SOC ANALYST. PRACTICE OF INFORMATION SECURITY EVENTS ANALYSIS AND WORKING WITH LOG FILES

The purpose of advanced training is to develop and deepen the knowledge and skills of specialists in the field of information security, with an emphasis on work in Security Operation Center, developing the competencies necessary for effective analysis, monitoring and response to cybersecurity incidents.

Course graduates receive a state-issued certificate of advanced training in cybersecurity.

Target audience:

- cybersecurity risk and compliance managers who need to understand the technical aspects;
- information security specialists;
- Cybersecurity professionals seeking to improve their skills in incident analysis and log processing;
- IT administrators and system administrators who want to develop their knowledge in the field of cybersecurity;
- IT graduates interested in a career in cybersecurity and want to learn the practical aspects of being a SOC analyst;
- specialists of all names and categories providing cybersecurity .

Form of study – distance learning
The cost of training – 1900 BYN.

The duration of the program is 65 academic hours.

Course curriculum

Item No.	**Course Topic Titles**
	Security Operation Center (SOC)
1.	Introduction of the concept of SOC
2.	SOC member roles and responsibilities
3.	SOC Analyst role
4.	SOC Analyst competencies
5.	Basic principles of SOC operation (processes, playbooks, runbooks)
6.	Handling alerts, escalations, company policies
	Tools and systems in SOC
7.	SOC Maturity
8.	SIEM
9.	FW/WAF/IDS/IPS/NGWF
10.	NTA
11.	IRP TIP
12.	EDR / AV / XDR
13.	UBA / UEBA
14.	SOAR
	Data collection, types and formats
15.	Text data formats
16.	Data sources
17.	Description of the event collection toolset

18.	Aggregation data (log management -> siem | log management + siem)
	Monitoring and analyzing information security events. The role of an analyst in the process of responding to information security incidents
19.	Event and incident definitions. FP TP FN TN
20.	Incident life cycle
21.	Using SIEM to analyze information security events
22.	Basic processes in event handling
	Detecting attacks and signs of compromise in network traffic
23.	OSI Network Model, TCP/IP
24.	Methods of obtaining and tools for capturing network traffic (TAP, SPAN, FPC Utility or Packet Capture tools)
25.	Detection and analysis tools (Suricata, Wireshark etc.)
26.	Network traffic analysis, detection of traces of attacks in network traffic
	Detecting complex attacks within office and server infrastructure
27.	Cyber killchain. The logic of the attacker's behavior. Practical application of the cyber methodology kill chain
28.	Methodology of working with MITREATT&CK for SOC
29.	The most common methods for gaining initial access to infrastructure
30.	Email Analysis: understanding email attacks
31.	VPO Review
32.	Methods and tools for analyzing attacker activity in the OS