Training: Centri
Certified Junior Detection Engineer (CJDE)

TRAINING GOALS:

The CJDE (Certified Junior Detection Engineer) course provides a pathway into detection engineering and cyber security operations, focusing on identifying, analyzing, and responding to threats using detection tools and strategies. It is ideal for roles such as Junior Security Analysts, Detection Engineers, SIEM Administrators, Incident Response Analysts, and SOC Analysts, and is suited to individuals with foundational cyber security knowledge who wish to specialize in detection and response or enhance their existing skills.

Why choose CJDE?

CJDE is designed to train students that are capable of responding to threat intelligence reports and are able to build test and deploy detections in your environments. Below are some examples of the skills and experience you will gain.

- Automate detection workflows with git.
- Creating and tuning network detection rules
- Creating and tuning Sigma Rules
- Utilising AI in detection engineering flows.
- … And much more

The skills and tools you'll learn in this course will be directly applicable to a range of security roles, and are actively used by defenders around the world.

Certified rewards

Once a student passes the practical exam and becomes CJDE certified, they will receive a number of rewards for their hard work:

- Become a Certified Junior Detection Engineer for life
- CJDE digital PDF certificate
- CJDE Credly digital badge
- CJDE printed certificate
- CJDE silver challenge coin (gold if 90%+ is scored on first attempt)

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

Who is the course for?

CJDE is perfect for security professionals that want to develop their practical detection engineering skills. Roles that we believe would benefit from this course include:

- Security Analysts
- Incident Responders
- Threat Intelligence Analysts
- Security Engineers
- Detection Engineers

Whilst our content is aimed primarily at entry-level or junior roles, read our course syllabus to see if CJDE is the right choice for you or your team!

CONSPECT:

- Networking Essentials
  - This module covers the basics of networking, including protocols, IP addressing, subnetting, and network troubleshooting.
    - Introduction and History
    - Network Components
    - Cabling
    - OSI Model
    - TCP/IP
    - IPv4
    - ARP
    - Routing
    - Transport Layer
    - DNS
    - ICMP
    - DHCP
    - IPv6
    - Basic Network Security
    - Network Troubleshooting
    - Wireless Networking
    - Final Quiz

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Windows Essentials
  - Learn the fundamentals of the Windows operating system, including system configuration, user management, security features, and administrative tools.
    - Section Introduction
    - Introduction to Windows OS
    - Windows OS Structure
    - Windows File System & Permissions
    - System Configuration and Resource Management
    - System Management Tools
    - Windows PE File
    - Windows Processes, Drivers and Services
    - User Accounts, Privileges, and Tokens
    - Windows Sessions
    - Windows Subsystem for Linux (WSL)
    - Active Directory Basics
    - Windows Authentication
    - Windows Security Essentials
- Linux Essentials
  - This module covers the basics of Linux operating systems, including command-line usage, file system navigation, user management, and security configurations.
    - Module Introduction
    - Introduction to Linux
    - Linux Operating System Architecture
    - Linux Shell Basics
    - System Navigation and Management
    - Authentication and User Management
    - File Permissions
    - File Management and Editing
    - Working with Data
    - Processes, Services and Tasks
    - Package Management
    - Networking and Web Services
    - Linux Essentials Consolidation
- Python Essentials
  - Gain fundamental programming skills with Python, focusing on scripting for automation, security tool development, and data manipulation.
    - Module Introduction

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Python Setup & Fundamentals
        - Intermediate Python & OOP
        - Data Handling & Parsing
        - Networking & Security with Python
        - Python Essentials - Final Lab
- Incident Response Essentials
    - Learn the basics of incident response, including preparation, detection, containment, eradication, recovery, and lessons learned to effectively handle cybersecurity incidents.
        - Introduction to Incident Response
        - Incident Response Frameworks
        - Incident Response Teams
        - Case Management
        - Metrics
- Git Workflows for Detection Engineering
    - Learn GitHub workflows, including automation with GitHub Actions, CI/CD pipelines, event triggers, and managing workflows for testing, deployment, and security in your environments.
        - Section Introduction
        - Automated Detection Workflow
        - Github Actions: Automation Engine
        - Detection Engineering Workflow
        - Summary
        - Capstone Project Challenge
- Network Analysis Essentials
    - Learn the fundamentals of network analysis, including packet capture, protocol inspection, traffic patterns, and identifying anomalies to support security monitoring and threat detection.
        - Introduction
        - Network Traffic Classification
        - Wireshark Fundamentals
        - Command Line Packet Analysis
        - Yet Another Network Analysis Tool: BruteShark
        - Moving Beyond Traditional Tools: Python Scapy
        - Module Quiz
- Yara & Sigma Essentials
    - Learn YARA and Sigma essentials, including rule creation, pattern matching, and threat detection to identify malware and suspicious activity across files and logs.
        - Section Introduction

