კიბერუსაფრთხოების საფუძვლები

ლექტორი

მაია სვანიძე

კურსის დრო

26 შეხვედრა (52 საათი)

სასწავლო კურსის მიზნები

კურსის მიზანია კურსდამთავრებულებს შეექმნას წარმოდგენა კიბერუსაფრთხოების სფეროზე, საფრთხეების განსაზღვრის მეთოდებზე და ინსტრუმენტებზე, შეისწავლოს კიბერუსაფრთხოების სფეროს ტენდენციები და მიმართულებები.

სასწავლო კურსის შინაარსი

ლექცია 1: კიბერუსაფრთხოების საფუძვლები

- თავდასხმითი უსაფრთხოება და თავდაცვითი უსაფრთხოება
- კარიერა კიბერუსაფრთხოებაში - როლები და მოვალეობები
- ინფორმაციული უსაფრთხოების პრინციპები CIA ტრიადა
- მავნე პროგრამული უზრუნველყოფის ტიპები
- Quiz #1

ლექცია 2: LINUX სისტემის საფუძვლები

- Linux-ის სტრუქტურა
- Shell-ის გამოყენება
- ლინუქსის ოპერაციული სისტემის ნავიგაცია
- ფაილებთან და დირექტორიებთან მუშაობა
- Linux-ის ადმინისტრირება
- სერვისების მენეჯმენტი
- უფლებების და წვდომების მართვა
- Quiz #2

ლექცია 3: WINDOWS სისტემის საფუძვლები

- Windows ოპერაციული სისტემის სტრუქტურა
- Windows ფაილური სისტემა
- ნებართვების მართვა
- Windows სერვისები
- პროცესები Windows-ში
- Windows უსაფრთხოება
- Microsoft Management Console (MMC)
- Windows ქვესისტემა Linux-ისთვის (WSL)
- Quiz #3

ლექცია 4: ქსელის საფუძვლები

- ქსელის სტრუქტურა
- ტოპოლოგიების გამოყენება
- ინტერნეტ კომუნიკაციის მოდელები და კონცეფციები
- განსხვავება OSI მოდელსა და TCP/IP-ს შორის
- IPv4/IPv6 სტანდარტი სხვადასხვა ქსელში
- Quiz #4

ლექცია 5: Active Directory საფუძვლები

- ფიზიკური Active Directory
- The Forest
- Users + Groups
- Trusts + Policies
- Active Directory Domain Services და აუთენტიფიკაცია
- AD ქლაუდში
- Quiz #5

ლექცია 6: ვირტუალიცაზიის საფუძვლები (Virtualization Fundamentals)

- ვირტუალიზაციის ტიპები
- ვირტუალიზაციის პლატფორმები
- ჰიპერვიზორების ტიპები
- Oracle VM VirtualBox ინსტრუმენტის გამოყენება
- Quiz #6

ლექცია 7: ქლაუდ ტექნოლოგიების და კონტეინერიზაციის საფუძვლები (Cloud/Container Fundamentals)

- Cloud Computing-ის ცნება
- Cloud Deployment მოდელები
- ძირითადი Cloud პლატფორმები
- ძირითადი Cloud კონცეფციები
- კონტეინერიზაციის ცნება
- კონტეინერიზებული გარემოს სტრუქტურა
- Quiz #7

ლექცია 8: OSINT მოდელი

- გარემოს მომზადება და წყაროების მოძიება
- ღია მონაცემთა ბაზები
- DNS ჩანაწერის ანალიზი
- ონლაინ ფორუმები, dark web
- Quiz #8

ლექცია 9: კრიპტოგრაფია

- შესავალი კრიპტოლოგიაში
- კრიპტოგრაფიის სახეები
- სიმეტრიული ალგორითმები
- ისტორიული შიფრები
- კრიპტოგრაფიის მიზნები
- შემთხვევითი რიცხვების გენერატორები
- Base64 კოდირება/გაშიფვრა
- ჰეშის ფუნქციები
- ციფრული ხელმოწერები
- SSL/TLS პროტოკოლი
- კრიპტოგრაფიული შეტევები
- Quiz #9

ლექცია 10: მოწყვლადობების მართვა

- მოწყვლადობების ტიპები
- SANS მოწყვლადობების მართვის მოდელი
- მოწყვლადობების შეფასების სისტემები (CVSS & VPR)
- მოწყვლადობების მონაცემთა ბაზები
- Quiz #10

ლექცია 11: საბოლოო წერტილების დაცვა (ENDPOINT SECURITY)

