Cisco CyberOps Associate

Cisco Certified CyberOps Associate sertifikatı, təhlükəsizlik əməliyyatları mərkəzlərində (SOC) çalışan şəxslər üçün nəzərdə tutulmuş başlanğıc səviyyəli bir sertifikatdır. Bu sertifikat, kiber təhlükəsizlik əməliyyatlarının əsaslarını və SOC analitiki kimi işləmək üçün lazım olan bacarıqları təsdiqləyir.

MÜDDƏT

– 70 saat

NÖV

– Ofisdə tədris

– Online tədris

BAŞLANĞIC SƏVİYYƏ

Təhlükəsizlik Əməliyyatları Mərkəzi (SOC) Analitikləri: Bu sertifikat, SOC komandalarında çalışan və ya çalışmaq istəyən şəxslər üçün idealdır. SOC analitikləri kiber təhdidlərə qarşı müdafiənin ön cəbhəsində yer alır və bu sertifikat onların təhdidləri aşkarlamaq və onlara qarşı mübarizə aparmaq bacarıqlarını təsdiqləyir.

Şəbəkə Təhlükəsizliyi Mütəxəssisləri: Şəbəkə təhlükəsizliyi sahəsində çalışan mütəxəssislər üçün də bu sertifikat faydalıdır. Sertifikat, onların şəbəkə təhlükəsizliyi anlayışlarını və təhdidlərə qarşı mübarizə strategiyalarını inkişaf etdirməsinə kömək edir.

Kiber Təhlükəsizlik sahəsində Karyera qurmaq istəyənlər: Bu sertifikat, kiber təhlükəsizlik sahəsində karyera qurmaq istəyən şəxslər üçün başlanğıc nöqtəsi ola bilər. Sertifikat, onlara bu sahədə tələb olunan əsas bilik və bacarıqları qazandırır və işə qəbul prosesində rəqabət üstünlüyü təmin edir.

İT Mütəxəssisləri: Kiber təhlükəsizliklə bağlı məsuliyyətləri olan İT mütəxəssisləri, bu sertifikatı əldə etməklə öz bilik və bacarıqlarını təsdiq edə və təşkilatlarının təhlükəsizlik duruşunu gücləndirə bilərlər.

MODULLAR

1. Təhlükəsizlik Əsasları:
Kiber Təhlükəsizlik Konsepsiyaları: Məxfilik, bütövlük, əlçatanlıq (CIA triadı), risklərin idarə edilməsi, təhlükəsizlik siyasətləri və prosedurları.

Təhlükələr, Hücumlar və Zəifliklər:Zərərli proqramlar (malware), sosial mühəndislik, şəbəkə hücumları (DoS, MitM), veb tətbiq hücumları (SQL injection, XSS) və digər yaygın təhdidlər.

Təhlükəsizlik Texnologiyaları və Alətləri:
Firewall-lar, IDS/IPS sistemləri, SIEM həlləri, antivirus proqramları, zəiflik skanerləri və digər təhlükəsizlik alətləri və onların iş prinsipləri. Kriptoqrafiya Əsasları: Simmetrik və asimmetrik şifrələmə, hash funksiyaları, rəqəmsal imzalar və sertifikatlar.

2. Təhlükəsizliyin Monitorinqi və Analizi:
Təhlükəsizlik Əməliyyatları Mərkəzi (SOC): SOC-un rolu, funksiyaları və SOC komandalarının təşkili.

Təhlükəsizlik Məlumatları və Hadisə İdarəetməsi (SIEM): SIEM sistemlərinin arxitekturası, SIEM-in tətbiqi və istifadəsi, logların toplanması, korrelyasiyası və təhlili. Təhlükəsizlik Hadisələrinin Aşkarlanması və Təhlili: Təhdidləri və anomaliyaları aşkarlamaq üçün qayda əsaslı aşkarlama, imza əsaslı aşkarlama, davranış analizi və digər texnikalar.

Şəbəkə və Sistem Monitorinqi:Şəbəkə trafikinin, sistem loglarının və təhlükəsizlik hadisələrinin real vaxt rejimində monitorinqi və analizi.

