JOB PROFILE

Position Title	MDR Threat Analyst / Threat Hunter
Main purpose of the role	The Threat Analyst / Hunter will be a key member of the Cyber Defence and MDR team, responsible for participating in threat-based investigations, creating new detection methodologies, and providing expert support to incident response and monitoring functions. The focus of the Threat Hunter is to detect, disrupt, and eradicate threat actors from enterprise networks, as well as uncover adversarial tactics, tools and procedures . To execute this mission, the Threat Analyst / Hunter will use data analysis, threat intelligence, and cutting-edge security technologies.
Job level	Level 2
Level of leadership	Level 1
Reports to [role]	Head of Cyber Defence
Required minimum education and work experience	• 4+ years' working experience in one of the following security areas: CSOC Analyst, Malware Researcher, Threat Analyst, Incident Response • 4+ years' experience in threat analysis and threat intelligence • Excellent familiarity with the current Threat Landscape and Cyber Attack Methodologies • Experience with advanced cyber security tools, network topologies, intrusion detection and secured networks • Proven internal or external customer facing experience • Broad understanding of the IT, networking, architecture, and security field, including TCP/IP, HTTP, UDP, ICMP, ARP, RARP, encryption, network access controls, and incident detection and prevention • Degree in Computer Science or Information Security through a reputable University would be advantageous • SANS Certifications (GCIA, GCIH, GREM, GCFA) or other industry certifications (CISSP, CISM, CISA, CEH, CHFI) would be advantageous • Knowledge of security standards, including NIST, ISO27001, ASD, PCI DSS would be desirable

	• 5+ years’ working experience in the Cyber Security Industry
Internal contacts	• Head of Cyber Defence • Senior Cyber Security Specialist
External contacts	• Global clients • Vendor technical support
Key performance areas	1. Threat analysis and incident response 2. Research and development (threat & security) 3. Reporting and documentation 4. Mentoring and technical guidance, including coaching 5. Delivery of quality security monitoring services 6. On-boarding of new clients
Technical knowledge / competencies	• Advanced experience in Information Security • Cyber threat hunting experience • Experience with incident management • Experience with cyber threat intelligence • Experience with software vulnerabilities & exploitation • Experience with analysing large amounts of data • Experience with malware analysis • Experience with APT/crime-ware ecosystems • Experience with exploit kits • Experience with current SOC operational methodologies • Experience with packet capture (PCAP) analysis using tools such as Wireshark • Experience with scripting languages, preferably Python • Experience with Windows, Linux, and Mac OS X • Knowledge of Endpoint Detection & Response technologies • Knowledge of TCP/IP networking, VPN, NAT, VLANS, firewalls, routers and switches, etc.

	• Knowledge of SIEM technologies • Knowledge of root cause analysis and escalation procedures • Knowledge of CVE, Google hacking, and threat intelligence • Knowledge of security threat and attack countermeasures • Ability to conduct in-depth forensic analysis and investigation • Ability to perform pattern analysis • Reporting skills, being able to articulate technical reports into business language in order to provide situational awareness and specialist advisory.
Behavioural competencies	• Leadership and climate setting • Team player and team building (creation of a cohesive division) • Adopting and accepting the organisation's professional standards • Structured thinking • Grit • Individual thinking within the current role • Collaboration - willingness and ability to collaborate with other Team Leaders / Supervisors • Action oriented - production of desired outcomes within the required timeframes • Work pro-actively – both independently and with peers • Assertive and confident • Ability to handle conflict • Ability to plan and organise work tasks • Strong sense of accountability and responsibility