**BNPP AM - Information Security Officer**

**Apply Now**

Company: BNP Paribas Real Estate

Location: Brussels

Category: computer-and-mathematical

**INFORMATION SECURITY OFFICER**

**CYBER SECURITY INCIDENT RESPONSE ANALYST / DATA SECURITY (M/F/X)**

**MISSION**

BNP Paribas Asset Management is looking for a motivated Information Security professional to join its **Cyber Security Incident Response Team** (CSIRT). They will join a diverse team of professionals in the domains of **Incident Response** (IR), **Data Loss Prevention** (DLP) **and Cyber Threat Intelligenc**e (CTI) and be responsible of monitoring operations, detecting suspicious events and qualifying adversarial activities. When a cybersecurity incident occurs, they will investigate, contain and eradicate it, ensuring return to normal operations. The candidate we are looking for is a seasoned **InfoSec enthusiast** , able to communicate fluently in both **French** and in **English** and possesses excellent **analytical skills**, **curiosity** and **precision**.

**CORE RESPONSIBILITIES**

 **CYBER INCIDENT RESPONSE**

· Monitor and investigate security alerts on multiple platforms;

· Ensure response to cyber security incidents when required;

· Monitor and manage DDoS incidents;

· Conduct incident post-mortems;

· Conduct confidential digital investgations and eDiscovery;

· Contribute to potential cyber crisis cells;

· Understand and adapt detection use cases to business requirements;

· Perform a security watch on different channels, observe the development of threats and prepare reports;

· Identify new threats;

· Support digital forensics and investigations (DFI);

· Draw lessons from past events and observations to continuously improve response capabilities;

· Communicate and collaborate at different levels of technical literacy, adapting contents based on the audience;

· Keep up-to-date with the latest security and technology developments, especially threats and vulnerabilities.

## DATA LOSS PREVENTION AND DATA SECURITY

· Monitor and manage data loss events through different channels (exfiltration, accidental disclosure, PII data breach, public/social media sharing);

· Act as L3 expert and coordinate L2 analysts in their day-to-day DLP activities;

· Ensure communication and coordination with all relevant (non-IT) stakeholders.

## METRICS AND REPORTING

· Generate and maintain KPIs/KRIs on incident response, data loss and other relevant activities;

· Create (or collaborate in creating) dashboards for cyber incident and crisis management, DLP and DDoS;

· Produce reports; summarize information for a wider audience;

· Maintain and improve automated reporting tools.

## KNOWLEDGE MANAGEMENT

· Analyze, propose and implement improvements to our CSIRT processes and procedures;

· Update and maintain procedures, wiki articles and internal training;

· Analyze and document new security processes when needed.

## BACKGROUND

The candidate can demonstrate a solid and consistent background in Cybersecurity and specifically Incident Response (IR):

· A minimum of 6 years' experience in pertinent cybersecurity roles such as "Blue Team" specialist, SOC analyst, incident responder.

· Broad and solid understanding of cybersecurity fundamental concepts, the risks associated with different technologies and ways to manage them.

· Good knowledge of common security issues inherent to corporate environments.

· Prior experience with corporate operational processes and procedures.

· Previous missions in a CIRT (Computer Incident Response Team) or equivalent constitute a significant plus.

· Prior experience in a multinational financial institution is an asset.

The candidate has a relevant degree in Information Security or related disciplines or possesses equivalent field experience.

**CONTACT PERSONS (MANAGER / HR)**

· Frederic Gleizer (Chief Information Security Officer) or Paul Sutherland (HR)


**ROLE REQUIREMENTS**

**REQUIRED SKILLS**

To succeed in this role, the candidate will demonstrate experience with cybersecurity operations, especially in the domain of Incident Response (IR). The following skills are required:

· Broad and solid knowledge of IT technologies (Windows, *NIX, networking, databases, web technologies, APIs, virtualization, containers, cloud architectures) and specifically IT security technologies;

· Good knowledge of Data Loss Prevention (DLP) processes and controls;

· Working experience with the following security tools/methodologies: DLP, SIEM, EDR, DDoS protection, Encryption, DMARC;

· A robust understanding of cyber threat actors, their techniques and the cybercrime ecosystem;

· Familiarity with Cyber Threat Intelligence tools and techniques (e.g. Diamond Model and MITRE ATT&CK), with the ability to use them during investigations;

· Knowledge of the most common data protection regulations and frameworks, especially the European GDPR;

· Experience with data analysis and presentation techniques;

· Experience with scripting languages such as Python, Powershell, VBA, Perl;

· Proficiency with Microsoft Office, SharePoint and PowerBI.