3. Hadisələrə Cavab Vermə və Rəqəmsal Kriminalistika:
Hadisələrə Cavab Vermə Prosesi: Hadisəyə hazırlıq, aşkarlama, təhlil, aradan qaldırma, bərpa və dərslərin öyrənilməsi mərhələləri daxil olmaqla hadisələrə cavab vermə prosesinin anlaşılması və tətbiqi.

Rəqəmsal Kriminalistika və Dəlil Toplama: Rəqəmsal dəlillərin toplanması, saxlanması və təhlili, hücum vektorlarının müəyyən edilməsi və hücumların təsirini qiymətləndirmə.

Hadisənin Bərpası və Dərslərin Öyrənilməsi: Hadisədən sonra sistemlərin bərpası, zəifliklərin aradan qaldırılması və gələcək hücumların qarşısını almaq üçün tədbirlərin görülməsi.

4. Şəbəkə Təhlükəsizliyi:
Şəbəkə Təhlükəsizliyi Nəzarətləri: Firewall-lar, IDS/IPS sistemləri, VPN-lər, NAC, content filtering və digər şəbəkə təhlükəsizliyi texnologiyaları.

Şəbəkə Hücumları və Müdafiə Texnikaları: DoS/DDoS hücumları, ARP spoofing, man-in-the-middle (MitM) hücumları və digər şəbəkə hücumları, eləcə də onlardan müdafiə üsulları.

Simsiz Şəbəkə Təhlükəsizliyi: WPA3, EAP və digər simsiz təhlükəsizlik protokolları və onların konfiqurasiyası.

Bulud Təhlükəsizliyi: Bulud mühitlərində təhlükəsizlik riskləri, bulud xidmət modelləri (IaaS, PaaS, SaaS) və bulud təhlükəsizliyi tədbirləri.

5. Son İstifadəçi Sistemlərinin Təhlükəsizliyi:
Əməliyyat Sistemlərinin Təhlükəsizliyi: Windows, macOS və Linux əməliyyat sistemlərinin sərtləşdirilməsi, yamaqların idarə edilməsi və təhlükəsizlik konfiqurasiyaları.

Zərərli Proqramların Aşkarlanması və Təhlili:
Zərərli proqramların növləri, zərərli proqramların yayılma üsulları və zərərli proqramların aşkarlanması və təhlili üçün alətlər və texnikalar.

Son İstifadəçi Təhlükəsizliyi: Güclü parol siyasətləri, iki faktorlu identifikasiya, təhlükəsizlik maarifləndirilməsi və təlimləri.

MÖVZÜ

Təhlükəsizlik konsepsiyaları:
- Məxfilik, bütövlük, əlçatanlıq (CIA triadı)
- Təhlükəsizlik siyasətləri
- Risklərin idarə olunması
- İnsidentlərə reaksiya
- Ümumi hücum növləri
- Şəbəkə əsasları (TCP/IP modeli, protokollar, topologiyalar)
- Təhlükəsizlik cihazları (firewall, IDS/IPS)
- Kriptoqrafiya əsasları

Təhlükəsizlik monitorinqi:
- Təhlükəsizlik məlumatları və hadisələrin idarə edilməsi (SIEM)
- Müdaxilənin aşkarlanması sistemləri (IDS)
- Təhlükəsizlik monitorinq alətləri (NetFlow, paket analizi)

Host əsaslı analiz:
- Əməliyyat sisteminin gücləndirilməsi
- Son nöqtə təhlükəsizlik alətləri (antivirus, anti-malware)
- Son nöqtələrdə insidentlərə reaksiya

Şəbəkə müdaxilələrinin təhlili:
- Şəbəkə trafikinin təhlili
- Müdaxilənin qarşısının alınması sistemləri (IPS)
- Təhdid kəşfiyyatı

Təhlükəsizlik siyasətləri və prosedurları:
- Təhlükəsizlik siyasətinin hazırlanması
- İnsidentlərə reaksiya prosedurları
- Biznesin davamlılığı və fəlakətlərdən qurtarma (BCDR)