RANGE
FORCE

Certificate of Continuing Education Completion

THIS CERTIFICATE IS AWARDED TO

Aleksandr Isoev

For successfully completing 251 modules, from 09/06/2024 to 09/07/2025, equivalent to 96 hours and 35 minutes of study, provided by the RangeForce Platform

Modules completed are shown in Annexes

09/06/2025

Date

Taavi Must, Founder of RangeForce

Annex 1

- Privilege Escalation: Introduction
- YARA Overview
- Understanding the Cyber Kill Chain
- Traffic Light Protocol Overview
- Overview of Data Breaches
- Kerberos Overview
- IAM Overview
- Introduction to Password Cracking Countermeasures
- Password Security In-Depth
- Red Team Functions and Tasks
- The Building Blocks of InfoSec
- History of Cybersecurity
- Module Tutorial
- Penetration Tester Capstone
- Pentest Reporting and Delivery
- File Transfers and Data Exfiltration
- Housekeeping After a Pentest
- Reverse Shells
- Lateral Movement with Metasploit
- Lateral Movement Overview
- Windows Active Directory Escalation: Kerberoasting
- Windows Local Privilege Escalation Techniques
- Privilege Escalation: SUID Bit 1
- Privilege Escalation: Docker Group
- Privilege Escalation: Linux Capabilities
- What is Privilege Escalation and Common Tactics
- Exploit Database
- Stealing NTLM Hashes With Responder
- NTLM
- Command Injection: Find & Exploit (PHP)
- DOM-based XSS: Find & Exploit (JavaScript)
- XSS Overview
- Unrestricted File Upload: Find & Exploit (NodeJS)
- Malicious Tomcat War File and LSASS Dump
- Microsoft Office Macro Malware
- Vulnerability Assessment: Wordpress with WPScan
- Burp Suite: Advanced
- Burp Suite: Basics
- Burp Suite Overview
- Password Spraying
- Uncovering Open Permissions
- Nmap: Basics
- Greenbone Vulnerability Management
- Nikto
- Introduction to Threat Modelling
- Setting up a Phishing Campaign
- Windows Active Directory Reconnaissance Methods
- Windows Active Directory Reconnaissance Basic Tools
- Situational Awareness
- Introduction to OSINT
- Introduction to Social Engineering
- Active Information Gathering
- Passive Information Gathering
- Windows Active Directory GPO
- Windows Active Directory Rights Management
- Introduction to Active Directory
- Preparing Your Pentest Environment
- Legal Considerations for a Pentest
- MITRE ATT&CK Overview
- WireShark Overview
- Firewall Overview
- Introduction to Network Security
- Network Models: OSI and TCP/IP
- Elastic Course Capstone
- Elastic: Case Management
- Elastic: Endpoint Security
- Elastic: Detection Engine
- Elastic: EQL - Analytics
- Elastic: EQL - Introduction
- Elastic: Osquery
- Elastic: Elastic Agent - Integrations & Policies
- Elastic: Elastic Agent - Installation On Windows
- Elastic: Elastic Agent - Installation On Linux
- Elastic: Packetbeat - Log Analysis
- Elastic: Packetbeat - Installation
- Elastic: Winlogbeat - Log Analysis
- Elastic: Winlogbeat - Installation
- Elastic: Filebeat
- Introduction to MISP
- Malware Analysis: VirusTotal
- Elastic: Elastic Security Basics
- Elastic: Introduction to Elastic Security
- Elastic: Introduction to Fleet and Elastic Agent
- Elastic: Introduction to Elastic Stack
- Wireshark - Analysis
- Wireshark - Telephony
- Wireshark - Display Filters
- Wireshark - Statistics
- Wireshark - Intro
- Sublist3r
- OSINT: Mapping Target Infrastructure
- Understanding TTPs
- Recorded Future: Browser Extension
- Firewall Policies: UFW
- Firewall Policies: IPTables
- Firewall Central NAT: FortiOS
- Firewall Application Control: FortiOS
- Firewall Policies Rule Ordering: FortiOS
- Firewall Source NAT: FortiOS
- Firewall URL Filtering: FortiOS
- Firewall Policies: FortiOS
- QRadar: Network Activity
- QRadar: Basics
- QRadar Overview
- Junior SOC Analyst 1 Capstone
- Anticipating Ransomcloud Attacks
- Incident Response in M365
- Introduction to KQL
- AWS CloudTrail Basics
- Introduction to Policies in AWS IAM
- Cloud Security Overview
- Importance of Logs
- Simple Incident Response Challenge
- Incident Handling
- Alerting
- Managing Incident Response
- Introduction to Microsoft Sentinel
- Splunk: Basics
- Event Analysis Basics - Wazuh
- Introduction to Windows Event Logs
- Introduction to SIEM and SOAR

