Incident Response PRO

De vraag is niet of uw organisatie getroffen zal worden door een cyberincident - de vraag is wanneer. Wij kunnen u helpen voorbereid te zijn op het ergste. Een Incident Response PRO abonnement garandeert u hulp in geval van een incident en helpt uw organisatie zich voor te bereiden.

Met Incident Response PRO kunt u:

Cyberincidenten oplossen

U weet wat te doen en wie te bellen als uw organisatie wordt getroffen door een cyberincident.

Ontdekken wat er is gebeurd

U krijgt hulp bij het uitzoeken wat er precies is gebeurd na een incident.

Voldoen aan wetgeving

U voldoet aan de vereisten voor incident response van regelgeving zoals NIS2 en DORA.

Waarom Incident Response PRO?

De kans dat uw organisatie getroffen wordt door een cyberaanval wordt groter. Daarom vraagt cybersecuritywetgeving, zoals NIS2 of DORA, de implementatie van een complete cyberincidentencyclus. Dit houdt in dat u **zich moet voorbereiden op incidenten**, goed moet kunnen **reageren op een aanval** en moet weten **wat u daarna moet doen**. U kunt dit vergelijken met brandveiligheid.
Branden blussen is natuurlijk nog steeds belangrijk.

Maar moderne brandweerkorpsen nemen ook preventieve maatregelen en evalueren hoe een brand is ontstaan. Hetzelfde geldt voor cyberincidenten. Wij kunnen u helpen bij de voorbereiding en afhandeling van cyberincidenten. Incident Response PRO garandeert u ook deskundige support in geval van nood, want aanvallers houden zich niet aan kantooruren. Laat ons u helpen bij de voorbereiding op en afhandeling van ernstige cyberincidenten.

Hoe Incident Response PRO werkt

Een Incident Response PRO abonnement heeft 2 belangrijke onderdelen:

Incident Response Retainer

Forensic en Incident Readiness Assessment

1. Incident Response Retainer

U bent gehackt - uw essentiële systemen zijn uitgevallen. Nu is het belangrijk om de schade te beperken en zo snel mogelijk weer aan de slag te gaan. U hebt onmiddellijk ondersteuning nodig om snel actie te kunnen ondernemen. Met deze retainer koopt u onze gegarandeerde beschikbaarheid in geval van een cyberincident. Het geeft u ook:

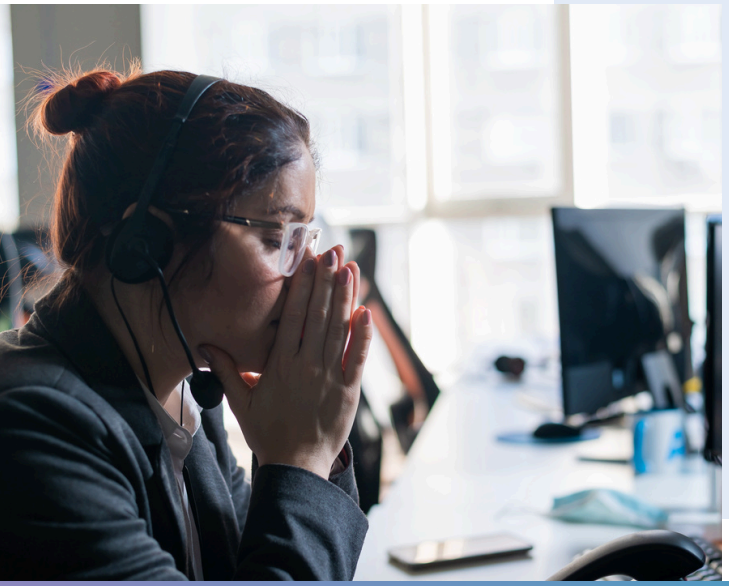
- Gegarandeerde responstijden
- On-site ondersteuning binnen 12 uur
- Korting op de kosten voor incident response.

2. Forensic en Incident Readiness Assessment

Het laatste waar u tijdens een incident achter wilt komen, is dat uw crisisteam niet weet wat te doen, of dat uw organisatie niet het juiste digitale bewijsmateriaal heeft bewaard.

Daarom helpen wij u zich voor te bereiden met onze **Forensic en Incident Response Assessment (FIRA)**. We beoordelen de huidige mogelijkheden van uw organisatie om incidenten te bestrijden, beleid, procedures, technische controles en het loggingbeleid.

