

Kibertəhlükəsizlik

Blue Team

Müdafiə, SOC və insident cavabı

Splunk | Wazuh | Elastic | Wireshark | Zeek

Səviyyə	Proqram	Format	Dərs növü
Sıfırdan	8 modul	Onlayn	Qrup və ya fərdi

Kurs haqqında

Hücum hər gün olur – fərq onu nə qədər tez gördüyündədir. SOC analitikinin gündəlik işini real loglar, alertlər və insident ssenariləri üzərində öyrənirsən.

Bu kurs kimin üçündür

01 **Sıfırdan başlayanlar**
Kibertəhlükəsizliyə ən geniş iş bazarı olan müdafiə tərəfindən girmək istəyənlər.

02 **IT dəstək və adminlər**
Helpdesk mütəxəssisi, sistem və ya şəbəkə administratorusansa – SOC-a keçid üçün ən qısa yol.

03 **Tələbələr**
SOC analitiki vakansiyalarının tələb etdiyi praktik bacarıqları diplomdan əvvəl qazanmaq istəyənlər.

Bir həftə necə keçir

01
Onlayn dərs
Mentor mövzunu real vaxtda izah edir, sualını dərsdəcə verirsən.

02
Laboratoriya
Eyni mövzunu brauzerdə açılan laboratoriyada öz əlinlə təkrarlayırsan.

03
Həftəlik tapşırıq
Real ssenariyə əsaslanan tapşırıqla bildiyini yoxlayırsan.

04
Mentor rəyi
Mentor işini yoxlayır, səhvini göstərir, növbəti addımı deyir.

Bu, video kurs deyil: dərslər onlayndır, mentorla real vaxtda. Qrupda maksimum 5 nəfər və ya fərdi: mentor hər kəsin işini görür.

Tədris proqramı

8 modul – təməldən peşəyə

Hər modul onlayn dərs, laboratoriya və həftəlik tapşırıqla bağlanır. Növbəti modula əvvəlkini praktikada mənimsədikdən sonra keçirsən.

01

Təhlükəsizlik və şəbəkə təməli

Normalı bilməyən anomaliyanı görə bilməz.

OSI və TCP/IP · Əsas protokollar · Firewall və seqmentasiya · Təhdid növləri

02

Windows və Linux logları

Hər hücum sistemdə iz qoyur – harada axtarmaq lazımdır.

Windows Event ID-lər · Sysmon · Linux auditd · Log mənbələri

03

Şəbəkə trafikinin analizi

Paket səviyyəsində şübhəli fəaliyyət.

Wireshark · Zeek · Suricata IDS/IPS · PCAP təhlili

04

SIEM və log analizi

Milyonlarla sətirdən bir hücumu tapmaq.

Splunk · Wazuh · Axtarış sorğuları · Korrelyasiya qaydaları

05

EDR və endpoint təhqiqatı

Kompüterin içində nə baş verib.

EDR alertləri · Proses ağacı · Velociraptor · Zərərli proqram əlamətləri

06

Təhdid kəşfiyyatı və MITRE ATT&CK

Hücumçunun taktikasını tanımaq.

MITRE ATT&CK · IOC və IOA · CTI mənbələri · Hücumun xəritələnməsi

07

İnsident cavabı

Alertdən bağlanmış insidentə qədər.

IR mərhələləri · Təcrid və təmizləmə · Kriminalistika əsasları · İnsident hesabatı

08

Threat hunting və SOC iş axını

Alert gözləmədən təhdidi axtarmaq.

Hipotez əsaslı ov · Triaj · Eskalasiya · Müsahibəyə hazırlıq

Kursun sonunda bacaracaqsan

- SOC L1 analitiki kimi alertləri triaj etmək
- SIEM-də axtarış sorğusu və korrelyasiya qaydası yazmaq
- Şəbəkə trafikində və loglarda şübhəli fəaliyyəti tapmaq
- Hücumu MITRE ATT&CK üzrə xəritələmək
- İnsident cavabı planına uyğun addım-addım hərəkət etmək
- Rəhbərliyə təqdim olunacaq insident hesabatı yazmaq

İşlədəcəyin alətlər

Splunk · Wazuh · Elastic · Wireshark · Zeek · Suricata · Sysmon · Velociraptor · MITRE ATT&CK · CyberChef

Məzunlarımızın çalışdığı qurumlar

Kapital Bank · Rabitəbank · birmarket · RISK COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Növbəti addım

Pulsuz onlayn sınaq dərsinə qoşul – mentorla tanış ol, sonra qərar ver.

Qrup və ya fərdi format – seçim sənindir. Qiymət, cədvəl və növbəti qrupun başlama tarixini WhatsApp-da yazırıq.

WhatsApp və zəng	+994 70 639 33 09
Sayt	compstyle.tech/kurslar/blue-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Özün öyrən, özün yarat.

© Compstyle Technology