საუნივერსიტეტო უწყვეტი განათლების

სასერტიფიკატო კურსი

კურსის სახელწოდება:	ქსელური ფაერვოლი Fortinet Fort iGATE NGFW Fortinet Fort iGATE NGFW
კურსის მოცულობა:	30 საათი
კურსის ხელმძღვანელი	ალექსანდრე კაზალიკაშვილი, მოწვეული სპეციალისტი.
კურსის განხორციელებისათვის აუცილებელი ადამიანური რესურსები (გთხოვთ, თან დაურთოთ CV)	ალექსანდრე კაზალიკაშვილი
სწავლების ენა:	ქართული/ინგლისური
სამიზნე ჯგუფი:	IT სპეციალისტები
კურსში ჩართვის წინაპირობა მსმენელთათვის:	ქსელური პროტოკოლების ზოგადი ცოდნა TCP/IP protocol architechture (OSI model) ზოგადი ცოდნა და გააზრების უნარი. ქსელური ფაიერვოლების/მარშრუტიზატორების/კომუტატორების მუშაობის ზოგადი პრინციპების ცოდნა და გააზრების უნარი. ინფორმაციული უსაფრთხოების (Information Security Awareness) ზოგადი პრინციპების/ტერმინოლოგიის ცოდნა და გააზრების უნარი.

კურსის მიზანი:	მსემენლებს განუვითარდეს შემდეგი უნარ-ჩვებვები: 1. Fortinet FortiGate NGFW/Fortiweb WAFკონფიგურაცია 2. Fortinet FortiGate NGFW/Fortiweb WAF კონფიგურაციის ოპტიმიზაცია 3. Fortinet FortiGate NGFW/Fortiweb WAF დაკავშირებული პრობლემების გადაჭრა და ანალიზი.
სწავლის შედეგები:	კურსის დასრულების შემდეგ მსმენელს შეეძლება: ტრადიციული ქსელური ფაერვოლების და NGFW მუშაობის პრინციპების აღწერა და განსხვავებების/უპირატესობების გააზრება. Fortinet FortiGate NGFW თავისუბურებების გააზრება და კონცეპციის სრულფასოვნად აღქმა. კურსის მსვლელობისას მსმენელი გაცნოს Fortinet Security fabric კონცეფციას და მის უპირატესობებს. FortiOS ოპერაციულ სისტემასთან მუშაობა და მისი გამოყენება კონკრეტული ამოცანების (NGFW კონფიგურაცია, პრობლემების ანალიზი) შესასრულებლად. კურსის დასრულების შემდეგ მსმენელს შეეძლოს: 1. Fortigate NGFW საბაზო კონფიგურაცია - Routing - NAT - HA - Logging 2. Fortigate NGFW application control კონფიგურაცია

	3. Fortigate NGFW Intrusion Prevention კონფიგურაცია 4. Fortigate NGFW Antivirus კონფიგურაცია 5. Fortigate NGFW Sandboxing (Anti-Malware) კონფიგურაცია 6. Fortigate NGFW SSL Inspection კონფიგურაცია 7. Fortigate NGFW FSSO კონფიგურაცია 8. Fortigate NGFW Firewall Policy კონფიგურაცია 9. FortiWeb WAF საბაზო კონფიგურაცია - Routing - Logging 10. FortiWeb WAF Server objects კონფიგურაცია 11. FortiWeb WAF SSL/TLS offloading კონფიგურაცია 12. FortiWeb WAF SSL/TLS სერტიფიკატებთან მუშაობა 13. FortiWeb WAF web protection profile კონფიგურაცია 14. FortiWeb WAF policy კონფიგურაცია
სწავლის შედეგების მიღწევის მეთოდები:	ლექცია დისკუსია დემონსტრაცია (Hands-on Lab, Production გარემო)

მსმენელის შეფასების სიტემა:	შუალდეური შეფასება: ქვიზის მეშვეობით, რომელიც ფასდება 10 ქულით. დასკვნითი (საბოლოო) შეფასება: ქვიზი (20 ქულა) და პრაქტიკული დავალება (20 ქულა)
სერტიფიკატის მინიჭების მოთხოვნები:	კურსის მინიმუმ 80%-ზე დასწრება და არა ნაკლებ ჯამური შეფასების 80%-ისა (40 ქულა).
კურსის განხორციელებისათვის საჭირო მატერიალურ–ტექნიკური რესურსები:	1. Hands-on Lab-ისთვის საჭირო რესურსები hardware/virtual: Compute: 8 CPU/64GB RAM Storage: 100GB OS: Ubuntu server 2. HDMI projector

კურსის სტრუქტურა და შინაარსი

I მოდული (იმ შემთხვევაში თუ კურსი რამდენიმე მოდულისაგან შედგება) (მიუთითეთ ძირითადი საკითხები, საათების რაოდენობა თითოეული საკითხისათვის, ლიტერატურა)

#	თემა / სესია	საათების რაოდენობა თითოეული თემისათვის	მეთოდები	სასწავლო მასალა*
1	NSE2 The Evolution of Cybersecurity	3	ლექცია დისკუსია	NSE2_Lesson_Scripts.pdf
2	NSE3 Fortinet Product Awareness	3	ლექცია დისკუსია	პრეზენტაცია
3	NSE 4 FortiGate Security 7.0	4	ლექცია დისკუსია	პრეზენტაცია quiz

			დემონსტრაცია	
5	NSE 5 FortiClient EMS	4	ლექცია დისკუსია დემონსტრაცია	პრეზენტაცია Lab quiz
4	NSE 6 FortiWeb 6.1	4	ლექცია დისკუსია დემონსტრაცია	პრეზნტაცია Lab quiz
5	FortiGate Essentials 7.0	4	ლექცია დისკუსია დემონსტრაცია	პრეზენტაცია Lab quiz
6	NSE 7 Enterprise Firewall	4	ლექცია დისკუსია დემონსტრაცია	პრეზენტაცია Lab quiz
7	NSE 7 Advanced Threat Protection	4	ლექცია დისკუსია დემონსტრაცია	პრეზენტაცია Lab quiz