

Cybersecurity

Blue Team

Defense, SOC and incident response

Splunk · Wazuh · Elastic · Wireshark · Zeek

Level	Program	Format	Lessons	Language
From zero	8 modules	Online	Group or one-to-one	Azerbaijani

About the course

Attacks happen every day – the difference is how fast you see them. You learn a SOC analyst's daily work on real logs, alerts and incident scenarios.

Who this course is for

01 **Complete beginners**
For those who want to enter cybersecurity through defense – the side with the widest job market.

02 **IT support and admins**
If you work in helpdesk or as a system or network administrator, this is the shortest path into a SOC.

03 **Students**
For those who want the hands-on skills SOC analyst vacancies ask for – before graduating.

What a week looks like

01
Online lesson
The mentor explains the topic live; you ask your questions right in the lesson.

02
Lab
You repeat the same topic hands-on in a browser-based lab.

03
Weekly assignment
You test what you know with an assignment based on a real scenario.

04
Mentor review
The mentor reviews your work, points out mistakes and tells you the next step.

This isn't a video course: lessons are online and live with a mentor. A group of up to 5 people or one-to-one – the mentor sees everyone's work. Lessons are taught in Azerbaijani.

Curriculum

8 modules – from fundamentals to a profession

Every module ends with an online lesson, a lab and a weekly assignment. You move on to the next module once you have mastered the previous one in practice.

01

Security and networking fundamentals

You can't spot an anomaly if you don't know what normal looks like.

OSI and TCP/IP · Core protocols · Firewalls and segmentation · Threat types

02

Windows and Linux logs

Every attack leaves a trace – where to look for it.

Windows Event IDs · Sysmon · Linux auditd · Log sources

03

Network traffic analysis

Suspicious activity at the packet level.

Wireshark · Zeek · Suricata IDS/IPS · PCAP analysis

04

SIEM and log analysis

Finding one attack in millions of lines.

Splunk · Wazuh · Search queries · Correlation rules

05

EDR and endpoint investigation

What happened inside the computer.

EDR alerts · Process tree · Velociraptor · Signs of malware

06

Threat intelligence and MITRE ATT&CK

Recognizing the attacker's tactics.

MITRE ATT&CK · IOCs and IOAs · CTI sources · Attack mapping

07

Incident response

From an alert to a closed incident.

IR phases · Containment and eradication · Forensics basics · Incident report

08

Threat hunting and SOC workflow

Searching for threats without waiting for an alert.

Hypothesis-driven hunting · Triage · Escalation · Interview prep

By the end of the course you will be able to

- Triage alerts as a SOC L1 analyst
- Write search queries and correlation rules in a SIEM
- Find suspicious activity in network traffic and logs
- Map an attack to MITRE ATT&CK
- Act step by step according to an incident response plan
- Write an incident report for management

Tools you'll use

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

Where our graduates work

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

Next step

Join a free online trial lesson – meet your mentor, then decide.

Group or one-to-one – the choice is yours. We'll send you the price, schedule and start date of the next group on WhatsApp. Lessons are taught in Azerbaijani.

WhatsApp and calls	+994 70 639 33 09
Website	compstyle.tech/en/courses/blue-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Learn it yourself, build it yourself.

© Compstyle Technology