uw Account Manager.

IngramMicro
FlexibleServices

INGRAM^{MICRO}