ISSP

ISSP Training Center

კიბერჰიგიენის უნარების განვითარება

www.issp.com

ნებისმიერი ორგანიზაციის კიბერუსაფრთხოების სისტემაში ყველაზე სუსტი ელემენტი საბოლოო მომხმარებლები არიან. კიბერუსაფრთხოების სისტემა უნდა მუშაობდეს თითოეული მომხმარებლის რისკების გათვალისწინებით და სიმეტრიულად პასუხობდეს შესაბამის საფრთხეებს. ISSP გთავაზობთ კიბერუსაფრთხოების სფეროში და კიბერჰიგიენის უნარების განვითარებაში თანამშრომელთა ცოდნის მაღლების უნიკალურ, კომპლექსურ პროგრამას.

რა არის ახალი?

პროგრამის პირველი ეტაპის შედეგები საშუალებას იძლევა გაირკვეს ცალკეული თანამშრომლების, მთელი განყოფილებების და ორგანიზაციის რისკების ზონები. შედეგები ორგანიზაციას აძლევს შესაძლებლობას მართოს კიბერსაფრთხეები, როგორც ორგანიზაციის, ასევე ცალკეული თანამშრომლების კონტექსტში. ეს მიდგომა, თავის მხრივ, ხელს უწყობს უსაფრთხოების პოლიტიკის ეფექტურ განხორციელებას და კიბერსაფრთხეების დასაძლევად ინვესტიციების გამოყოფისათვის ინფორმირებული გადაწყვეტილებების მიღებას.

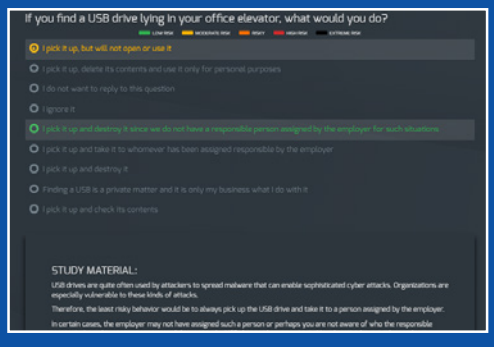
რა არის უნიკალური?

კიბერუსაფრთხოების სფეროში თანამშრომელთა თვითცნობიერების ამაღლების ყოვლისმომცველი პროგრამა მრავალი კომპონენტისგან შედგება.

ხოლო, თანამშრომელთა ნარჩენი კიბერ-რისკებს ცოდნის გადაცემის და შეფასების ძირითადი ტექნიკური პლატფორმა შემუშავებული იქნა 2015-2017 წლებში ესტონეთის და ლატვიის თავდაცვის სამინისტროების მიერ განხორციელებული პროექტის საფუძველზე, მიზნობრივი კიბერშეტევების საპასუხოდ. Cybexer-ის ტექნიკური პლატფორმა წარმოადგენს ინტერაქტიულ ინსტრუმენტს, რომელიც შედგება ერთი სასწავლო და კიბერსივრცეში მომხმარებლის ქცევის შესამოწმებელი ორი მოდულისგან.

პროგრამის 5 შემადგენელი

- ყველა თანამშრომლის კიბერჰიგიენის არსებული დონის შემოწმება CybExer ონლაინ პლატფორმაზე;
- ავტომატურ ინტერაქტიულ რეჟიმში Cyber Hygiene პროგრამის მიხედვით თანამშრომელთა ტრენინგი, 3 დონე;
- რეალური ფიშინგის შეტევების სიმულაციური გზით სწავლის შედეგების პერიოდული გადამოწმება;
- უმაღლესი რისკის მატარებელი მომხმარებლებისთვის გამოცდილი ინსტრუქტორის მიზნობრივი ტრენინგები;
- რეგულარული კომუნიკაციური მხარდაჭერა და სტიმულირება



კიბერჰიგიენის მიმდინარე დონის ტესტირება CybExer პლატფორმაზე

- პროგრამა გამიზნულია თანამშრომლების სამი კატეგორიისათვის: მენეჯერები, რიგითი მომხმარებლები და IT სპეციალისტები (მათი IT ცოდნის გათვალისწინებით) და ეხმარება ამ კატეგორიების თითოეული წარმომადგენლის ქცევის საფრთხეების აღმოფხვრაში;
- ტესტირება და ტრენინგი ემყარება კომპიუტერისა და სხვა პორტატული ციფრული აღჭურვილობის გამოყენების ყოველდღიური სიტუაციების ანალიზს;
- შეუძლებელია გამოცდის «ჩაბარება» ან «არჩაბარება» - ყველა თანამშრომელი მიიღებს საკუთარ კიბერჰიგიენის პროფილს კიბერსივრცეში მათი უნიკალური რისკ ზონების მითითებით.

CybExer პლატფორმაზე კიბერჰიგიენის ტრენინგი

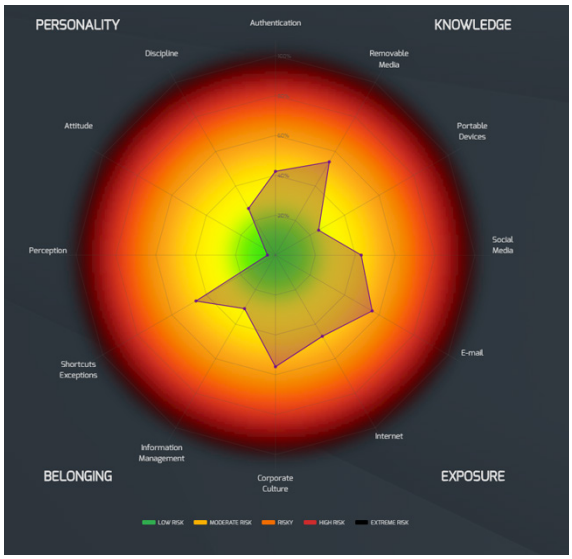
- ტრენინგებისა და ტესტირების შესაძლებლობა მრავალჯერადი და მათთვის მოსახერხებელი სიხშირით;
- პროგრამა რეგულარულად ახლდება გლობალური, ეროვნული ან ინდუსტრიული ახალი საფრთხეების გათვალისწინებით;
- სწავლება მიმდინარეობს მწვრთნელის, პროექტის მენეჯერის და ტექნიკური სპეციალისტების თანხლებით.

