SIEM/SOC Assessment

Werken uw Security Operations Centre (SOC) en uw Security Incident Event Management (SIEM)-oplossing zoals ze zouden moeten werken? Of mist uw detectie bedreigingen? Het SIEM/SOC-assessment test dit.

Het SIEM/SOC Assessment helpt u met het volgende:

Verifiëer uw detectie

Detecteert uw systeem daadwerkelijke bedreigingen? Wij helpen u dit te controleren.

Verbeter uw detectievermogen

Het assessment vermindert het aantal valse positieven zodat echte bedreigingen niet worden gemist.

Valideer claims van uw SOC

Werkt u met een externe SOC-leverancier? Dit assessment kan hun claims valideren.

Waarom het SIEM/SOC Assessment?

Als uw **Security Operations Centre (SOC)** u niet waarschuwt voor security events, weet u niet wat er aan de hand is. Dit vormt een risico. Het kan zijn dat er geen security events plaatsvinden. Het kan ook betekenen dat uw **Security Incident Event Management (SIEM)**-oplossing niet goed werkt. Hier kunnen allerlei technische redenen voor zijn, maar het resultaat is hetzelfde: het is alsof uw analisten geblinddoekt rondtasten in het duister.

Er is maar één manier om te controleren of uw detectie naar behoren werkt, en dat is door deze te testen. Onze Red Team-leden en pentesters weten hoe ze vijandig gedrag kunnen simuleren om uw SOC en SIEM-oplossing te testen. Het SIEM/SOC Assessment helpt u de juiste balans te vinden tussen sensitiviteit (het detecteren van elke mogelijke bedreiging) en specifiteit (het vermijden van foutieve meldingen). Wij kunnen helpen uw detectie te verbeteren.

Zo werkt het SIEM/SOC Assessment:

Detectie: ‘use cases’
Detectie gebruikt zogenoemde use cases om relevante afwijkingen te vinden. Een use case kan zijn: ‘waarschuw ons wanneer een grote hoeveelheid data buiten kantooruren wordt verstuurd.’ Deze regels zijn bedoeld om gedrag van aanvallers te detecteren.

Use cases uitproberen
Om uw detectiecapaciteiten te testen, voeren onze experts één voor één use cases uit. Hiervoor simuleren wij een security event in uw netwerk, meestal zonder de activiteit uit te voeren die normaal gesproken dat event zou veroorzaken. Bijvoorbeeld door attack signatures over het netwerk te sturen of door verdachte acties op servers uit te voeren.

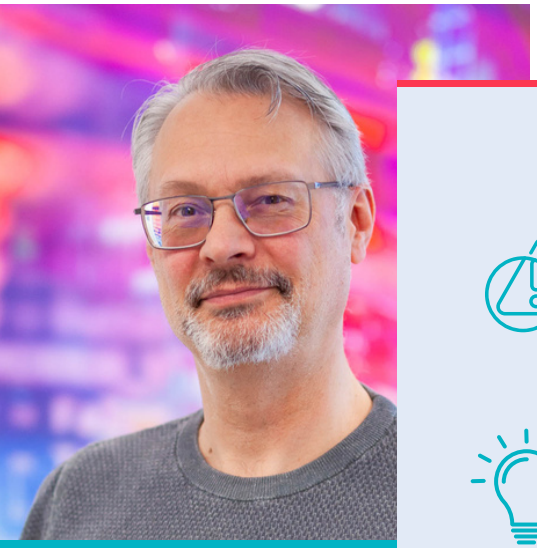
Worden de alerts geactiveerd?
Samen met uw team of het team van uw aanbieder controleren onze experts of de alerts op de juiste manier worden geactiveerd. Elke ontbrekende alert wordt in detail geanalyseerd en zo mogelijk stellen wij de hoofdoorzaak van het probleem vast.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.



Voorbeeld | SIEM/SOC Assessment

Welk probleem had de klant?
Een klant in de Nederlandse publieke sector gebruikte een externe detectiepartij. Zij namen contact met ons op omdat ze het gevoel hadden dat ze events en alerts misten.

Resultaat
Tijdens het SIEM/SOC Assessment kwamen wij erachter dat slechts 30% van de TTP's die onder de use cases vielen daadwerkelijk werden gedetecteerd, ook al werden de gerelateerde security events goed geregistreerd. Samen met het SOC-team konden wij veel van de problemen lokaliseren en oplossen.
De detectiecapaciteit van de klant verbeterde hierdoor drastisch.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com
+31 (0) 88 888 3100
secura.com