PayNet
PAYMENTS NETWORK MALAYSIA

Job Description	
Position	Team Lead (Senior Engineer) - Secops, Advisory & Engineering
Department	IT Security
Division	Information Services

SUMMARY OF RESPONSIBILITIES

The Lead Security Threat Analyst shall be the lead for PayNet's Security Operations Blue Team and works closely with the other members of the team to continuously improve the overall practices and processes of cyber security operations. This includes analysis of security events, performing incident response from identify, protect, detect, contain to recovery. He/she shall be part of the Technical Security council to recommend improvements in defences, in addition to provide inputs into definition of leading practical security policies and processes. This role will report directly into the Head of SecOps, Advisory and Engineering and he/she will work closely with the head and wider Information Security team

KEY AREAS OF RESPONSIBILITIES

- Gather and analyse from a culmination of open-source and commercial security tools, private and industry threat intelligence sources for relevance and impact to PayNet.
- Work with internal security and cross-departmental teams, 3rd party to provide data driven insights into existing and emerging threats.
- Leverage threat intelligence to improve the prioritization of detective and preventive controls, recommend mitigations to improve defences.
- Support and lead response to incidents.
- Leads the team on security events analysis as detected by various security controls, monitoring, and recording security events in daily and weekly reports.
- Perform 2nd or 3rd level analysis on escalated security events, notifications, and alerts from managed Security Operation Centre (SOC).
- Leads the team on forensics, including the identification, collection, preservation, and processing of relevant incident data.
- Improve the information security operations processes and procedures, including developing incident response playbooks and workflows using automation tooling.
- Reports to Head of SecOps, Advisory and Engineering and Cyber Resilience Committee concerning security events, incident trends, residual risk, vulnerabilities, and other security exposures, including misuse of information assets and noncompliance.
- Works with other Departments and Business functions to resolve security events, incidents and service requests.
- Ensures compliance of security processes and procedures, to ensure that security controls are managed and maintained.
- Contributes through Security Advisories, Wikis, Knowledge Transfers and other communication channels on current and emerging security threats to drive awareness.
- Be available to provide reactive support to critical security incidents outside standard business hours.
- Assisting in audit exercises by providing artifacts, charting action plans and supporting remediation requirements.
- Be responsible on tracking progress and provide status updates to Security Management team for reporting purposes.

- Provide feedback and recommendations on existing and new security tools and techniques for the improvement of analysis, incident investigation and security controls

QUALIFICATIONS

- Minimum of five years information and cyber security experience as a Security Analyst and Incident Response, a good degree of involvement in Threat Hunting and intelligence, Security Operations Centre role, IT System Administration or Network Administration.
- Bachelor's degree in information systems or equivalent work experience in relevant information and cyber security domain.
- Security certification from a recognised organisation such as: Splunk Enterprise Certified Admin, Elastic Certified Engineer, CISSP, OSCP
- Technology standard certification such as from Linux, Cisco, VMware, Microsoft is an advantage

Technical Competencies

- Good understanding of cyber threat attack vectors, how they are used, and methods to detect and mitigate them.
- Excellent technical knowledge of Microsoft Operating Systems. Knowledge and experience of Linux and Macintosh.
- Well verse with Packet analysis tools such as Wireshark, covering Network traffic and protocol analysis of security events from network devices, firewalls, intrusion detection and prevention systems
- Familiarity with Security controls such as:
    - Endpoint Detection and Response solutions
    - Endpoint protection and anti-malware solutions
    - Identity and access management (IAM) systems
    - User access monitoring
    - Email and phishing protection
- Forensic evidence handling
- Cloud security, such as CloudFlare, AWS
- Applied-practice of the Mitre ATT&CK framework and how it can be used to learn an adversary's tactics and techniques.
- Experience using scripting, automation, and API's with languages such as Bash, Powershell and Python is an advantage.
- Familiar in the use of Ansible or Terraform to support routine tasks
- Experience using Security Information and Event Management (SIEM) and analysing log data sources.

Occupational Personality

- Strong analytical skills with strong written and verbal communication with a good attention to detail.
- Ability to work both independently and collaboratively, be curious and to ask questions.
- Ability to interact with PayNet's personnel at all levels and across all business units and organizations, and to understand business objectives and values.
- Passionate about security, independent and self-motivated to develop one's skills and knowledge outside of working environment.
- Confident in presenting key findings and conclusions.