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Introduction to Detection Rules
        - Yara Rules
        - Sigma Rules
        - Writing Sigma Rules
        - Lab) Yara and Sigma Essentials
- Zeek Essentials
    - This module introduces learners to Zeek, a powerful network analysis framework used for detecting suspicious activity.
        - Section Introduction
        - What is Zeek?
        - Configuring and Running Zeek
        - Detection using Zeek
        - Summary
        - Module Quiz
- Malware Analysis for Detection Engineering
    - This module covers the basic of Malware Analysis for Detection Engineering such as pulling IoCs out and how to retrieve information vital to Detection Logic.
        - Section Introduction
        - Introduction to Malware Analysis
        - Malware Lab Setup
        - Malware Fundamentals
        - Static Analysis
        - Static Analysis Practical
        - Dynamic Analysis
        - Dynamic Analysis Practical
        - Understanding the Findings
        - IoC and Rule Creation
        - Lab) Malware Analysis for Detection Engineering
- Detection Rule Creation and Tuning
    - This module teaches the fundamentals of writing, deploying, and refining detection rules to identify malicious activity across environments. Learners will develop the skills to fine-tune rules for accuracy and efficiency.
        - Section Introduction
        - Splunk Primer
        - Your First Detection Rule
        - Detection Logic in AWS
        - Real World Scenarios

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Rule Tuning
        - Capstone) Detection Rule Creation and Tuning
    - Threat Intelligence Integration for Detection
        - Learn threat intelligence for detection, including IOC analysis, threat actor profiling, and integrating intel into detection rules to improve threat visibility and response.
            - Module Introduction
            - The Intelligent SOC
            - Threat Intelligence in the SOC Data Lifecycle
            - Rule Development Lifecycle
            - Analytical Models and Pivoting using Diamond Model
            - Detection Metrics and Success Criteria
            - Creating Intelligence-Driven Detection
            - Adversary Emulation
            - The Role of the Intelligence Community in Collaborative Detection Sharing
            - Module Quiz
    - Behavioural Analytics for Threat Detection
        - This module focuses on identifying threats through the analysis of user and entity behaviour. Learners will explore techniques for establishing baselines, detecting anomalies, and leveraging behavioural patterns.
            - Section Introduction
            - Foundations of Behavioural Analytics
            - Baseline Establishment Techniques
            - User Behaviour Analytics
            - Entity Behaviour Analytics
            - ML for Behaviour Analytics
            - Module Quiz
    - AI for Defenders
        - This module explores how artificial intelligence and machine learning are transforming threat detection and response. Learners will gain practical insights into leveraging AI-driven tools to enhance detection capabilities and automate analysis.
            - Module Introduction
            - AI for Defenders: Introduction
            - Core Components: The Building Blocks
            - ML Foundations for Detection Engineering
            - AI in Soc Automation & Alert Triage
            - Generative AI & LLMs for Defenders
            - Explainability & Adversarial Awareness

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

        - Operationalizing AI in Detection Pipelines
        - Summary & Final Reflections
        - Module Quiz
    - CJDE Exam Preparation
        - Preparation for CJDE exam. including details about what to expect, and how to prepare.
            - Exam Preparation

REQUIREMENTS:

CJDE is made for junior level professionals with 1-3 years' cybersecurity experience. You'll start with the basics and build up to real-world detection skills using industry-standard operational tools. If you're a junior level analyst and possess curiosity about threat detection, you're ready.

Difficulty level



CERTIFICATE:

Upon passing the CJDE exam, you'll receive a digital PDF certificate, a Credly digital badge, a printed certificate, and a silver challenge coin (gold if scoring 90%+ combined on the first attempt).

In the price you will get CJDE practical exam, with the option to retake either part for free if necessary.

ADDITIONAL INFORMATION:

What's included in the price?

The course includes 4 months of access to more than 500 topics, 27 quizzes, and 41 practical labs. The CJDE certification process includes a 100% practical exam. You will receive 24 hours of access to an emulated MSSP environment in order to respond to an incident. The exam includes two attempts, with a second attempt (free retake) available if necessary. Upon passing, you receive a digital PDF certificate, a Credly digital badge, a printed certificate, and a silver challenge coin (gold if scoring 90%+ combined on the first attempt).

Lessons available in 9 languages with native text-to-speech (beta)

- English
- Polish
- German
- French

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Portuguese
- Italian
- Spanish
- Dutch
- Japanese

Note: the exams are available in English only.

How long is the access?

After gaining access to the course, you have 4 months on-demand access to the training material.

In summary, the CJDE license includes:

- 4 months of access
- Approximately 40 to 60 hours to complete
- Over 500 topics, 27 quizzes, 41 practical labs
- The CJDE practical exam, with the option to retake either part for free if necessary.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310