CTAC

Validate

Weten hoe weerbaar je écht bent

Cybersecurity

Cybersecurity draait niet alleen om maatregelen nemen. Het draait om weten of die maatregelen daadwerkelijk werken.

Met de Validate-diensten van Ctac toets, valideer en verbeter je continu de cyberweerbaarheid van je organisatie. We brengen kwetsbaarheden in kaart, simuleren realistische aanvallen en toetsen securitymaatregelen aan de praktijk. Zo krijg je inzicht in risico's, compliance en de effectiviteit van je beveiliging.

1 Continuous Automated Red Teaming (ART)

Continue inzicht in je weerbaarheid

Cyberaanvallers testen continu jouw omgeving. Waarom zou je jouw beveiliging dan slechts één keer per jaar testen? Met Continuous Automated Red Teaming valideren we doorlopend de effectiviteit van jouw securitymaatregelen. Via geautomatiseerde, realistische cyberaanvallen valideren we continu de effectiviteit van jouw securitymaatregelen en toetsen we endpoints, netwerken, Active Directory, Microsoft 365, internet-facing infrastructuur, cloud, malware- en ransomwarescenario's, phishing en interne aanvallen op een gecontroleerde en veilige manier, zonder verstoring van de bedrijfsvoering. Waar een traditionele penetratietest een momentopname biedt, geeft Automated Red Teaming continu inzicht in jouw actuele weerbaarheid. Je ziet welke aanvalspaden daadwerkelijk beschikbaar zijn, welke kwetsbaarheden misbruikbaar zijn en hoe effectief jouw detectie-, response- en beveiligingsmaatregelen functioneren. Zo verbeter je niet alleen je securitypositie, maar toon je ook aantoonbaar de effectiviteit van je beveiligingsmaatregelen aan.

Weet waar je staat

Je krijgt continu inzicht in de weerbaarheid van je IT-landschap en ontdekt kwetsbaarheden voordat aanvallers dat doen. Tegelijkertijd verbeter je de effectiviteit van detectie, response en security controls.

Ideaal voor organisaties die:

- Hun Security Operations verder willen professionaliseren.
- De effectiviteit van securitymaatregelen continu willen valideren.
- Aan willen tonen dat detectie- en responseprocessen effectief functioneren.
- NIS2-, DORA- en ISO 27001-verplichtingen willen ondersteunen.
- Continu inzicht willen in hun cyberweerbaarheid en aanvalspaden.

2 Vulnerability Scanning

Altijd zicht op kwetsbaarheden

Nieuwe kwetsbaarheden ontstaan dagelijks. De uitdaging is niet alleen om ze te vinden, maar vooral om te weten welke direct aandacht vragen. Met Vulnerability Scanning identificeren we bekende kwetsbaarheden binnen servers, endpoints, netwerkapparatuur, cloudomgevingen en webapplicaties. Door periodieke of continue scans krijg je inzicht in risico's en concrete aanbevelingen voor herstel.

Weet waar je staat

Je krijgt grip op kwetsbaarheden voordat ze misbruikt worden. Daardoor verbeter je patchmanagement, verlaag je risico's en houd je controle over een steeds veranderend dreigingslandschap.

Ideaal voor organisaties die:

- Compliance-eisen aantoonbaar willen ondersteunen
- Structureel inzicht willen in kwetsbaarheden
- Cyberrisico's actief willen verminderen
- Patchprocessen willen verbeteren

3

Audit

Aantoonbaar in control

Steeds vaker vragen klanten, auditors en toezichthouders om bewijs dat cybersecurity goed is ingericht. Met onze auditdiensten toetsen we governance, processen en securitymaatregelen aan standaarden zoals NIS2, BIOS, ISO 27001 en ISO42001. We brengen sterke punten, verbeterkansen en compliance-risico's in kaart en geven duidelijke aanbevelingen om verder te groeien in volwassenheid. Geen vinkjes zetten, maar inzicht creëren.

Weet waar je staat

Je weet waar je staat ten opzichte van de relevante normen en je kunt onderbouwd aantonen dat cybersecurity dusdanig structureel aandacht krijgt binnen de organisatie.