- საბოლოო წერტილების დაცვის მექანიზმები
- EPP, EDR, XDR ინსტრუმენტები
- ინციდენტების მართვა და გამოძიება
- საბოლოო წერტილების მოწყვლადობის გამოყენების მაგალითები
- Quiz #11

ლექცია 12: ქსელის დაცვა (NETWORK SECURITY)

- უსაფრთხო ქსელური წვდომის განსაზღვრა
- ქსელის მიკროსეგმენტაცია
- Zero-trust არქიტექტურა
- ქსელური უსაფრთხოების მოწყობილობები: Firewalls, IPS, NAC
- Quiz #12

ლექცია 13: შუალედური გამოცდა

ლექცია 14: ვებ აპლიკაციების დაცვა (WEB APPLICATION SECURITY)

- OWASP ტოპ-10

- ვებ აპლიკაციების მუშაობის პრინციპი
- SQL ინექციის შეტევების გამოვლენა
- ჯვარედინი საიტის სკრიპტის (XSS) შეტევების გამოვლენა
- საბრძანებო ინექციის შეტევების გამოვლენა
- დაუცველი პირდაპირი ობიექტის მითითების (IDOR) შეტევის გამოვლენა
- RFI და LFI შეტევის გამოვლენა
- Quiz #13

ლექცია 15: LINUX FOR BLUE TEAM

- ძირითადი ტერმინალის ბრძანებები
- ნებართვების მენეჯმენტი
- მომხმარებლის მენეჯმენტი და ჯგუფები
- არქივის ფაილის ფორმატები
- პროცესის მართვა
- ქსელის მენეჯმენტი
- პაკეტის მენეჯმენტი
- სერვისის მენეჯმენტი
- დაგეგმილი ამოცანები
- Quiz #14

ლექცია 16: CYBER THREAT INTELLIGENCE ცნება

- Cyber Threat Intelligence (CTI) კონცეფცია
- CTI სასიცოცხლო ციკლი
- თავდასხმის ზედაპირის განსაზღვრა
- საფრთხის ინდიკატორების შეგროვება
- მონაცემთა ინტერპრეტაცია
- Quiz #15

ლექცია 17: ფიშინგი და სოციალური ინჟინერია

- სოციალური ინჟინერია, როგორც შეტევის ვექტორი
- ფიშინგის ტიპები
- მეილის header და body ანალიზი
- ფიშინგ მეილების და საიტების მაგალითები
- Quiz #16

ლექცია 18: LOG-ის მართვა და SIEM სისტემები

- SIEM სისტემის დანიშნულების განსაზღვრა
- Log-ის შეგროვების მეთოდები
- Log-ის აგრეგაცია და პარსინგი
- გაფრთხილების სისტემის ქასთომიზაცია

- Quiz #17

ლექცია 19: BREACH & ATTACK SIMULATION საფუძვლები

- საფრთხიდან გამომდინარე დაცვის კონცეფცია
- BAS ინსტრუმეტების დანერგვის ვარიანტები
- სიმულაციური ტესტების სახეობები
- BAS ტესტირების გამჭვირვალობის მიდგომები
- Quiz #18

ლექცია 20: MITRE ATT&CK ფრეიმვორქის გამოყენების საფუძვლები

- რა არის MITRE ATT&CK ფრეიმვორქი
- MITRE ATT&CK-ის გამოყენება
- შემტევის ემულაცია და Read Teaming -ის ცნება
- კომპანიის პერიმეტრის დაცვა და Blue Teaming-ის ცნება
- Purple Teaming-ის კონცეფცია
- Quiz #19

ლექცია 21: MITRE ATT&CK უსაფრთხოების კონტროლების შეფასების გეგმა

- უსაფრთხოების ინსტრუმენტების შეფასების გეგმის შედგენა
- კითხვების განსაზღვრა
- ტესტირების მიზნების დასახვა
- ტესტირების სცენარის შემუშავება
- ტესტირების განრიგის შედგენა
- შედეგების შეფასება
- Quiz #20

ლექცია 22: პროექტი MITRE ATT&CK SECURITY STACK MAPPINGS: AZURE/AWS

- Security Stack Mappings პროექტის არსი და დანიშნულება
- Azure და AWS პლატფორმებისთვის არსებული საფრთხეების შეფასება
- Azure და AWS პლატფორმების არსებული დაცვის მექანიზმების შეფასება
- რისკების და უსაფრთხოების მექანიზმების ATT&CK ნავიგატორზე დატანა
- Quiz #21