კიბერუსაფრთხოებაში მიზნობრივი სწავლების ჩატარება

- კიბერჰიგიენის ამჟამინდელი დონიდან გამომდინარე განისაზღვრება უმაღლესი რისკის დონის მატარებელი თანამშრომლები;
- კიბერუსაფრთხოების პროფესიონალი ინსტრუქტორები, ორგანიზაციის CISO-სთან ერთად, აჯგუფებენ თანამშრომლებს რისკის ტიპის მიხედვით;
- გარკვეული ჯგუფებისა და მათი ძირითადი რისკების შესაბამისად ინსტრუქტორები ქმნიან მოკლე და ინტენსიურ ტრენინგებს. შემდგომში სწავლება ტარდება შესაბამისი ჯგუფებისთვის.

ფიშინგის შეტევის სიმულაცია

- თანამშრომლებისათვის ფიშინგის ელ. წერილების შექმნა და დაგზავნა, მათ მიერ გავლილი სწავლების შედეგების გათვალისწინებით და კიბერსივრცეში რისკების ზონების გამოვლენა;
- მოულოდნელობის ეფექტი და პირადი გამოცდილება მნიშვნელოვნად აუმჯობესებს კომპანიისთვის საფრთხეების და უარყოფითი შედეგების აღქმას;
- თანამშრომლების რეაქცია ფიშინგის შეტევის სიმულაციაზე საშუალებას იძლევა დაიგეგმოს საშიში ქცევის წინააღმდეგ ბრძოლის ეფექტური ზომები: დამატებითი სწავლებები, ადმინისტრაციული ზომები და ა.შ.



კომუნიკაციური მხარდაჭერა და სტიმულირება

- პერიოდული ბიულეტენების შექმნა და დაგზავნა კიბერუსაფრთხოების სფეროში წარმატებული კიბერშეტევების, სხვა აქტუალურ მოვლენებისა და საფრთხეების შესახებ;
- ინფორმაციის ასოციაციური დამახსოვრების და სასწავლო ეფექტის გაძლიერების მიზნით ტექსტური, გრაფიკული და ვიდეო მასალების დაგზავნა;
- ბეჭდვისა და სუვენირული პროდუქციის წარმოება და მიწოდება კიბერჰიგიენის წესების დაცვის დამატებითი შეხსენებისთვის.

კიბერპიგიენის მიზნობრივი ტრენინგი

- «ინფორმაციის უსაფრთხოების ზოგადი პრინციპები»
- «სოციალური ინჟინერია»
- «ფიშინგი: შეტევა ელ. წერილების საშუალებით»
- «სოციალური ქსელები»
- «ინტერნეტ-დათვალიერება (browsing)»
- «მობილური პროგრამების დაცვა»
- «პაროლები»
- «დაშიფვრა»
- «მონაცემთა უსაფრთხოება»
- «მონაცემთა განადგურება»
- «უსაფრთხო WIFI»
- «დისტანციური მუშაობა»
- «ტექნიკური დახმარება»
- «IT დეპარტამენტი»
- «ფიზიკური უსაფრთხოება»
- «პერსონალური კომპიუტერის დაცვა»
- «თქვენ გაგტეხეს, ახლა რა?»
- «განვითარებული მუდმივი საფრთხე (ART)»
- «ღრუბელური მომსახურება»
- «ნაბიჯები უსაფრთხოების უზრუნველყოფისთვის»

რატომ ISSP?

- ISSP- ს სასწავლო ცენტრს აქვს ISC2-ის, EC-Council, Mile2-ის აკრედიტაცია;
- ISSP არის CybExer-ის სტრატეგიული პარტნიორი უკრაინაში, საქართველოში, ყაზახეთსა და პოლონეთში;
- საკუთარი მეთოდოლოგია ThreatSCALE აღიარებულია მსოფლიოს წამყვანი ტექნიკური უნივერსიტეტების (MIT, Darthmounth Collegegue), ინდუსტრიული ორგანიზაციების (SANS ინსტიტუტი) და გლობალური მომწოდებლების (Honeywell) მიერ;
- მსოფლიოში აღიარებული საერთაშორისო სერთიფიკატების მოპოვების შესაძლებლობა, როგორებიცაა: სერთიფიცირებული ეთიკური ჰაკერი (CEH), კომპიუტერული ჰაკერების სასამართლო ექსპერტიზის გამომძიებელი (CHFI) და სხვა;
- ავტორიზებული სასწავლო პროგრამები, რომლებიც შედგენილია ლაბორატორიის, SOC-ისა და ISSP საინჟინრო განყოფილების გამოცდილების საფუძველზე;
- კიბერპოლიციის, შინაგან საქმეთა სამინისტროს, ცესკოს და სხვა სამთავრობო უწყებებშის სასწავლო პროგრამების ჩატარების გამოცდილება.