Ideaal voor organisaties die:

- Governance en risicobeheersing willen versterken
- Compliance inzichtelijk willen maken
- Certificeringstrajecten ondersteunen
- Voorbereid willen zijn op audits

4

Pentesting

Kijk door de ogen van een aanvaller

Hoe veilig is jouw omgeving écht? Met een penetratietest simuleren onze securityspecialisten gerichte aanvallen op applicaties, infrastructuur, API's, cloudomgevingen of netwerken. Daarbij zoeken we actief naar exploiteerbare kwetsbaarheden en toetsen we de effectiviteit van bestaande beveiligingsmaatregelen. Een pentest geeft een scherp beeld van de risico's op een specifiek moment.

Pentest versus Continuous Automated Red Teaming

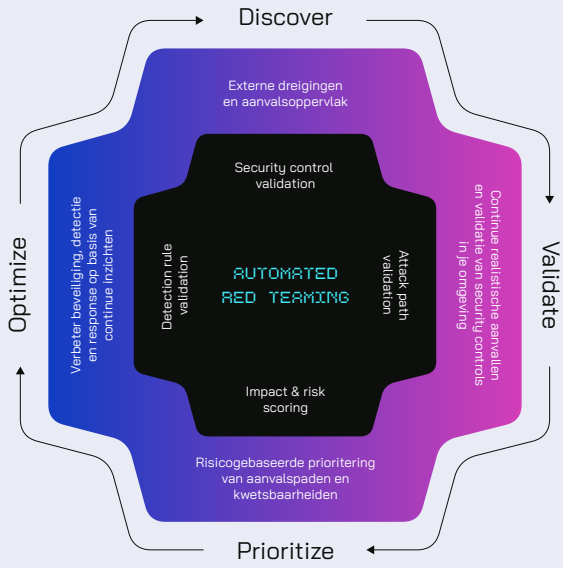
Een pentest is een momentopname: een foto. Continuous Automated Red Teaming is een doorlopende validatie: een film. Beide leveren waardevolle inzichten, maar dienen een ander doel. Waar een pentest diepgaand onderzoek doet naar een specifieke omgeving, biedt Continuous Automated Red Teaming continu inzicht in de veranderende weerbaarheid van het totale landschap.

Weet waar je staat

Je krijgt grip op kwetsbaarheden voordat ze misbruikt worden. Daardoor verbeter je patchmanagement, verlaag je risico's en houd je controle over een steeds veranderend dreigingslandschap.

Ideaal voor organisaties die:

- Compliance-eisen aantoonbaar willen ondersteunen
- Structureel inzicht willen in kwetsbaarheden
- Cyberrisico's actief willen verminderen
- Patchprocessen willen verbeteren



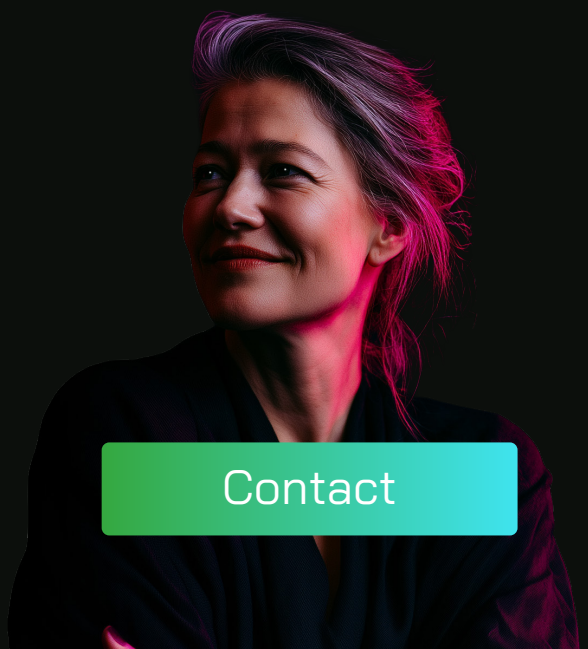
Red teaming

Valideer jouw cyberweerbaarheid met realistische aanvallen op netwerken, applicaties, identiteiten en endpoints.

Set objectives → Gather intelligence → Simulate attack → Report findings

Business driven security.

Getest.
Gevalideerd.
Aantoonbaar weerbaar.



Grip op cybersecurity begint met de juiste validatie

Of je nu aan het begin staat van je securityreis of je cybersecurity verder wilt professionaliseren: Ctac helpt je om de juiste keuzes te maken, risico's te beheersen en aantoonbaar in control te zijn.

Contact