ლექცია 23: პროექტი: MAPPING MITRE ATT&CK TO CVE FOR IMPACT

- რა არის გავრცელებული მოწყვლადობა და ექსპოზიცია (CVE) ?
- Mitre Attck&CK Navigator-ზე CVE-ს დატანის მეთოდოლოგია
- მოწყვლადობების გამოყენების მეთოდები და შეტევის ტექნიკები
- არსებული შაბლონების გამოყენება
- Quiz #22

ლექცია 24: პროექტი: ATTACK FLOW -შეტევის მოდელირება და თანმიმდევრობა

- Attack Flow ობიექტების მიმოხილვა

- Attack Flows ინსტრუმენტების გამოყენება;
- Attack Flows შეტევების ბიბლიოთეკის გამოყენება;
- არსებული Attack Flows გარჩევა და ანალიზი
- ახალი Attack Flows-ს შექმნა
- Quiz #23

ლექცია 25: პროექტი: TOP ATT&CK TECHNIQUES

- Top ATT&CK Techniques ინსტრუმენტის მიმოხილვა
- შეფასების კრიტერიუმების განსაზღვრა
- ინსტრუმენტის პრაქტიკული გამოყების მეთოდები
- მიღებული შედეგის ანალიზი
- Quiz #24

ლექცია 26: ფინალური პროექტის განხილვა

სასწავლო კურსის შედეგები

კურსის მსმენელებს ეცოდინებათ და შეძლებენ:

- განსაზღვრონ და შეაფასონ შესაძლო კიბერ საფრთხეები და რისკები;
- გამოიყენონ კიბერუსაფრთხოების საბაზისო ინსტრუმენტები;
- მოიძიონ და გამოიყენონ ინფორმაციის ღია წყაროები;
- უზრუნველყონ საბოლოო მომხმარებლის მოწყობილობის უსაფრთხოება;
- განსაზღვრონ უსაფრთხოების ჯგუფური პოლიტიკები.

სასწავლო კურსის მოთხოვნები

- კურსის გასავლელად, სტუდენტს უნდა შეეძლოს კომპიუტერის გამოყენება საბაზისო დონეზე;
- სტუდენტი უნდა ფლობდეს ინგლისურ ენას იმ დონეზე, რომ შეძლოს ინგლისურენოვანი მასალის წაკითხვა და გარჩევა.

სასწავლო კურსის შეფასება

კურსის დასრულების შემდეგ გაიცემა ორენოვანი სერტიფიკატი:

- კურსის წარმატებით დასრულების სერტიფიკატის მისაღებად სტუდენტმა უნდა მოაგროვოს მინიმუმ 70 ქულა.
- კურსის მინიმუმ 90 ქულაზე დასრულების შემთხვევაში, სტუდენტი ლექტორისგან მიიღებს წერილობით დახასიათებას/რეკომენდაციას.

ლექტორის შესახებ

- მაიკო სვანიძეს აქვს 9 წლიანი პრაქტიკული გამოცდილება ინფორმაციული ტექნოლოგიების სფეროში, ბოლო ორი წელი უშუალოდ კიბერუსაფრთხოების მიმართულებით კიბერსუფრთხოების ინჟინრის პოზიციაზე;
- მას აქვს მსოფლიოს წამყვანი მწარმოებლების მიერ გაცემული სერტიფიკატები: AttackIQ Partner Academy certified professional, Proofpoint Certified Ransomware Specialist, Logsign SIEM/SOAR Administrator, Bitdefender Certified MSP Specialist, Bitdefender Certified Technical Specialist, ObserveIT InsiderThreat Management Certified Administrator, Proofpoint Accredited Channel Sales Engineer(PACSE), Tenable Certified Sales Engineer-VM, Tenable Certified Pre-Sales Integrator- Tenable.io, VTSP - CB (Carbon Black Endpoint Protection 2020);
- 2021 წელის დეკემბერში მაიკო გახდა საერთაშორისო უსაფრთხოების ბრენდის AttackIQ-ს Defender of the month ნომინაციის გამარჯვებული, ხოლო 2022 წლის მაისში AttackIQ Informed Defenders Champion სტატუსი მოიპოვა;
- 2020 წლიდან დღესმდე მაიკო არის მოწვეული სპეციალისტი ბიზნესისა და ტექნოლოგიების უნივერსიტეტში, არის ციფრული ტექნოლოგიების პრინციპების კურსის ლექტორი;
- ამჟამად არის კიბერ თავდაცვის მიმართულების ხელმძღვანელი 42digital-ში.