Leerlijn	Software Security	
Kenmerken	**Code:** **Studiepunten:** **Aantal cursussen:** **Competentiegebied:** **Aantal bijeenkomsten:** **Toetsvorm:**	SWS 30 EC 6 24 Werkstuk
Studiegidsbeschrijving	n.v.t	
Beschrijving leerlijn	Software is in onze wereld niet meer weg te denken. Alle apparaten die we gebruiken, van computer tot de slimme thermostaat en koelkast, bevatten software. Dit maakt het voor cyber criminelen uitermate aantrekkelijk om misbruik te maken van deze software. In deze leerlijn kijken we naar software vanuit een security oogpunt; hoe kan er misbruik van worden gemaakt om de moderne wereld te beïnvloeden. De leerlijn is opgebouwd uit 2 samenhangende groepen cursussen. De eerst groep kijkt naar applicatie en data security. Wat zijn aspecten waarop applicaties beveiligd moeten worden en onderzoek op welke vlakken het hierbij fout gaat. Ook wordt er hierin gekeken naar hoe data wordt opgeslagen en op welke wijze dit op een veilige manier kan, door bijvoorbeeld encryptie. Veel software is eenvoudig te onderzoeken. Zo hebben de meeste applicaties een vorm van interface waarmee we de uitvoering kunnen manipuleren. Maar wat als dit niet kan? Denk bijvoorbeeld aan een malware zoals ransomware, software gemaakt door cybercriminelen specifiek om bestanden te versleutelen en losgeld te eisen. Dit soort software kan enkel bestudeerd worden door te kijken naar het binaire product door middel van Reverse Engineering, de 2de groep cursussen. Reverse Engineering is dan ook het proces waarbij het ontwerp en de interne werking van software bestudeerd wordt. Dit kan met kwaadaardige software zoals malware, maar ook met mobiele applicaties die je regulier op jouw telefoon zou draaien. Je leert programma's te bestuderen en de werking ervan in kaart te brengen om, bijvoorbeeld, de effecten van een ransomware ongedaan te maken. Ter ondersteuning van deze leerlijn is het Lab beschikbaar. Het lab bevat 125+ kwetsbare machines waarop verschillende applicatie en data security Tools, Techniques and Procedures (TTPs) kunnen worden geoefend om een praktisch begrip te krijgen van de werkelijke gevolgen van beveiligingszwakheden. Ook bevat het Lab verschillende uitdagingen op het gebied van Reverse Engineering.	

Cursussen	Reverse Engineering 1. Reverse Engineering (5 EC) 2. Mobile and IoT Application Analysis (5 EC) 3. Malware Analysis (5 EC) Application and Data Security 4. Web Application Security(5 EC) 5. Modern API Security (5 EC) 6. Exploit Development (5 EC)

Cursus	**Reverse Engineering**
Leeruitkomst	De student kan systematisch en volgens geldende richtlijnen analyses uitvoeren op onbekende software en de werking ervan in kaart brengen.
Toelichting cursus	Reverse Engineering analyseert en onderzoekt een software object om de interne werking en het ontwerp van het object zichtbaar te maken. De reverse engineer draagt in verschillende vakgebieden bij aan het begrip over en de impact van mogelijk kwaadaardige software en kan verschillende andere cyber security vakgebieden ondersteunen met waardevolle informatie die enkel door technische onderzoek mogelijk zijn.
Prestatie indicatoren	• De student heeft inzicht in de werking van gecompileerde software objecten • De student analyseert de werking van onbekende software systemen op basis van level applicatie code (assembly) • De student toont aan het ontwerp van een software systeem op basis van de werking en de low level applicatie code terug te kunnen redeneren
Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Cursus	**Mobile and IoT Application Analysis**
Leeruitkomst	De student kan verschillende architecturen van mobiele en IoT apparaten onderzoeken, emuleren en decompileren om de werking ervan te analyseren met als doel kwetsbaarheden zichtbaar te maken. De student kan zijn/haar bevindingen op logische wijze rapporteren.

Toelichting cursus	Het digitale landschap wordt steeds breder en mobieler. Zo draagt iedereen een mobiel en worden huizen en bedrijven voorzien van slimme Internet of things (IoT) apparaten. Deze apparaten draaien allemaal software die normaliter niet inzichtelijk zijn voor de eindgebruiker. In deze cursus wordt de wereld van Mobiele applicaties en IoT software opengebroken. Mobiele applicaties spelen een grote rol in ons dagelijks leven en apps krijgen steeds meer toegang tot onze data. Hoe verwerken deze apps de data en wat wordt er allemaal verzameld? Die vragen kunnen alleen beantwoord worden door naar de broncode van de applicaties te kijken en die is niet zomaar beschikbaar. Door technieken en procedures toe te passen om gecompileerde bestanden om te zetten naar leesbare code wordt er inzicht verkregen in de werking van deze applicaties. Voor IoT apparaten geldt hetzelfde; als samenleving geven we veel vertrouwen in deze apparaten, maar is dat wel terecht? Door te kijken naar de software die draait op een IoT apparaat, hoe het communiceert met de buitenwereld en welke gegevens het deelt kan een beeld worden gemaakt wat de betrouwbaarheid van IoT in kaart brengt. De reverse engineering technieken worden toegepast om de werking van de apparaten in kaart te brengen en eventuele kwetsbaarheden zichtbaar te maken.
Prestatie indicatoren	• De student toont aan inzicht te hebben in de verschillende software formaten voor mobiele applicaties en IoT apparaten. • De student is in staat mobiele applicaties om te zetten naar leesbare broncode door gebruik te maken van geldende methodieken en richtlijnen. • De student onderzoekt de werking van mobiele applicaties om deze te beoordelen op kwaadaardig gedrag • De student beschrijft en rapporteert over de bevindingen
Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Cursus	**Malware Analysis**
Leeruitkomst	De student is in staat passende technieken toe te passen om kwaadaardige software op een veilige wijze te analyseren en de werking ervan te beschrijven.