The following skills are also required:

· Autonomy and proactivity;

· An analytical and rigorous mindset;

· Ability to ensure confidentiality and discretion in performing sensitive tasks;

· Ability to coordinate and coach more junior analysts;

· A continuous learning mindset;

· Excellent communication, both written and verbal;

· Fluency in both French and English - spoken and written;

· Being able to manage conflict and divergent positions;

· Ability to explain and defend a security policy;

· Being consistent in the decisions made, and take responsibility for them;

· Ability to prioritize and follow-up on task completion;

· Ability to work under pressure, particularly when dealing with multiple threats and during peak times;

These additional skills and experience will make the profile more attractive:

· Experience with Digital Forensics;

· Threat Modeling techniques;

· Cybersecurity frameworks and standards (NIST, ISO27000, CIS).

## QUALIFICATIONS AND CERTIFICATIONS

One among the following certifications (or others pertinent to this role): (ISC)2 **CISSP** ;

CREST **CIM** , GIAC **GCED** or **GCIH**

**Apply Now**

---

**Cross References and Citations:**

**1. BNPP AM - Information Security Officer  Sciencejobsnearme  Jobs Brussels Sciencejobsnearme** ↗

**2. BNPP AM - Information Security Officer  Bahrainjobs Jobs Brussels Bahrainjobs** ↗

**3. BNPP AM - Information Security Officer  Thecareerjobs Jobs Brussels Thecareerjobs** ↗

**4. BNPP AM - Information Security Officer  Automobilejobs  Jobs Brussels Automobilejobs** ↗

**5. BNPP AM - Information Security Officer  Projectmanagementjobs  Jobs Brussels**

**Projectmanagementjobs** ↗

6. BNPP AM - Information Security Officer  HoustonjobsJobs Brussels Houstonjobs↗

7. BNPP AM - Information Security Officer  Germanyjobs   Jobs Brussels Germanyjobs ↗

8. BNPP AM - Information Security Officer  Automobilejobs  Jobs Brussels Automobilejobs ↗

9. BNPP AM - Information Security Officer  Developerjobs Jobs Brussels Developerjobs ↗

10. BNPP AM - Information Security OfficerIrelandjobs   Jobs Brussels Irelandjobs ↗

11. BNPP AM - Information Security OfficerHtmljobsJobs Brussels Htmljobs↗

12. BNPP AM - Information Security OfficerRiyadhjobs   Jobs Brussels Riyadhjobs ↗

13. BNPP AM - Information Security OfficerParisjobs   Jobs Brussels Parisjobs ↗

14. BNPP AM - Information Security OfficerIndustryjobsearch  Jobs Brussels Industryjobsearch ↗

15. BNPP AM - Information Security OfficerAnyeventhire   Jobs Brussels Anyeventhire ↗

16. BNPP AM - Information Security OfficerIsraeljobs  Jobs Brussels Israeljobs ↗

17. BNPP AM - Information Security OfficerMedicalassistantjobs Jobs Brussels Medicalassistantjobs↗

18. BNPP AM - Information Security OfficerLondonjobscentral Jobs Brussels Londonjobscentral↗

19.  Bnpp am - information security officer Jobs Brussels ↗

20.  AMP Version of Bnpp am - information security officer ↗

21.  Bnpp am - information security officer Brussels Jobs ↗

22.  Bnpp am - information security officer Jobs  Brussels ↗

23.  Bnpp am - information security officer Job Search ↗

24.  Bnpp am - information security officer Search ↗

25.  Bnpp am - information security officer Find Jobs ↗