Ook krijgt u aanbevelingen voor verbetering, gebaseerd op waarschijnlijkheid en impact. Het assessment resulteert in een schriftelijk rapport en is de perfecte onboarding voor Incident Response PRO.



Hulp bij een cyberincident

Bent u getroffen door een incident? Wij kunnen u helpen het op te lossen. We kunnen u ook helpen erachter te komen wat er is gebeurd - om te voorkomen dat het opnieuw gebeurt, of omdat u een juridische procedure start. We kunnen **post-mortems uitvoeren** op systemen en apparatuur.

Omdat we als particulier onderzoeksbureau geregistreerd staan bij het Ministerie van Justitie en Veiligheid, kunt u onze rapporten en documenten gebruiken in juidische procedures.

Omgaan met een cyberincident

Tijdens een cyberincident doorlopen we stappen om de gevolgen voor uw organisatie te beperken. Deze stappen zijn gebaseerd op het NIST-framework.

1. Triage

Wat is er gebeurd? U moet duidelijkheid hebben over het wat, wanneer, hoe en waar. Daarom voeren onze experts eerst een triage uit. De uitkomst bepaalt de reactie en de urgentie.

2. Containment

De meeste cyberincidenten worden veroorzaakt door malware - meer specifiek: ransomware. Tijdens een incident willen we voorkomen dat malware zich verspreidt, bijvoorbeeld door de toegang tot de getroffen systemen af te sluiten of te blokkeren.

3. Mitigation

Als een incident zich verder ontwikkelt, ontdekken we mogelijk nieuwe entry points die aanvallers kunnen gebruiken of hebben gebruikt. Het is belangrijk om deze gaten te dichten. Daarom repareren we vaak kwetsbaarheden, installeren we patches, configureren we systemen opnieuw en wijzigen we wachtwoorden.

4. Eradication

Vervolgens verwijderen we alle schadelijke software, tools voor toegang op afstand of code die het incident heeft veroorzaakt.

5. Recovery

Het is belangrijk om de bedrijfsactiviteiten zo snel mogelijk te hervatten. Stappen die we hiervoor kunnen nemen zijn onder andere het herstellen van back-ups, het herconfigureren van getroffen systemen en testen of deze goed werken.

Secura
A BUREAU VERITAS COMPANY

Aanvallers houden zich niet aan kantooruren. Deze dienst garandeert dat onze Incident Response-experts beschikbaar als u getroffen wordt door een cyberaanval.

NOODGEVAL? BEL +31 (0)88-8883107

Wat onze klanten zeggen

“De communicatie was to-the-point”

“We waren onder de indruk van Secura's snelle reactie tijdens ons onverwachte cyberincident. Hun communicatie was to the point. Wat we ook waardeerden was hoe de experts meedachten om ervoor te zorgen dat dit niet nog een keer gebeurt.”

Gerelateerde diensten

SIEM/SOC Assessment

Een incident betekent vaak dat uw detectie niet goed heeft gewerkt. Wij kunnen evalueren of uw SIEM- of SOC-oplossing correct werkt.

External Attack Surface Assessment

Hoe hebben aanvallers aanvankelijk toegang gekregen? Is er informatie over uw organisatie beschikbaar op het dark web waar u niets van weet? Het External Attack Surface Assessment helpt u hier achter te komen.

Cyber Crisis Oefeningen

Oefening baart kunst: leer omgaan met een cyberincident via interactieve workshops en gesimuleerde scenario's.

SAFE Awareness en Behavior Programma

Om een incident te voorkomen is het belangrijk dat uw werknemers zich bewust zijn van cybersecurity. Wij kunnen u helpen hun bewustzijn te vergroten met het SAFE Awareness en Behavior Programma.

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 | Incident Response PRO

Welk probleem had de klant?

Verschillende klanten namen contact met ons op toen een nieuw kritiek lek in Citrix werd ontdekt. Deze klanten vermoedden dat aanvallers mogelijk schadelijke activiteiten hadden uitgevoerd als gevolg van deze kwetsbaarheid.

Resultaat

We konden snel onze onderzoeken opschalen en uit verschillende bronnen informatie ophalen. Deze informatie toonde inderdaad activiteiten aan die werden uitgevoerd door aanvallers. We konden de klanten helpen maatregelen te nemen om de problemen op te lossen en de schade te beperken.

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