Toelichting cursus	Cyber criminelen zetten kwaadaardige software, malware, in om mensen en bedrijven te saboteren, chanteren en te bestelen. De meeste bekende vorm van malware is Ransomware, waarbij bestanden op een computersysteem gegijzeld worden in ruil voor losgeld. Tijdens de cursus Malware analysis leert de student op een veilige manier kwaadaardige software te analyseren, technieken die ingezet worden om analyse te voorkomen te omzeilen en de werking ervan dermate te analyseren dat een “vaccin” gemaakt kan worden.
Prestatie indicatoren	• De student is in staat een veilige analyseomgeving op te zetten waarin malware geanalyseerd kan worden • De student herkent en kan tegenmaatregelen formuleren om anti-analyse software te omzeilen • De student kan encryptie methodieken herkennen en analyseren met als doel decryptie methodieken te beschrijven
Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Cursus	**Web Application Security**
Leeruitkomst	De student kan systematisch webapplicaties onderzoeken op de aanwezigheid van kwetsbaarheden. Tevens toont de student aan de impact van deze kwetsbaarheden in te kunnen schatten en passende tegenmaatregelen formuleren en gemaakte keuzes onderbouwen.
Toelichting cursus	Het internet en internet applicaties zijn niet meer weg te denken uit het dagelijks leven. Veel van deze applicaties zijn Web Applicaties. In deze cursus worden de kwetsbaarheden van web applicaties in detail onderzocht en leert de student zelfstandig kwetsbaarheden in web applicaties te vinden. De onderliggende oorzaak van de kwetsbaarheden wordt uitgediept en de mogelijke tegenmaatregelen in kaart gebracht.
Prestatie indicatoren	• De student toont inzicht in de werking van actuele web applicatie kwetsbaarheden • De student kan web applicatie kwetsbaarheden identificeren en de oorzaak analyseren • De student kan een oordeel vormen over de gevolgen van een kwetsbaarheid
Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Cursus	Modern API Security
Leeruitkomst	De student heeft kennis van verschillende API technieken en is in staat APIs van diverse applicaties te onderzoeken op aanwezigheid van kwetsbaarheden. Van mogelijke kwetsbaarheden kan de student de werking en impact beschrijven.
Toelichting cursus	APIs zijn een complex en uitgebreid onderdeel geworden van web applicaties, mobiele applicaties en IoT apparaten. Het is hierdoor ook een compleet zelfstandig Attack Surface geworden. In deze cursus leert de student moderne API technieken te onderzoeken die gebruikt worden in applicaties om data uit te wisselen.
Prestatie indicatoren	• De student toont inzicht te hebben in de werking en verschillende API technieken • De student onderzoekt het gebruik en misbruik van API technieken in een variëteit van applicaties. • De student kan een oordeel vormen over de implementatie en het gebruik van een API door een applicatie
Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Cursus	Exploit Development
Leeruitkomst	De student kan technieken en methoden ontwikkelen waarmee gevonden kwetsbaarheden worden omgezet in toegang tot computersystemen. Tevens toont de student daadwerkelijke impact van een kwetsbaarheid aan door middel van een Proof of Concept.
Toelichting cursus	In de andere cursussen van de Software Security leerlijn worden op verschillende wijzen software geanalyseerd en kwetsbaarheden blootgelegd. In deze cursus worden de gevonden kwetsbaarheden uitgebuit door het creëren van een methodiek om deze te gebruiken, het maken van een zogeheten exploit. Van het ontwikkelen van een Binary Exploit voor software systemen waar geheugen kwetsbaarheden aanwezig zijn, tot het uitbuiten van een SQL Injection. Een cyber security onderzoeker toont de daadwerkelijke impact van een kwetsbaarheid aan door middel van een Proof of Concept (bewijs van werking). Een PoC stelt de maker van de software ook in staat te toetsen of de gevonden kwetsbaarheid daadwerkelijk is verholpen.
Prestatie indicatoren	• De student is in staat een methodiek te bedenken waarmee een kwetsbaarheid uitgebuit kan worden • De student combineert kennis van kwetsbaarheden en software systemen om een methodiek te formuleren • De student ontwikkelt een Proof of Concept applicatie om de kwetsbaarheid uit te buiten

Omvang	5 EC
Literatuur (BUKU) of andere bronnen	

Lesdag	Cursus	Lesdagvoorbereiding

Toetsing
Voer een security assessment uit op een IoT apparaat en levert een rapportage in. *- RE: Emulation / Firmware Extraction* *- RE: binary exploitation* *- ADS: Web Application analysis* *- ADS: Data security analysis* *- Reporting* De student onderzoekt een IoT apparaat, zoals een router of een product zoals een IP camera. Er wordt een gedetailleerde analyse gedaan van de componenten die zich in het product bevinden. Elk component wordt onderzocht op zwakheden. - Binary components worden door middel van reverse engineering onderzocht - Mobiele applicaties worden gedecompileerd en onderzocht - Er wordt onderzocht hoe data wordt verzameld en gedeeld - Wat voor encryptie methoden worden gebruikt - De applicaties die onderdeel zijn van het product worden onderzocht op kwetsbaarheden. Bijvoorbeeld; een web interface op een IoT apparaat. De student schrijft een rapportage over het product, het ontwerp, de onderliggende componenten, de datastromen en identificeert eventuele kwetsbaarheden.