Job Title Senior Security Operation Analyst

Department Technology Operations

Location Hybrid - 1-2 days in the office a week.

Reporting Line Security Operations Team Lead

**Job Purpose**

Our Information Security team help maintain the availability, confidentiality, and integrity of BPP’s data and systems. As the **Senior Security Operations Analyst.** You will support the day-to-day operations of the security function, leading on technical investigation, and driving threat detection initiatives, and ensure security controls are implemented consistently across the Group. This role requires deep technical expertise and a passion for continuous security improvement in evolving environment’s

**Key Responsibilities**

* Analyse network traffic, system logs, and SIEM tooling to identify anonymities.
* Detect, investigate, and respond to incidents and events, including leading on root cause analysis.
* Conduct proactive threat hunting on key systems in line with the MITRE ATT&CK framework.
* Define and execute vulnerability assessments and penetration testing, owning remediation plans, and ensuring they are implemented within agreed timelines.
* Develop and maintain playbooks for recurring events and incidents across the Group.
* Working collaboratively with the external SOC partner to ensure timely incident response within agreed SLA’s.
* Creating and updating security documentation.
* Act as a subject matter expert on security technologies and practises in brownfield and cloud environments.
* Partner with stakeholders to ensure security controls are implemented in line with best practise.
* Mentor junior members of the team.

**Skills**

* Knowledge of the MITRE ATT&CK framework.
* Strong technical knowledge of EDR, SIEM and SOAR tools, with experience of Devo and Google Analytics, and Sentinel One being an advantage.
* Experience in leading incident response in line with industry framework.
* Threat hunting and modelling experience using industry leading tools.
* In-depth understanding of vulnerability management tooling, with experience of Tenable One and Wiz being an advantage.
* Experience of Microsoft Security and Compliance toolkits.
* Strong technical knowledge of cloud security concepts, including AWS and Azure.
* Effective verbal and written communication skills, with the ability to collaborate with cross-functional teams with varying technical ability.
* Experience working with security frameworks and compliance standards, including ISO27001, Cyber Essentials Plus, NIST and PCI-DSS.
* Analytical thinking.
* Strong problem-solving skills.
* Takes ownership of own development by ensuring that skills are kept up to date, in line with industry changes.