Annex 2

- Scoping and Budgeting for a Pentest
- Offensive Security Assessments
- Junior SOC Analyst 2 Capstone
- Alert Monitoring & Triage Challenge
- Threat Intelligence: OSINT and Tooling
- Identifying False Positives
- Indicators of Compromise, Attack, and Fraud
- Understanding Alert Prioritization
- Sources of Logs
- Types of SOC and Common Setup
- Monitoring Techniques in SOC
- Introduction to Logs, Events, Alerts, and Incidents
- Commodity Malware Overview
- Signature-Based Malware Detection
- Windows Malware
- Identifying Signatures with Microsoft Defender
- Introduction to Ransomware Challenge
- Hades Detection and Response
- Ransomware Kill Chain
- Introduction to Hades Ransomware
- Introduction to Ryuk Ransomware
- Introduction to Conti Ransomware
- CVE-2018-13382 FortiOS 6.0.4: SSL VPN Improper Authorization
- CVE Overview
- Vulnerability Management
- Introduction to Vulnerability Scanning
- Types of Vulnerabilities
- Simple Email Challenge
- Email URL Analysis Basics
- Email Header Analysis Basics
- OSINT & Phish
- Types of Phishing Emails and Techniques
- Wireshark Basics
- SIEM Basics - Wazuh
- DLL Search Order Hijacking Exercise
- DLL Search Order Hijacking Introduction
- DLL Search Order Hijacking Detection
- Mshta Introduction
- Mshta Exercise
- Mshta Detection
- Parent PID Spoofing Exercise
- Parent PID Spoofing Detection
- Access Token Manipulation Introduction
- Rundll32 Exercise
- Rundll32 Detection
- Rundll32 Introduction
- Process Injection (Process Hollowing) Exercise
- Process Injection (Process Hollowing) Detection
- Process Injection (Process Hollowing) Introduction
- Boot or Logon Autostart: Registry Run Keys Exercise
- Boot or Logon Autostart: Registry Run Keys Detection
- Boot or Logon Autostart: Registry Run Keys Introduction
- Scheduled Tasks Exercise
- Scheduled Tasks Detection
- Scheduled Tasks Introduction
- Accessibility Features Exercise
- Accessibility Features Detection
- Accessibility Features Introduction
- Regular Expressions In Splunk
- Splunk Webapp IR: Brute Force Detection
- Splunk: Input Configuration
- Splunk: Lookups
- Splunk: API
- Splunk: Visualizations
- Splunk: Alerts
- Splunk: Fields and Transforms
- Splunk: Filters and Queries
- Keys to Useful Threat Intelligence
- Threat Intelligence
- Introduction to Email Based Threats
- Ransomware Overview
- Known vs. Unknown Malware
- Meet the Adversaries
- Understanding the Threat Landscape
- MITRE D3FEND Overview
- Cybersecurity Kill Chain
- Handover Procedures
- Blue Team Functions and Tasks
- Introduction to the SOC
- Cybersecurity Teams
- Anticipating Ransomware Attacks
- Cybersecurity Terminology
- Ransomware Prevention and Mitigation
- Network-Based Ransomware Detection
- Behavior-Based Ransomware Detection
- Signature-Based Ransomware Detection
- PowerShell Fundamentals Challenge
- PowerShell Remoting
- PowerShell Filtering and Formatting
- PowerShell Objects and Data Piping
- PowerShell Commands
- PowerShell Modules
- Introduction to PowerShell
- Introduction to the RangeForce Readiness Program
- Introduction to the (AR)² Framework
- NICE Roles for Cybersecurity Workforce Overview
- Introduction to Defense Readiness Index
- NIST Cybersecurity Framework Overview
- Networking Basics Challenge
- Network Interface Layer: Overview
- Internet Layer: IP Addresses and Subnet Masks
- Internet Layer: Overview
- Introduction to Network Address Translation (NAT)
- Transport Layer: Overview
- Application Layer: Overview
- Introduction to Networking
- Linux CLI Fundamentals Challenge
- Linux Tmux Introduction
- Linux System Info Gathering
- Linux Log Management: Systemd
- Basic Shell Scripting
- Linux Execution Context
- Linux Software Management
- Linux Environment Variables
- SSH Basics
- Linux User Management
- Linux Authentication
- Linux File Permissions and Ownership
- Linux File Management

Annex 3

- Office Macros Detection
- Office Macros Exercise
- Office Macros Introduction
- System Services: Service Execution Exercise
- System Services: Service Execution Detection
- System Services: Service Execution Introduction
- WMI Exercise
- WMI Detection
- WMI Introduction
- Basic Linux File Editing
- Linux CLI Introduction