# Poland Jobs Expertini®

**Threat Detection Engineer - Splunk Developer**

**Apply Now**

Company: Euroclear

Location: Poland

Category: computer-and-mathematical

**Division: CISO**

Cyber Defense Center is part of the Chief Information Security Officer Office. The main responsibility of the team is to reduce the risk of Euroclear cyber threat surface by monitoring for malicious intent targeted at Euroclear's services, it's supporting assets and people. We do this through the Cyber Threat Management (CTM) capabilities, Security Operations Centre (SOC) which includes monitoring (Tier 1 & Tier 2) and Cyber Incident & Response Team (CIRT; Tier 3), Detection & Response Engineering Team (D&R , and Compliance and Assurance Team (C&A). This includes cyber threat intelligence, brand and digital footprint monitoring, security incident and event monitoring, cyber analytics, incident management and forensic analysis.

CDC supports capabilities within the security domain and acts as subject matter expert across all divisions in the company as well as interacts with external stake holders, including customers, oversight bodies, threat intelligence providers, and third parties.

The Detection & Response Engineering team is comprised of –

Detection Engineers/Splunk Developers – who implement and maintain threat detections capabilities.

SOAR developers – who develop response capabilities via playbooks, automation etc.

**Role**

Candidates in this role are responsible for the development and maintenance of correlation searches and dashboards on the SIEM (Splunk ES) platform.

Candidates will report to the Manager of Detection & Response Engineering and will work jointly with threat intelligence, design, engineering, and response teams, to gather and define requirements, specify clear priorities, evaluate technical tradeoffs, and build and maintain threat detection capabilities.

The candidates' main responsibilities will be to:

Interact with the different stakeholders to gatherand define requirements for the development and testing of threat detection capabilities.

Cooperate with log source onboarding team to assure correct log source onboarding and log mapping to data models according to Splunk best practices.

The development and tuning and continuous improvement of correlation rules.

Develop and maintain dashboards, reports, and alerts.

Create Splunk Knowledge Objects to address stakeholders needs in context of using Splunk as security tool.

Prepare correlation search tests, conduct tests, and document evidence from test that shows correlation search addresses scenario described in use case.

Responsible for the creation of procedures, high-level/low-level documentation, implementation of processes and development of staff in relation to SIEM detection logic

Coach a team (from a technical perspective); review work outputs and provide quality assurance.

Analyses and identifies areas of improvement with existing processes, procedures, and documentation.

Demonstrates how to use SIEM & Enterprise Security products to both technical/non-technical personnel.

Provides expert technical advice and counsel in the design, monitoring and improvement of SIEM security systems.

Prioritize and coordinate backlog of threat detection requests, making sure we have a healthy balance between defect resolution and new features.

**Qualifications**

**Technical Skills**

In depth experience in development and maintenance of SIEM use cases

Fluent in Splunk's search processing language (SPL)

Excellent knowledge of Splunk Enterprise and Splunk Enterprise Security

Sound knowledge about Splunk Common Information Model (CIM) and log normalization using Data Models

Strong understanding of cybersecurity technologies, protocols, and applications

Excellent English communication skills (written and oral)

**Assets**

Splunk Core Certified (Advanced)Power User (essential)

Splunk Certified Developer (nice to have)

Splunk Enterprise Certified Admin (nice to have)

Splunk Enterprise Security Certified Admin (nice to have)

Any other Security Certifications (. CEH, GIAC, CISSP, OSCP …)

**Soft Skills**

Strong analytical skills to evaluate complex multivariate problems and find a systematic approach to gain a quick resolution, often under stress.

Strong problem solving, documentation, process execution, time management and organizational skills.

Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.

Fast and independent learner, with ambition to self-improve.

At ease in a fast-changing environment, flexible and pragmatic, open-minded

Accurate, acting with attention to details.

Client focus and delivery oriented

A team-focused mentality with ability to work & collaborate effectively in a team environment.

Good leadership and communication skills, whether on the field, in the team or with management: you are a keen team player and coordinate work amongst people from different areas or divisions. A good relationship builder with strong diplomacy skills

Able to work autonomously.

#LI-NS1

**Apply Now**

**Cross References and Citations:**

**1. Threat Detection Engineer - Splunk Developer Southkoreajobs Jobs Poland Southkoreajobs ↗**

**2. Threat Detection Engineer - Splunk Developer Resume-score Jobs Poland Resume-score ↗**

**3. Threat Detection Engineer - Splunk Developer Colombiajobs Jobs Poland Colombiajobs ↗**

**4. Threat Detection Engineer - Splunk Developer Johannesburgjobs Jobs Poland Johannesburgjobs↗**

**5. Threat Detection Engineer - Splunk Developer Bangladeshjobs Jobs Poland Bangladeshjobs ↗**

**6. Threat Detection Engineer - Splunk Developer HungaryjobsJobs Poland Hungaryjobs↗**

**7. Threat Detection Engineer - Splunk Developer Projectmanagementjobs Jobs Poland Projectmanagementjobs ↗**

**8. Threat Detection Engineer - Splunk Developer Jobscanada Jobs Poland**

**Jobscanada ↗**

**9. Threat Detection Engineer - Splunk Developer Newyorkcityjobs Jobs Poland Newyorkcityjobs ↗**

**10. Threat Detection Engineer - Splunk Developer Datascientistjobs Jobs Poland Datascientistjobs ↗**

**11. Threat Detection Engineer - Splunk Developer Greecejobs Jobs Poland Greecejobs ↗**

**12. Threat Detection Engineer - Splunk Developer Oilandgasjobs Jobs Poland Oilandgasjobs ↗**

**13. Threat Detection Engineer - Splunk Developer Warsawjobs Jobs Poland Warsawjobs ↗**

**14. Threat Detection Engineer - Splunk Developer Austinjobs Jobs Poland Austinjobs ↗**

**15. Threat Detection Engineer - Splunk Developer Swedenjobs Jobs Poland Swedenjobs ↗**

**16. Threat Detection Engineer - Splunk Developer Tutorjobs Jobs Poland Tutorjobs ↗**

**17. Threat Detection Engineer - Splunk Developer Weldingjobs Jobs Poland Weldingjobs ↗**

**18. Threat Detection Engineer - Splunk Developer Psychiatristjobsnearme Jobs Poland Psychiatristjobsnearme ↗**

**19. Threat detection engineer - splunk developer Jobs Poland ↗**

**20. AMP Version of Threat detection engineer - splunk developer ↗**

**21. Threat detection engineer - splunk developer Poland Jobs ↗**

**22. Threat detection engineer - splunk developer Jobs Poland ↗**

**23. Threat detection engineer - splunk developer Job Search ↗**

**24. Threat detection engineer - splunk developer Search ↗**

**25. Threat detection engineer - splunk developer Find Jobs ↗**