

|                     | Type test                                           | Kenmerk                                                                                                                                                | Doel / aanpak                                                                                                                                                         | Scope                       | NIST-functies                       | Minimale volwassenheid SURFaudit toetsingskader | Indicatie verloop test     | Aanbevolen ervaring en capaciteit                                                                                                                                                                                                                                                      | Hulpmiddelen                                                                                                                                     |
|---------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-------------------------------------|-------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Basisniveau         | Vulnerability scanning (VS)                         | Geautomatiseerde scans op technische kwetsbaarheden                                                                                                    | In de breedte van de techniek opsporen van bekende technische kwetsbaarheden                                                                                          | Techniek                    | Identify, protect                   | Niveau 1 of hoger                               | 1-2 dagen                  | <ul style="list-style-type: none"> <li>Geen ervaring vereist</li> <li>Capaciteit nodig om uitkomsten op te volgen</li> </ul>                                                                                                                                                           | <br><a href="#">Handreiking kwetsbaarheidsscan</a>            |
|                     | Deelname Coordinated Vulnerability Disclosure (CVD) | Kaders en informatie publiceren om vrijwilligers te laten zoeken naar kwetsbaarheden                                                                   | Gelijk aan vulnerability scanning, maar een focus op het open staan voor meldingen van vrijwilligers                                                                  | Techniek                    | Identify, protect                   | Niveau 1 of hoger                               | Voortdurend                | <ul style="list-style-type: none"> <li>Gelijk aan vulnerability scanning</li> </ul>                                                                                                                                                                                                    | <br><a href="#">HALON, handreiking CVD</a>                    |
|                     | Cybercrisis of -incident tabletop oefening          | Korte oefening waarbij een kleine groep mensen een scenario doorloopt waarbij mondeling de ontwikkelingen van het incident of crisis worden beschreven | Processen en samenwerking tijdens een groot incident of cybercrisis testen en verbeteren                                                                              | Mensen, processen           | Respond                             | Niveau 1 of hoger                               | 2 uur (uitvoering)         | <ul style="list-style-type: none"> <li>Geen ervaring vereist</li> <li>Enige incident- en crisismanagementprocessen op papier</li> </ul>                                                                                                                                                | <br><a href="#">NOZON, Tabletop oefeningen handleiding</a>    |
|                     | Penetration testing (pentest)                       | Cyberaanval “boven de radar” uitgevoerd met tools en handmatige acties                                                                                 | Gericht op 1 of beperkt aantal systemen. Uitputtend kwetsbaarheden opsporen en deze gebruiken om binnen te komen                                                      | Techniek                    | Identify, protect, detect           | Niveau 1 of hoger                               | 1-2 weken                  | <ul style="list-style-type: none"> <li>Vulnerability scanning uitgevoerd en bevindingen (grotendeels) opgevolgd</li> </ul>                                                                                                                                                             | <br><a href="#">Whitepaper pentesten</a>                    |
| Geavanceerde testen | Purple teaming (PT)                                 | Cyberaanval uitgevoerd door een ‘red team’ (ingehuurde ethische hackers) in samenwerking met het ‘blue team’ (het eigen CERT of SOC)                   | Identificeren van aanvalspaden en het verbeteren van de detectie en response effectiviteit van het blue team om daarmee de cyber weerbaarheid te verhogen             | Techniek, mensen, processen | Identify, protect, detect, respond  | Niveau 2 of hoger                               | 1-10 weken                 | <ul style="list-style-type: none"> <li>Vulnerability scanning en evt. pentests uitgevoerd en bevindingen (grotendeels) opgevolgd</li> <li>Monitoring en detectie- capaciteit ingericht en operationeel</li> </ul>                                                                      | <br><a href="#">Purple teaming guide (TIBER)</a>            |
|                     | Simulatie cybercrisisoefening                       | Oefening waarbij de gehele escalatie van een crisis wordt getest en men daadwerkelijke acties kan uitvoeren                                            | Testen en verbeteren samenwerking op alle niveaus binnen en tussen organisaties om voor te bereiden op een cybercrisis                                                | Techniek, mensen, processen | Identify, protect, respond, recover | Niveau 2 of hoger                               | 1 tot 3 dagen (uitvoering) | <ul style="list-style-type: none"> <li>Tabletop oefening gedaan en verbeterpunten (grotendeels) opgevolgd</li> <li>Crisismanagement proces op papier</li> </ul>                                                                                                                        | <br><a href="#">OZON, Whitepaper Cyber Crisis Exercises</a> |
|                     | Red teaming (RT) / Advanced red teaming (ART)       | Cyberaanval “onder de radar” gebaseerd op generieke dreigingsinformatie                                                                                | Realistisch simuleren van een specifieke actor om te kijken in hoeverre de kroonjuwelen hier tegen beschermd zijn en de organisatie als geheel hiervan te laten leren | Techniek, mensen, processen | Identify, protect, detect, respond  | Niveau 2 of hoger                               | 7–14 weken                 | <ul style="list-style-type: none"> <li>VS en pentest uitgevoerd en bevindingen (grotendeels) opgevolgd</li> <li>Monitoring en detectie- capaciteit ingericht en operationeel</li> <li>Genoeg capaciteit om een white team te kunnen leveren die los staan van het blue team</li> </ul> | <br><a href="#">SURF raamwerk ART</a>                       |